A cybersecurity information sharing process for Storm Surge Barriers

Thesis Supervisors:
Dr. Pieter Burghouwt, The Hague University of Applied Science
Prof.dr.ir. Jan van den Berg, TU Delft & Leiden University

Thesis for the completion of the executive master in Cybersecurity from the Cyber Security Academy

Author: Ing. Jeroen A. M. Gaiser CISSP (S1942476)
Version: 1.0 (final)
Date: 16 December 2018

This thesis is dedicated to my dad who always inspired me to reach my full potential.

Abstract

Storm Surge Barriers (SSBs) are vital to keeping society safe and economically stable. These SSBs are complex objects that increasingly depend on Operational Technology (OT) and Information Technology (IT) to operate reliable. This growing dependency and interconnectedness via networks, introduces new risk that engineers must address. Numerous examples can be found that the risk introduced by OT and IT is real and current, both by intentional threat sources (attacks) and unintentional threat sources (human error). Keeping SSBs cybersecure therefore is an increasingly important task.

The Netherlands are world renowned in the field of watermanagement and this extends to SSBs and are one of the founders of I-STORM. This is an international community aimed at improving SSB operations by sharing good practices. The topics I-STORM discusses are divided into knowledge domains. Due to the importance of cybersecurity, I-STORM wants to include cybersecurity in sharing information between members as a new knowledge domain.

Cybersecurity process difficult to introduce, because I-STORM members mainly have an engineering background and cybersecurity is only recently part of their role. I-STORM has identified that an overview of what comprises cybersecurity and how to discuss this topic is needed. This thesis addresses this need, enabling the process of cybersecurity knowledge sharing thus fulfilling the new knowledge domain.

To provide the required artifacts, this thesis presents a cybersecurity information sharing process compatible with the I-STORM knowledge strategy. The presented information sharing process populates the new knowledge domain by providing a solution on *what* to share and *how* to share it. This information sharing process is therefore presented as two components; a cybersecurity vocabulary (ontology) for engineers and a model for cybersecurity information sharing.

To support the *what*, the ontology enables understanding through a shared vocabulary and enables discussions on cybersecurity at a conceptual level that does not include (too) sensitive information. To support the *how*, the information sharing model supports the implementation of the process by providing guidance on how to address challenges in information sharing.

The *what* and *how* are combined using the I-STORM knowledge strategy template to form an information process that describes how I-STORM can share cybersecurity information. This process is understandable by I-STORM members and compatible with the other knowledge domains in I-STORM.

This result enables I-STORM to share information on cybersecurity in a structured way thus creating the new cybersecurity knowledge domain. The knowledge sharing in this new domain leads to more international cooperation on cybersecurity, increasing the resiliency of SSBs against cyber threats and therefore supporting a safer society.

Preface

In 2017 I met Marc Walraven, the senior advisor on Storm Surge Barriers (SSBs) of Rijkswaterstaat, in a project to explore the cybersecurity aspects of social media on SSB operations. During this process, he introduced me in more detail to the world of SSBs. He knows not only the Rijkswaterstaat side of SSB operations, but also described to me how the international network of engineers on SSBs, I-STORM, helps to improve operations through the sharing of good practices. The Netherlands as global forerunners in the field of watermanagement have taken a lead role in this network. I asked him how he shares good practices on cybersecurity within I-STORM, and he answered that this was very difficult but felt it was very necessary.

At that time, I was starting to think about a good thesis subject. I wanted to contribute to the safety of the Netherlands and to challenge myself. I knew little about the engineering world or SSB operations, but the conversations with Marc triggered the insight that I knew very little about the assets that matter most. The 'aha-erlebnis' came when Marc casually remarked that it would be so much easier if they just had a 'menu' of what cybersecurity meant for the SSB engineer. This resonated as a challenge for me to address, and the idea for my thesis was born.

I proposed to Marc to write my thesis on addressing the challenge of addressing cybersecurity topics in sharing good practices in I-STORM. The challenges Marc described, resonated with the social sciences insights provided during the master's program. This led to the realization that cybersecurity in the engineering world is mainly addressed by experts from the IT domain who not necessarily understand engineering. It therefore was no wonder that the engineers in I-STORM had difficulties addressing this domain. This thesis attempts to provide support to the British and Dutch engineers as core members of I-STORM in sharing good practices on cybersecurity. Only by helping each other, can we truly address the global cybersecurity threat to critical infrastructure like SSBs.

I would like to thank the UK Environment Agency, colleagues at Rijkswaterstaat, ENCS and TNO for their help and insight during this thesis. The frank remarks about 'IT-guys', guided tours on SSBs, quick reactions to requests for information and willingness to discuss difficult topics helped make this thesis laying before you today. There is a Dutch short film about the SSBs: 'On the shoulders of giants'. I very much feel this thesis rest on the shoulders of giants like the SSB experts, NIST employees, researchers quoted and Rijkswaterstaat's 220 years of experience in preventing flooding.

Last, but certainly not least, I want to thank my supervisors, Dr. Pieter Burghouwt and Prof.dr.ir. Jan van den Berg for their invaluable insights. The quick and exact feedback of Pieter during writing was a great help, and I think the little voice in my head yelling 'Scientific rigor!' will always sound like Jan. Additionally, I want to thank my fellow students in not only discussing ideas but also in providing the feeling I was not alone in this challenge. Finally, I want to thank my wife for her support these two years. They felt very long as they flew by, but together we did it!

Contents

Table of Figures

1 Introduction

This chapter gives a general introduction to this thesis on cybersecurity information sharing on Storm Surge Barriers. First, background is given on why this thesis subject is chosen, which leads to the presentation of the main research question. Next, the scope of this thesis is defined, and the academic relevance is presented. This will provide the reader with a clear view on the context of the research and how the results add to the body of knowledge. Concluding this chapter is a paragraph that gives insight into how the design science methodology is implemented by presenting the structure and reasoning line of this thesis.

The audience of this thesis is focused on teachers and students of the Cyber Security Academy and members of I-STORM. This audience is diverse and although terminology is avoided where possible, terms and abbreviations are used. To support the legibility, Appendix 1; List of abbreviations and terminology is included for reference.

1.1 Motivation

Storm Surge Barriers (SSBs) are a vital part in the water management of most nations to protect its citizens against events like floods. SSBs are complex engineering objects, in which the IT component is increasingly important for safe and reliable operations. Examples of IT implementations are remote operation of functionality, decision supporting models based on sensors and increasing expansion of Operational Technology (OT) component capabilities (like networking and webservices for remote administration and configuration). These IT and OT components can be attacked, leading to undesired behavior resulting in risk to human life.

There is a delicate balance here. The growing dependency on IT and OT on one hand enables more efficient and reliable operation of SSBs but on the other hand increases the risk from cybersecurity incidents. All involved feel that cyber aspects should be addressed, but they lack a good perspective to act. To address the challenge, the engineers[1] responsible for the operation of SSBs need support in dealing with cybersecurity. Cybersecurity must be structurally addressed in formal processes and procedures as a risk factor with significant impact on safety.

Besides the growing *impact* of cyber incidents on SSB operations, the *likelihood* of an incident occurring must be considered as well. Until recently, cybersecurity for SSBs relied on 'security by obscurity', like most of critical infrastructure (CI). In the past, SSB operations relied on electrical OT with no to very-low computational capacity based on proprietary protocols. The likelihood of a cyber incident was low, due to the requirement of having to be on-site to act. A threat actor had to have detailed knowledge of obscure protocols and electrotechnical operations. Connectivity to networks and 'discoverability' over the internet through dedicated search engines like Shodan [01] has changed this attack surface dramatically.

[1] The three types of engineers on SSBs, civil, electrical and mechanical engineers are referred as 'engineer' in this thesis

In the initial interview with the EA and RWS (Appendix 5, 1.1), the question was posed on how important cybersecurity is for SSBs. The respondent from the UK explicitly mentioned the growing connectivity as a factor. Desk research supports this [02, 03, 04], and identifies three factors that are generally given as examples of increasing the likelihood on cyber incidents on OT.

- **Increased connectivity to networks**; components of SSBs (both OT and IT) must communicate across an object and with remote IT (e.g. for monitoring, for remote adjustments of OT, controlling PLC (programmable Logic Controller) software, operator workstation). This connectivity results in a larger threat surface for SSB components and is an essential prerequisite for *cyber*security. The need for threat actors to act on-site decreases due to the decrease in isolation.
- **Increased interest of threat actors**; CI is recognized more and more as a target for threat actors as a way of impacting a society.
- **Increased use of common technologies**; more common technology is used in SSB operations (e.g. protocols like TCP/IP and webservers embedded in PLC). This increased the likelihood of incidents by lowering the knowledge threshold needed by threat actors. This decreases the 'security by obscurity' protection.

These factors underly the growing sense of urgency that the risk from the cyber domain must be addressed. This sense of urgency has been addressed by models, products, best practices, frameworks and theoretical approaches, with varying degrees of success and effect. This thesis will focus on the sense of urgency felt for cyber risk at SSBs and how information sharing on cybersecurity can be achieved in I-STORM to help the UK and NL to address this challenge.

1.2 Main question

The importance of incident free reliable operations of SSBs is one of the main tasks of Rijkswaterstaat. Therefore, the increased risk of cybersecurity incidents impacting the operations of SSBs is top of mind. The Netherlands has a long history of being an exemplary nation on watermanagement. This role has amongst others, translated to SSBs by Rijkswaterstaat being one of the founding organizations for I-STORM. In I-STORM, Rijkswaterstaat has identified that this sense of urgency for cyber safe and secure operation of SSBs is felt internationally.

I-STORM is an international network of SSB operators. Their mission [05]: "*The I-STORM network brings together professionals that build, manage, operate and maintain Storm Surge Barriers.*". Rijkswaterstaat is part of the launching organizations, and Marc Walraven (SSB lead advisor for the Netherlands within Rijkswaterstaat) has expressed the need to introduce the topic of cybersecurity in the I-STORM network community. Marc indicated that "*With the strong regulations on keeping cyber information restricted we haven't found a method yet to learn from each other on this topic. Nevertheless, we share the interest for this topic as the connection between the reliability of SSB's and cybersecurity it is universal.*" (Appendix 5, 1.1).

Rijkswaterstaat has defined several knowledge domains for SSBs, and this knowledge strategy is currently being adopted by the I-STORM community. The knowledge domains in the strategy describe

the required knowledge needed to operate the SSBs and how to organize that knowledge. The currently defined knowledge domains are:

- Tactical connecting knowledge
- Risk-based management and maintenance
- Object knowledge
- Discipline knowledge

In the exploratory interview with an I-STORM member (Appendix 5, 1.1), he indicated that there is a sense of urgency on cyber risk. This creates a need within I-STORM to include a new knowledge domain; cybersecurity.

In a network of engineers as I-STORM, the topic of cybersecurity presents challenges. Cybersecurity is a new subject, and it is therefore hard to grasp what the topic entails. Cybersecurity is experienced as an indivisible and complex topic with national security aspects. Members are therefore hesitant to address cybersecurity and don't know where to start. The threshold to include cybersecurity within I-STORM is therefore high.

In order to include cybersecurity as knowledge domain within I-STORM, the current threshold for sharing information must be lowered. To do this, an information sharing process is needed for cybersecurity within I-STORM. This process will enable I-STORM members to have a clear overview of cybersecurity topics that can be discussed, combined with a clear description of how those topics can be discussed. These goals can be summarized in the main research question:

How can the I-STORM community share cybersecurity information on Storm Surge Barriers?

To answer this effectively, two sub-questions are identified:

1. What are relevant topics on cybersecurity for SSBs?
2. What information sharing model supports the needs of I-STORM on information sharing?

The first sub-question is required to break up the general term of cybersecurity into recognizable topics. This will enable a more granular approach to what topics are available for information sharing, like a 'menu'. This topic list can be used by engineers in I-STORM as a basis for a shared vocabulary.

The second sub-question is needed to provide support on how to share information. When sharing information, I-STORM members encounter challenges (e.g. confidentiality, funding, building trust, etc.). The model will support the implementation of information sharing within I-STORM, by referencing best practice information. For adaptation in I-STORM, integration with current information sharing processes is key for a good fit.

These sub-questions result in an information sharing process for I-STORM, that addresses the main research question. I-STORM shares knowledge in knowledge domains. The information sharing process will results in I-STORM being supported in addressing cybersecurity in information sharing. The process therefore supports the creation of a new knowledge domain on cybersecurity.

1.3 Scope

Scoping is essential for this thesis, to reduce complexity, ensure proper validation and concluding the research within the given time frame. I-STORM has glob al members, therefore the scoping mainly focuses on the countries between information is shared. The I-STORM community has members world-wide, e.g. the United States (US), Korea, Singapore, the United Kingdom, the Netherlands, Russia, Italy, etc. This is divided into a core member group with paying members and a non-paying member group. Within I-STORM, there is a very wide variety of maturity levels, operating standards, cooperation effort, culture, threat actors, etc. between members.

For this thesis, the scope has been limited to the information sharing between two core members; the Environment Agency (EA) in the United Kingdom and Rijkswaterstaat (RWS) in the Netherlands.
Several factors influenced this scope:

- Incentive; both the UK and Netherlands are launching countries for I-STORM and have a close working relationship as core-members. Therefore, they are very well positioned as 'launching customers';
- History of cooperation; there is a history of information sharing within I-STORM and outside;
- Geographic proximity; facilitating interviews, face-to-face discussion (trust building) and low threshold for communication (time zone for remote conferences, similar cultures);
- Language; the English language is used for the thesis, and is clear for both parties;
- Similarities on threat actors; both the UK and Netherlands have similar relevant threat actors as indicated by the NCSC UK [06], Dutch General Intelligence and Security Service (AIVD) [07] and NCSC NL [08].

Additionally, the Netherlands is a country with very strict watermanagement and a way of including all parties in deliberation; the 'poldermodel'. This results in a sentiment within I-STORM that as Marc Walraven described it: '*If it's good enough for the Dutch, it will be good for all*". The UK has a very well-regarded reputation on cybersecurity within I-STORM. Therefore, if the Netherlands and the UK support a process on cybersecurity information sharing, the acceptance by the rest of the I-STORM community is expected to be high.

CI is highly interdependent, and it is therefore important for this thesis to address the boundaries of SSB operations. SSBs are part of larger national CI and have dependencies on other sectors like electrical power. European action like the Directive on security of network and information systems (the NIS Directive) [09] underscore this dependency. An incident in one CI domain (e.g. electrical power) can influence SSB operations and vice versa. This thesis focuses on the primary operations on the SSB itself. The effects of cybersecurity incidents in other sectors (e.g. power loss or loss of communications) are out of scope.

1.4 Academic relevance

The academic relevance of this thesis is two-fold. First, it presents in a systematic way the cybersecurity topics of SSBs aimed at asset engineers. Information sharing frameworks focus on the 'how' and do not

link well to the 'what' part. None of the sharing information frameworks discussed in 2.4.2 for instance include or reference a shared vocabulary outside the technical domain. E.g. the Dutch ISAC's and ENISA [10] only reference technical taxonomies like STIX, but no broad vocabulary for identifying shared challenges.

Therefore, when implementing a framework, the possible information sharing topics to share on are not clear to engineers. Additionally, the focus of information sharing in cybersecurity is on technical aspects (e.g. software vulnerability advisories or mandatory incident reporting). A '*survey on the dimensions of collective cyber defense through security information sharing*' by Skopik, et al. [11] identified this focus, for example in table 1. This table shows that the focus of sharing by regulatory initiatives focusses on risks, incidents and vulnerability information. This focus can lead to the bias that technical issues are the main cause of cybersecurity incidents. This thesis might provide a more balanced approach to what cybersecurity topics can be addressed in information sharing for critical infrastructure. This is done by including socio-technical and governance aspects of cybersecurity for SSBs besides the purely technical aspects. As a result, this thesis will present a balanced list of topics to address in information sharing for SSBs.

Second, a selection methodology for information sharing networks is presented using a new viewpoint from Knowledge Transfer and Cross-boundary Information Sharing as assessment basis. There are several information sharing frameworks available, but they have not been assessed for implementation in SSB context. This thesis will assess popular frameworks for information sharing for their use in I-STORM. The assessment is performed using the viewpoint of Knowledge Transfer and Cross-boundary Information Sharing [12]. Each framework will be assessed on how well they address the critical factors for information sharing as defined by Gharawi [12]. Interviews will identify the factors that are used to determine the fit for I-STORM. This assessment method for evaluating information sharing models using the viewpoint of information- and knowledge is a new approach to gain insights. It can be used for both selection of a model and as an assessment methodology for improving existing models.

1.5 Societal relevance

Storm Surge Barriers are an essential part of critical infrastructure, and effects of incidents are felt across national borders. Likewise, the cybersecurity threats to critical infrastructure like SSBs cross borders and threat-actors affect multiple nations simultaneously. It is therefore only logical to address risk as a community like I-STORM. International cooperation is seen as a cornerstone of resiliency for critical infrastructure. This thesis enables I-STORM to facilitate this international cooperation, therefore strengthening the resiliency of the assets of its members against cybersecurity risk. Increased resiliency of SSBs against cyber-risk protects societal and economic stability.

1.6 Thesis outline

This thesis applies the design science methodology. This thesis will therefore first explore the need for cybersecurity in SSBs in more depth in chapter 0. This chapter will give context and insight into the challenges and roles involved when addressing the research questions. This is done by first presenting the threats in more detail, followed by a use case to provide an example on working with these threats in information sharing. To give insight into the viewpoint of the target audience of the thesis results, the engineers perspective is presented. Next, the role of information sharing in mitigation is presented and how I-STORM plays a role for SSBs on this. Interviews identify important factors and requirements for information sharing in I-STORM. Concluding this chapter, the identified factors and requirements for answering the research questions are summarized. The requirements provide input and guidance for the next chapter.

Chapter 3 will address if an existing artifact exists fulfilling the requirements, and if not, design a new one. This method is applied using the two sub-questions, given the requirements identified in the previous chapter. To address the first research question, paragraph 3.1 first presents why the ontology format is chosen and selects a methodology to creating that ontology. The ontology creation method is applied and paragraph 3.1.6 presents the resulting cybersecurity ontology for SSBs. Next, paragraph 3.2 will address the second sub-question on *how* to share information. This is done by analyzing three common frameworks using a viewpoint from the field of information and knowledge sharing. Interviews with key stakeholders in information sharing in both the UK and Netherlands identify the most important factors for I-STORM in this viewpoint. The analysis results are presented in a matrix and the best fit model is identified. A short summary presenting the answers to the sub-questions concludes this chapter.

Chapter 4 combines the selected ontology and sharing model and presents a new artifact: *a sharing process on cybersecurity for I-STORM*. This is done by using the knowledge management strategy of I-STORM as the structure to present the information sharing process of this thesis. Paragraph 4.3 provides examples of how the presented process can be implemented in practice. The concluding paragraph presents the cybersecurity information sharing process for I-STORM as the answer to the overall research question.

Chapter 5 presents the validation of the new artifact (the cybersecurity information sharing process). The validation is done in three parts; for each sub question and on the main research question. The ontology is assessed through interviews with four relevant roles in both the UK and NL. This not only validates the ontology but prevents circle reasoning by using the same interviewees for requirements and validation. The model selected for sub question 2 is validated using the use case. Finally, the information sharing process is validated using the requirements presented in chapter 2 and by assessing the effect of the process on the use case. Concluding this chapter, validation limitations are presented closing the chapter with a conclusion on the validation of the presented answer to the main research question.

Chapter 6 presents the conclusions on the main and sub questions of this thesis. The societal and scientific relevance of the thesis results are presented to give insight into the addition to the body of

knowledge. Next, future research is presented that can improve or expand on this thesis. Further topics of future research are presented in the generalization paragraph that presents the potential of the results for use outside the scope of this thesis.

Chapter 7 concludes this thesis with a reflection on the journey of researching and creating the cybersecurity information sharing process for I-STORM.

2 Mitigating cyber risk through information sharing

This chapter analyzes the need for cybersecurity information sharing for mitigating cyber risk for SSB and the role of I-STORM in information sharing in general on SSBs. First, this chapter briefly addresses the threat landscape for CI and SSBs, addressing both a general sense of urgency for cyber threats to CI and more specific threats to SSBs. After exploring the threat landscape, a use case is presented to exemplify the challenges. Understanding of the viewpoint of the engineer is key for this thesis, and paragraph 2.3 provides the basis for understanding that viewpoint. Next, the role of information sharing in mitigation of cyber-threats is explored. This gives insight into how information sharing is recognized as a control and therefore its importance in mitigation. Available mainstream information sharing models are assessed on their fit for the need in I-STORM. In conclusion of this chapter, the requirements are presented for an information sharing process, based on interviews, desk research and the mission of I-STORM in addressing cyber risk mitigation in SSBs. A short treatment of the relevance of the requirements to the research question provides insight into whether all research questions are addressed.

2.1 Cybersecurity threats to CI

SSBs are part of the Dutch and British CI. National strategies and threats are formulated against categories of CI, and not at a level of SSBs. The specific threats to SSBs are confidential as part of national security. This level of threat analysis is not needed to support the need for information sharing. Therefore, the threats to SSBs are analyzed at the level of CI in general.

'Threat' is a term that is used with a wide variety of meanings within the domain of cybersecurity. Therefore, it is imperative to first define what is meant by 'threat' in the context of this thesis. This thesis uses the ISO27000 definition of threat: "*Potential cause of an unwanted incident, which may result in harm to a system or Organization*". Threats are analyzed in this paragraph by first giving insight into the general threat to CI, before focusing on the stated threats to both UK and Netherlands CI. This identifies if the threat actors for both nations are comparable, which is one of the factors in sharing information on mitigation [12].

2.1.1 Sense of urgency

CI like SSBs has gained increasing attention from threat actors (see Figure 1) and this is felt by key stakeholders like CISO's, CEO's and political leadership. Historically, operational technology (OT) was predominantly focused on function and safety. Stuxnet [13] in 2010 brought the cyberthreat to OT to the forefront of public debate for the first time. In subsequent years, Havex [14] (2013), BlackEnergy [15] (2015, Ukrainian power grid hack), Triton/Trisys [16] (2017) demonstrated this risk has not diminished. The active malware development and resulting incidents lead to a continued and growing sense of urgency to face this problem.

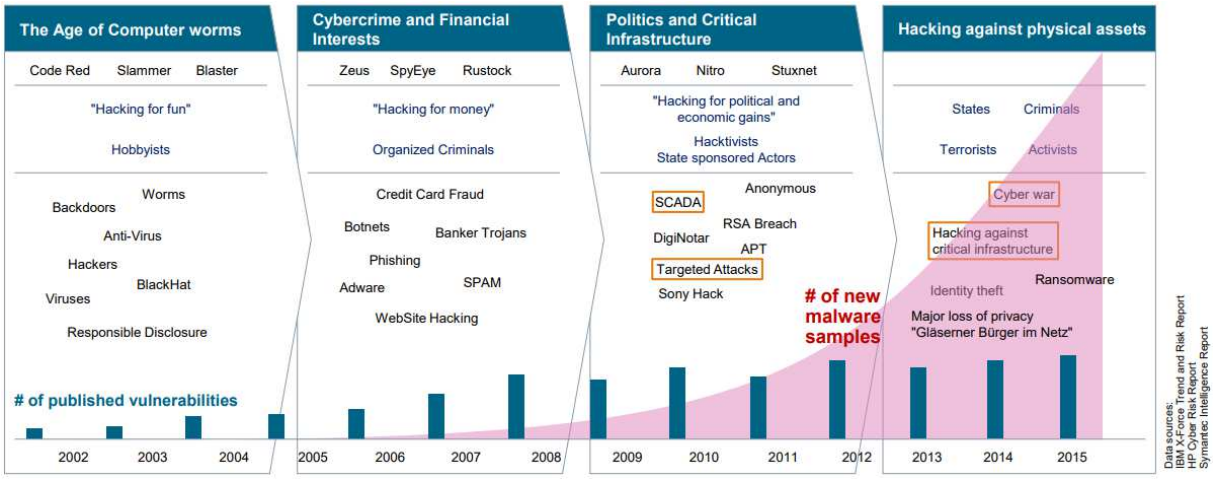

Figure 1, Evolution of attacker motives, vulnerabilities and exploits [17]

Even before Stuxnet demonstrated cyber risk to OT, Deibert and Rohozinski [18] stated in 2010 based on earlier work by Adler that "*a growing "community of practice" is emerging in the area of CI protection that is spreading internationally. This community of practice includes a large cross section of states and private sector actors.*". More recently, both the US (e.g. Executive Order 13636) [19] and European Union (e.g. NIS Directive) [20], have set policy goals and implemented programs to secure CI (CI). A joint alert [21] by the DHS and FBI warning of a Russian intrusion campaign targeting the US energy grid, exemplifies that the threat to CI is undiminished.

In the EU, this sense of urgency creates a drive for increasing resilience in the CI domain. The European Parliament [22] has stated "[…] *that Europe's fragmented defence strategies and capabilities have made it vulnerable to cyber-attacks. They therefore urge EU member states to enhance the ability of their armed forces to work together and to strengthen cyber cooperation at EU level, with NATO and other partners.*". This goal is aimed at general cyber resilience but underpins the sense of urgency that led to the NIS directive, which does focus on CI.

2.1.2 Threats to CI in the Netherlands

In the Netherlands, the task of cyber threat analysis for (amongst others) CI is mandated to the National Cyber Security Centre (NCSC NL), part of the ministry of Justice and Safety. The NCSC publishes the yearly Cyber Security Assessment Netherlands (CSAN) in which they present the digital threats to Dutch society. The CSAN is the product of broad input from both public and private parties and is widely peer reviewed before publishing. This makes the CSAN an authoritative source in the Netherlands for defining the threat landscape.

The CSAN 2018 [08] explicitly mentions threats to CI (the CSAN uses the term 'vital'). SSBs are explicitly mentioned (p22) as an example of a physical system in which an attack can occur. The CSAN 2018 quotes the Dutch Security and Intelligence Service (AIVD) in presenting the threats to CI. For the Netherlands, state actors are seen as the main threat actor against CI using malware compatible with OT to create backdoors. These backdoors can be used later on for further actions like espionage or control of objects. Active malware can influence the operations of an OT system, and is therefore a threat onto itself.

2.1.3 Threats to CI in the United Kingdom

In the UK, the identification of threats to CI is mandated to the National Cyber Security Centre (NCSC UK). The NCSC UK is not as public in publishing the threats to CI as the NCSC NL. The 2017 annual review [23] for instance, mentions only that CI (the NCSC UK refers to CI as Critical National Infrastructure or CNI) are part of their mandate, but presents no further threat analysis. The advisories the NCSC UK publishes do give some insight into the threats to CI. For example, the advisory "*Hostile state actors compromising UK organisations with focus on engineering and industrial control companies*" [06] explicitly refers to state actors as threat actor for CI. A joint statement [24] even goes as far as naming the Russian government by name.

2.1.4 Comparison of the threat landscapes

The analysis in the previous chapters lead to the conclusion that the UK and Netherlands have similar threat actors for CI. Both the UK and Netherlands explicitly name Russia in their threat assessments. It is very expensive to develop nation-state cyber capabilities like tooling and expertise. It is therefore very likely that the modus operandi (e.g. tools, reconnaissance, infection process) used to compromise CI are similar as well. This shared threat landscape will have a positive influence on information sharing [12].

2.2 Use case: embedding cybersecurity into contracts for a fictional SSB

To illustrate the need for information sharing and to provide an example for concepts discussed, this use case is presented. Elements in this use case are explained using a fictional SSB but are related to experiences within Rijkswaterstaat. The best practices developed within Rijkswaterstaat to address the challenges in this use case are candidates for sharing within I-STORM with the UK.

2.2.1 Context

An SSB is a large object that has moving elements that manage the flow of water. The main function is to protect against floods, but a minor function of SSBs is to control the water level. An SSB is generally comprised of the SSB itself, land based supporting structures (like anchoring, engine space, electrical transformation, maintenance buildings, etc.) and a control center. The terrain of an SSB contains cabling, camera's, roads, walkways and other elements. All are parts needed for maintenance and the correct functioning of an SSB. These elements might have IT or OT components embedded that support the functions. Examples of these elements are IP cameras to view areas of the asset, OT like PLC to operate machinery (e.g. switch on a pump), 3G/4G antennas for connectivity, network cabling connecting all elements to a control room or sensors measuring wind speed. All these asset components are managed by the asset manager and staff in a public-private cooperation.

Objects like SSBs are built in two contract forms; DBFM (Design – Build – Finance – Maintain) and D&C (Design & Construct). In the case of D&C, the maintenance is contracted separately. These contracts are awarded for long periods, sometimes for decades. Tenders are the basis for the contracts awarded, for they contain the requirements for the object in question. Cybersecurity is one of those requirements.

The main challenge is how to embed cybersecurity in tenders and contracts that are valid for long periods. How do you define a very dynamic requirement like cybersecurity in a way that enables the winning party to define how they will abide to the terms of the contract that may span decades? Any requirements not explicitly defined in contracts are considered extra work which must be payed separately, resulting in an overly costly implementation. Additionally, the contract must be explicit in the roles of the legal parties in order to establish liability and duty of care.

If a vulnerability is discovered in PLC software, the procedure to update firmware can be months. All maintenance is planned, and the safe operations of an object is paramount. This means that plans for upgrading must include testing, determining the complete safe state of an object and rollback scenario before an upgrade can be performed. For an SSB, this means no foreseeable closing or interference with other planned work. This briefly sketches the complexity of something that in regular IT would be a simple change. The impact on safety of installing a patch is weighed against the risk of not installing a patch. For these objects, all changes are implemented with a very strict and careful managed process. This is at odds with the sometimes urgency felt with cybersecurity.

The role of contracts in this use case is critical. Contracts provide the formal language on who is responsible for cybersecurity activities, such as installing patches or reporting incidents. The tender specifies what security requirements must be met, for example implementing patches. The contractors in their bid, justify their fulfilment of the requirements in a cybersecurity execution plan. This plan details per requirement how the responsible party will comply. It will detail how it will install patches, and the cost and impact on operations are included in the tender bid and agreed compensation.

If these requirements are not made explicit in the contract, responsibilities and costs must first be agreed upon before the change can be planned as assignment. This would result in unexpected cost and increased risk through e.g. longer response times to cyber events like patching vulnerabilities.

2.2.2 The use case for I-STORM

RWS has developed a process to address this issue and knows this challenge is shared by members within I-STORM. It would therefore be valuable in several ways to address this within I-STORM. Examples of the goals of discussion within I-STORM are:

- Do other members recognize this challenge?
- Is the challenge comparable to the Dutch situation?
- Would other members be helped with the good practice developed by RWS?
- Could an evaluation by a member state help to improve the Dutch approach?
- Do other members have good practices on this challenge they can share?

Best practices on embedding cybersecurity in tenders and contracts could therefore be very interesting and beneficial to exchange within I-STORM. Examples of challenges to discuss this within I-STORM are:

- Do the members understand the effects of not addressing cybersecurity in contracts (e.g. what operational impact this might have)?

- Does a member have (formal) permission to share information on how we treat cybersecurity in contracts with other members?
- How does a member know other members will treat the confidentiality of the information I share in the correct way?
- Are members allowed to discuss cybersecurity topics?
- Does management support the initiative of sharing cybersecurity information?
- How do members share information? Orally or written, original material of RWS or create I-STORM specific adaptations of knowledge (e.g. customized documents for I-STORM or share internal documents)?
- With whom are members obliged to share information?
- How are members facilitated in sharing information, e.g. meeting location, travel and lodging expenses.

The examples listed above, and the need described in the following paragraphs lead to the conclusion that cybersecurity is an issue that should be addressed in I-STORM. An opposite force to information sharing on cybersecurity is caused by the unfamiliarity of cybersecurity as it relates to the engineers' work and the fact that cybersecurity of SSB is considered part of national security. These forces result in the current situation in which cybersecurity is a difficult topic to address in I-STORM without any further support.

2.3 The engineering perspective

An engineer's main concern is mitigating the physical risk (safety) of the object using the 'RAMS' acronym. RAMS stands for Reliability, Availability, Maintainability and Safety [25]. This focus is one of the first things that surprised me (coming from an IT background where the focus is continuity) when discussing cybersecurity with engineers. This thesis must support engineers to address cybersecurity issues. Therefore, it is imperative to recognize this different focus between safety in the engineering view and continuity in the IT view. This paragraph highlights the engineer's approach to mitigating risk in order to provide the context to incorporate cybersecurity.

The building and operations of an SSB by engineers, is focused on continued assurance of safe functional reliability. The design and management of objects is commonly approached through Systems Engineering (SE) [26]. SE is based on Systems Thinking [27] and is characterized by a holistic and interdisciplinary approach. SE in essence has four phases:

- Decomposition and definition
- Implementation
- Integration and Recomposition
- Operations and maintenance

The first three phases are predominantly employed in construction of new assets, with most of the asset lifespan positioned in the final operations and maintenance phase.

The main model to visualize the lifecycle of SE (and the asset) is the V-Model (Figure 2) in various representations. My experience within RWS has shown me there is still little experience on integrating

cybersecurity in the V-model. This contributes to the lack of attention to this domain by engineers. NIST has addressed this issue in NIST SP800-160, Systems Security Engineering (SSE) [28]. This publication is a handbook on how to achieve cyber resilience through a SE approach. It describes the security activities per stage in the V-Model.

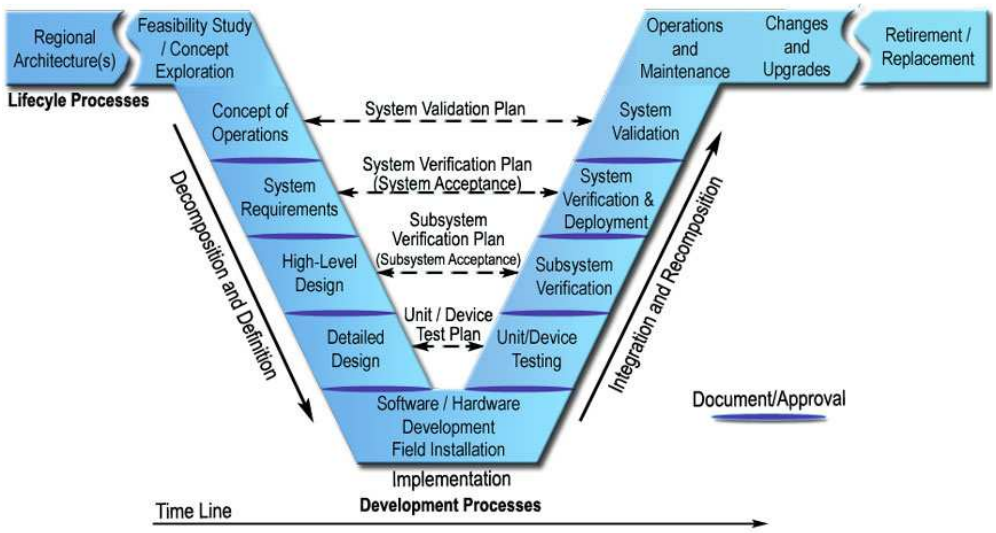

Figure 2, V-Model in Systems Engineering [29] as used by Rijkswaterstaat Cybersecurity Centre

The IT and OT systems in SSB are approached within SE, so with primarily safety in mind. Any changes to systems must be implemented in a way that does not compromise functionality or safety. Cybersecurity features are perceived by engineers as adding changes without any need from a safety of functionality perspective; a solution without a problem. Implementing controls for cybersecurity do introduce a possible negative effect on safety of functionality (e.g. a network sensor could delay network traffic leading to malfunction).

An engineer who has only dealt with engineering risk (which is good to quantify), therefore is reluctant to understand the benefits of implementing cybersecurity. The impact of cybersecurity incidents on safety is not yet well recognized. This lack of recognition of the impact of cyber incidents means that cybersecurity is hard to accept as part of the engineer's responsibilities. Addressing cybersecurity governance from an IT perspective, only reinforces this sentiment.

The NIST SP800-82 Guide to ICS [30] advises to implement a specific ICS (OT) security program. The controls in the NIST framework are specific for the engineering environment, so will fit better than IT based frameworks like ISO27000. When a threat actor attacks, it's attack path would not treat OT and IT as separate domains. The separation in mitigation between IT and OT would therefore not be optimal. An effective defense in depth will require a mix of OT and IT in mitigation, a holistic delivery chain approach.

In conclusion, the mitigation process and all supporting aspects (e.g. language used, embedding in existing processes, governance, etc.) should be presented from an engineering viewpoint to ensure the mitigation approach is effective. This engineering viewpoint enables the engineer to translate cyber risk to safety risk and support taking appropriate action. Clarity on how to act results in embedding

cybersecurity in the overall safety culture in SSBs. To do this, the SE approach must include cyber threats, leading to *Security* Systems Engineering. NIST SP 800-82 provides the controls, whereas NIST SP 800-160 provides the tasks mapping to the V-Model to facilitate implementation within SE processes.

2.4 Addressing cyber threat through sharing information

This paragraph explores how common cybersecurity frameworks or models can provide support for information sharing in mitigating cyber threat and which frameworks might be a fit for I-STORM. The exploration is performed by first researching the role of information sharing as mitigating control. Next, information sharing frameworks are identified for potential use for I-STORM. This paragraph concludes with a short-list of frameworks to assess for implementation in I-STORM.

2.4.1 Information sharing as control in common security frameworks

Mitigation frameworks like the NIST or ISO/IEC are typically implemented within an organization and not holistically in a supply chain. Each organization implements controls for their 'stovepipe', and little support is given for alignment across the supply chain. NIST 800-82 for instance only addresses incident information sharing to governmental organizations in AC-21 [30, G-19], but no inter-organizational information sharing is mentioned. The ISO27002:2013 mentions contact with special interest groups in section 6.1.4a [31, p5] but does not give any specific guidance on how to implement this control.

This leads to the conclusion that from a security framework viewpoint, information sharing as a control is seen as relevant, but no specific requirements to this information sharing in the form of goals or empiric criteria is given. A similar sentiment on the role of information sharing in mitigating cyber threats was identified by The World Economic Forum (WEF) and McKinsey. In 2014, they collaborated to raise the visibility of cybersecurity among top executives at the WEF 2014 annual meeting. In preparatory interviews, several findings were identified as essential for cyber resilience. The results of that study by Kaplan et al. [32, xii] presented in finding four, that cooperation between all stakeholders is essential for digital resilience. They too identified that there is no clear consensus on how this ecosystem should evolve and state that "*[…] increased collaboration across the public, private and not-for-profit sectors will be critical.*". These real-world findings support the conclusion on information sharing based on security framework analysis.

2.4.2 Available cybersecurity information sharing models

In the section above, the conclusion is reached that security frameworks identify information sharing as relevant to mitigation, but they do not offer a solution on how to address this (a sharing model). Therefore, this paragraph explores what specific information sharing models exist for cybersecurity that are suitable for I-STORM.

Desk research has been performed to identify candidate frameworks. To do this, frameworks in use by governments (the owners of SSB assets) in the EU, UK and NL have been inventoried. Sources like ENISA, NCSC UK and NCSC NL as well as frameworks assessed at Rijkswaterstaat have been used as primary source. Due to the international character of I-STORM, in the second phase of this desk research, a widening of the scope has been performed. This is done to prevent a focus on the EU, UK

and NL from excluding relevant information. In this short expansionary phase of desk research, an additional model has been identified; the Information Sharing and Analysis Organization model (ISAO).

This model is published by the ISAO Standards Organization, a non-governmental organization in the US that supports information sharing. They have created a conceptual framework (ISAO 300 and 100 series) [33, 34, 35] "[…] *for information sharing, information sharing concepts, the types of cybersecurity information an organization may want to share, ways an organization can facilitate information sharing, as well as privacy and security concerns to be considered.*". This model provides both factors on how to share and gives guidance on the content of what may be shared. This scope matches the goal of this thesis, and therefore this model is included for evaluation.

Summarizing, desk research has identified the following sharing frameworks and sources:

- **Information sharing and common taxonomies between CSIRTs and Law Enforcement** [10]
  An ENISA report on 11 information sharing taxonomies used for sharing between these entities. Focus is on automated and formalized exchange of incident and threat information.
- **CiSP (Cyber Security Information Sharing Partnership)**
  "*CiSP is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.*" [36]
- **US-CERT Information Sharing Specifications for Cybersecurity**
  Presents "*TAXII, STIX and CybOX* […] *community-driven technical specifications designed to enable automated information sharing for cybersecurity situational awareness, real-time network defense and sophisticated threat analysis.*"
- **ISAC (Information and Sharing Analysis Center)**
  Both the UK (CPNI Information Exchanges) [37] and Netherlands (NCSC ISACs) [38] use the ISAC's model to facilitate information sharing with both public and private parties. ENISA's National Cyber Security Strategy experts' group has identified the ISAC model as a good practice for information sharing within the EU [39, 40].
- **GCCS best practices**
  For the Global Conference on Cyberspace 2015 (GCCS2015), the Netherlands presented a framework based upon Dutch best practices in information sharing on cybersecurity [41].
- **ISAO (Information Sharing and Analysis Organization)**
  The ISAO model [33, 34, 35] is in use in the US for independent information sharing on cybersecurity. This framework is similar to the ISAC model, with the main difference being that an ISAO is meant as standalone organization, so not part of a governmental organization.

To assess if the desk research identified the correct models, this point was addressed in a conversation with a TNO researcher on cybersecurity on October 31st, 2018. It was indicated that no relevant models were omitted in the desk research phase.

To assess this longlist of frameworks, two selection criteria for the shortlist are evaluated:

1. Scope of the framework using the three-layer model of Berg et. al [42] (technical, socio-technical and governance)
2. Target audience

The first three frameworks are aimed specifically at the sharing of (technical) incident and/or threat data [10, 36, 43] with cybersecurity professionals as target audience. Information on incidents and vulnerabilities to SSBs is the domain of national security. The mandate for sharing this type of information is mandated to the NCSC UK and NCSC NL and not to sharing organizations like I-STORM. Therefore, this type of information sharing is not of much relevance to I-STORM.

The last three information sharing frameworks have a broader set of topics they address like asset management, restore procedures, awareness, etc. These frameworks are aimed at members that represent this broad scope of topics, so covering expertise in technical, socio-technical and governance topics. The GCCS (and in lesser extend the ISAC mode) have an additional focus on critical infrastructure.

Desk research on candidate information sharing models therefore identified three models for evaluation in paragraph 3.2: ISAC, GCCS and ISAO.

2.5 The role of I-STORM in information sharing for SSBs

The role of I-STORM is important to define, for it gives the context in which the main research question is addressed. This is addressed by interviewing two key stakeholders on this topic and by reviewing I-STORM documentation. One of the interviewees is from Rijkswaterstaat, and the other is from the Environment Agency. This ensures that input is provided by both organizations in the scope of this thesis. The results of the interviews and desk research are presented in this paragraph by first summarizing the answers given in the interviews and secondly summarizing the I-STORM strategy on knowledge domains.

In the exploratory interview (Appendix 5, 1.1 and 1.2), both respondents indicate that information sharing is a high priority. The respondent from RWS indicated that I-STORM is the network for information sharing on SSBs, and that knowledge and experiences on cybersecurity should be addressed as crucial topic for ensuring the reliability of SSBs. Both respondents identify cybersecurity as an important topic, but because of the UK respondent not being a direct I-STORM member, could not expand in detail.

This focus on information sharing is reflected on the I-STORM website: "*I-STORM aims to continuously improve standards of operation, management and performance in order to reduce the risk of severe flooding of people, property and places around the world, by facilitating knowledge exchange amongst members.*". To further develop this, I-STORM is in the process of formalizing knowledge domains, based on the RWS domains for SSBs. These domains are:

- **Discipline knowledge**
- **Knowledge- and risk-controlled management and maintenance**

- **Object knowledge**

These domains are dependent on methodological knowledge like safety, politics, market technology, etc. Cybersecurity is part of the methodological knowledge on SSBs that need to be embedded in operations. I-STORM has visualized this flow of knowledge in Figure 3.

The lemniscate depicts the (unending) flow of information, catching the environmental information and including it in the SSB knowledge domain. It connects different levels, from strategic topics at the top to tactical and at the bottom the operational level. The strategic level represents the overall goals and requirements of the organization. This can include both internal forces like policy and management contracts, but also external factors like national politics, scientific/market developments and environmental changes. These inputs must be translated to operational goals like discipline knowledge required to fulfill the strategic goals. The tactically binding knowledge translates the strategic goals to coherent operational actions. In an unstructured interview on October 30th, 2018 the senior advisor on SSBs commented: "*Without that continuous connection and flow of information, things will go wrong, and the organization will not meet its objectives.*". Paragraphs 4.1 and 4.2 further expand on these levels.

The role of I-STORM lies in providing the central linking pin as tactically binding knowledge facilitator through sharing good practices between members on the knowledge domains.

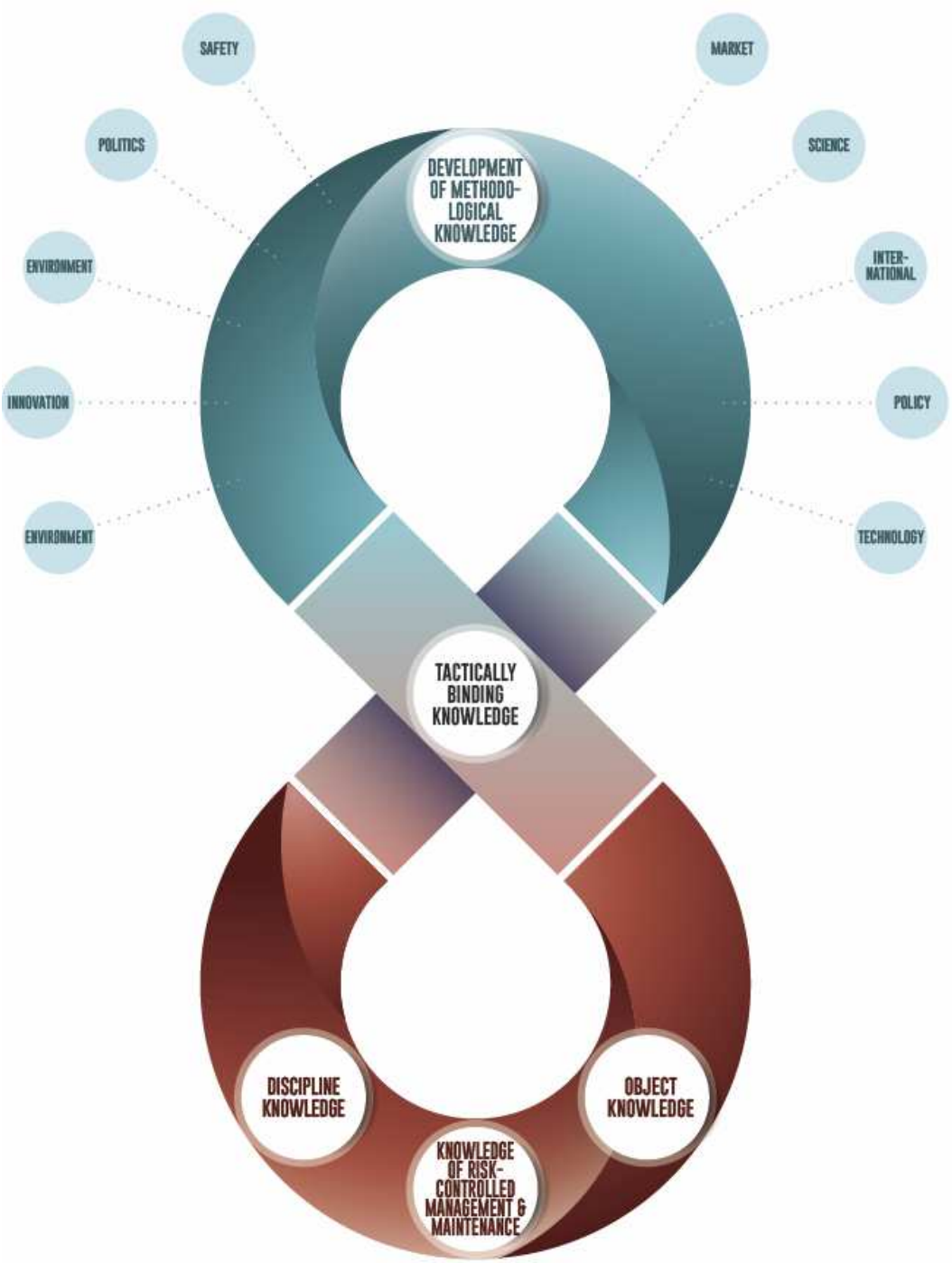

Figure 3, Conceptualizing the Flow of Knowledge concerning SSBs [44]

The need to address cybersecurity for SSBs as stated in the beginning of this chapter, can be visualized in Figure 3 as part of the bottom half. It is recognized that cybersecurity as a strategic goal with supporting policies is present (top half of Figure 3), but no clear method is available to operationalize this for SSBs (bottom half of Figure 3).

The role of I-STORM therefore is in the center by connecting strategic information to operational activities on information sharing. The information sharing process delivered by this thesis enables I-STORM to address cybersecurity in the bottom half of Figure 3. Chapter 4 and in particular paragraph 4.2 expand on how the knowledge conceptualization in Figure 3 is used as a basis for the information sharing process presented in this thesis.

2.6 Requirements for information sharing within I-STORM

To answer the second sub question on *how* to share information, requirements for a sharing process must be identified to select a suitable model from the shortlist presented in 2.4.2. Therefore, this section first presents the requirement criteria used for selection of a model. Second, the requirements that are relevant to I-STORM and SSB information sharing are presented, based on interviews and the literature research presented in previous paragraphs. Additionally, experience with information within I-STORM on other domains sharing is taken into account through an unstructured interview with interviewee 2.

This paragraph concludes with the requirements for the information sharing model that are used in chapter 3.2 to select an information sharing model for I-STORM.

2.6.1 Selection of the requirement criteria for the information sharing model

The core of the need in I-STORM, is the sharing of information and knowledge. In selecting a methodology for evaluating the shortlist of models, desk research focused at selecting papers that defined a set of requirements for information of knowledge sharing.

Two papers are identified that support the selection of a model for this thesis. First, a paper on the dimensions of collective cyber defense by Skopik et al. [11] was selected. This paper was selected because it analyses the impact of information sharing on '[…] *large-scale cyber-attack situations*'. It does so in three steps, the first of which details requirements for information sharing. The second paper by Gharawi and Dawes [12] approaches information sharing in transnational networks and presents 19 factors that influence knowledge and information sharing. This second paper has no focus on a specific domain like the first paper, but it does focus on transnational sharing, which supports the scope of this thesis.

The second paper by Gharawi and Dawes [12] was selected for this thesis. The paper by Skopik approaches information sharing from a Cyber Security Incident Response Team (CSIRT) viewpoint. It therefore has a focus on the technical aspects of cybersecurity information sharing as opposed to the more general approach of Gharawi and Dawes. Gharawi and Dawes have identified factors at a more granular level, enabling a more detailed identification of desired factors in an information sharing model.

Therefore, the 19 factors influencing Knowledge and Information Sharing presented by Gharawi and Dawes are used to select a suitable model for I-STORM.

2.6.2 Information sharing factors to address

The previous paragraph presented the viewpoint for assessing the models based on the factors identified as critical for information sharing by Gharawi and Dawes. To gain insight into what factors most important, an interview was held with interviewee 1 (Environment Agency Process Leader for Operational Technology) and interviewee 2 (RWS Senior Advisor SSBs (board member of I-STORM)). The interviews results are presented in Appendix 5, 1.1 and 1.2, including a table explaining the factors in more detail for the interviewees (Appendix 2; Exploratory interview on Cybersecurity Information Sharing requirements). The results of the interview are referenced in various chapters.

The interviews were conducted via emailed questionnaire with additional information gathered through a semi structured interview with open questions regarding answers given in the questionnaire. The respondents were asked to indicate the five most important factors from a list of 19 key factors for information sharing [12]. This is done to identify the critical factors in sharing for I-STORM (the scope of this thesis), and not what model is the most complete (potential future research). The identified factors make it possible to evaluate which model is the best fit for I-STORM.

In the exploratory interview, question 9 (Appendix 5, 1.1) explicitly asked: "What are the five most important aspects in your opinion that should be addressed to enable information sharing?". Interviewee 1 indicated at that he found it "*Difficult to say. At this moment I think two things are most relevant*". He did not explicitly use the factor description provided, but used his own words:

- *"The amount of freedom to share by law and policy*
- *The definition of those general aspects that could be shared and those that are to sensitive and we don't share (yet)"*

The first bullet refers to "Laws and policies". The second bullet refers to "Value, sensitivity and confidentiality". Due to the explicit mentioning of '*definition of those general aspects'*, the factor "Lacking for data standards and definitions" is identified as well. Interviewee therefore identified three factors. Interviewee 2 selected a list of five factors he deemed most important, identifying them by using the identifiers in the provided table:

- Laws and policies
- Organizational rules
- Sensitivity and confidentiality
- Political support
- Resources

The results are that interviewee 1 identified five factors and interviewee 2 identified three factors. With two factors overlap, this results in six factors for evaluation. The two factors that overlap (presented below) are the most important factors to address:

1. Laws and policies;
2. Value, sensitivity and confidentiality.

Both factors are strongly connected. Laws and policies refer to information with indicators of confidentiality (classification schemes), therefore information sensitivity must be known. Law and policy can only decide on what to share, if sharing partners agree upon which information can be shared.

This implies a shared codification on how to identify and mark information that is shared. Both parties indicate that a clear mandate is desired from management on what information can be shared.

Concluding, the following factors are identified as the most important as indicated by interviews. The factors indicated by both interviewees are marked in bold. These sic factors are used to score the three models identified in 2.4.2 as part of the selection process in 3.2. Per factor, the scoring interviewee number is indicated in parentheses.

1. **Laws and policies** (1 & 2);
2. **Value, sensitivity and confidentiality** (1 & 2);
3. Organizational rules (1);
4. Political support (1);
5. Resources (1);
6. Lacking for data standards and definitions (2).

2.6.3 Past experience with information sharing in I-STORM

Information Sharing in I-STORM is being done in different formats. From peer-reviews in which members invite other members to assets for an independent review and advice of operations, to conferences where presentations and knowledge sharing sessions are held and a newsletter. These formats ensure that professionals can get to know each other and exchange information on SSB operations.

Within RWS, a structured and formalized approach was presented in April of 2018 to ensure that relevant knowledge for SSB operations is secured. The 'Knowledge strategy SSBs' [44] presents a long-term vision to secure knowledge resilience and operating excellence. This knowledge strategy approach was introduced to members of I-STORM and was very well received. This led to the translation of the Dutch knowledge strategy to English for adoption by I-STORM.

This I-STORM knowledge strategy provides a structure (knowledge domains) for the information sharing within the network. This structure provides I-STORM with a shared view of how knowledge is defined, structured and how knowledge relates to SSB operations. Any new information sharing initiatives should fit into this approach to knowledge management.

There is little past experience with cybersecurity topics as compared to the other domains. Therefore, the support of sharing on the cybersecurity domain is focused on the first steps. Therefore, at this point it should be possible to grow the maturity of sharing, but no very formal artifacts are required.

2.6.4 Compatibility with Systems Engineering

In discussions with colleagues of researcher at Rijkswaterstaat, one of the pitfalls of cybersecurity that is mentioned often, is that the topic of cybersecurity is presented from an IT point of view. Paragraph 2.3 gives insight into how engineers mitigate risk during the lifecycle of an asset. These two approaches/views differ, so the engineering point of view must be considered to effectively discuss cybersecurity. Therefore, the information sharing process must be compatible with the

viewpoint/context of the engineers in I-STORM. Using their viewpoint will promote acceptance and integration in their way of work. This approach also ensures that the language used in the process is understood by engineers and cyber-jargon that might lead to confusion is minimized.

2.7 Relevance of the requirements to the research questions

The previous paragraphs discussed important aspects for a solution to the research questions. In 2.3, the importance of the engineer's viewpoint is presented. Paragraph 2.4 presented the importance of sharing information on cybersecurity with 2.5 focusing on the role of I-STORM in sharing information. Paragraph 2.6 explored the requirement of I-STORM in sharing information by identifying sharing models for evaluation and the factors to base the evaluation on. The resulting insights of these paragraphs are requirements for the artifacts needed in answering the main research question of this thesis.

In design science, the requirements are used to assess if existing artifacts are available. If no artifact is available, the requirements guide the construction of a new artifact. Chapter 3 represents that part of design science. Chapter 4 presents the new artifact and chapter 5 evaluates the new artifact according to the design science methodology.

These requirements therefore are key in the methodology applied ensuring the resulting process answers the main research question. Below, each requirement is presented and how they relate to the research sub question.

1. The process must be compatible with Systems Engineering;
    - The process must use language and good practices understandable for I-STORM members with an engineering background). It must also fit in the lifecycle steps of an asset. Both these aspects are predominantly addressed in research sub question 1.
2. The process must provide a list of topics on which to share information in a way understandable by engineers.
    - The topic list presented must be presented in the viewpoint of the engineer. This is explicitly addressed in research sub question 1. Research sub question 2 also addresses the important factors as indicated by engineers in the exploratory interviews. Therefore, sub question 2 is also relevant for this requirement.
3. The process must address the six important knowledge sharing factors identified by the exploratory interviews in 2.6.2;
    - Research sub question 2 addresses that the selected information sharing model presents good practices on the important sharing factors identified in the interviews.
4. The process must fit within the knowledge management strategy of I-STORM as described in 2.5;
    - Research sub question 2 provides a basis for this by selecting a model that supports the dilemma's presented in the use case, but this requirement is mostly addressed in chapter 4 in the construction of the information process itself.

In the next chapter, these requirements are used as input for answering the two research sub questions.

3 Designing an information sharing process for SSBs

In chapter 2, the role of information sharing I-STORM on mitigation have been presented. The need for information sharing is broken down into two elements; the *what* and the *how*, referring to sub-question 1 and 2. Chapter 2 concluded with a list of four requirements for an information sharing process and how these relate to the sub-questions. This chapter addresses these requirements and propose a solution for both elements.

Each element is addressed in a paragraph, starting with sub-question 1; "What are relevant topics on cybersecurity for SSBs?". To answer this question, this thesis first explores what form this list is presented in. Next, the construction of the list in the selected form is presented in a manner that supports validation and reproducibility. Having defined the form of the list, researcher explores how to identify the topics that populate the list. Following this, the topics in the list are related to each other and SE, to ensure practical application by engineers. Concluding, the resulting structured list of topics is presented, and validation based on the requirements is addressed.

Next, this chapter addresses sub-question 2; "What is the best way to share information for the I-STORM community?". To do this, the viewpoint of critical knowledge sharing factors [12] is applied to common information sharing models. First, common information sharing models are selected and evaluated on how well they address the critical factors. The factors indicated as important in the interviews in 2.6.2 are marked in the resulting matrix, to highlight which factors are essential in selection of a sharing method. Based on this matrix, a sharing framework can be constructed for implementation in I-STORM by selecting the best-practices from the models that best address key factors for I-STORM. Concluding, this paragraph presents a sharing framework for I-STORM.

This chapter concludes with a discussion of the selected topics and sharing framework.

3.1 Cybersecurity topics for SSBs

This chapter addresses sub-question one by constructing and presenting a list of cybersecurity topics for use within I-STORM. The form and construction of the topic list is based on literature research. Common OT security frameworks like those mentioned in 2.4.1 and concepts from SE serve as the main source of input for the content of the topic list. This paragraph concludes with a presentation of the resulting topic list, as input for the next chapter; a cybersecurity information sharing process for I-STORM.

3.1.1 Defining the topic list structure

There are many ways to compile a structured list of information, but for structured lists a taxonomy and ontology are most prevalent in science. A taxonomy is a hierarchical arrangement of topics (e.g. parent-child relations), whereas an ontology facilitates more complex relationships between topics. Additionally, ontologies support information sharing by making knowledge transferable: "*Ontologies have set out to overcome the problem of implicit and hidden knowledge by making the conceptualization of a domain (e.g. mathematics) explicit.*" [45].

Ontologies also support requirement 2 stated in 2.7 by incorporating SE principles (like those visualized in the V-model [Figure 2]) to describe the relationship between topics. To further support this relation in the ontology creation, the NIST SP800-160v2 [28] guideline is referenced. The purpose of this guideline is to provide "[…] *guidance on how to apply cyber resiliency concepts, constructs, and engineering practices, as part of systems security engineering.*". This use of a proven bridging guideline increases the usability of the ontology for both engineers and cybersecurity professionals. This creates a shared vocabulary between the two domains and organizations that use the ontology (e.g. the UK and NL), facilitating information sharing.

An additional strength of an ontology is that because of the formalized and structured form, it is easier to connect with other CI domains, e.g. the energy sector. Ontologies used in other sectors, can be cross referenced with the I-STORM ontology to facilitate cross-domain information sharing.

For this thesis, it is not necessary to construct a detailed ontology with a high level of formality. The needs of I-STORM require a structured list of topics that can be discussed in a very early stage of sharing cybersecurity information (see 2.6.3). Ontologies are a 'living document', that can grow with the needs of the organization. Therefore, it is not necessary to present a highly formalized and detailed ontology for it to be usable within I-STORM. As the information sharing on cybersecurity within I-STORM grows, so can the underlying ontology grow accordingly. This paragraph therefore constructs an ontology at a level that enables the start of information sharing within I-STORM. The information within Rijkswaterstaat available for sharing with I-STORM is used as example of the abstraction level of the ontology.

Summarizing, the benefits of using an ontology are:

1. Facilitates more complex relationships between topics;
2. Makes knowledge transferable (shared vocabulary) in the context of information sharing;
3. By using the engineering context of a proven framework (NIST), the ontology topics can more easily be related to engineering work on SSBs
4. The formalized structure and form facilitate cross-domain information sharing;
5. An ontology can be implemented in increments, growing in step with the needs of the organization.

3.1.2 An ontology for cybersecurity of SSBs

This paragraph first presents the requirements for the ontology. Next, desk research shows that no existing ontologies are available and that an ontology needs to be designed. This paragraph therefore next selects a methodology for ontology creation. This methodology is then applied in the next paragraph to create a new artifact; the ontology for cybersecurity of SSBs.

Research on existing ontologies was performed by looking for ontologies that were not limited to the technical domain and were designed for the SE domain. Desk research identified three published ontologies that might fit.

1. "*An ontology-based approach to information systems security management*" by Tsoumas et, al. [46].
2. "*Conflict and Cooperation in Cyberspace: The Challenge to National Security*" by Panayotis and Yannakogeorgos [47].
3. "*Ontology for Systems Engineering*" by van Ruijven [48]

The first two ontologies were not aimed at the SE domain and could not be easily adapted. Additionally, both had a focus on the technical aspects. The third ontology does not fit because it has a focus on the physical engineering domain. Therefore, researcher concluded there is no existing ontology available for I-STORM.

In design science, if no existing artifact satisfies the requirements, a new artifact is constructed. Research on creating ontologies was based on three aspects. First, I-STORM has no specific approach to sharing cybersecurity information. Therefore, the artifacts of this thesis must support the first steps while it is preferred to support long term maturity growth in using ontologies. Second, researcher has no prior experience in creating ontologies, so an approach should not require much prior knowledge and offer support for 'first time creators'. Lastly, the approach should give some assurance of its efficacy.

Desk research identified two ontology creation methodologies as candidates based on the requirements presented above:

1. "*Developing an Ontology of the Cyber Security Domain*" by Obrst et, al. [49]
2. "*Ontology development 101: a guide for creating your first ontology*" by Noy and McGuiness [50]

The second methodology was selected, based on the support of different levels of use of ontology, low threshold of required previous knowledge, competency questions, well reputed source (Stanford), extensive description of the reasoning and design choices and finally the methodology is example driven.

The methodology of Noy and McGuiness describes seven steps to create an ontology:

1. Determine the domain and scope of the ontology
2. Consider reusing existing ontologies
3. Enumerate important terms in the ontology
4. Define the classes and the class hierarchy
5. Define the properties of classes/slots
6. Define the facets of the slots
7. Create instances

As described in the conclusion of 3.1.1, this thesis does not require the construction of a complete and formalized ontology. To support the main research question, a shared vocabulary is needed. A full ontology with detailed and strict classes is overkill and therefore out of scope for this thesis.

Therefore, steps 1-3 are used to construct an ontology for use within I-STORM. This results in a list of topics relevant to the cybersecurity aspects of SSBs. Steps 4 and further can be implemented if a more complete or formal extension of the presented ontology is needed as maturity of information sharing and participating members grows. The following paragraphs describe the three steps in the methodology to create an ontology for I-STORM.

3.1.3 Step 1, The domain and scope of the ontology

The first step in creating an ontology is defining the scope and domain of the ontology. This sets the boundaries and viewpoint in which the ontology is created. The scope, use, and domain of the ontology have been discussed in the previous chapters. The scope of the ontology is presented in 1.3 with a further detailing in 2.5 and 2.6. In summary, the ontology scope is cybersecurity for SSBs. The ontology describes cybersecurity aspects, within the context of using those subjects in a SE environment. The ontology user is an engineer or cybersecurity professional working in the field of engineering, detailed in 2.3.

The user of the ontology references the ontology to answer the following questions:

- What topics are relevant to share information on for SSBs?
- What does a topic entail and what is its importance to SSB operations?
- What are the considerations to address before sharing information on this topic?
- Which topics are related to each other?
- How do the topics relate to SE?

3.1.4 Step 2, Possible reuse of existing ontologies

The second step in creating an ontology is researching if any existing ontologies exist for reuse. This prevents unnecessary work and gives an insight into possible related ontologies that give inspiration on how to approach the creation of the new ontology.

Possible available ontologies are researched by using two approaches. First, a review of literature is done to explore what existing ontologies for SE exist that include cybersecurity aspects. The second approach will explore if any cybersecurity ontologies exist for the engineering domain of critical infrastructure. These two approaches are presented in the following two sub-paragraphs and identify possible existing ontologies that can be reused.

3.1.4.1 Cybersecurity SE ontologies

The literary review has not identified any ontologies on cybersecurity specifically for SE. Available ontologies focus on creating a common language for the physical characteristics of an object [51] or focus on the process of SE [48], but do not include cyber(security) aspects. To verify these results, an additional approach was chosen to look for ontologies for Cyber Physical Systems (CPS) that include cybersecurity aspects. CPS is the general term for an object like an SSB and refers to any object in which "[…] *computation, communication and physical processes are tightly integrated.*" [52]. There are some ontologies presented for CPS, but like the ontologies for SE, they only include the physical engineering aspects [53, 54].

Based on the literature research, it is concluded that there is no existing ontology for SE that includes cybersecurity that can be used as a source for an ontology for I-STORM. Therefore, a new ontology must be constructed.

3.1.4.2 Ontologies based on cybersecurity frameworks

There are several mitigation frameworks for critical infrastructure. Internationally, two frameworks are dominant for critical infrastructure; the NIST 800-82rev2 guide to Industrial Control System security [30] and the IEC 62443 standard series [55]. Within Rijkswaterstaat, the security baseline used for SE projects (Cybersecurity Implementatie Richtlijn objecten RWS or CSIR [56]) is derived from the ISO/IEC 27001:2013 standard. This CSIR guideline has been proven efficient in practice and is applied as baseline for SSB as well. The CSIR is a basis for best practices within Rijkswaterstaat and would therefore be preferential to include in an ontology.

The literature research has not identified an existing ontology that is based on these frameworks for use in SE. The research did identify the NIST Cybersecurity Framework (CSF) [57, 58] as a suitable candidate to base an ontology on. This framework provides a common taxonomy and includes links to six cybersecurity frameworks, including ISO/IEC 27001:2013 and ISA 62443-3-3:2013. This taxonomy can be extended by relating it to SE to form a domain specific ontology. The framework consists of three components;

- The Framework Core
- Implementation Tiers
- Profiles

The CSF Core "[…] *provides a set of desired cybersecurity activities and outcomes using common language that is easy to understand. […] The Framework Core is designed to be intuitive and to act as a translation layer to enable communication between multi-disciplinary teams by using simplistic and non-technical language.*" [59, 60]. This makes the Framework Core very well suited as the basis for an ontology for I-STORM. An ontology based on the Framework Core facilitates a common language and set of topics for use between different organizations. The references to cybersecurity frameworks in the Framework Core enable the translation to organization specific security baselines.

The Framework Core has three levels;

- Functions; the main functions within risk management
- Categories; the high-level cybersecurity objectives for an organization
- Subcategories; statements on control objectives that provide considerations for creating or improving a cybersecurity program

These levels are illustrated in Figure 4 below. The category level is very well suited as a basis for the ontology on which information can be shared. The subcategories are suited to provide examples for identifying common challenges and best-practices. By relating the categories of the Framework Core to the context of SE and SSBs, an ontology is created for I-STORM. The subcategories are referenced for examples within this ontology.

In the next paragraph, the approach is described, transforming the taxonomy of categories into an ontology. The categories are assessed in the context of SE and SSB thus resulting in an ontology for use with SSB in I-STORM.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figure 4, Levels within the Cybersecurity Framework Core [60]

3.1.5 Step 3, Enumerate important terms in the ontology

In this phase, the terms that make up the taxonomy of the CSF (the categories) are explained to the target user (I-STORM member). In this process, the categories of the CSF are explained within the context of the ontology domain; SE and SSB. To do this, the CSF columns in Figure 4 are appended by adding two additional columns;

1. **Relevance in Systems Engineering** (column C)
   This explanation describes the importance of the category concept for the specific SE phase, enabling the engineer to understand what that cybersecurity concept means for the activities in that phase. The description supports the understanding of the reasoning line of addressing that concept in the SE lifecycle. This understanding helps to correctly implement the concepts of cybersecurity into SE. For example, if the engineer understands that it is important to include cybersecurity aspects (like firmware version) into the asset management of an SSB in order to quickly assess vulnerable components when an exploit for firmware is discovered, he/she can better implement that category.
2. **Threat states of Storm Surge Barriers** (column D)
   For use in I-STORM, there is a need to further explain the category and presenting examples. In this column, the category is explained in three threat states (for details, see 3.1.5.2). A threat state refers to how threats are treated in asset operations. An asset is resilient against a known threat level, so this 'state' is the baseline against which mitigation is implemented. If a new threat is identified, this threat is evaluated against asset resilience. This represents a different process and information need than the baseline resilience state. The third state describes the state in which an asset is compromised through a manifested threat. This threat state focuses on

different processes and information than the other two states; containment, identification of impact and return to normal operations.

The description and examples for each threat state are not exhaustive but serve as an example to enable a deeper understanding of the category relation to an SSB. The description and examples increase understanding of the category, which improves discussion and processing of cybersecurity topics by engineers.

In the sub-paragraphs below, the population of the two additional columns is presented. This approach was discussed in a discussion with the RWS senior advisor on SSBs on September 13th, 2018 and a UK engineering manager for SSB on September 14th, 2018. Both interviewees are active members in I-STORM. The RWS senior advisor and his UK colleague indicated that this approach is recognizable to the engineer and facilitates the identification of shared challenges and best practices. The RWS adviosor suggested to include an explanatory word list, to further minimize misunderstandings and to clear up any domain specific abbreviations and terms. This suggestion has been implemented by including an appendix of abbreviations and terminology (Appendix 1; List of abbreviations and terminology).

3.1.5.1 Relevance in Systems Engineering

In the column 'Relevance in Systems Engineering' the category is explained in the context of the main phases in the SE V-model (Figure 2):

1. **The decomposition and definition phase**; this phase begins with defining all aspects of the asset. Requirements like operational specifications, legal requirements, cybersecurity requirements, etc. are specified in the bid and formalized in a contract. Based on the description in the contract, the project decomposes the functionality into smaller units. This decomposition is presented in design plans on different levels of detail. The result of this phase are design plans for the implementation phase.
2. **The implementation phase**; the designs are implemented in physical constructions, hardware and software. During this phase cybersecurity requirements are implemented in hard- and software, like physical access control to server rooms, secure software development, network zoning, hardware certification and identity and access management enforcing roles and responsibilities.
3. **Integration & Recomposition phase**; built components are tested all levels from unit to system integration testing. In this phase, all requirements are tested and validated like the controls that operate an asset. For cybersecurity, this phase can use different cybersecurity validation methods like red-teaming, penetration testing, code validation, crisis simulation and vulnerability scanning to determine the assurance level of the implementation of cybersecurity requirements.
4. **Operations & Maintenance phase**; this is the regular operations phase in which the asset is operated and maintained. During this phase, the asset will provide the functionality and is part of a national infrastructure. A Security Operations Centre monitors the cyber-health of the asset and provides support (e.g. forensics, disaster recovery) if cyber-incidents occur. The contractual agreements are the main guiding principle for roles and responsibilities, with extra-contractual work being very costly. Mitigating cybersecurity risk is very dynamic, so if the operations and

maintenance phase spans decades, good cybersecurity requirements in the contract are essential for efficient and cost-effective operations.

This explanation describes the importance of the category concept for the specific SE phase, enabling the engineer to understand what that cybersecurity concept means for the activities in that phase. The description supports the understanding of the reasoning line of addressing that concept in the SE lifecycle. This understanding helps to correctly implement the concepts of cybersecurity into SE. For example, if the engineer understands that it is important to include cybersecurity aspects (like firmware version) into the asset management of an SSB in order to quickly assess vulnerable components when an exploit for firmware is discovered, s/he can better implement that category. This understanding facilitates a more effective design of asset management, because the engineer now knows in the example cited above, what cybersecurity aspects of the SSB could be relevant to include in the asset management system.

3.1.5.2 Cybersecurity relevance for Storm Surge Barriers

In the previous sub-paragraph, the categories are explained in general SE context. For use in I-STORM, there is a need to further explain the category in terms of cybersecurity relevance to SSB. In this column, the category is explained in three cyber-threat situations. These three situations represent the three 'states of cybersecurity' of an SSB, loosely based on the states of an asset that can be identified in the Lockheed-Martin Kill chain model [61], illustrated in Figure 5.

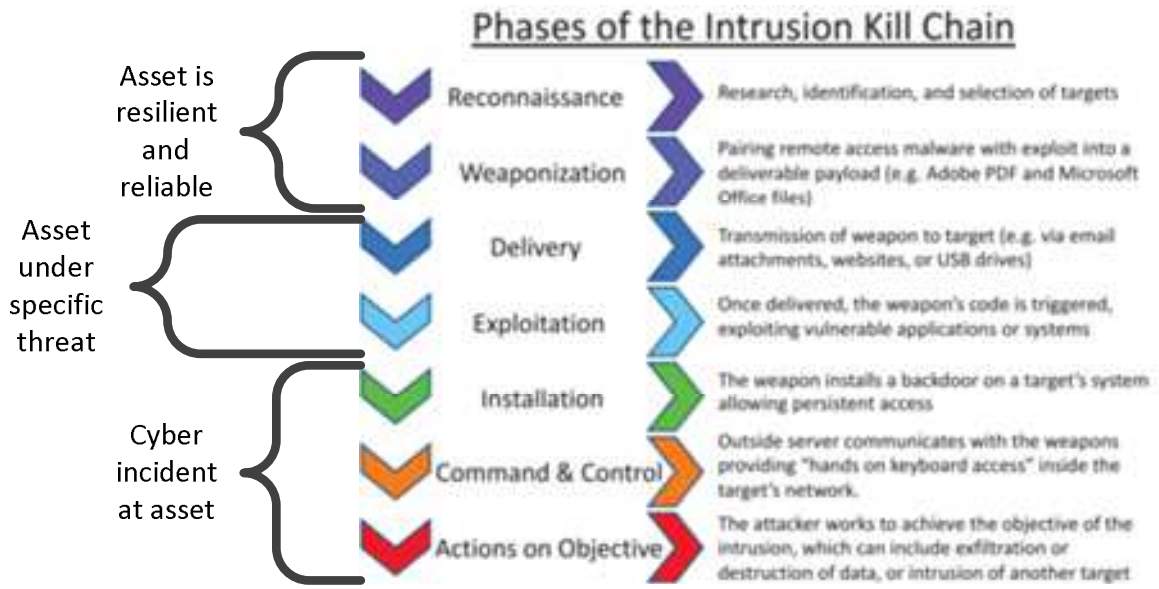

Figure 5, The threat states (left) of an asset Cyber and the Kill Chain (right, taken from [61])

The Kill Chain above shows how a threat can manifest itself to an asset. A threat is a given and is dynamic over time; known threats can be mitigated; a new threat can emerge that needs to be evaluated against the current mitigation or a threat has manifested itself on an asset as a cyber incident. These states influence what the cybersecurity posture is by asset management (Figure 6):

- Resilient/reliable → 'business as usual' security operations like detection
- Cybersecurity threat → assess the risk of the new threat for the asset based on current mitigation

- Cyber incident → analyze, reduce impact and recover

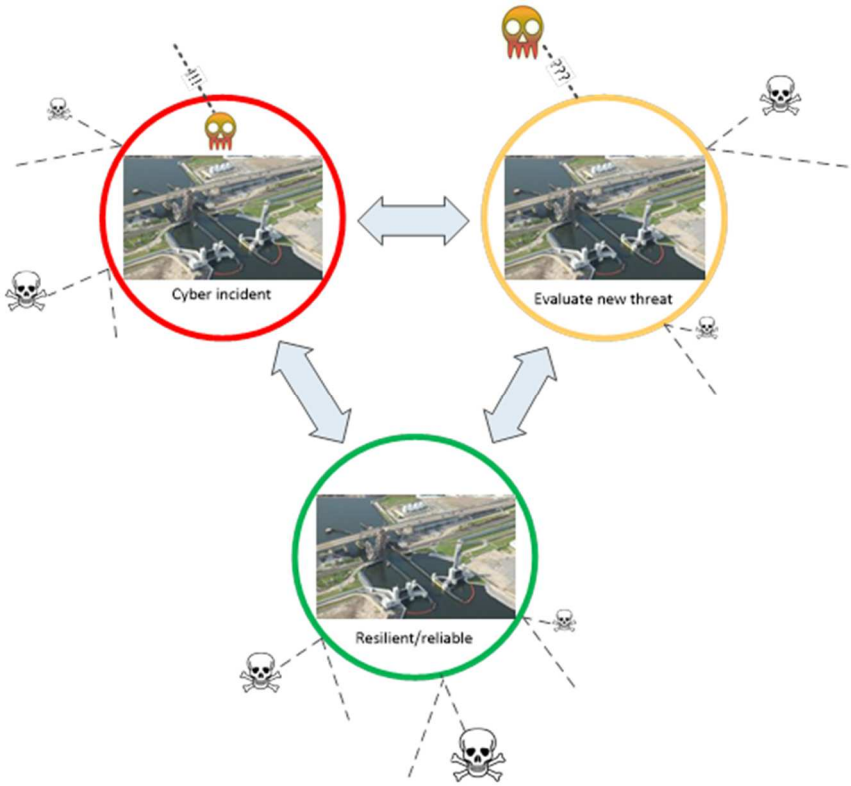

Figure 6, Threat states of a Storm Surge Barrier

The description for each threat state is not done exhaustive but give examples to enable a deeper understanding of the category relation to an SSB. The description of category for the threat state leads to understanding, which facilitates the further discussion and treatment of the category. The three states used to illustrate the category in the context of SSBs are briefly discussed below.

For resilience/reliability

There are threats against assets and these are addressed according to the risk management policy of the organization. The mitigation strategy ensures the resiliency of the asset which is input for the general reliability of asset operations.

The SSB must work as designed, and the assurance (defined in RAMS) of this can be affected by cyber threats. Therefore, it is very important or engineers to understand how categories support the overall SSB resilience/reliability, ensuring operating effectiveness. The mitigation strategy of the organization is based on threat actors and the means they employs to attack.

The broad definition of resilience from the field of information science is used, including both the prevention of attacks being successful and the recovery after an incident [62]. This broad definition matches the definition of resiliency from the field of engineering: "*[…] the ability to respond, absorb, and adapt to, as well as recover in a disruptive event.*" [63]. To prevent misunderstandings in use, the label 'resilience/reliability' is used.

In case of a cybersecurity threat

During the lifecycle of the asset, but especially during regular operations, threats may be identified. These can come from industry experts, national security sources or other advisories. For this threat state, an organization wants to assess if the basic mitigation strategy is sufficient to mitigate against this threat, in other words "are we vulnerable?".

This threat state of a cybersecurity is identified, because the threat environment is much more dynamic than threats for physical aspects of the SSB (like metal fatigue or temperature extremes). By addressing this threat dynamic in relation to the categories, the engineer gains understanding in how to deal with that dynamic. The engineer understands that new threats can regularly emerge, and these threats must be evaluated. This threat state therefore helps the engineer to understand the much higher pace of the cybersecurity threat landscape than s/he is used to, and how to address this challenge within the engineering processes.

In case of an incident

This threat state describes the relevance of the category when an incident has occurred (the threat has manifested itself). Vulnerability(ies) have been exploited, and operations may be affected. The goal is to assess the impact, minimize escalation of the incident and restore operations to normal.

This threat state gives insight into why preparations benefit the quick and effective response in case of incidents. By understanding this (instead of just performing an assigned task), the engineer can better address this category and work together with cybersecurity advisors on how to act.

This threat state in which a cyber incident has occurred is chosen because of the growing support for the 'Assume breach' principle by both large organizations [64], the hacking community [65] and governments [66]. This principle states that an organization must assume that it will be breached by a cyberattack, resulting in an incident. Therefore, this threat level is included to indicate to engineers what the relevance of the category is in case of an incident. This aspect is closely related to the aspect of resilience, with this aspect focusing on recovery to the resilient/reliable state.

3.1.6 Presenting an ontology for cybersecurity in SSBs

This paragraph presents the results of the approach described in the previous paragraphs. The NIST CSF model used as a basis is available in Microsoft Excel format. This format facilitated the easy addition of the two columns described in 3.1.5.1 and 3.1.5.2. The two additional columns are added between the 'Category' and 'Subcategory' columns, thus becoming columns C and D. These two extra columns relate the categories to a specific domain, Systems Engineering, with a translation with examples to the SSB domain. By extending the CSF taxonomy with domain specific relations, an ontology for the SE is created. By including a specific translation to SSBs, the ontology has been further customized for use in I-STORM. All 23 categories in the CSF have been addressed using these two added columns.

This two-step approach enables the target audience of engineers to first relate the categories to SE. The examples in the cybersecurity relevance to SSB column help to take that general SE process recognition and apply it to cybersecurity situations for the SSB. This firstly supports the use of the ontology as a common frame of reference for discussions between cybersecurity professionals and engineering SSB personnel. Secondly, it supports the identification of shared challenges between the United Kingdom and Netherlands which is the start of possible information sharing.

This approach leads to the ontology presented in 9.4, an excerpt of which is shown below in Table 1. The ontology is comprised of the following columns (the letters refer to the Excel column identifier):

- *Column A: Function*

  There are five high level functions (Identify, Protect, Detect, Respond, and Recover) that are present in risk management at large. These represent the general goals of cybersecurity risk management.
- *Column B: Category*

  "*The Categories were designed to cover the breadth of cybersecurity objectives for an organization, while not being overly detailed. It covers topics across cyber, physical, and personnel, with a focus on business outcomes.*" [59]
- *Column C: Relevance in Systems Engineering (3.1.5.1)*

  The specific translation of the categories to the domain of Systems Engineering by describing the category in the context of the four phases of the V-model.
- *Column D: Cybersecurity relevance for Storm Surge Barriers (3.1.5.2)*

  Describing the category relevance to cybersecurity in SSBs, based on three 'states of cybersecurity' in which an SSB can exist. The examples give additional insight into the effect of the cybersecurity function (category) on reliable SSB operations.
- *Column E: Subcategory*

  These are "[…] *outcome-driven statements that provide considerations for creating or improving a cybersecurity program.*" [59]. Subcategories can give more specific goals, enabling a growth to a more detailed discussion of topics. This level is not addressed in the first introduction of the ontology to I-STORM but is included to enable growth at a later stage.
- *Column F: Informative References*

  These are the references to common cybersecurity frameworks and enable a translation of cybersecurity goals in the ontology to regulatory compliance. This column is aimed at the cybersecurity professional and links the ontology to cybersecurity processes and procedures.

Table 1, An illustrative excerpt of the first of 23 categories of the cybersecurity ontology for SSBs (taken from Appendix 4; An ontology for cybersecurity in SSB)

Function	Category	Relevance In Systems Engineering	Threat states of Storm Surge Barriers	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational assetives and the organization's risk strategy.	**The decomposition and definition phase**: a proper data structure must be defined to support the creation of a suitable asset management system (AMS). This structure must include all OT & IT components and relevant information like version, type and network address. It must also include the roles and responsibilities of personnel for security aspects (e.g. incident coordinator, implementing firmware updates, etc.). **The implementation phase**: this asset management system must be populated with configuration items (CI) that make up the asset. This system must not only contain the CIs, but the relation between them as well. **Integration & Recomposition phase**: during the testing, verification and validation steps, the asset management systems content must be referenced and validated. Additionally, roles and processes for the maintenance of the asset management system are verified to ensure consistency with the real-world situation. **Operations & Maintenance phase**: during changes, the asset management system is referenced and altered according to real-world changes.	**For resilience/reliability** like monitoring and hardening a SSB, the AMS supports the decision like what and where to monitor or how to protect (harden) computing components. Monitoring and hardening can be implemented safely, because the impact of implementation of e.g. a sensor is known and controlled. Monitoring information is well defined and usable to assess the state of the SSB. Knowing your asset helps to manage risks leading to better resiliency. **In case of a cybersecurity threat**, the asset management systems is referenced to determine the impact on the SSB. For instance with a vulnerability to a type and version of PLC, the AMS provides information if that configuration is present, and if so, what SSB system(s) it supports. This decreases the reaction time to threats and supports effective mitigation planning. The AMS will contain information on who is responsible for mitigating the threat. **In case of an incident**, for instance an IP can quickly be referenced to a specific component and its higher level systems within the SSB. With incidents, determining what system is affected and how to react is greatly improved when it is known what CI compose the SSB. Roles and responsibilities contained in the AMS reduce reaction and decision times. The AMS therefore is a key component in incident analysis.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
				ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
				ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
				ID.AM-4: External information systems are catalogued	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
				ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	· **CIS CSC** 13, 14 · **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
				ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **CIS CSC** 17, 19 · **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

3.2 Selecting an information sharing model for SSBs

In the previous paragraph 3.1, the first sub-question is answered, presenting a list of cybersecurity topics for SSBs. In this paragraph, the second research question is addressed: "What is the best way to share information for the I-STORM community?".

To do this, the shortlist of candidate information sharing models presented at the end of 2.4.2 is assessed for use in I-STORM. This is done by using the methodology identified in 2.6.1 and resulting six factors presented as requirements in 2.6.2. This paragraph therefore first presents a description of the six factors that are the basis for the assessment. Next, the assessment approach is described, addressing the scoring system used and a description of the matrix in which the results are presented. Following the description of the assessment process, the assessment is performed, and the results are presented. The results are presented a matrix showing the models and the extend in which they address the six factors. This leads to the conclusion of this paragraph with the identification of the most suitable model for information sharing within I-STORM, answering the second research question.

3.2.1 Description of the assessment factors

It is important to present a clear understanding of the six most important factors used for selecting the information sharing model presented in 2.6.2. These factors were identified through interviews with an I-STORM board member from Rijkswaterstaat, and a senior advisor from the Environment Agency. Two factors were mentioned by both interviewees, and therefore have a more significant weight in selection of the information sharing model. These factors are used to score the candidate-model to evaluate which has the best fit for I-STORM.

The description of the factors is based on the description given by Gharawi and Dawes [12], and where needed, by referring to their reference to other scientific sources for factors. An example is given to illustrate the factor within the context of I-STORM.

3.2.1.1 Laws and policies

This factor highlights awareness of the organizational laws and policies in place. In transnational sharing of information, parties should be aware of their own legal and policy environment and communicate that to the other party/parties. Laws and policies create the regulatory constraints on sharing information, so having clarity on addressing this factor help to reduce uncertainty on how to share information. The model must therefore include how to address the laws and policy differences between sharing parties.

Example: in the Netherlands we have a law (Freedom of Information act (FOIA) or in Dutch: Wet Openbaarheid Bestuur [67] [41, p32] that requires governments to publish information it uses or produces. Similar laws exist in other countries. If any party shares confidential information with Rijkswaterstaat, we must be able to assure the sharing party on how that information is impacted by the FOIA. If this is not the case, this creates uncertainty thereby raising the threshold for information sharing.

3.2.1.2 Value, sensitivity and confidentiality

This factor revolves around trust between parties that the information shared is treated in the correct manner. The model must address how to explicitly establish the value, sensitivity and confidentiality of the information between sharing partners. This includes elements like how to build trust between persons involved in the sharing process. The value of the information shared and the treatment of said information should be clear and agreed upon by all partners with whom is shared.

Example: the UK and NL want to share information on asset management. The model should support a means to assess the identification and labelling of the information, which leads to a shared and explicit view of both the UK and NL on how to treat that information. It is determined that general information can be shared using the Traffic Light Protocol [68, 69], indicating confidentiality and use. This insight might lead to the conclusion that only general information can be shared, because more in depth information is too sensitive (TLP:RED) and proper treatment cannot be guaranteed at this stage of I-STORM cybersecurity information sharing.

3.2.1.3 Organizational rules

This factor focuses on the internal process for an organization wanting to engage in information sharing. As Gharawi and Dawes [12] describe it: "*[…] organizational level factors are important especially for the creation and maintenance of inter-organizational relationships*.". Both RWS and the EA have internal procedures for interacting with other organizations, especially in international settings. These procedures might include who can decide if/how information can be shared, what parties are to be included and what departments support this. The model should be cognizant of these internal organizational processes.

Example: when sharing cybersecurity information like a best practice on cyber-asset management, an advisor must be aware that s/he asks permission of the Chief Information Security Officer (CISO). The CISO is the owner of the processes and procedures for cybersecurity, and therefore the owner of the best practice information. It is therefore important for the CISO to support information sharing. Consequently, international contacts may be managed by another organizational unit. This unit must be informed as well of the intent to share information. Both the CISO and international relations unit can perform their role more efficiently if the sharing model helps them in providing clarity on the process.

3.2.1.4 Political support

This factor addresses the effect of top management support on information sharing. If there is no support from top-management for sharing information, it's very hard to initiate or continue information sharing. It is therefore important for the model to address the creation and continuance of political support. The model should support the business case for an organization to engage in information sharing.

Example: in the European Parliament, one of the goals on cybersecurity is to improve information sharing [70]. The Dutch Cybersecurity Agenda [71] mentions the international aspect of cybersecurity

and expresses that efforts therefore should be internationally oriented. These broad political goals are an excellent rationale to address in support for the sharing of cybersecurity information between the UK and NL on SSB. The sharing model must incorporate these rationales, so all parties understand the strategic goals that underly the political support for information sharing.

3.2.1.5 Resources

This factor addresses the (mainly financial) resources that "*[…] initiate and sustain the collaboration that underlies sharing knowledge and information.*" [12]. Information sharing needs resources for e.g. travel expenses, meeting space, communication products and promotional materials. Adequate resources for collaboration support the autonomy of participating organizations, by not having to use corporate sponsoring or other financial backer who might steer results away from the core goals.

Example: in I-STORM, core members pay a contribution as the financial resource needed for I-STORM to fund its activities. These resources are used to pay for the website, meeting events and the creation of educational materials for the core members.

3.2.1.6 Lacking for data standards and definitions.

When sharing information, one of the fundamental principles to address is a shared vocabulary. Jargon can not only be knowledge domain specific, but also organizational specific. Even when the same term is used, it might have different meanings between information sharing partners. This factor addresses the fact that a shared understanding of data, topics and definitions is addressed by the sharing model. Standards and definitions relate to both the technical definition (e.g. the technical data definition in electronic exchanges of incident information) and the linguistic definition (e.g. what do we mean by the term 'asset'). The model should address the creation of a shared vocabulary and the definition of a technical structure for automated information exchange.

Example: in sharing information on cybersecurity aspects of asset management, the parties must define what the view as the aspects of cybersecurity for assets, what is meant by an asset (the whole SSB, or parts of it) and how both parties define a data structure for describing an asset. If these aspects are discussed, the sharing of information on this topic is understood in the right context by all parties.

3.2.2 Assessment approach

In this paragraph, the relevant factors for I-STORM presented in 2.6.2 and detailed in the previous paragraph, are used to assess the information sharing models presented in 2.4.2. The main model documentation is referenced to assess how each model addresses the factor. Below the referenced documentation is given for each evaluated model.

- ISAC [39]
- ISAO [33, 34, 35]
- GCCS [41]

For the scoring of each factor, a five-point scale is used. The values assigned are listed below in Table 2. This scoring system gives a good visual queue if a factor is addressed in a good or bad way more clearly than assigning numbers from 1-5.

Table 2, scoring rationale for information sharing model selection

Score	Rationale for scoring the factor
- -	The factor is not addressed in the model, and there is no clear indication on how to incorporate this factor in the model.
-	The factor is not addressed in the model, but the model facilitates the incorporation of this factor in a model-consistent way.
o	The factor is mentioned in the model, but no description is given on how to address this factor in information sharing.
+	The factor is addressed in the model, but in a (general) way that requires further design effort before it is usable in I-STORM.
++	The factor is addressed in the model in a way that makes the model directly usable within I-STORM.

To score the models, the documentation aimed at supporting the creation of an information sharing organization is reviewed. For each factor, the documentation is assessed in addressing the factor. The findings that result in the score per factor are recorded to enable independent review or validation of the scoring. Where relevant, the scoring rationale references chapters or paragraphs in the model documentation.

This approach results in a systematic evaluation of the relevant factors for I-STORM. The scoring system enables insight in the rationale and a clear comparison of the three models for their fit for I-STORM.

3.2.3 Assessment results

In this paragraph, a short overview of each model is given. Next, the approach described in the previous paragraph is presented in a matrix.

3.2.3.1 ISAC model

The initiation of the ISAC principle was initiated on May 22nd, 1998 in the US by presidential decision directive 63 [72]. No real formal model description of what an ISAC has been made, but the idea has been implemented in practice, leading to a general description of the ISAC model. Since 1998, many ISAC's have been implemented worldwide with the same general goals on information sharing. The Dutch ISAC's were initiated in July 2014.

ENISA acknowledged the increasing experience with establishing ISAC's in the EU and has performed a study of the ISAC implementations in the EU. The results [39] are presented in this study are explicitly intended to be a guide for creating an ISAC (paragraph 1.1). Therefore, this study can be considered as a description of the ISAC model.

Additionally, ENISA has a scope that coincides with the scope of this thesis (NL-UK information sharing) and incorporates EU wide lessons learned into a recent advice on the ISAC model. This makes the study by ENISA a good reference to evaluate the ISAC model for use in I-STORM context.

When the model is assessed on the six factors, the results in Table 3 emerge. It is instantly recognizable that the ISAC model mentions most of the factors but does not give any further direction on how to address the factor. An outlier is the treatment of the factor 'Resources', that is well described within the document. Overall the model describes the factors at a high level of abstraction, so the question arises if this document uses the right format and conceptual level to enable creation of an ISAC. It presents a general framework but requires further detailing by experts to create the operational design for an ISAC. This finding was supported by research into how the ISAC 'Keren en beheren' (Surge protection and water management) was created by the Dutch NCSC [73]. This process showed that experts guided the ISAC members in further addressing details for information sharing.

Table 3, scoring results for the ISAC model

ISAC Model				
Layer	**Factor**	**Source [15]**	**Scoring**	**Rationale**
Knowledge and information content	**Lacking for data standards and definitions**	CBIS	o	The need for a common vocabulary is very briefly addressed on p37 and a token reference (reference to the MISP project on Github [74]) is made to data standards for information exchange. The study gives some overview of the types of information that can be shared, but in a general way not aimed at presenting definitions.
	Value, sensitivity and confidentiality	CBIS/KT	o	The study describes NDA, Code of Conduct and other confidentiality measures, with references to the Traffic Light Protocol [66] for labelling information. The treatment of this factor is at a high level, intended for further dissemination as part of the ISAC establishment. No more detailed guidelines are presented.
Organizational context	**Organizational rules, procedures and regulation**	CBIS	-	Participating organizations are presented as singular entities, with no references to internal dynamics. Internal rules, procedures and regulation result in behavior in/towards an ISAC, but these internals are not addressed. Because the results of the internal dynamics are addressed, it is not difficult to include this factor.
	Resources	CBIS	++	Funding and lack of resources are addressed in 6.1 as challenges, which are addressed as a recommendation on p40. This recommendation is very succinct but paragraph 4.2 offers guidance on the aspect of funding. Other resources that might be needed like staffing, location, catering, etc are referenced as part of government subsidies. The factor description is directly applicable within I-STORM.
External Environment	**Laws and policies**	CBIS	o	Paragraph 3.2.1 indicates that the role of public administration is to create *'a legal framework for both the exchange of information and creating ISACs.* ' [p25]. The study mentions EU policies and strategic goals like the NIS directive, but does not explicitly address the role of laws and policies that influence the parties that want to share information. This factor is presented as environment variables in which the ISAC operates, and not as a factor to be addressed between sharing partners.
	Political support	CBIS	o	Incentives for participating organizations are presented, for instance in 1.1, but addressing the organization as one rational entity. The incentives are not given in a way so as to enable the creation of a business case to create support within an organization to participate or create an ISAC.

3.2.3.2 ISAO model

The FAQ page of the ISAO organization states that an ISAO is "*any entity or collaboration created or employed by public- or private-sector organizations, for purposes of* […] *gathering and analyzing critical cyber and related information* […] *communicating or disclosing critical cyber and related information* […] *and voluntarily disseminating critical cyber and related information to its members* […]." [74].

The main difference between and ISAC and an ISAO, is that an ISAO is an independent organization which facilitates information sharing. An ISAC is part of an existing organization, for instance an NCSC. This infers that ISAC's are subject to the legal framework of the parent organization and its focus and scope are determined by the parent organization. In case of an NCSC, this means having certain legal instruments like protecting information against mandatory disclosure acts (like Freedom of Information act (FOIA) or in Dutch: Wet Openbaarheid Bestuur [67] [41, p32]). Additionally, because the ISAC's in the UK and NL are part of the national NCSC's, the ISAC's have a national focus.

For I-STORM, the transnational membership, goals and independent nature of the organization therefore match up with the characteristics of an ISAO.

The ISAO model is described in series [75], from which two series are used for the evaluation:

- ISAO 100 SERIES: ISAO CREATION AND OPERATION
- ISAO 300 SERIES: INFORMATION SHARING

Three documents are used for the evaluation: 300-1 [33], 100-1 [34] and 100-2 [35]. These three documents represent the information needed to describe the ISAO model and steps for implementation.

When scoring the ISAO model based on these documents, the results show strong and weak points. The ISAO model addresses the resources factor very well, something the other models do not. This can be explained by the fact that the ISAO model is meant for forming an independent organization. Still, even for and ISAC (which is part of an existing organization), resources are an important factor. As with the ISAC and GCCS model, the ISAO model references the Traffic Light Protocol, but takes it one step further than the ISAC model. This is the case as well with the factor 'Political support', in which the model provides with guidance on value proposition to gain board level buy-in for participating organizations. Like the ISAC model, the ISAO model treats organizations as singular entities without referencing internal dynamics influencing participation in an ISAO.

These conclusions on the ISAO model, result in the following scoring, presented in Table 4.

Table 4, scoring results for the ISAO model

ISAO Model				
Layer	**Factor**	**Source [15]**	**Scoring**	**Rationale**
Knowledge and information content	**Lacking for data standards and definitions**	CBIS	o	In ISAO-3001-1, paragraph 4.1, it's indicated that standardized data formats and protocols enable interoperability, but only the technical exchange of information using the STIX language solely for exchange threat information is explicitly presented. A shared set of definitions in human information sharing is not addressed further.
	Value, sensitivity and confidentiality	CBIS/KT	+	This factor is addressed in several places, e.g. ISAO-3001-1, on p20 (on marking and sharing), p32 (on vetting and labelling) and as a topic in 10.1.5 (data classification, distribution and labelling). Chapter 10 of ISAO-3001-1 and paragraph 3.2 of ISAO 100-2 are dedicated to broad information security aspects of information sharing. Although the description of this factor is extensive, it is focused on a technical information exchange, so some adaptation is needed for use in I-STORM.
Organizational context	**Organizational rules, procedures and regulation**	CBIS	-	The ISAO 100 and 300 series do not address the internal dynamics of an organization. It treats the organization as a single rational entity that has rules, regulations and procedures, but it does not address the role of these in information sharing. The outcome of this internal dynamic can be integrated into the ISAO model if treated by other means outside the ISAO model.
	Resources	CBIS	++	ISAO-100-1, paragraph 5.5.2 refers to membership fees to provide for financial resources with ISAO 100-2 dedicating paragraph 4.2 to creating a business model including providing resources (ISAO 100-2 paragraphs 4.2.3 and 4.2.4). The ISAO therefore is very explicit in developing a business model for resources.
External Environment	**Laws and policies**	CBIS	o	ISAO-3001-1 chapters 5 and 9 briefly mention legal aspects, but mainly in the context of compliance with privacy laws. The 100-2 mentions legal aspects as a point of attention but offers no operational guidelines beyond 'address this topic'.
	Political support	CBIS	+	ISAO-3001-1 treats the goals in 3.4 in a general setting not related to board-level buy-in. ISAO 100-1 addresses the value proposition to participants in chapter 4, but in a general way. The importance of board-level buy-in is not stated. This is in line with the treatment of the participant organizations as singular entities as stated at the findings for 'Organizational rules, procedures and regulation'.

3.2.3.3 GCCS model

The GCCS model [41] is the result of collecting best practices during the Global Conference on Cyberspace in 2015 in the Netherlands. The GCCS is therefore less structured than a formalized model like ISAC and ISAO. It presents good practices on the different aspects that are important for information sharing on critical infrastructure, without a very strict process or order for implementing them. The absence of an implementation strategy would be an obstacle for implementation in a greenfield implementation. The information sharing context of I-STORM already has an organization in place, so this provides an organizational framework in which to implement the good practices. Therefore, implementing the GCCS model is equally feasible as the ISAC and ISAO models.

The scoring of the GCCS model shows that it addresses certain areas very well. This might be due to the more 'bottom-up' approach of creating a model by starting with best practices instead of a theoretical model. This is an interesting possibility that warrants future research. Like the other three models, little attention is given to the internal organizational dynamics in the factor 'Organizational rules, procedures and regulation', but more so than the other models. The clear strongpoints of the GCCS model are the treatment of 'Value, sensitivity and confidentiality' and 'Laws and policies'. Both are addressed in a way that enables direct implementation within I-STORM, both in coverage of the topic and language used. There is no direct reference to a common language, but it references frameworks that can be incorporated in the model. This 'placeholder' for a shared vocabulary can therefore be used to reference the ontology presented in 3.1.6 when working with the GCCS model.

Table 5, scoring results for the GCCS model

GCCS Model				
Layer	**Factor**	**Source [15]**	**Scoring**	**Rationale**
Knowledge and information content	**Lacking for data standards and definitions**	CBIS	+	Paragraph 2.9 addresses the different standards available for exchange of information, with 2.16.3 and 2.17 referring to information exchange. The focus of the paragraph is on the sharing of indicators of incidents and threats. No mention is made on addressing the need for a common understanding of the problems/challenges. There are several referrals to other bodies of work that enable more in-depth support on available data standards and information types.
	Value, sensitivity and confidentiality	CBIS/KT	++	Paragraph 2.11 addresses this factor explicitly and gives considerations and possible schemes to address this factor, for instance the Traffic Light Protocol [65]. The paragraph gives good insight into what must be addressed, and references two approaches for vetting and providing clearance to discuss sensitive information. The GCCS explicitly addresses building trust in 2.3 to support the right treatment of information.
Organizational context	**Organizational rules, procedures and regulation**	CBIS	o	Paragraph 2.8 and 2.13.4 touch lightly on the subject of internal organizational dynamics, but from a narrower perspective of information sharing within an organization. No further attention to internal rules, regulations and procedures is given.
	Resources	CBIS	-	There is an oblique mention of resources in 2.15 (bullet 4) and 2.5, but this factor is not addressed in the GCCS model. There is no real strict structure to implementing the GCCS model, so it will not be a problem to address this factor as an addon.
External Environment	**Laws and policies**	CBIS	++	In 2.13.6 en 2.14, the legal perspectives are specifically addressed. A strong point is the treatment in 2.4 of the (negative) effects of legally mandating sharing. The GCCS addresses this factor in a way that gives a good foundation for I-STORM to implement actions on this factor for the sharing of information.
	Political support	CBIS	+	This factor is addressed in 2.2 and includes links to recommendations by international organizations on the need for information sharing. References support the argument of information sharing should be a board level point of attention. It does not give direction on how to address this, only that this needs to be addressed.

3.2.4 An information sharing model for SSBs

Using the factors presented by Gharawi and Dawes [12] as a viewpoint to assess the fit of the three selected models for use in I-STORM, results in the scoring summarized in Table 6.

Table 6, summary of the information model assessments

Summary of models assessed					
Layer	**Factor**	**Source**	**ISAC**	**ISAO**	**GCCS**
Knowledge and information content	Lacking for data standards and definitions	CBIS	o	o	+
	Value, sensitivity and confidentiality	CBIS/KT	o	+	++
Organizational context	Organizational rules, procedures and regulation	CBIS	-	-	o
	Resources	CBIS	++	++	-
External Environment	Laws and policies	CBIS	o	o	++
	Political support	CBIS	o	+	+

The assessment shows that the GCCS model is the best fit for use in I-STORM, based on the criteria identified in interviews. In those interviews (2.6.2), two factors were indicated as important by both interviewees; 'Value, sensitivity and confidentiality' and 'Laws and policies'. Both these factors are clear strong points of the GCCS model compared to the other two. It is advisable to reference the ISAO or

ISAC model for the factor of 'Resources' when implementing the model in I-STORM. This inclusion of the ISAO/ISAC model treatment of that factor strengthens the GCCS model implementation.

In conclusion, it can be observed that all models treat organizations as singular entities with little attention to internal politics. Organizations are in general referred to as single rational entities that 'have an incentive for information sharing'. A study by Kim and Lee [76] referenced by Gharawi and Dawes for this factor, presents the role management plays in facilitating information sharing: "*In addition, managers may emphasize a participatory management approach as a means of promoting flexibility and encouraging sharing and collaboration within and across organizational boundaries and stakeholders.*". Therefore, in addressing the implementation of the model in I-STORM (chapter 4), this hiatus in the GCCS model must be a point of attention.

3.3 Discussion of selected topics and framework

This chapter has given answers to the two sub research questions presented in 1.2. Sub question 1, "*What are relevant topics on cybersecurity for SSBs?*", has been answered by the ontology presented in 3.1.6. The answer to sub question 2, "*What information sharing model supports the needs of I-STORM for information sharing?*", has been answered in 3.2.4 by the selection of the GCCS model. These answers are presented as the result of a transparent and scientific approach.

But these separate answers are not fit as an answer to the main research question, because the main research question requires the combination of the two. Therefore, for the use in I-STORM, the implementation of the ontology and model are presented as an information sharing process. This implementation combines the two artifacts of the sub questions into an information sharing process for use in I-STORM. The next chapter combines the ontology and model presented in this chapter and presents them as an information sharing model for use in I-STORM.

4 A Cybersecurity information sharing process for SSBs

Chapter 3 presented an ontology that provides the engineer with a common language to address the diverse topics that comprise cybersecurity for SSBs. The chapter also selected a suitable model to support the information sharing in I-STORM. These two artifacts enable researcher to describe how the cybersecurity knowledge domain can be implemented. This chapter describes the cybersecurity information sharing process that implements the new knowledge domain.

The description of the information sharing process is presented by describing how the artifacts of chapter 3 support the sharing of information conformant the knowledge strategy of I-STORM. To illustrate this, the I-STORM flow of knowledge presented in 2.5, Figure 3, is appended with the information sharing process and its components resulting in Figure 7.

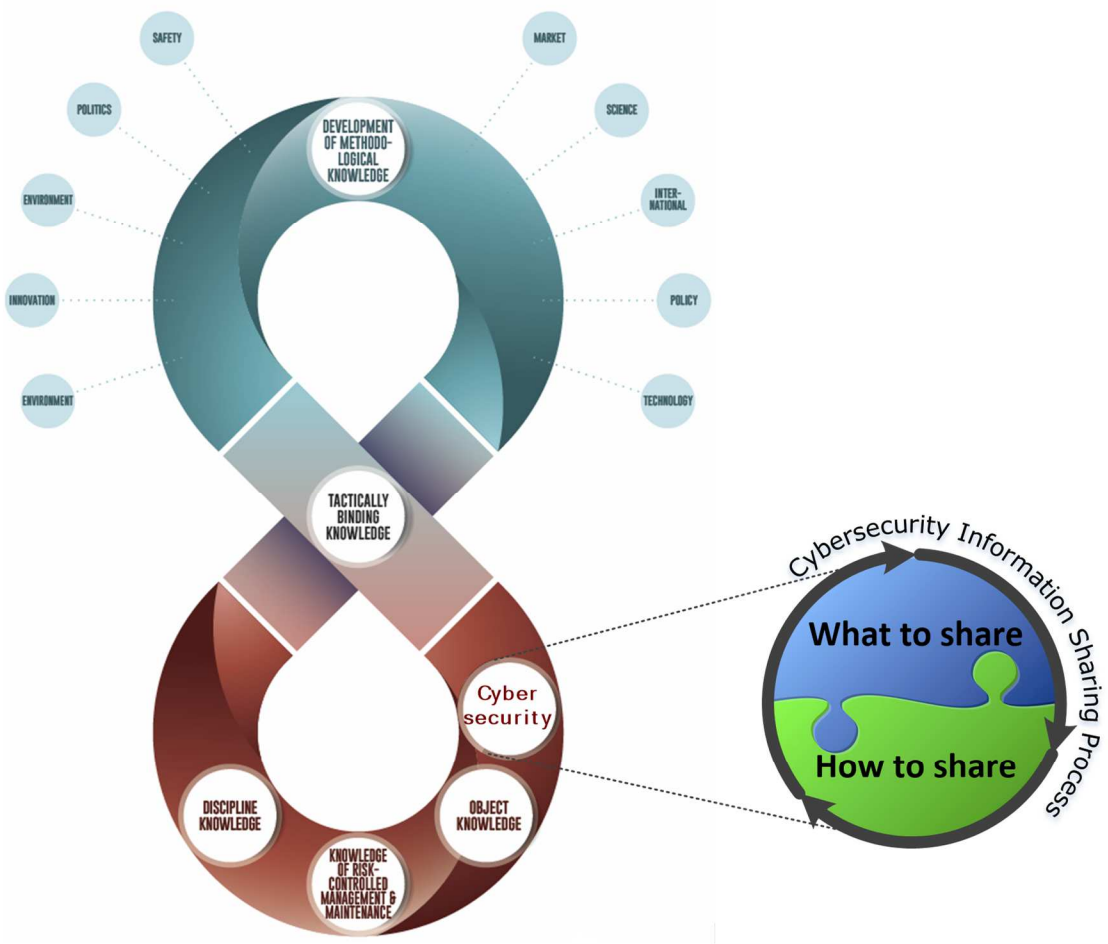

Figure 7, the new knowledge domain, process and process components

To present this information sharing process, first, the knowledge strategy of I-STORM is explored in 4.1 to give insight into the structure that the information sharing process must follow. Next, the description of how to support that knowledge strategy with the artifacts in chapter 3 is presented in paragraph 4.2 as the information sharing process.

Due to the novelty of the topic to I-STORM, it is important to support taking the first step in sharing cybersecurity information thus starting the new knowledge domain. Therefore, paragraph 4.3 provides short-, medium- and long-term recommendations for implementing the information sharing process. This provides an initial roadmap for the new knowledge domain. This chapter concludes with an overview of the presented process and a look-ahead to the need for validation.

4.1 Knowledge management within I-STORM

Knowledge management within I-STORM is not yet very formalized. Knowledge domains (e.g. SSB operations or knowledge of the asset) are identified and shared (e.g. peer reviews or presentations at meetings), but an overarching strategy or management has not yet been formalized. In April 2018, RWS formalized its own knowledge strategy on SSBs. The goal of this strategy is: "[…] *to assist in structurally embedding critical knowledge on management, maintenance and operations of Storm Surge Barriers in the organization.*" [77] (translated from Dutch). This approach was well-received within I-STORM, and the strategy is being translated to benefit both I-STORM as well as individual members. Due to these characteristics, this approach is chosen as 'backbone' for the process.

The approach of RWS consists of three connected, but individually usable parts [77]:

A. Knowledge strategy (strategic level)
- Provides context and urgency for the need of the strategy using the unique nature and role of SSBs as viewpoint.

B. Analysis framework (tactical level)
- Provides a methodology to assess what knowledge is critical, where knowledge should be secured (internally, market partners, etc) and how to secure that knowledge. This framework expands on goals in A and provides a basis for C.

C. Application of analysis framework on knowledge domains (operational level)
- Identifies what knowledge should be secured and structures that knowledge in knowledge domains [44]. Additionally, supportive strategies like creating documentation and training are identified.

This methodical and layered approach offers an approach that is familiar in I-STORM in which the products of this thesis can be integrated. Additionally, by using a familiar and agreed upon approach, stakeholder support from RWS is more likely. Therefore, this RWS approach is used as a template on how to introduce the information sharing process in I-STORM.

4.2 The information sharing process for I-STORM

This paragraph describes how the three parts above are addressed, using the ontology and information sharing model presented in chapter 3. The implementation of the thesis artifacts in the context of I-STORM knowledge management describes the cybersecurity information sharing process for I-STORM.

This paragraph presents the broad outline of the information sharing process and is not an implementation guide. The goal is to give insight into how the information sharing process can be introduced and what high level actions are suggested. Therefore, this paragraph presents the high-level

information sharing on cybersecurity. The information sharing process presented in this paragraph provides broad guidance per part of the knowledge strategy of I-STORM on how to use the artifacts of chapter 3.

4.2.1 Part A; the Knowledge Strategy

The three-part approach (parts A, B and C) described in paragraph 4.1 starts with defining a sense of urgency of the impact of cybersecurity as a risk factor on SSB operations (part A). This risk and the sense of urgency need to be formalized in a statement in which core members state their desire to address cybersecurity within I-STORM. This statement represents the mandate to address cybersecurity as a new knowledge domain.

To help with defining the need and strategic goals of the knowledge strategy, chapter 2 of this thesis gives input to define the need for addressing SSB cybersecurity. Additionally, the GCCS framework [41] provides some supporting arguments in 1.1 and 1.2. In this strategy, the ontology is referenced as a shared vocabulary and the GCCS framework is referenced as a source of advice for addressing topics in the analysis framework (part B).

4.2.2 Part B; the Analysis Framework

The knowledge strategy SSBs of RWS [79] presents the following three aspects for part B. For I-STORM, the categories in the ontology are evaluated on these aspects. The ontology provides a shared vocabulary that enables I-STORM members to agree on the topic, before discussing the aspects given below.

1. What knowledge (category) is essential for SSBs?
2. Where should the knowledge be present/embedded? E.g. within the SSB organization, commercial partners, other partners in a network.
3. How can points 1 and 2 be implemented in practice?

Addressing the ontology in these three aspects provides input for part C, the operationalization of the information sharing process.

The three aspects above prioritize the categories in relation to SSB operations, identify what roles play a part in addressing the category and if any good practices can be shared. In this analysis framework, the critical factors identified in 2.6.2 should be addressed in general and for each ontology category. The GCCS model is referenced for more details about the factor, and to identify best practices in addressing the factor. The application of the analysis framework of part B in combination with the ontology and information sharing model identify high priority categories that should be addressed first. Additionally, 'low hanging fruit' categories' may be identified that can be addressed early on. This insight is the input for part C.

4.2.3 Part C; Application of analysis framework on knowledge domains

In this part, the knowledge strategy of part A operationalized into practical actions using the analysis framework of part B to give guidance on aspects like priority and roles. Categories in the ontology that are very similar or related in practice (as one interviewee remarked in the evaluation interviews), can be combined. Categories that are identified as complex, may be split into more manageable parts.

Categories that are low hanging fruit, can be addressed first for short term results. RWS can act as sponsor of the knowledge domain by supporting development in I-STORM. This can be done through writing documents and referencing the knowledge domain as structure for sharing. For example, RWS can select a category and create an information sharing product like a masterclass of booklet on this topic in which RWS shares its good practice and experience.

The GCCS model helps to address points of attention (e.g. the factors in 2.6.2), like confidentiality, management support and resources. An example of addressing the need for resources is by researching funding from the EU to promote information sharing on cybersecurity to improve the resilience of critical infrastructure. On confidentiality for example, the adoption of the Traffic Light Protocol and instructions on its use can be a good first step (GCCS [41], 2.11 and 2.16).

This part yields the operational products and procedures to facilitate the exchange of cybersecurity information on SSBs. It therefore is the operational part of the information sharing process.

4.3 Taking the first step in sharing information

The information sharing process described in the previous paragraph is a high-level guidance on how to implement the new knowledge domain within I-STORM. The three parts are related to the strategic, tactical and operational levels of knowledge management. To help start the new knowledge domain using the cybersecurity information sharing process, recommendations are provided in this paragraph.

The first steps described here are aimed at three horizons; short-term (<12 months), mid-term (12-24 months) and long-term (2 year+) results. These horizons are accounts for the fact that contact between I-STORM partners is not very frequent, which has impact on the planning. The three-horizon approach ensures that I-STORM can see results on the short term, strengthening confidence in the overall goal, but also formulate a long-term vision to match organizational strategic goals.

These steps can be discussed within I-STORM as a basis for a plan to implement the information sharing process.

4.3.1 Short-term recommendations

There are some parallel actions that can be taken for 2019, these are summed up below. They are not ordered in any way, and

- In the next year, RWS can use the ontology to select a good practice on cybersecurity on which to share knowledge on with the UK within I-STORM.
- The ontology can be transformed into another more practically accessible form like a booklet, accompanied by an explanation on the context of Systems Engineering and the V-model. This has been suggested during interviews as one of the good first steps.
- Present the results of the thesis to the I-STORM core members, of which NL and the UK are members.
- Start the process of exploring EU funding for construction of the new knowledge domain.

- Include the cybersecurity knowledge domain in the RWS knowledge management strategy for SSBs.

4.3.2 Mid-term recommendations

Although the actions for mid-term recommendations can be started in 2019, results are expected on the 12-24-month horizon.

- Expand the information sharing from just the UK-NL to other core members of I-STORM.
- Embed the development of the cybersecurity knowledge domain in the planning of I-STORM.
- Build trust between core I-STORM members and organizational support for the cybersecurity knowledge domain in order to have formal backing to address this topic.
- Reach consensus on which categories take priority to share good practices on.
- Formulate a 'code of conduct' for participation in the cybersecurity knowledge domain.

4.3.3 Long-term recommendations

The long-term recommendations rely on a strategic vision on how cybersecurity is addressed by I-STORM. This is not just a goal for I-STORM itself, but also for the participating organizations. They must have a clear vision of how I-STORM support organizational goals on the domain of cybersecurity. This vision depends on the short- and mid-term recommendations. If these recommendations are successful, support for strategic goals is more likely. Therefore, for the only long-term recommendation is to include cybersecurity as a knowledge domain and treat it like the other domains as a vital part of SSB operations.

4.4 Conclusion

In this chapter researcher presents the process for sharing cybersecurity information thus supporting the implementation of the new knowledge domain in I-STORM. Since sharing cybersecurity within I-STORM is new and still has many challenges to overcome, no strict implementation guidance has been presented, but a series of recommendations. These should first be discussed in I-STORM between the UK and NL to determine the way forward.

Researcher has presented that the created ontology and selected GCCS model are a good fit in presenting the process to implement a new knowledge domain within the I-STORM knowledge strategy.

One of the pitfalls mentioned in chapter 1 is that most cybersecurity advise for OT originates from the IT domain and does not consider the different approach of the OT domain. The background of the researcher is predominantly in the IT domain, so this pitfall is relevant for this thesis. Even though the design science approach of this thesis is a scientific approach, effects like assumptions and bias play a role. Therefore, in the next chapter, the artifacts (ontology, sharing model and process) presented in chapters 3 and 0 are validated, in line with design science methodology. This validation not only evaluates if the solutions fit the requirements but also validates their quality with the intended target audience.

5 Validation of the information sharing process for SSBs

This thesis has presented a new artifact (the ontology) and has identified an existing artifact (information sharing model) that fits the requirements of I-STORM. These artifacts are combined in the previous chapter and presented as the information sharing process for SSBs. In this chapter, the designed process is validated to ensure the artifacts fit the requirements. The validation gives insight into the ability of the presented process to answer the main research question of this thesis.

How can the I-STORM community share cybersecurity information on Storm Surge Barriers?

The validation has three components;

- Validation of the ontology;
- Validation of the information sharing model;
- Validation of the process design.

The validation of the ontology gives insight if the first sub research question is answered. The validation of the model validates the answer to the second sub question. Finally, the validation of the process validates the main research question.

To perform the validation, first the validation approach is presented. This paragraph gives insight into the approach taken for validation. Next, this approach is applied to validate the artifacts presented as a solution for the sub-questions (the ontology and information sharing model) that comprise the information sharing process. Finally, the main research question is validated.

After the validation of the information sharing process, the limitations of the validation process are discussed, presenting findings that can be a basis for further research. The results of this validation chapter are the basis for the conclusion presented in chapter 0.

5.1 Validation approach

This thesis employs the design science methodology as described by Hevner [78] [79] in researching the need for a solution (artifact) by stakeholders (chapter 0), constructing the artifact (chapter 3) and presenting the artifact (chapter 4). Edgar and Manz [80] have presented a checklist for the core of the design science, which includes the validation of an artifact. This checklist therefore is suited as validation methodology for the artifacts of this thesis.

In the Netherlands, Wieringa has done a lot of work on implementing design science, including the validation phase. Therefore, his work is referenced to give further insight in the core goals of artifact validation. This results in the validation activities presented by Edgar and Manz [80, Appendix A] as quoted below with a clarification as stated by Wieringa [81, slide 26] as sub-bullet (-).

1. *(Artifact x context) produce effects? Why? (Mechanisms)*
   - Does it work?
2. *Effects satisfy requirements?*
   - Does it work as desired?

3. *(Alternative artifact x context) produce effects? Why? (Mechanisms)*
    - Trade-offs for different artifacts?
4. *(Artifact x alternative context) produce effects? Why? (Mechanisms)*
    - Sensitivity for different Contexts?

These validation activities are the underlying methodology of the validation performed and are referenced in the following paragraphs. The validation activities reference concepts, so for clarity, the concepts used are explained in relation to this thesis. This improves the understanding of the validation description in relation to the applied methodology.

The **artifact** is the information sharing process for cybersecurity information within the I-STORM context. This artifact can be divided into two sub-artifacts:

- The created cybersecurity ontology for SSBs
- The selected information sharing model for I-STORM

The **context** is the scope as defined in 1.3, cybersecurity information sharing on SSB within I-STORM between the UK and NL.

The **effect** of the ontology of the information sharing process is to give insight to what cybersecurity topics are relevant for the context, and to enable engineers to identify shared challenges and best practices. The effect of the information sharing model is to describe *how* information can be shared in the context.

The **alternative artifact** for the ontology has been researched in 3.1. No cybersecurity ontology for SE or SSBs has been identified, but the unaltered CSF taxonomy for critical infrastructure can be considered the alternative artifact. For the sharing process, an existing information sharing model has been identified that supports the stated need, so no new artifact is created. The alternative artifact evaluated is the current information sharing model in I-STORM. This process has proven insufficient for the requirements, hence the need for the new artifact.

The **alternative context** is assessed in two ways:

1. The use of the ontology outside the I-STORM SSB domain
    - Example: other critical infrastructure domains
2. The use of the ontology outside the scope of UK-NL information sharing
    - Example: other I-STORM members

Both are addressed as part of the generalization assessment in paragraph 6.3.

5.2 Validation of the ontology

This paragraph gives insight into the validation of the ontology by using three steps. First, the validation interview methodology is presented, followed by the results. Concluding the validation of the ontology, the use case presented in 2.2 is revisited and the effect of the ontology on the use case is discussed.

5.2.1 Validation interview

The main goal of the interview is to validate if the ontology meets the requirements presented in 2.7:

1. The process must be compatible with Systems Engineering;
2. The process must provide a list of topics on which to share information in a way understandable by engineers.

These requirements are related to the first two validation activities as presented in the paragraph above. In the interview, the contrast between the unaltered CSF and the ontology was important to identify. This contrast gives insight into the added value of the ontology. The contrast is evaluated by validation activity 3 by giving insight into alternative solutions. Therefore, it is important to gain insight into if the unaltered NIST CSF could be used in I-STORM. The combination of the three validation activities and artifact requirements are translated into two main goals for the interview:

1. Does the NIST CSF without alterations fulfill the requirements?
2. Does the ontology fulfill the requirements (better)?

5.2.1.1 Interview structure and questions

To gain insight into the interview goals presented above, eight interview questions have been composed, asked in two parts. The first part explores the fit of the CSF for as solution and the second part evaluates if the ontology fits the requirements. In order to minimize influencing the interviewee, first the CSF function and category have been given as reference when answering questions 1, 2 and 3. The 'Subcategory' and 'Informative reference' columns are not part of the taxonomy aspect of the CSF and are aimed at non-engineering roles. Therefore, these columns were not presented to the interviewees. Especially the 'Informative reference' column is aimed at the cybersecurity compliance role and therefore not relevant for engineers.

After evaluating the CSF, the interviewee is directed to assess the ontology and proceed to questions 4-8. The CSF and ontology were attached as an Excel file, with each on a separate tab. The full questionnaire used is included as Appendix 3; Validation questionnaire. The Excel file is not included in this appendix, because the contents are already presented as the ontology in Appendix 4; An ontology for cybersecurity in SSB.

The interview was performed face-to-face, with the researcher taking only brief notes and recording the interview. Later, the recordings were used to record the answers to the questions. Direct quotes are indicated in italic and between quotes. Any additional remarks by the researcher needed to clarify context are indicated between brackets. The questions and answers then were sent to the interviewee, with the question if it represented the position of the interviewee correctly. Only after a positive reply were the answers used in this thesis.

Due to confidentiality requirements of the interviewees, the complete answers are included in a confidential appendix, available to the assessors only. The audio recordings are available to the assessors on request. These are deleted after grading is completed, as per request of the interviewees.

5.2.1.2 The interviewees

The interview was performed with four interviewees:

1. An Asset Performance and Engineering MEICA manager, Environment Agency
    - Knows of I-STORM but is not an active member. Electrical engineering background and OT cybersecurity lead at the tactical level.
2. Lead Advisor Storm Surge Barriers, Rijkswaterstaat

   - Co-Founder of I-STORM and board member. Lead advisor on SSBs within RWS, engineering background with some cybersecurity knowledge. Strategic/tactical level.
3. A Head of Operations of a Storm Surge Barrier, Rijkswaterstaat
   - I-STORM member, engineering and IT systems background, knowledgeable on cybersecurity. Engaged with tactical and operational cybersecurity topics on some SSBs.
4. Implementation lead cybersecurity of four SSBs, Rijkswaterstaat
   - I-STORM member, electrical/telematics engineering background. Responsible for the operational aspects of cybersecurity of the SSBs in the south-west of the Netherlands. Knowledgeable in cybersecurity, has experience with the peer-review aspect as part of I-STORM.

The interviewees 1 and 2 were interviewed at an earlier moment as well to gain insight into the need and requirements of the thesis results. These interviews did not include or hinted at specific models or actions to be taken to create an ontology. Therefore, there is no circular reasoning in a second interview concerning this part of the validation. To validate this, the independent third and fourth interviewees are also used to validate that no circular reasoning is present.

5.2.2 Interview results

In this sub paragraph, the results of the interviews are presented. The answer is presented per interview goal (5.2.1). Where relevant, direct quotes are presented per interviewee (see: 5.2.1.2). In closing, the conclusions of the ontology validation are presented.

5.2.2.1 Interview goal 1; Does the NIST CSF without alterations fulfill the requirements?

The answers given to questions 1-3 are to provide insight into the understanding of the unaltered CSF. This not only identifies if the CSF could meet the requirements for use in I-STORM, but it also underlies the understanding of the framework itself. If the terms used or logic behind the taxonomy of the CSF is unclear, the ontology based on that unclear basis could lead to further problems in the implementation in I-STORM.

A description of the columns was given as part of the interview (see 9.3) and the interviewees were asked if they understand the descriptions of the columns. In this section, the contents of the columns was addressed as well. This section therefore gives insight into the goal of the columns as well as the content of it in relation to understanding cybersecurity by an engineer. The responses given are presented in the list below:

- All four interviewees indicate that they understand the principles of 'Function' and 'Category' used in the CSF based on the given description.
- Interviewee 2 indicated some terms were not well understood because not all I-STORM members are native English speakers.
- All four indicated that their work in cybersecurity is a factor in them understanding the columns. This is illustrated by interviewee 1: "*We know cyber*" and interviewee 3: "*It's nice to see the whole spectrum of cybersecurity presented in this way.*".

- Interviewee 2 gave the caveat, that it is important to be clear on the conceptual level on which you discuss the categories. A discussion on the operational level will differ from the tactical or strategic level.
- Interviewee 2 indicated that for the less cyber-aware engineer in I-STORM, a more accessible version with simpler wording or translation to a native language should be considered.
- Three interviewees (1, 2 and 3) indicated that functions are sometimes closely related and the purpose of splitting up of functions is not always clear.
- When reading the columns, examples in their work came to mind with all interviewees.
- Interviewee 1 indicated that the categories needed "*more meat on the bones*" to be well understood, e.g. to gain insight into roles and responsibilities on cyber. The understanding is not only needed for operational engineers, but for the operations management as well. This is echoed by interviewee 4 who remarked: "*In principle they do, but more simple language with examples would help understanding.*".

Next, the interviewees were asked if the understand how 'Function' and 'Category' columns relate to their daily engineering work on an SSB. This was to assess whether the terms used are relatable to (their) daily engineering work. The responses given are presented in the list below:

- Interviewee 2 indicated that the list would not really work for engineers in general on an SSB, because the functions lack detail. This detail is needed especially for less cybersecurity knowledgeable engineers to understand the link to daily operations. This view is shared by interviewee 1 and 4. Interviewee 1 indicated that it needs additions (meat on the bones) to resonate with operations and the management levels above. Interviewee 4 suggested to use less obvious examples and not focus on easy ones, because that's not where the real challenges lie.
- Interviewees 1, 2 and 3 indicate that cyber security training on the IT side, spills over in awareness for the topic on the OT side.
- Interviewee 3 explained the three kinds of engineers on the SSB. All three know cyber is important and grasp the basics. The electrical engineer (the common background for asset managers) is closely involved with OT, so has to have a deeper understanding because the actually work with OT components like PLC's. "*They can use this, and we already do some of these things like Protect and Detect.*"

5.2.2.2 Interview goal 2; Does the ontology fulfill the requirements (better)?

To gain insight into the effectiveness of the ontology and the possible improvement over the taxonomy of the standard CSF, questions 4-8 have been posed (see 9.3). As with interview goal 1, first the description and wording used in the added columns is evaluated. The responses given are presented in the list below:

- Interviewee 1 remarked: "*You've broken it down into the lifecycle, the specification, design, construct and the operate/maintain, and I think that's the right way. Because good systems engineering is the same.*".
- Interviewee 3 remarked: "*The descriptions are clear, and this is applicable for the supply chain to get across why awareness/actions have to be taken* [in light of cybersecurity].".

- Interviewees 1 and 2 indicated that although the V-model logic is used in practice, the model itself is not (well) known. Interviewee 4, coming from the more operational side, indicated that SE and the V-model are known at the operational level in his experience.
- Interviewee 2 emphasized multiple times that the assumed knowledge of the engineer about SE and the V-model in particular is too high. The engineers can certainly understand the V-model when explained, but it's not referenced as such in daily practice. The use of the V-model is more a theoretical approach, than the daily language. Therefore, he indicated that it is vital to first explain the context of the V-model and how it pertains to the ontology, before discussing the ontology itself. This aspect is mentioned too by interviewee 3, but with less emphasis. Interviewee 4 had a contrary view of this.
- Both interviewees 1 and 2 indicated that in the V-model, the operations/maintenance phase is just a small part of the V-model, but an asset resides most of its lifecycle in that phase. The attention this phase gets in the ontology column 'Relevance in Systems Engineering', does not reflect the emphasis on this phase in daily practice of the asset lifecycle.
- The examples in column D, 'Threat states of Storm Surge Barriers', are focused on the operations/maintenance phase. Interviewee 2 indicated this is a good focus, because this helps the engineer with examples to relate the category to daily practice. He suggests to visually link the operations/maintenance phase in column C with the examples in column D is in line with the I-STORM goal of "*sharing maintenance and operational good practices*".
- Interviewee 2 indicated that two approaches can be seen: the theoretical (intellectual) approach using the model 'as is' to discuss conceptual topics, and the practical approach in what is recognizable to the engineer in daily work. The second might result in a simpler list than this with joined topics that an engineer experience as the same.
- All interviewees indicate they understand the explanation of the added columns and do not see too much jargon that would hinder understanding by an engineer.
- All interviewees indicate that the description and contents of the added columns are understandable by engineers. Interviewee 4 remarked that this is what he missed in the standard CSF model: "*Yes. This is what I meant just now* [in the CSF needing more examples and description]."
- Interviewee 2 indicated column C could be more compact, "*has a bit too much words, needs to be more concise, and column D could use more examples*". But also acknowledges: "*You then have to stop and present it as it is. Then you can start a dialog on how to further develop/use this list.*".

Next, the effect of the added columns is evaluated on the understanding of cybersecurity by an engineer on the daily work on an SSB.

- All interviewees indicate that the added columns, and therefore the ontology, helps them to understand the topic of cybersecurity better. Interviewee 1: "*Yes, yeah, absolutely. Use of language means that more people will understand it. Good use of language, simple terms, means the non-technical guys will be able to assist the technical guys.*". Interviewee 3: "*Yes. As I indicated before, column D contains practical tips to help reflect on if we have done this, yes or no. That [reflection] leads to good topics to talk about.*". Interviewee 2 reiterated his position that understanding is achieved only if the context of SE and the V-model is first explained.

- Interviewee 3 indicated: "*The attractiveness of this model* [ontology] *is that by adding column C* [indicated D], *this is the daily practice. This* [column] *engages the people* [on the subject]. *This is an added value of column C* [indicates D]."
- Interviewee 1 indicated that using this model helps create the exchange of challenges and good practices; "*That is what I-STORM is all about, identifying good or bad practice.*". "*We need to learn from you, and you need to learn from us. Different situations that we both face.*".
- Interviewee 4 indicated that the ontology is useful outside I-STORM as well [within RWS]; "*This* [ontology] *would also help the person that has to bring the message* [of cybersecurity] *to project members* [who are less knowledgeable].".
- Interviewee 3 reflected on trying to introduce cybersecurity in an October 2018 I-STORM meeting: "[…] *with this* [ontology] *under my arm, would help during workshops to identify certain topics to discuss. You would do this on a certain abstract level. You have to properly prepare, but I'm convinced that if I were to go to I-STORM with or without this* [ontology], *I would feel more comfortable with it.*".
- Interviewee 1 indicated that the ontology would help to align terms and principles between both parties when using it in I-STORM.
- Interviewee 4 indicated that "t*here still are some gray areas,* [e.g.] *when is something cyber and when is it technical? For example, a hard disk that crashes. Is that maintenance or a cyber incident?*". This ontology could help to discuss these issues.
- Interviewee 3 indicated that the ontology would help to discuss cybersecurity topics on a higher conceptual level, removing sensitive information as basis for discussion. "*The benefits of this menu [the ontology], helps to discuss topics without having to discuss operational information.*". The phases [column D] enable the discussion of concepts or situations without "*lifting the curtain too much*".
- Interviewee 4 remarked that in some countries, the level of digitization of SSBs is low(er), so this ontology might not be of any relevance (yet). "*This* [ontology] *would help others in the future* [when SSBs are more digitized], *and in the Netherlands to improve current systems and support future developments.*".

5.2.3 Conclusions on the ontology validation

The interviews confirmed that the ontology is understandable by engineers and helps them in understanding cybersecurity in the engineering and SSB context. The input of interviewee 3 and 4 was important to validate that the responses from interviewees 1 and 2 were not based on their input on the requirements, but on genuine operational merit of the ontology. Interviewee 1 was from the UK and the other interviewees from the NL. The results did not identify a significant different position between the interviewee countries. This validates that no significant 'Dutch bias' is present in the validation.

The fact that all interviewees agree on the improvement of the ontology over the taxonomy indicates the ontology fulfills the first sub research question of this thesis "What are relevant topics on cybersecurity for SSBs?".

The use of the CSF as a peer-reviewed framework ensured that the taxonomy on which the ontology is based, is a complete representation of the cybersecurity domain. This was validated by the fact that no interviewee indicated that topics were not addressed.

The main improvement mentioned on the ontology, is that it relied too heavily on assumption that all engineers understand the V-model. This context is not as well-known as assumed, and therefore requires attention when using the ontology in I-STORM. The fact that the interviewee with an operational focus gave indications that the understanding of the V-model is present, indicates that this challenge might be focused at the strategic/tactical level. This would need more research to give a clear recommendation. It is a safe approach for I-STORM to give attention to the context of the ontology, before introducing the ontology itself.

An unexpected aspect that was presented by the interviews, was that the model helps to share information by enabling a discussion on a more hypothetical level. The better understanding of the topic and the examples given in the column 'Threat states of Storm Surge Barriers' remove the need for actual examples to be used. This means that sensitive information is not needed for the identification of shared challenges and good practices. The ontology supports conceptualization of real-world situations for sharing in I-STORM.

The remarks made on the ontology are considered for further research and implementation in practice. The ontology as presented to the interviewees is suitable for its goal in I-STORM in giving insight in cybersecurity topics for SSBs.

5.3 Validation of the information sharing model selection

The implementation of cybersecurity information sharing in I-STORM uses the GCCS model to support addressing key factors (2.6.2). The model supports the implementation and daily use of the cybersecurity information sharing within I-STORM. This use of the GCCS model in practice, means that it can only be validated when used in practice. The purpose of the information sharing process is to start the cybersecurity information sharing. Therefore, the GCCS model cannot be evaluated at this time using the approach applied to the ontology. However, the GCCS model can be validated by assessing how it supports the challenges of the use case in 2.2. If the model provides adequate support for the challenges, this validates the selection for its use in I-STORM.

5.3.1 Validation of the GCCS model using the challenges in the use case

For the validation of the GCCS model for use in I-STORM, the use case of paragraph 2.2 will be used. The evaluation looks at how the challenges identified in the use case, are supported by the GCCS model. Per challenge, the GCCS model document "Sharing Cyber Security Information - Good Practice Stemming from the Dutch Public-Private-Participation Approach" [41] is used, the same as for the model selection. In this approach, the other factors that were not used as selection criteria, may be referenced. The GCCS model presents the good practices in the form of 'Building Blocks' in chapter 2, therefore, this chapter is referenced for support. Below, the eight challenges given in the use case are addressed using the approach described.

1. **Do the members understand the effects of not addressing cybersecurity in contracts (e.g. what operational impact this might have)?**

This challenge relates to the overall understanding of cybersecurity in daily operations. When an engineer understands what cybersecurity aspects there are, and how they influence daily operations, the engineer can deduce what functionality is affected if no agreements exist on how to address cybersecurity aspects.

Paragraph 2.1 presents the building block "*Information Sharing: Speculate to Accumulate*". This building block describes how sharing information can help to gain insight into challenges, like the one described in the use case. Using the ontology as a common vocabulary, sharing or discussing this topic between the UK and NL within I-STORM helps to gain insight into how to create awareness on how well-defined cybersecurity goals in contracts can help during the lifecycle of the SSB. The GCCS building block support the members in understanding why sharing information helps to increase clarity and give them an overview on what topics must be addressed before sharing can start.

Creating understanding on the challenges of cybersecurity is not explicitly addressed in the GCCS model. This challenge has been addressed in the short-term steps that I-STORM can take in implementing the information sharing process (see 4.3.1). GCCS paragraph 2.1 can help in creating and presenting the approach to the I-STORM board.

2. **Do I have (formal) permission to share information on how we treat cybersecurity in contracts with other members?**

This challenge is solved within an organization, but the position on participation within I-STORM helps to build an internal business case and mandate for sharing information. Chapter 2.2 addresses how to get buy-in from top management. This paragraph helps I-STORM in providing the aspects to address in helping the UK and NL in getting top-level support. The NL can explain that sharing the good practice of RWS of embedding cybersecurity in contracts, produces feedback of reviewers and thus improves the RWS practice. This makes embedding cybersecurity in contracts even more effective. In the UK, the good practice has the same effect. The formal permission includes guidance on what can and cannot be shared.

The advice in the GCCS helps to create a template business case with arguments on the benefits of sharing information within I-STORM. The assurances that the information is treated in the correct way projects a mature image of information sharing. This helps boost confidence that information is treated the right way, and that rules can be established for sharing, further boosting confidence.

3. **How do I know other members will treat the confidentiality of the information I share in the correct way?**

This challenge has two parts; is the confidentiality of the information shared known and does the other party know how to handle that confidentiality level. The GCCS model provides an answer in 2.11. This paragraph describes how to agree on rules for treatment of shared information and how to label that information. This creates a duo of labelling and formalized treatment per label. This combination gives

assurance that the confidentiality of the information is known and respected. Chapter 2.3 gives advice on trust-building, which plays a significant part for the assurance level that both parties perceive. The GCCS model support the formation of a formal agreement containing the rules on cybersecurity information sharing.

For the use case, this means that shared information is labelled and sharing partners have agreed on how to treat that information. The owner of the good practice on contracts labels the information (e.g. TLP-GREEN). This means the I-STORM RWS member knows s/he can share the information with the UK Environment Agency member. The EA member knows that s/he can use the information within the EA, but not share it outside the EA.

4. Are other members allowed to discuss cybersecurity topics?

This challenge is a generalization of the one described in challenge 2. The GCCS supports securing buy-in at management levels. Various building blocks refer to the elements that should be included in sharing agreements. These elements help to build support and trust, that lead to a green light on discussing cybersecurity topics. The GCCS model describes in 2.6 on how to start this cycle of sharing and 2.13.6 specifically addresses cross-border sharing attention points.

Members should be transparent on their ability to share information so other members can help to address this issue, for instance by facilitating board-level talks on expanding mandate to share. In the use case, the NL member can ask who else recognizes the challenge in the use case. S/he can then ask if information can be shared on this topic, using the ontology to create a shared vocabulary on topics. If sharing is not allowed, members can discuss how permission might be attained based on their own experience and tips from the GCCS model.

5. Do we have management support on the initiative of sharing cybersecurity information?

This has been addressed in challenge 2. This challenge regards support for the general initiative on sharing cybersecurity information within I-STORM. There is already support and experience on the positive effects for this on other domains of SSB operations, so this helps with including the cybersecurity domain. GCCS paragraphs 2.6 and 2.15 support creating the business case for management on including the cybersecurity domain. This transparent approach helps decision-making by management on supporting the initiative. It is advisable for the UK and NL to come to a joint statement on the need for this sharing in I-STORM as a signal to management. Paragraph 2.12 provides an overview of possible pitfalls on trust in the sharing process and how to address this.

Like in challenge 2, the GCCS supports the use case in building a business case on why it's important to share good practices on embedding cybersecurity in contracts. Members realize management support is important and have support on how to attain it. I-STORM partners can help to give insight into cost savings and added SSB resilience in operations. The Netherlands can be an advocate within I-STORM on cybersecurity in contracts, just like RWS does on the domestic market.

6. **How do you share information? Orally or written, original material of RWS or create I-STORM specific adaptations of knowledge (e.g. customized documents for I-STORM or share internal documents)?**

The form in which I-STORM members share information is very dependent on the topic, setting and goals of sharing. The GCCS model doesn't provide specific guidance on this but does give considerations on confidentiality when sharing internal documents. Examples of these considerations are legal considerations (2.14), addressing confidentiality (2.16) and controlling information after sharing (2.11). These paragraphs should be translated in a document with considerations for I-STORM. This guidance booklet can be referenced when faced with challenges like in what for information should be shared.

For the use case, members use the GCCS considerations to assess if an agreed upon form fits the sharing goal. I-STORM can use the use case to create a 'checklist before sharing' and/or to include terms of use that are included with the information shared on cybersecurity in contracts.

7. **With whom are my partners obliged to share information with?**

There might be legal or other obligations that may mandate an organization to share information with another party. This obligation might trump any agreements made on confidentiality. Examples of such obligations like the Freedom of Information act in the Netherlands are presented in 3.2.1.1. These obligations might lead to disclosure to parties that the sharing organization did not intend the information. To address this issue, it is important to be transparent to all relevant partners on what obligations apply, and what the effect is on information that is shared within I-STORM.

The GCCS addresses these legal show stoppers in 2.14.1. The main paragraph gives an overview of more legal aspects that might influence information shared, like the GDPR. One important obligation is not mentioned in this paragraph, which is an obligation of providing relevant information to the national security service(s). The obligation to share information with intelligence services should be addressed within I-STORM, but this might be relegated to the respective security services of the UK and NL to discuss this. Further research here is required.

For cybersecurity in contracts, sharing partners know that for example in the EU, bids for large assets are public. Any supporting documents therefore are publicly available, but there are legal possibilities to 'white out' sensitive information.

8. **How will we meet to discuss this, are travel, lodging, materials and a meeting location facilitated?**

Although 2.15.1 briefly mentions facilitating costs as an incentive, this challenge is not well addressed in the GCCS model. As mentioned in the model selection presented in 3.2.4, it is advisable to reference the ISAO and/or ISAC model for this challenge. In ISAO 100-1, paragraph 5.5.2, membership fees are suggested, which is already implemented in I-STORM. The business model presented in ISAO 100-2 could be input for evaluation of current I-STORM resources to see if adding cybersecurity to the sharing topics might increase funding. Likewise, in the ISAC model, paragraph 4.2 can be referenced for guidance on resources.

I-STORM and participating members already have resources in place for the other topics, so a possible lack of resources is not an important factor in introducing the cybersecurity information sharing process. During regular meetings, the topic of cybersecurity in contracts can be put on the agenda for discussion with selected members.

5.4 Validation of the information sharing process

The definitive validation of the information sharing process can only be confirmed by its use in practice. Still, the requirements for the process have been set and these give insight into its validity. The requirements for the process (presented in chapter 4) have been defined in paragraph 2.7. This paragraph evaluates the presented information sharing process, by validating if these requirements are met. The requirements are treated as indicators that provide assurance on the performance of the information sharing process. Therefore, the fulfillment of the requirements is considered indicators of the validity of the process. Additionally, the effect of the information sharing process on the use case is explored.

5.4.1 Fulfillment of the process requirements

Requirement 1: "The process must be compatible with Systems Engineering"

The SE context is used for the ontology to ensure a shared vocabulary on cybersecurity for engineers. The process presented in chapter 4 is based on a knowledge strategy that has been developed and used by engineers for other SSB domains as confirmed by interviewee 2. Therefore, the validation of the ontology in 5.2 confirming the compatibility of the process with SE and use of a proven strategy, indicate that this requirement is fulfilled.

Requirement 2: "The process must provide a list of topics on which to share information in a way understandable by engineers"

The validation of the ontology in 5.2 by interviews with engineers has given validation that the ontology is understandable and usable for engineers. It therefore provides a source of common vocabulary to use in the information sharing process. The ontology is addressed in various parts of the selected GCCS model, so the use of the ontology in the process is supported by the best practices in the GCCS model.

Requirement 3: "The process must address the 6 factors presented in 2.6.2"

The 6 factors identified in the initial interviews as being of most importance to the information sharing process (2.6.2) have been validated in the previous paragraph, 5.3. The factors have led to the selection of the GCCS model, which was validated using the use case presented in 2.2.

Requirement 4: "The process must fit within the knowledge management strategy of I-STORM"

The knowledge strategy approach of RWS adopted by I-STORM that is used as backbone for the process, has been implemented in practice and is successful. Interviewee 2 (see 5.2.1.2) confirmed that using this knowledge management strategy for the cybersecurity sharing process is a good approach. Still, the requirements for the information sharing process presented in 2.7 should be explicitly addressed.

5.4.2 Applying the information sharing process to the use case

In this paragraph, the effect of the information sharing process is evaluated on the use case presented in 2.2. This gives insight into how the challenges presented in the use case can be addressed by the information sharing process. This insight indicates if the process has a positive effect on information sharing within I-STORM.

The process gives strategic direction (part A) within I-STORM on the high-level goals that members agree on. This agreement is supported by a business case containing the benefits for participating members. These are used to create stakeholder buy-in and management support at the individual member organizations. At this level, requirements on conduct and clarity on (legal) sharing obligations are defined that set the ground rules for sharing. These aspects provide clarity in addressing challenges in the use case focused on management support for sharing and assurance that information is treated correctly.

Part B identifies what cybersecurity topics are essential for SSBs, which leads to prioritization for information sharing. The process gives insight into what parties should be involved and in what role. Here, the ontology plays a vital role in providing a common vocabulary to identify shared challenges. As indicated in the interviews, the ontology facilitates discussion on an abstract level by talking about the topics and examples in the ontology. This removes the need to include sensitive information in the discussion. This part therefore addresses challenges that focus on the discussion of what topics to address and the aspect of confidentiality.

Part C helps to identify cybersecurity topics that can be introduced in I-STORM as a proof of concept of the information sharing process. Using parts A and B, these topics can be related to strategic goals, with part C facilitating the creation of concrete sharing initiatives. This helps to give members insight into the practical effects of information sharing which they can use to prove that information works. By providing a guiding process, starting sharing at an operational level can help members to identify challenges and reach consent on how the should be addressed by referencing the GCCS model. This initial startup period is also important for creating trust between parties, which plays a part in several challenges presented in the use case. By having a clear vision on all levels on how to address these based on the presented information sharing process, I-STORM can show to its members it is in control and mature enough to include cybersecurity as topic for information sharing.

5.5 Limitations of the validation

This chapter so far has given insight into the validation of the information sharing process and its component parts. To fully understand and value this evaluation, it is important to present the limitations of the validation process taken. The limitations presented in this paragraph give insight into the context of the validation. This not only gives context, but also provides input for further research on the approach of this thesis.

The limitations touch upon the two approaches of the validation: the interviews and the use case. First, three of the four interviewees are from RWS, the same organization the researcher works for. This

resulted from the (physical) accessibility to relevant RWS personnel and the fact that the UK is very careful in discussing this topic. The 75%/25% distribution of interviewee nationality might create a bias stemming from similar thinking on the thesis subject due to culture and internal policies. Although there has been very little interaction between the researcher and the interviewees prior to this thesis, organizational processes do create a link. In the validation, this is explicitly addressed as part of the conclusion in 5.2.3.

Additionally, all interviewees had an affinity with cybersecurity, whether as part of their role (interviewee 1, 3 and 4) or personal interest (interviewee 2). This creates a slight positive bias in their understanding of the ontology, because they are familiar with the cybersecurity field and its jargon. This should be a point of attention when using the ontology in I-STORM.

As a final point on the validation interviews, the intention was that the interviewees filled in the questions beforehand. The face-to-face interview was meant as follow up to clear up any responses or expand on remarks. Due to time constraints of the interviewees, they all were unable to prepare for the interview by completing the validation questionnaire beforehand. The interview therefore used the questionnaire as structure to gather information. During the interview, the interviewees were given time to read the material. The reason behind the initial written response was to minimize influencing the interviewee by the researcher. Due to the pure face-to-face validation interviews, the bias of the researcher might still have had an effect.

Secondly, the use case validation was used because the process has not been implemented. Therefore, it wasn't possible to validate the process by its use in practice. The use case gives some level of insight into the validity of the process. Only the actual implementation and use of the process in I-STORM gives better assurance into its validity. Interviewee 2 addressed this in the interview by understanding that the process is a basis for 'learning as we go', and not a definitive solution that can be implemented 'as is'.

5.6 Validation conclusions

The individual artifacts of the information sharing process, the ontology and sharing model, are evaluated, as well as the information sharing process as a whole. Different validation techniques were used and bias in the interviews is addressed where possible. The validation results indicate that the ontology and model fit the requirements and answer the sub research questions stated in 1.2. The validation of the process indicate that it is suitable to answer the main research question of this thesis.

6 Conclusions and Discussion

This chapter highlights the deliverables presented as answer to the main research question; the ontology and information sharing model that result in the cybersecurity information sharing process for I-STORM. This is done by first presenting the deliverables in the context of the need for cybersecurity of SSBs and the applied approach for constructing the deliverables. Next, the results of this thesis are presented in the context of the benefit to the scientific body of knowledge and the English and Dutch society. Finally, this chapter presents potential further research.

6.1 Conclusion

Storm Surge Barriers (SSBs) have a vital function in protecting civilian life and the economic stability of countries like the UK and NL. Due to the increasing use of Information Technology (IT) and Operational Technology (OT) in SSB operations, the risk of a cyber incident severely impacting operations is a risk that needs to be addressed. I-STORM is an international network of experts that aim to improve SSB operations through information sharing. I-STORM recognizes the cybersecurity risk to SSBs, and therefore wants to address this topic.

This thesis has identified the main challenges for addressing cybersecurity in I-STORM; the lack of a shared view on what cybersecurity means for SSBs and guidance on how to share cybersecurity information. To support a view on what cybersecurity means for SSBs, no suitable ontologies for cybersecurity of critical infrastructure were available for selection. Therefore, an ontology has been created based on the NIST Cybersecurity Framework taxonomy. The ontology was created by extending the taxonomy using the Systems Engineering V-model used in the SSB lifecycle. Further extension is realized by including examples for SSBs in three states of risk the asset can exist in.

To support the sharing of cybersecurity information within I-STORM, a desk study resulted in three candidate models; the ISAC, ISAO and GCCS model. The model selection was performed using a viewpoint from the scientific field of Knowledge Transfer and Cross-boundary Information Sharing in the context of Transnational Knowledge Networks. This viewpoint uses 19 critical factors for information sharing. A selection of six most important factors was identified using interviews. The models were scored on these six factors which led to the identification of the GCCS model as most suitable model to support information sharing in I-STORM.

The deliverables for these challenges are presented as a cybersecurity sharing process for I-STORM. This process is based upon the I-STORM knowledge strategy currently being implemented. This strategy provides a backbone for information sharing on SSB operations on the strategic, tactical and operational level. The validation phase confirmed that all deliverables of this thesis fit in this knowledge strategy and answer the main research question. The cybersecurity information sharing process for I-STORM therefore support the implementation of information sharing for the cybersecurity knowledge domain.

6.2 Future research

During the research, topics for further research or improvement are identified. This paragraph presents these topics for further research. The first topic identified is the validation of the ontology. The validation

of the ontology has been performed by interviewing stakeholders within the scope of the thesis, the UK and NL. This gives a good validation for the scope of this thesis but would have merit if researched in a broader scope. Larger scale empirical research into the effects of an ontology on the understanding of the cybersecurity domain by engineers would give insight in how to (better) embed cybersecurity in their field of work on critical infrastructure. Likewise, more research into *why* cybersecurity is a hard topic to address in the engineering world would benefit any solution presented for this domain.

Secondly, this thesis only evaluated three (cybersecurity) information sharing models on six factors. Further research could expand both on the number of models and on all factors to present a complete overview of how well these models address the critical knowledge sharing models. This research could be a valuable reference for improvement of those models and organizations selecting a model for implementation.

Thirdly, during the interviews, interviewees remarked that the ontology enabled them to better discuss cybersecurity without using confidential information by using the categories and examples. This approach on discussing sensitive topics was not mentioned in the three information sharing models analyzed. Further research into this effect might help to address this confidentiality issue for information sharing as a new good practice.

Fourthly, after writing this thesis was completed, the Dutch NCSC has published a new set of supporting documents [38] to support cooperation between organizations. Although these documents are focused on the Dutch market, future research on this approach might identify good practices for I-STORM where the GCCS model is lacking. Additionally, TNO will present information on next-generation ISACs in the first quarter of 2019. Further research can be done to see if this improved model yields advice relevant for I-STORM, for example on how to address internal dynamics in participating parties.

Finally, the generalization of the ontology presented might benefit cybersecurity efforts outside the SSB domain. The next paragraph explores this generalization in more detail.

6.3 Generalization of the ontology

In this thesis, the scope of research was strictly defined by the type of critical infrastructure (SSBs) and information sharing members (UK and NL). During the interviews and desk research, it was indicated that engineering work on an SSB has many parallels with engineering in general. During the deduction phase of the research, the threat against critical infrastructure (CI) in general was used for SSBs. The need for addressing cybersecurity in engineering of CI is broadly agreed on. It was therefore surprising that in researching the ontology, the researcher concluded that a common vocabulary that enables stakeholders to define challenges on cybersecurity in engineering, did not exist. The ontology created in this thesis therefore could support a broader need than just the SSBs domain. Further research on the generalization of this ontology is needed.

The ontology presented for the domain of SSBs, uses a two-step approach. First the taxonomy of the CSF is extended by describing the categories in the context of the V-model. The V-model is used widely

in construction of large assets, not just SSBs. Therefore, the V-model description of cybersecurity in the ontology is applicable in a wider context. The ontology with the first added column therefore could be used for any asset that uses the V-model and contains IT and OT.

In an interview[2] on the generalization of the ontology, Maarten Hoeve (director technology at the European Network for Cyber Security (ENCS)) indicated that "*The ontology can be transferred 1-on-1 with only minor adjustments in terminology (e.g. replace 'PLC' with 'device')*.". Maarten remarked that the ontology could also be useful in creating alignment on cybersecurity topics between the operational, tactical and strategic level with an organization.

Secondly the taxonomy gives relevant examples of the impact of the categories on the asset in the three threat states of an SSB. The examples are presented using three threat states, based on the Cyber Killchain of Lockheed-Martin. The Cyber Killchain is widely applicable as evident by its success and popularity. Although the examples in the ontology in this thesis are specific for the SSB domain, the approach of using the three threat states of an asset to present cybersecurity examples can be applied outside the SSB domain. This can be in a different domain (e.g. the energy sector) or in another domain within an organization that manages SSBs (e.g. tunnels and bridges at RWS).

Therefore, the use of a generalized cybersecurity ontology critical infrastructure helps to improve resiliency of CI assets against the risk of cybersecurity threats. This generalization requires further research.

[2] Delft, 23rd of November 2018

7 General reflection

The writing of this thesis has taught me more than I had anticipated. What started as an idea in a conversation about SSBs over coffee led me down the rabbit hole of the complex and challenging world of engineering and the unique task of SSBs. During this journey, my goal was to help the engineers tasked with keeping societies safe from flooding cope with the new threat of the cyber domain.

This confronted me with my own IT bias in approaching cybersecurity challenges by giving me insight into a world focused on safety using computing equipment solely designed for decades long continuous use. The patience and professional commitment of my colleagues at RWS and abroad at the Environment Agency in the UK proved helped me to understand their world.

As my understanding of the engineering viewpoint grew, so did my understanding that the field of cybersecurity for OT has a focus on technical solutions. Here, the holistic approach of the executive master program enabled me to realize that a focus on just the technical aspects of cybersecurity doesn't necessarily leads to a good solution. The socio-technical and governance aspects of cybersecurity deserve more attention, and I hope my information sharing process supports the engineers in addressing socio-technical and governance challenges.

At the start of writing this thesis, I was aware that I had a preconception on what the possible solution would look like. The scientific rigor and an open mind ingrained during the three semesters gave me the methodology to research the thesis research question and arrive at a result that I would never have thought of six months ago.

It was a very interesting and exhilarating process to write this thesis which has expanded my horizon and at the same time taught me to focus. Most important of all, I feel it is a small contribution in making society a little bit safer.

8 References

[01] Shodan, "Shodan - ICS Radar." [Online]. Available: https://ics-radar.shodan.io. [Accessed: 23-Nov-2018].

[02] European Union Agency for Network and Information Security (ENISA), "Window of exposure … a real problem for SCADA systems? - Recommendations for Europe on SCADA patching," no. December, pp. 1–19, 2013.

[03] Dave McMillen, "Attacks Targeting Industrial Control Systems (ICS) Up 110 Percent." [Online]. Available: https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/. [Accessed: 23-Nov-2018].

[04] J.-P. AUFFRET *et al.*, "Cybersecurity Leadership: Competencies, Governance, and Technologies for Industrial Control Systems," *J. Interconnect. Networks*, vol. 17, no. 01, p. 1740001, 2017.

[05] "I-STORM Homepage English." [Online]. Available: https://www.i-storm.org/. [Accessed: 23-Jul-2018].

[06] NCSC UK, "Advisory: Hostile state actors compromising UK organisations with focus on engineering and industrial control companies," no. April, pp. 1–20, 2018.

[07] Dutch General Intelligence and Security Service, "Annual report 2017."

[08] NCSC NL, "Cyber Security Assessment Netherlands 2018 - NCSC." [Online]. Available: https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html. [Accessed: 26-Jul-2018].

[09] European Union, "DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," *Off. J. Eur. Union*, no. July 2016.

[10] ENISA, *Information sharing and common taxonomies between CSIRTs and Law Enforcement, Heraklion, Greece*, no. December. 2015.

[11] F. Skopik, G. Settanni, and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," *Comput. Secur.*, vol. 60, pp. 154–176, 2016.

[12] M. Gharawi and S. Dawes, "Conceptualizing knowledge and information sharing in transnational knowledge networks," *Proc. 4th Int. Conf. Theory Pract. Electron. Gov. - ICEGOV '10*, p. 121, 2010.

[13] NJCCIC, "Stuxnet." [Online]. Available: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet. [Accessed: 24-Jul-2018].

[14] NJCCIC, "Havex." [Online]. Available: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/havex. [Accessed: 24-Jul-2018].

[15] NJCCIC, "BlackEnergy." [Online]. Available: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/blackenergy. [Accessed: 24-Jul-2018].

[16] NJCCIC, "TRISIS-TRITON." [Online]. Available: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/triton. [Accessed: 24-Jul-2018].

[17] R. Rammig, "Security Standardization and Regulation An Industry Perspective," 2017. Available: https://www.enisa.europa.eu/events/enisa-cscg-2017/presentations/rammig

[18] R. J. Deibert and R. Rohozinski, "Risking security: Policies and paradoxes of cyberspace security," *Int. Polit. Sociol.*, vol. 4, no. 1, pp. 15–32, 2010.

[19] Office of the Press Secretary, "Executive Order on Improving Critical Infrastructure Cybersecurity | The White House." [Online]. Available: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0. [Accessed: 26-Jun-2018].

[20] European Commission, "The Directive on security of network and information systems (NIS Directive) | Digital Single Market," 2016. [Online]. Available: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive. [Accessed: 26-Jun-2018].

[21] US-CERT, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors | US-CERT," *Alert (TA18-074A)*, 2018. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA18-074A. [Accessed: 26-Jun-2018].

[22] European Parliament, "[04] MEPs want robust EU cyber defence and closer ties with NATO - Nieuws - Europees Parlement." [Online]. Available: http://www.europarl.europa.eu/news/nl/press-room/20180607IPR05242/meps-want-robust-eu-cyber-defence-and-closer-ties-with-nato. [Accessed: 26-Jun-2018].

[23] NCSC UK, "The 2017 Annual Review - NCSC Site." [Online]. Available: https://www.ncsc.gov.uk/news/2017-annual-review. [Accessed: 26-Jul-2018].

[24] NCSC UK, "Joint US - UK statement on malicious cyber activity carried out by Russian government," 2018. [Online]. Available: https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government. [Accessed: 26-Jul-2018].

[25] Wikipedia, "Reliability, Availability, Maintainability, and Safety (RAMS)." [Online]. Available: https://en.wikipedia.org/wiki/RAMS. [Accessed: 23-Nov-2018].

[26] Wikipedia, "Systems engineering." [Online]. Available: https://en.wikipedia.org/wiki/Systems_engineering. [Accessed: 09-Aug-2018].

[27] Wikipedia, "Systems Theory." [Online]. Available: https://en.wikipedia.org/wiki/Systems_theory. [Accessed: 09-Aug-2018].

[28] R. Ross and J. C. OREN, "Systems Security Engineering - NIST Special Publication 800-160 VOLUME 2," *NIST Spec. Publ.*, vol. 800, p. 160, 2014.

[29] US department of Transportation, "Systems Engineering for ITS Handbook - Section 3 What is Systems Engineering?" [Online]. Available: https://ops.fhwa.dot.gov/publications/seitsguide/section3.htm. [Accessed: 08-Aug-2018].

[30] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security," no. May, p. 247, 2015.

[31] NEN/IEC, "Nen-iso/iec 27002 Information technology - Security techniques - Code of practice for information security controls," 2013.

[32] Kaplan, Bailey, O'Holloran, Marcus, and Rezek, *Beyond Cybersecurity*. 2015.

[33] ISAO, "ISAO 300-1: Introduction to Information Sharing," 2016.

[34] ISAO, "ISAO 100-1: Introduction to Information Sharing and Analysis Organizations (ISAOs)," 2016.

[35] ISAO, "ISAO 100-2: Guidelines for Establishing an Information Sharing and Analysis Organization (ISAO)," 2016.

[36] NCSC UK, "Cyber Security Information Sharing Partnership (CiSP)." [Online]. Available: https://www.ncsc.gov.uk/cisp. [Accessed: 02-Aug-2018].

[37] CPNI UK, "CPNI partners in Government, Police, Industry and Academia" [Online]. Available: https://www.cpni.gov.uk/who-we-work. [Accessed: 01-Jul-2018].

[38] NCSC NL, "Sectorale samenwerking (ISAC)." [Online]. Available: https://www.ncsc.nl/samenwerking/_samenwerken/sectorale-samenwerking-isac.html. [Accessed: 30-Jun-2018].

[39] European Union Agency for Network and Information Security (ENISA), "Information Sharing and Analysis Centres (ISACs) Cooperative models," 2017.

[40] European Union, *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*, no. December. 2015.

[41] E. Luiijf and A. Kernkamp, "Sharing Cyber Security Information - Good Practice Stemming from the Dutch Public-Private-Participation Approach," *GCCS*, no. March 2015.

[42] J. Van Den Berg *et al.*, "On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education," *NATO STO/IST-122 Symp. Tallin*, no. c, pp. 1–10, 2014.

[43] US-CERT, "Information Sharing Specifications for Cybersecurity." [Online]. Available: https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity. [Accessed: 23-Nov-2018].

[44] K. Vrolijk and M. Walraven, "Kennisstrategie Stormvloedkeringen RWS," Rijkswaterstaat, 2018.

[45] H. Stuckenschmidt and F. van Harmelen, "Ontology-based information sharing," *Inf. Shar. Semant. Web*, p. 276, 2005.

[46] B. Tsoumans, S. Dritsas, and D. Gritzalis, "An Ontology-based approach to Information Systems Security Management," *Gorodetsky V., Kotenko I., Skormin V. Comput. Netw. Secur. MMM-ACNS 2005. Lect. Notes Comput. Sci. vol 3685.*

[47] A. B. Panayotis A Yannakogeorgos, *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Taylor & Francis, 2014.

[48] L. C. Van Ruijven, "Ontology for systems engineering," *Procedia Comput. Sci.*, vol. 16, pp. 383–392, 2013.

[49] L. Obrst, P. Chaseb, and R. Markeloffa, "Developing an Ontology of the Cyber Security Domain," *CEUR Work. Proceedings.*, vol. 966, pp. 49–56.

[50] N. F. Noy and D. L. McGuinness, "Ontology Development 101: A Guide to Creating Your First Ontology," *Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880, March 2001*. Stanford University.

[51] B. Sarder and S. Ferreira, "Developing Systems Engineering Ontologies," *IEEE Int. Conf. Syst. Syst. Eng.*, 2007.

[52] Y. Sun, G. Yang, and X. Zhou, "A novel ontology-based service model for cyber physical system," *2016 5th Int. Conf. Comput. Sci. Netw. Technol.*, 2016.

[53] L. Petnga and M. Austin, "An ontological framework for knowledge modeling and decision support in cyber-physical systems," *Adv. Eng. Informatics*, vol. 30, no. 1, pp. 77–94, 2016.

[54] Y. Sun, G. Yang, and X. Zhou, "A novel ontology-based service model for cyber physical system," *2016 5th Int. Conf. Comput. Sci. Netw. Technol.*, 2017.

[55] NEN/ISO, "NEN-EN-IEC 62443 - Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements.".
[56] T. Yildirim, "Cybersecurity Implementatierichtlijn Objecten – RWS," 2013.
[57] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," 2018.
[58] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," April 16th, 2018.
[59] NIST, "New to the Cybersecurity Framework." [Online]. Available: https://www.nist.gov/cyberframework/new-framework. [Accessed: 06-Sep-2018].
[60] NIST, "An Introduction to the Components of the Framework." [Online]. Available: https://www.nist.gov/cyberframework/online-learning/components-framework. [Accessed: 06-Sep-2018].
[61] Lockheed Martin, "Cyber Kill Chain." [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Accessed: 01-Nov-2018].
[62] W. A. Conklin and D. Shoemaker, "Cyber-resilience: Seven steps for institutional survival," *Edpacs*, vol. 55, no. 2, pp. 14–22, 2017.
[63] Wikipedia, "Resilience (engineering and construction)." [Online]. Available: https://en.wikipedia.org/wiki/Resilience_(engineering_and_construction). [Accessed: 15-Sep-2018].
[64] T. Shinder, "An Insider's Look at the Security of Microsoft Azure – Assume the Breach! – Microsoft Azure Security and Compliance." [Online]. Available: https://blogs.msdn.microsoft.com/azuresecurity/2015/10/19/an-insiders-look-at-the-security-of-microsoft-azure-assume-the-breach/. [Accessed: 15-Sep-2018].
[65] D. Backman, "Blackhat USA 2017 - ASSUME BREACH. YES. ALWAYS." [Online]. Available: 15-9-2018.
[66] D. Ormrod and B. Turnbull, "The cyber conceptual framework for developing military doctrine," *Def. Stud.*, vol. 16, no. 3, pp. 270–298, 2016.
[67] Dutch Government, "Wet openbaarheid van bestuur," 2018. [Online]. Available: https://wetten.overheid.nl/BWBR0005252/2018-07-28. [Accessed: 12-Oct-2018].
[68] US-CERT, "Traffic Light Protocol (TLP) Definitions and Usage | US-CERT," 2016. [Online]. Available: https://www.us-cert.gov/tlp. [Accessed: 12-Oct-2018].
[69] ENISA, "Considerations on the Traffic Light Protocol." [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol. [Accessed: 12-Oct-2018].
[70] European Commission, "EU Cybersecurity Initiatives," *Factsheet*, p. 8, 2017.
[71] NCTV, "Nederlandse Cybersecurity Agenda: Nederland digitaal veilig," *Rijksoverheid.nl*, 2018.
[72] The White House, "Presidential Decision Directive 63, Critical Infrastructure Protection." 1998.
[73] NCSC NL, "Proces: Opzetten en faciliteren ISAC's."
[74] ISAO, "Frequently Asked Questions." [Online]. Available: https://www.isao.org/faq/ [Accessed: 15-Oct-2018].
[75] ISAO, "Future Products." [Online]. Available: https://www.isao.org/resources/future-products/. [Accessed: 14-Oct-2018].

[76] H. Kim, Soonhee; Lee, "The Impact Of Organizational Context And Information Technology On Employee Knowledge-Sharing Capabilities.," *Public Adm. Rev.*, vol. 66, no. 3, pp. 370–385, 2006.

[77] K. Vrolijk and M. Walraven, "Kennisstrategie Stormvloedkeringen - Bijlage: Uitgewerkte Kennisterreinen," 2018.

[78] B. A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information," *MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004.

[79] A. R. Hevner, "A Three Cycle View of Design Science Research A Three Cycle View of Design Science Research," *Scand. J. Inf. Syst.*, vol. 19, no. 2, 2007.

[80] R. Wieringa, "Design Science Methodology for Information Systems – Appendix A, Checklist for the Design Cycle Checklist for the Empirical Cycle," 2014.

[81] P. R. Wieringa, "Design Science Methodology," November 2015.

9 Appendices

9.1 Appendix 1; List of abbreviations and terminology

Abbreviation / Terminology	Explanation
Asset	The whole SSB structure that performs a watermanagement function
CI	Configuration Item
CIA	Confidentiality, Integrity and Availability
Control	A measure that mitigates a risk (e.g. a firewall, user instruction, policy or physical lock)
CSIRT	Cyber Security Incident Response Team
CSF	Cyber Security Framework NIST
IOC	indicators of compromise
IT	Information technology (e.g. desktop computer)
NCSC (UK & NL)	National Cyber Security Center
OT	Operational technology (e.g. a PLC)
PLC	Programmable Logic Controller
RAMS	Reliability, Availability, Maintainability and Safety
SE	Systems Engineering
SIEM	Security and Incident Event Management system
SSB(s)	Storm Surge Barrier(s)

9.2 Appendix 2; Exploratory interview on Cybersecurity Information Sharing requirements

Questionnaire to explore requirements for an information sharing process

Information about this questionnaire

This questionnaire is focused on gathering information on the sharing of cybersecurity information on Storm Surge Barriers (SSBs). The questions are the basis for defining requirements for a cybersecurity information sharing process on SSBs for I-STORM. The questions are split up in three categories.

References to information sharing in this questionnaire are focused on the sharing of cybersecurity information, unless expressly mentioned otherwise.

If it not possible or allowed to answer a question, please indicate so, and if possible, provide a reason. The reason may also be relevant for defining an information sharing process.

The answers given in this questionnaire are treated as personal opinion, and not formal statements of the organization.

General information on respondent

Name	
Job title	
Organization	
How may this questionnaire be included as a thesis appendix	In full / Anonymized / Not included (confidential)[3]
Date	

1. General questions

1. What is your relation to cybersecurity for SBBs?
2. How important is cybersecurity seen as topic to address for SSBs?
3. Is cybersecurity recognized as a topic that should be addressed within I-Storm?
    a. Impact on safety by cybersecurity incidents
4. What is the importance of information sharing on cybersecurity issues for SSB's?

2. What information to share

1. What security related topics are discussed within I-STORM?
    a. How are they discussed?
2. What cybersecurity topics (if any) are discussed within I-Storm?
3. What information is shared on SSBs with the Netherlands/UK in general (so also outside I-STORM)?
4. What topics or best practices can you list that could be discussed as part of cybersecurity information sharing on SSBs?
    a. Awareness, contracting, incidents prevention, etc.

3. How to share information

1. What is the reason in your opinion cybersecurity is not included as domain for information sharing within I-STORM?
2. How is the decision made to share information within international settings?
3. What would be the most important obstacles (points of attention) be in sharing security information on SSB with the Netherlands/UK?
4. Below these questions, a table is given with aspects that play a part in information sharing. What are the five most important aspects in your opinion that should be addressed to enable information sharing?
5. Are any important requirements for sharing information missing in the table below?

Domain	**Aspects of information sharing**	**Description**
	Type of knowledge shared	The type of knowledge that is being shared.

[3] The results are referenced and used for the thesis but are only shared with the exam board. The questionnaire is not made public and treated as confidential information.

Knowledge and information content		1. Tacit knowledge (experience someone has, not formalized in procedures or processes). 2. Explicit knowledge (procedures, best practices, instructions, etc)
	Lacking for data standards and definitions	Is there a structure in which to share information like a framework providing a common language and structure?
	Value, sensitivity and confidentiality	Are these aspects of information known and explicit between sharing partners? E.g. do they know if the information of another party is sensitive?
	Codefiability (Articulability)	The degree to which knowledge can be expressed in language, numbers, formal procedures, and explicit techniques.
	Embeddedness of information in processes/people/procedures	The degree to which knowledge is situated in or generated by ongoing practice and learning by doing.
Organizational context	Goals and interests of participating organizations	What are the goals/interests of organizations who share information, and do those goals/interests align?
	Trust and past relationships	The trust between sharing organizations, and if they have a history of sharing information (information in a broad context here)
	Executive support and organizational commitment	
	Perception of risk, costs and benefits	How the sharing organizations perceive the risks, costs and benefits of sharing information. In short; the business case for sharing.
	Organizational culture	How the organizational structure impact information sharing. Centralization for instance can slow sharing through long procedures.
	Leadership	Do leaders have the ability to use their power to guide cooperation and develop influence without formal authority?
	Authority and hierarchical structures	How are decisions made, how does authority to share information flow, is it quick, slow, (in)formal, etc. Can decision making be delegated to sharers of information?
	Organizational rules, procedures and regulation	Are there formal ways to steer information sharing? E.g. there is a department who must be included in all international information

		sharing. Or all information sharing must be vetted by the CISO.
	Resources	Are any resources available for information sharing? E.g. is there any support for the sharing of information with means like time allotment, travel expenses, etc.
External Environment	Culture	If there is a big difference in culture between sharing countries, this has impact on sharing. E.G. the Dutch are very direct, which can impact sharing if the Dutch are seen as rude.
	Laws and policies	The regulatory limitations on sharing, for instance confidentiality mandates on critical infrastructure, or mandates to share incident information (e.g. EU NIS directive).
	Political support	Is there a national agenda for information sharing?
	Language	Is language a barrier, how do you communicate?
	Geographical location	How possible is it to physically meet? Time differences in virtual meetings.

9.3 Appendix 3; Validation questionnaire

Evaluation of the cybersecurity topics for Storm Surge Barriers in I-STORM

Goal and structure of this document

The goal of this document is to prepare for the interview to evaluate if the topics and description in the Excel sheet can explain cybersecurity topics in an understandable way to engineers. This document is a short explanation on the Excel sheet which will be discussed in the interview. The Excel sheet is based on an existing model. This goal of the evaluation is to determine if the extension of the standard topic list with explanations aimed at the Systems Engineering context, help to use this list within I-STORM for Storm Surge Barriers (SSBs) in information sharing.

It is not the goal for the topic list to be completely self-explanatory, but the terminology used in the columns should in general be recognizable to the engineer. The list will be used as a basis for products like workshops, instructions, discussion, etc. within I-STORM.

The questions in the interview will focus at identifying if the topic list supports the engineer in the understanding of cybersecurity for engineering in general, and SSBs in particular. To do this, the interview will consist of two phases:

1. Answering the questions given at the end of this document by email.
2. A follow up interview in person to further explore the answers given in (1).

Before answering the questions, this document will first explain the context of the questions, concluding with the questions themselves.

Why this interview?

For my master thesis, I'm presenting a list of topics that comprise the concept of cybersecurity for Storm Surge Barriers (SSB). This is done to make the subject of cybersecurity more approachable to non-security professionals like the engineers working on Storm Surge Barriers (SSBs). The goal is to create a shared vocabulary that helps to identify shared cybersecurity challenges and to facilitate the exchange of best practices for these challenges.

The result is the list of cybersecurity topics (categories) presented in the Excel sheet presented in tandem with this document. The categories represent the different subjects into which the topic of cybersecurity can be divided for SSBs, described in a non-technical way aimed at an engineering audience.

Explanation of the cybersecurity topics Excel sheet columns

To create an ontology, I've taken a framework of cybersecurity for critical infrastructure (the NIST Cyber Security Framework) and added two columns. These columns tailor the framework for use in SSBs by translating the general framework to the SSB domain from a Systems Engineering viewpoint and giving examples for cybersecurity situations.

This results in an Excel sheet with the following columns:

- *Function*

  There are five high level functions (Identify, Protect, Detect, Respond, and Recover) that are present in risk management at large. These represent the general goals of cybersecurity risk management.

- *Category*

  "*The Categories were designed to cover the breadth of cybersecurity objectives for an organization, while not being overly detailed. It covers topics across cyber, physical, and personnel, with a focus on business outcomes.*"

- *Relevance in Systems Engineering*

  This explanation describes the importance of the category concept for the specific SE phase, enabling the engineer to understand what that cybersecurity concept means for the activities in that phase. The description supports the understanding of the reasoning line of addressing that concept in the SE lifecycle. This understanding helps to correctly implement the concepts of cybersecurity into SE. For example, if the engineer understands that it is important to include cybersecurity aspects (like firmware version) into the asset management of an SSB in order to quickly assess vulnerable components when an exploit for firmware is discovered, he/she can better implement that category.

- *Cybersecurity relevance for Storm Surge Barriers*

  For use in I-STORM, there is a need to further explain the category in terms of cybersecurity relevance to SSB. In this column, the category is explained in three situations. These three situations are based on the three 'states of cybersecurity' an SSB

can exist. The description for each situation is not done exhaustive, but as an example to enable a deeper understanding of the category relation to an SSB. The description of category for the cybersecurity state leads to understanding, which facilitates the further discussion and treatment of the category.

Questions that are the basis for the interview

In the interview, we will further discuss the questions below on the Excel sheet with cybersecurity topics. As a preparation, the questions below need to be answered. In the interview, I will use these answers as a basis for follow up questions.

The context for the questions is the cybersecurity of an SSB from the viewpoint of an engineer who works using Systems Engineering principles. The aim of the topics is to give a more detailed understanding of what cybersecurity for an SSB entails, so shared challenges and suitable topics for information sharing can be identified.

--- Start of questions ---

! Please open the file "*I-STORM Cybersecurity Ontology - Interview preparation.xlsx*" and open the **first** tab (located at the bottom). Please answer the questions below for step 1.

Step 1: basic understanding of the topics

(use sheet 1 in the Excel document)

Question 1: **Do you understand how the descriptions in column A and B relate to the engineering work on assets like Storm Surge Barriers?**
Hint; what the effect of the topic is on the reliability is of the asset, so how does incorporating cybersecurity components in asset management relate to safe and reliable operation of the asset. *Yes/No, explain if possible on why the topic description is clear or unclear.*

Question 2: **Can you relate the description in column A and B to cybersecurity aspects in your work in engineering?**
Yes/No, explain if possible on why it is clear or unclear.

Question 3: **Do the columns give an understanding of the cybersecurity aspects of Storm Surge Barriers?**
Hint; do they help to better understand what cybersecurity of an asset means, or describe challenges more clearly *Yes/No, explain if possible on why it is clear or unclear.*

! Please open the file "*I-STORM Cybersecurity Ontology - Interview preparation.xlsx*" and open the **second** tab (located at the bottom). Please answer the questions below for step 2.

Step 2: understanding the topics with the added columns

(use sheet 2 in the Excel document)

Question 4:
Do you understand the description of columns C and D?

Hint; do I know what the contents of column C and D represent based on the explanation in this document on the four columns.

Yes/No, explain if possible on why it is clear or unclear.

Question 5:
Do I understand the terms that are being used in column C and D?

Hint; is terminology used that is unclear or vague. If so, please indicate with examples.

Yes/No, explain if possible on why it is clear or unclear.

Question 6:
Do I understand the topics in columns A and B better with the added descriptions in columns C and D?

Hint; think back on reading just column A and B and answering question 1. Do the extra columns help in understanding the cybersecurity topics.

Yes/No, explain if possible on why it is clear or unclear.

Question 7:
Do the columns give me a better understanding of cybersecurity aspects in the daily work in engineering?

Hint; think back on reading just column A and B and answering question 2. Do the extra columns C and D help in better understanding the cybersecurity aspects for engineers in their daily work.

Yes/No, explain if possible on why it is clear or unclear.

Question 8:
Do the columns give me a better understanding of the cybersecurity aspects of Storm Surge Barriers?

Hint; think back on reading just column A and B and answering question 3. Do the extra columns C and D help in better understanding how cybersecurity topics impact SSB operations.

Yes/No, explain if possible on why it is clear or unclear.

9.4 Appendix 4; An ontology for cybersecurity in SSB

Function	Category	Relevance In Systems Engineering	Threat states of Storm Surge Barriers	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM)**: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational assetives and the organization's risk strategy.	**The decomposition and definition phase**: a proper data structure must be defined to support the creation of a suitable asset management system. This structure must include all OT & IT components (configuration items) and relevant information like version, type and network address. It must also include the roles and responsibilities of personnel for security aspects (e.g. incident coordinator, implementing firmware updates, etc.). **The implementation phase**: this asset management system must be populated with the components (configuration items) that make up the asset. This system must not only contain the configuration items, but the relation between them as well. E.g. the type, configuration, IP and firmware version of a PLC are stored in asset management system as object and the function of the PLC in engaging a pump is stored as a relationship to the pump configuration item. **Integration & Recomposition phase**: during the testing, verification and validation steps, the asset management systems content must be referenced and validated. Additionally, roles and processes for the maintenance of the asset management system are verified to ensure consistency with the real-world situation. **Operations & Maintenance phase**: during changes, the asset management system is referenced and altered according to real-world changes. E.g. if a PLC firmware is updated, the new formware version is entered in the system.	**For resilience/reliability** like monitoring and hardening a SSB, the AMS supports the decision like what and where to monitor or how to protect (harden) computing components. Monitoring and hardening can be implemented safely, because the impact of implementation of e.g. a sensor is known and controlled. Monitoring information is well defined and usable to assess the state of the SSB. Knowing your asset helps to manage risks leading to better resiliency. **In case of a cybersecurity threat**, the asset management systems is referenced to determine the impact on the SSB. For instance with a vulnerability to a type and version of PLC, the asset management system provides information if that configuration is present, and if so, what SSB system(s) it supports. This decreases the reaction time to threats and supports effective mitigation planning. The AMS will contain information on who is responsible for mitigating the threat. **In case of an incident**, for instance an IP can quickly be referenced to a specific component and its higher level systems within the SSB. With incidents, determining what system is affected and how to react is greatly improved when it is known what CI compose the SSB. Roles and responsibilities contained in the AMS reduce reaction and decision times. The AMS therefore is a key component in incident analysis.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	• **CIS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8, PM-5
				ID.AM-2: Software platforms and applications within the organization are inventoried	• **CIS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 • **NIST SP 800-53 Rev. 4** CM-8, PM-5
				ID.AM-3: Organizational communication and data flows are mapped	• **CIS CSC** 12 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
				ID.AM-4: External information systems are catalogued	• **CIS CSC** 12 • **COBIT 5** APO02.02, APO10.04, DSS01.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
				ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	• **CIS CSC** 13, 14 • **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
				ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **CIS CSC** 17, 19 • **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1 • **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE): The organization's mission, assetives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**The decomposition and definition phase**: a clear design of the organization's information security structure must be available as a reference. The elements in the decomposition and definitions used must be able to align with the information security organization in place. The business goals, mission and assetives must be translated to system requirements. The cybersecurity CIA requirements for the SSB being designed must be transposed/aligned to RAMS. Critical functions and threats of the SSB are defined based on business wide risk management and key organizational processes ('crown jewels'). Security policy of the	**For resilience/reliability**, the alignment with the business environment risk ensures that the SSB resilience and reliability matches the general risk appetite. The SBB is not under- or overprotected to cyber threats. Existing cybersecurity roles and risk management represent the risk appetite are the context in which the SSB risk is positioned. The security aspects of the SSB operations must align with the business environment requirements that are defined in the RAMS aspects. Recovery times after incidents are defined. **In case of a cybersecurity threat**, the risk management processes of the business environment support the SSB	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	• **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** CP-2, SA-12
				ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	• **COBIT 5** APO02.06, APO03.01 • **ISO/IEC 27001:2013** Clause 4.1 • **NIST SP 800-53 Rev. 4** PM-8
				ID.BE-3: Priorities for organizational mission, assetives, and activities are established and communicated	• **COBIT 5** APO02.01, APO02.06, APO03.01 • **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 • **NIST SP 800-53 Rev. 4** PM-11, SA-14
					• **COBIT 5** APO10.01, BAI04.02, BAI09.02

		organization are embedded in contracts as requirements. **The implementation phase**: risk management processes are used to guide design and implementation decisions. These processes ensure core business processes are protected according to design. Decisions on implementation that have an effect on risk appetite or the exposure to risk by the organization are handled through existing risk management procedures and roles. Decisions are formalized within the project documentation as well as business risk management records. **Integration & Recomposition phase**: results of testing of security aspects are reported on a high level to the designated role(s) within the security organization. Testing will also cover the integration with organizational processes and roles. **Operations & Maintenance phase**: evaluation of the contractual obligations on security are monitored by contract management. Changes in the organizational risk posture are translated to changes to the requirements for the SSB.	with a current threat profile. This profile can be assessed against the contractually defined requirements, clearly identifying if a SSB is facing a threat level it's designed for. If the threat exceeds the designed requirement, additional mitigating measures can be identified. **In case of an incident**, the roles within the organization e.g. the CISO or incident manager, must align with agreed upon incident procedures with external parties who maintain the SSB. This ensures that if an incident occurs, the process leads to a handling of the incident as stipulated in the contract. The correct roles are addressed for decisions on mitigating actions. The RAMS specifications in the contract are used to determine if an incident will exceed the agreed upon operational requirements. SSB procedures including actions by all parties involved, are aligned with organizational crisis management processes, so escalation procedures due to an incident are clear.	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established	· **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 · **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
				ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	· **COBIT 5** BAI03.02, DSS04.02 · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**The decomposition and definition phase**: all legal requirements for cybersecurity are delivered to the project team for reference in the bid and contract. The governance process for cybersecurity must be clear to contract- and bid-management roles, so they can translate the alignment of the SSB. The governance of the organization must include the outsourcing of security tasks and how to incorporate such arrangements in the internal governance body. The requirements for governance of the outsourcing company are well defined in contracts. **The implementation phase**: the implementation of the governance processes, policies and procedures is performed. Activities are documented so an audit can confirm the implementation according to contractual requirements. **Integration & Recomposition phase**: the	**For resilience/reliability**, governance is essential to have the correct persons assess the risk of cyber to the safety and operational specifications of the SSB. The governance processes of the organization will ensure that SSB managers are informed about risk and required actions. SSB personnel work together with the organizational governance roles to ensure the right level of cybersecurity to ensure regulatory requirements and operational goals of the SSB. **In case of a cybersecurity threat**, a threat can be detected through SSB operations, or through the threat intelligence function of the organization (in RWS, this is part of the Security Operations Center function). Governance processes ensure that a threat is communicated quickly to relevant stakeholders, and that action is being taken in the correct way. The processing of threat information is well defined, ensuring that action can be taken efficiently and effectively. Organizational governance is the linking pin to other supporting organizations e.g. National Cyber Security Centers or intelligence services.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	· **CIS CSC** 19 · **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 · **ISA 62443-2-1:2009** 4.3.2.6 · **ISO/IEC 27001:2013** A.5.1.1 · **NIST SP 800-53 Rev. 4** -1 controls from all security control families
				ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	· **CIS CSC** 19 · **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 · **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
				ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· **CIS CSC** 19 · **COBIT 5** BAI02.01, MEA03.01, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.7 · **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 · **NIST SP 800-53 Rev. 4** -1 controls from all security control families
					· **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02

		functioning of all governance processes is tested across the whole governance chain. This means including both the organizational and outsourcing partners to test the governance end-to-end. In this phase, evidence is generated and verified to confirm compliance with the contractual requirements. **Operations & Maintenance phase**: during this phase, periodical verification is done as part of contract management to conform governance requirements perform as specified. Organizational governance changes must be communicated to the SSB to assess its impact.	**In case of an incident**, governance dictates who has what responsibility, and provides a process and role-structure to respond in a correct way. Good governance leads to minimal misunderstandings in taking action, and ensures that the learning ability of an organization based on the incident is present.	**ID.GV-4:** Governance and risk management processes address cybersecurity risks	· **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · **ISO/IEC 27001:2013** Clause 6 · **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**The decomposition and definition phase**: organization risk management performs a risk analysis on the SSB, resulting in a risk profile for the SSB. The required cybersecurity requirements to mitigate the risk (the controls), are therefore derived from this risk assessment. In the requirements definition and decomposition, the SSB risk profile is translated to specific design and operations specifications for security controls. The risk management is the underlying justification for the security requirements, therefore guiding design choices. **The implementation phase**: during implementation, risk management provides a reasoning process supporting the decision process. When a choice needs to be made, a risk assessment is performed to present the cyberrisk effects of an option. This can then be related to the risk appetite, leading to recommendations and makes cyber risk explicit in design . Various types of risk can be evaluated in design choices, e.g. decreasing the risk of hacking by implementing a network control versus the risk of operational failure caused by the network.control influencing time sensitive network traffic. **Integration & Recomposition phase**: during implementation, vulnerable components are identified (e.g. missing patches, unscreened construction personnel working on critical components, etc.). Both risk and mitigating	**For resilience/reliability**, risk assessment gives a clear view of the vulnerabilities of the SSB that impact reliability. This helps to implement additional controls in order to decrease the risk of an incident below the risk tolerance level of the organization. Known cyber risk and threats must be related to the impact on safe and reliable operations defined in RAMS specifications. Threat intelligence must be communicated to the SSB operator to ensure that proper action by the operator can be taken to ensure operations or proper recovery after an event. **In case of a threa**t, known vulnerabilities in the SSB are assessed for exposure. This will lead to quick and efficient action on threats. Example: an operator must report the delayed replacement of vulnerable software so the risk is known. If a threat is known to use this vulnerability, quick action can be taken, preventing that the threat becomes an incident. Threat intelligence report a heightened threat by activists to the SSB operator, so additional measures can be evaluated against this possibly new threat, preventing its exploitation leading to an incident. **In case of an incident**, the risk assessment is a basis for containing the incident by supporting the quick evaluation of exposure to the vulnerability. It can be determined if other SSB are likely to be affected by the same incident cause. European regulation (NIS directive) may require incidents on SSB to be reported to designated authorities, in which case risk assessment results help in providing supporting content.	**ID.RA-1:** Asset vulnerabilities are identified and documented	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
				ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	· **CIS CSC** 4 · **COBIT 5** BAI08.01 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16
				ID.RA-3: Threats, both internal and external, are identified and documented	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
				ID.RA-4: Potential business impacts and likelihoods are identified	· **CIS CSC** 4 · **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
				ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	· **CIS CSC** 4 · **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
				ID.RA-6: Risk responses are identified and prioritized	· **CIS CSC** 4 · **COBIT 5** APO12.05, APO13.02

		action are recorded in a risk log, and acted upon. **Operations & Maintenance phase**: the risk to the SSB is part of the regular risk assessment cycle. Changes to the risk profile are communicated with the responsible parties for the SSB, in which the SSB process owner and the cyber risk owner (e.g. the CISO), periodically assess the risk.			• **ISO/IEC 27001:2013** Clause 6.1.3 • **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**The decomposition and definition phase**: the asset has been evaluated according to the organization wide risk management process, and risk tolerance for the asset and its criticality is formalized. The mitigation strategy mandated by the organization is translated to requirements for the asset. A protection profile as part of the CSF is defined. **The implementation phase**: In development of hard- and software, requirements based on the risk profile must be implemented. Developed mitigation aspects must support the organization's risk management strategy. **Integration & Recomposition phase**: testing in this phase must confirm the correct operations of mitigating functions developed based on contractual specifications. Resilience to risk in process chains is tested and proven during integration tests. **Operations & Maintenance phase**: periodical reviews of contract performance are input for proving the asset matches the risk profile as stated in the decomposition and definitions phase. This compliance is incorporated in the in-control statements on risk of the organization.	**For resilience/reliability**, risk management defines the boundaries for resilience, e.g. against what types of cyber attacks the SSB must be protected. Not all risk can be mitigated, and risk management defines what risk level is acceptable (risk appetite). The resilience of the asset is therefore directly derived from the overall risk management strategy of the organization. This leads to a clear agreement on what risks are present when normal operations of the SSB are performed. **In case of a threat**, risk management is referenced to assess if a threat is within the risk appetite or outside it. Threat assessment is performed in the context of the risk management strategy of an organization, e.g. the criticality of the asset combined with the likelihood of a threat is weighted against the resilience to the threat of the object in determining further action. **In case of an incident**, the risk management strategy is used as a context in which to evaluate action. In the analysis of an incident, if the cause is within the risk appetite, analysis is done on how mitigation failed. If the incident cause is outside the risk appetite but the incident effect was unacceptable, this can lead to a revision of the organizational risk appetite.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	• **CIS CSC** 4 • **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • **ISA 62443-2-1:2009** 4.3.4.2 • **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 • **NIST SP 800-53 Rev. 4** PM-9
				ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.2.6.5 • **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 • **NIST SP 800-53 Rev. 4** PM-9
				ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	• **COBIT 5** APO12.02 • **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 • **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established	**The decomposition and definition phase**: in this phase, right to audit, roles and responsibilities regarding risks are made explicit in contracts. The responsible parity for the asset (the organization) and the contractor(s) responsible for designing, building and maintenance of the asset have clear responsibilities regarding cybersecurity. It is acknowledged that the whole supply chain is an active party in addressing cybersecurity.	**For resilience/reliability**, it is important that risks are evaluated, known and mitigated across the supply chain. This will result in an increased asset resilience due to a uniform risk mitigation. If all parties in the supply chain mitigate against malware, the reliability of the SSB is increased through mitigation of that risk. Possible incidents are identified and dealt with more quickly due to clear roles and responsibilities known by all parties.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	• **CIS CSC** 4 • **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 • **ISA 62443-2-1:2009** 4.3.4.2 • **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
				ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and	• **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03

	and implemented the processes to identify, assess and manage supply chain risks.	**The implementation phase**: during implementation, audits and other assessments are performed to ensure secure design and building of OT and IT components. Agreements make clear what the roles and responsibilities are. **Integration & Recomposition phase**: testing on security requirements are performed on all levels, both unit/device and system validation level. Testing includes cybersecurity processes, procedures and role recognition of all stakeholders in the supply chain. **Operations & Maintenance phase**: contract management assesses if the roles, responsibilities, requirements and actions described in the contracts are performed as agreed. Auditing of supply chain partners are part of the periodical evaluation of contract performance.	**In case of a threat**, good control over risk in the supply chain ensures that the effect of a threat can be quickly assessed, and appropriate action taken. E.g. the audit results of a supplier gives insight into how vulnerable that supplier is to a threat. **In case of an incident**, due to clear roles and responsibilities reaction to, and recovery from, incidents is faster. Due to the resilience in the whole supply chain, propagating effects of an incident are reduced, e.g. the infection with malware at a supplier, will not likely propagate along the supply chain, due to the implementation of segmentation of networks stipulated as requirement in the contract for the asset.	assessed using a cyber supply chain risk assessment process	• **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 • **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
				ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the assetives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	• **COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 • **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 • **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 • **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
				ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	• **COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 • **ISA 62443-2-1:2009** 4.3.2.6.7 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
				ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	• **CIS CSC** 19, 20 • **COBIT 5** DSS04.04 • **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 • **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 • **ISO/IEC 27001:2013** A.17.1.3 • **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

Function	Category	Relevance In Systems Engineering	Threat states of Storm Surge Barriers	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**The decomposition and definition phase:** the requirements for the asset must explicitly define the roles and processes for identity and access management. It must be clear what the policies for access are, who regulates these, and who is responsible. This must be formalized in contracts leading to verifiable processes, procedures and access control lists. Risk management gives insight into the mitigation achieved by this category. There is recognition of the fact that physical and logical access management are connected, e.g. the physical access to a device by threat actors has impact on the logical access controls on that device. **The implementation phase:** in this phase, the policies are implemented. Verification of developed policies to strategic/tactical policies is recurrent to ensure compliance. During development, it is controlled who has access to information like source code. Need-to-know and need-to-use are core principles embedded in authorization matrices when designing system components.	**For resilience/reliability**, controlling access to systems of the asset is a very important factor in ensuring resilience and reliability. Access control limits the actions that can be performed by any single entity, decreasing the effect of stolen credentials on the asset operations. Core functions are strictly restricted to key personnel, increasing reliability of those functions. Resilience of the asset due to identity theft can be greatly increased by implementing two-factor authentication and controlled remote access as part of the identity management policies. **In case of a threat**, it can be determined which identities/locations are most at risk, and those identities/locations can be monitored more closely. The impact of threats is lowered if access and identity management limits the access to critical functions of the asset. Need-to-know implemented for identities limits the amount of knowledge threat actors can gather from a single source during the reconnaissance phase of an attack. **In case of an incident**, access to systems (logical and physical) is auditable and therefore is relatable to	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	• **CIS CSC** 1, 5, 15, 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
				PR.AC-2: Physical access to assets is managed and protected	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
				PR.AC-3: Remote access is managed	• **CIS CSC** 12 • **COBIT 5** APO13.01, DSS01.04, DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6 • **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15

	Integration & Recomposition phase: access provided through identities and credentials is tested across the integrated process. Elements like central user identity management solutions are tested for relevant situations, and logging and auditing of user actions is verified. Physical and logical access is tested rigorously, for instance through pentesting or red teaming. **Operations & Maintenance phase:** the commissioning and decommissioning of identities (due to personnel changes) is implemented and verified according to contractual performance parameters. Physical and logical access rights are reviewed periodically.	natural persons in case of an incident. This helps to quickly identify which identities are used at the cause of the incident. Because identities, access and devices are known, it can more easily be determined in case of an incident what processes, locations or asset functions are impacted. The chance of escalation of an incident is decreased because access is controlled and segregated. E.g. a stolen login will impact a certain system or location, but will not impact other systems or locations the person did not have access rights to.	**PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	• **CIS CSC** 3, 5, 12, 14, 15, 16, 18 • **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.7.3 • **ISA 62443-3-3:2013** SR 2.1 • **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 • **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
			PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	• **CIS CSC** 9, 14, 15, 18 • **COBIT 5** DSS01.05, DSS05.02 • **ISA 62443-2-1:2009** 4.3.3.4 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8 • **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
			PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	• **CIS CSC**, 16 • **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 • **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 • **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
			PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	• **CIS CSC** 1, 12, 15, 16 • **COBIT 5** DSS05.04, DSS05.10, DSS06.10 • **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 • **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**The decomposition and definition phase**: awareness by all parties must be addressed in the bid and security plan for the asset. The asset owner will set the desired awareness goals, that must be implemented by all parties involved with the asset. Awareness is an element of ensuring secure design, so awareness sessions must start at the earliest moment. Creating cyber awareness is a joint effort over the supply chain with parties helping and cooperating. Awareness is part of organizational culture, so it is advisable to include social scientific methods to address awareness.	**For resilience/reliability**, awareness is key for all personnel to realize what the impact of cyber risks are, and cooperate in the mitigation. Awareness of potential risks make attacks like phishing less likely. Possible issues are identified earlier when engineers who know the physical SSB known how cyber attacks can influence it. Social engineering techniques are less effective for cyber-aware SSB personnel. **In case of a threat**, awareness results in warnings to personnel result in personnel knowing what is expected of them (how to act on information). Personnel can	**PR.AT-1:** All users are informed and trained	• **CIS CSC** 17, 18 • **COBIT 5** APO07.03, BAI05.07 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 • **NIST SP 800-53 Rev. 4** AT-2, PM-13
			PR.AT-2: Privileged users understand their roles and responsibilities	• **CIS CSC** 5, 17, 18 • **COBIT 5** APO07.02, DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-3, PM-13
				• **CIS CSC** 17 • **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05

		The implementation phase: the effect of awareness in the preceding phase leads to security being addressed during implementation, e.g. security is explicitly mentioned and referenced. Questions by thought leaders and management during development show that security awareness is supported top-down.\ **Integration & Recomposition phase**:awareness can be verified by diverse testing methods like phishing tests, quizzes, conversations and simulated exercises. Awareness processes and programs are validated in this phase, focusing on individual organizational elements as well as supply chain processes and roles. **Operations & Maintenance phase**: awareness is periodically tested as in the previous phase. Management addresses this topic in regular meetings and personnel performance reviews. Management translates the need for awareness support from the asset to general security management roles to secure support and verify organizational alignment on awareness.	join in assessing the impact of a threat on a SSB creating a holistic threat assessment. Personnel who are aware of cyber threats can alert on deviations and suspicious events. **In case of an incident**, personnel on a SSB can recognize potential incidents in an earlier stage, facilitating a faster response. In incident analysis, the information provided by cyber-aware personnel is of a higher quality, increasing response time and quality.	**PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	• **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
			PR.AT-4: Senior executives understand their roles and responsibilities	• **CIS CSC** 17, 19 • **COBIT 5** EDM01.01, APO01.02, APO07.03 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-3, PM-13
			PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	• **CIS CSC** 17 • **COBIT 5** APO07.03 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**The decomposition and definition phase**: in the bid information, it must be made clear what confidentiality is attached to information. Access to sensitive information required for a bid must be facilitated in a controlled manner. Organizational classification schemes for information are part of the requirements of contractors. All documents in this phase are labelled with the correct classification marking, and instructions on how to classify documents are available to all stakeholders. If data security is supported by software like Digital Rights Management (DRM) solutions, the use of DRM by the supply chain partners must be assessed and implemented. **The implementation phase**: all information must be labelled and treated accordingly. It must be recognized that (PLC) configurations, manuals, source code and drawings are also information that needs to be labelled and protected. **Integration & Recomposition phase**: test data	**For resilience/reliability**, correct data security ensures that through labelling, everyone knows how to treat information. This helps with the correct protection, increasing resilience to the information leaking to unauthorized persons. The integrity of data is high through assurance by implementing the correct data security. This supports the quick recovery to known-good states of the asset after an incident. The information on systems and the data exchanged between systems is protected, ensuring reliability of operations. **In case of a threat**, integrity checking mechanisms can be an early waring is a threat is manifesting within the asset. Based on the threat, data classification can be used to identify the highest value information sets that should be monitored more closely. **In case of an incident**, data security supports a quick assessment of the impact, through identifying what type of information is compromised. Data security implements controls that limit the effect of an incident in altering data, e.g. limiting rights to alter large sets of data in a short period of time. This control will prevent	**PR.DS-1:** Data-at-rest is protected	• **CIS CSC** 13, 14 • **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 • **ISA 62443-3-3:2013** SR 3.4, SR 4.1 • **ISO/IEC 27001:2013** A.8.2.3 • **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
			PR.DS-2: Data-in-transit is protected	• **CIS CSC** 13, 14 • **COBIT 5** APO01.06, DSS05.02, DSS06.06 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
			PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• **CIS CSC** 1 • **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 • **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
			PR.DS-4: Adequate capacity to ensure availability is maintained	• **CIS CSC** 1, 2, 13 • **COBIT 5** APO13.01, BAI04.04

		can be confidential (e.g. real IP addresses, software settings, PII data), and must be protected like operational data. Protection is based on the data, not the action or environment in which its used (operational data is protected the same in an operational system as in a test system). **Operations & Maintenance phase**: the data classifications are continued during this phase. Classification is the basis for access and protection profiles.	that an event like ransomware will render large sets of data unavailable.		• **ISA 62443-3-3:2013** SR 7.1, SR 7.2 • **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 • **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
				PR.DS-5: Protections against data leaks are implemented	• **CIS CSC** 13 • **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 • **ISA 62443-3-3:2013** SR 5.2 • **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
				PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	• **CIS CSC** 2, 3 • **COBIT 5** APO01.06, BAI06.01, DSS06.02 • **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 • **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** SC-16, SI-7
				PR.DS-7: The development and testing environment(s) are separate from the production environment	• **CIS CSC** 18, 20 • **COBIT 5** BAI03.08, BAI07.04 • **ISO/IEC 27001:2013** A.12.1.4 • **NIST SP 800-53 Rev. 4** CM-2
				PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	• **COBIT 5** BAI03.05 • **ISA 62443-2-1:2009** 4.3.4.4.4 • **ISO/IEC 27001:2013** A.11.2.4 • **NIST SP 800-53 Rev. 4** SA-10, SI-7
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**The decomposition and definition phase**: organizational baselines and procedures are translated to requirements for the asset. These can include backup/recovery, change management processes, data deletion standards and Recovery Time Objectives. These tasks are aimed at embedding the desired information protection goals into bid, contract and design, as a (legal) basis during the lifecycle of the asset. Environments, datasets and procedures for testing procedures are defined. **The implementation phase**: the hardware/software development facilitates protection requirements, e.g. by documenting known-good baseline configurations, facilitating backup/recovery techniques, change control and documentation (both of systems and in code). **Integration & Recomposition phase**: procedures and processes like backup &	**For resilience/reliability**, because known-good situations exist, deviations that may lead to incidents are quickly detected and corrected through tested recovery procedures. In case of an incident, the processes and procedures ensure that a quick recovery to a known good situation is performed. Through testing and validation, the recovery times are known and are part of the operational specifications of the SSB. **In case of a threat**, the vulnerability plan is referenced to assess exposure. Existing recovery plans are assessed for effectiveness if the threat manifests itself. Additional backups can be made in a controlled manner and recovery procedures can be prepared for better response times (e.g. ordering the right backup components like tapes on premise to decrease reaction time in case of a recovery order). **In case of an incident**, recovery options are known and decisions to execute a recovery can be made by	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	• **CIS CSC** 3, 9, 11 • **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
				PR.IP-2: A System Development Life Cycle to manage systems is implemented	• **CIS CSC** 18 • **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 • **ISA 62443-2-1:2009** 4.3.4.3.3 • **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 • **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
				PR.IP-3: Configuration change control processes are in place	• **CIS CSC** 3, 11 • **COBIT 5** BAI01.06, BAI06.01 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6

	recovery of systems are tested. Likely scenarios are tested and results are reported to responsible management for review. Scenario based working can support testing of processes. Actions like recovery of units are evaluated as having effects on the complete process chain to ensure that cascading effects are known and managed. **Operations & Maintenance phase**: periodical tests of processes and procedures are performed to verify their effectiveness. During changes in the SSB, the backup & recovery procedures are referenced. These processes and procedures are maintained as part of the lifecycle of the asset.	management with a high level of confidence. Personnel have practices the recovery procedures, increasing the chance of successful recovery.		• **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
			PR.IP-4: Backups of information are conducted, maintained, and tested	• **CIS CSC** 10 • **COBIT 5** APO13.01, DSS01.01, DSS04.07 • **ISA 62443-2-1:2009** 4.3.4.3.9 • **ISA 62443-3-3:2013** SR 7.3, SR 7.4 • **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 • **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
			PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
			PR.IP-6: Data is destroyed according to policy	• **COBIT 5** BAI09.03, DSS05.06 • **ISA 62443-2-1:2009** 4.3.4.4.4 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 • **NIST SP 800-53 Rev. 4** MP-6
			PR.IP-7: Protection processes are improved	• **COBIT 5** APO11.06, APO12.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 • **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
			PR.IP-8: Effectiveness of protection technologies is shared	• **COBIT 5** BAI08.04, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
			PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	• **CIS CSC** 19 • **COBIT 5** APO12.06, DSS04.03 • **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 • **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
			PR.IP-10: Response and recovery plans are tested	• **CIS CSC** 19, 20 • **COBIT 5** DSS04.04 • **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.17.1.3 • **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
			PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	• **CIS CSC** 5, 16 • **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4

					• **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
				PR.IP-12: A vulnerability management plan is developed and implemented	• **CIS CSC** 4, 18, 20 • **COBIT 5** BAI03.10, DSS05.01, DSS05.02 • **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 • **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**The decomposition and definition phase**: agreement on maintenance processes are stipulated in the bid and contracts, including roles, documentation and repair metrics (time, cost, periodicity). Approved tools and equipment is defined. **The implementation phase**: secure options for remote maintenance and logging of maintenance activities is built in during development. E.g. software or configurations can be maintained through use of secure third party access terminals in use by the organization. Physical access to equipment is logged and monitored according to agreed upon procedures. **Integration & Recomposition phase**: maintenance procedures are tested using real-world scenarios. Both predicted maintenance (e.g. firmware update) and unexpected maintenance (e.g. failure of a PLC) are tested and validated. **Operations & Maintenance phase**: maintenance performed is evaluated and monitored. Deviations from procedures are logged and addressed.	**For resilience/reliability**, maintenance introduces changes in a SSB. If these changes are controlled and done securely, the chance of a change negatively impacting the operational reliability is low. Because maintenance is implemented securely, the chance is low that maintenance procedures are abuse by attackers to affect an SSB (e.g. unauthorized access through remote maintenance interfaces). **In case of a threat**, maintenance procedures can be assessed for vulnerability and more closely watched or halted in response. Because maintenance of the SSB is known and controlled, that process is likely to lead to being used as an attack path.E.g. if the secured remote SSB maintenance workstation only can be used by certain persons after a work order is received, that workstation is resilient to misuse by a threat actor. **In case of an incident**, maintenance procedures ensure that a secure process of recovering/repairing from the incident is possible. Documented maintenance procedures are easier to correct than casual processes. Contractual agreements on maintenance procedures are a basis for analyzing who is the party at fault for the cause of an incident if the incident is maintenance related.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	• **COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 • **ISA 62443-2-1:2009** 4.3.3.3.7 • **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 • **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
				PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• **CIS CSC** 3, 5 • **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 • **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 • **NIST SP 800-53 Rev. 4** MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**The decomposition and definition phase**: security policies like hardening, encryption requirements and treatment of removable media are included in the requirement specifications of the asset, so the contractor can describe how these policies are embedded in the design, build and maintenance of the asset. Requirements for logging, including definitions on what the results should be of the logging, are defined and included in the design on all levels. Protection of data-in-transit and data-at-rest is defined as a basis for implementing controls in the design of the asset.	**For resilience/reliability**, logging and auditing support the assurance level that the right security measures are taken and work. Logs are a valuable source in detecting anomalies, regardless of the cause. Therefore, logs help early detection of potential incidents. By implementing least functionality, the resilience of a SSB increases by limiting the number of functionalities that could be exploited. It also keeps configurations and processes more simple, supporting the early detection of deviations. Because communications and computing components are hardened, an attacker has a limited attack surface, increasing resilience and reliability. **In case of a threat**, logs can be analyzed more closely,	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	• **CIS CSC** 1, 3, 5, 6, 14, 15, 16 • **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 • **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • **NIST SP 800-53 Rev. 4** AU Family
				PR.PT-2: Removable media is protected and its use restricted according to policy	• **CIS CSC** 8, 13 • **COBIT 5** APO13.01, DSS05.02, DSS05.06 • **ISA 62443-3-3:2013** SR 2.3 • **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9

		The implementation phase: solutions are built according to agreed upon security policies. When configuring design elements, the principle of least functionality is applied, and the documentation must describe why functions are needed. logging is implemented in a way to not only give insight into the specific element generating the log, but it must be possible to aggregate the logs (e.g. a SIEM or logserver) to enable a analytic view of the complete system. **Integration & Recomposition phase**: Configurations must be reviewed to test the implementation of least functionality. Logs are tested to evaluate the specified goals as described in the contract. Logs are evaluated on unit and system level for usability and integration with e.g. a SIEM or logserver. Resilience of the system is tested, e.g. with real-world scenarios for normal and adverse situations. **Operations & Maintenance phase**: the usability of logs is evaluated during operations for instance by the engineering team and SOC. Adherence to security requirements are evaluated as part of the contract management process. For any maintenance, the impact on security policies is part of the preparation for changes.	based on the specific threat, e.g. if a threat targets a specific PLC, that PLC can be monitored more closely by analyzing its logs and defining detectors for indicators-of-compromise. **In case of an incident**, logs provide an excellent source to analyze the cause of the incident, supporting a faster remediation. Cascading effects of an incident, e.g. an attacker moving around in a network, can be analyzed more accurately. Log aggregation provides a quick assessment of effects of an incident on a SSB as a whole. By implementing least functionality, the possible sources of an incident is reduced, making the forensic process of finding a root-cause easier.		· **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
				PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	· **CIS CSC** 3, 11, 14 · **COBIT 5** DSS05.02, DSS05.05, DSS06.06 · **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 4** AC-3, CM-7
				PR.PT-4: Communications and control networks are protected	· **CIS CSC** 8, 12, 15 · **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
				PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	· **COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 · **ISA 62443-2-1:2009** 4.3.2.5.2 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
Function	**Category**	**Relevance In Systems Engineering**	**Threat states of Storm Surge Barriers**	**Subcategory**	**Informative References**
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**The decomposition and definition phase**: security events must be analyzed by professionals, knowledgeable in the field of engineering, e.g. a skilled SOC. The requirements to integrate with organization's SOC are embedded in the requirements for the asset. E.g. logfile format, incident thresholds, use of network sensors and (incident)process procedures. Events that must be detected are defined, including their impact. Unit monitoring is derived from the event definitions to support detection. In the design phase, a design for the normal operational baseline is drafted.	**For resilience/reliability**, the SOC and SSB operations both monitor the SSB for unwanted and/or unexpected behavior, so possible incidents are detected early in the attack process, increasing the chance of preventing an incident. Attacker activity is detected in a much earlier phase with monitoring and well-defined baseline operations. Network traffic is a prime candidate that can yield information on the normal operations of an SSB. Monitoring based on network traffic must not impact normal operations of the SSB. Processes supporting detection ensure that the correct roles are part of the handling of potential incidents. When recovering, the normal network traffic can be used to determine if normal operations is achieved, supporting	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	· **CIS CSC** 1, 4, 6, 12, 13, 15, 16 · **COBIT 5** DSS03.01 · **ISA 62443-2-1:2009** 4.4.3.3 · **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
				DE.AE-2: Detected events are analyzed to understand attack targets and methods	· **CIS CSC** 3, 6, 13, 15 · **COBIT 5** DSS05.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4

		The implementation phase: the operational baseline (known good configuration) of units comprising the asset are finalized and documented. Means for detection (e.g. log shipping or sensor integration in networks) are part of the implementation of hard- and software. Processes and role descriptions are finalized, and relevant personnel is trained. **Integration & Recomposition phase**: logs are tested to evaluate the specified goals as described in the contract. Logs are evaluated on unit and system level for usability and integration with e.g. a SIEM or logserver. Procedures and processes are tested for effectiveness in real-world scenarios. **Operations & Maintenance phase**: a SOC monitors the asset as a whole, supporting the monitoring by operational management. These are two separate lines of defense in detecting unwanted behavior in the asset. Procedures to integrate the monitoring of the asset are practiced and reviewed periodically. Multi disciplinary meetings (e.g. cybersecurity, crisis management and asset operations) test and discuss procedures and evaluate these after an incident or significant change. Documentation regarding baseline configurations and monitoring are maintained to ensure correctness.	assurance levels and the quick return to normal operations. **In case of a threat**, logs can be analyzed more closely, based on the specific threat, e.g. if a threat targets a specific PLC, that PLC can be monitored more closely by analyzing its logs and defining detectors for indicators-of-compromise. Threat alerts are processed according to well defined processes, ensuring that all relevant roles are alerted in time, e.g. operational managers of the SSB know if the threat level by terrorism is raised through established channels to threat management. **In case of an incident**, monitoring increases the chance of early detection and analysis of incidents, including its cause. The corrects actions can be taken quickly due to predefined processes and thresholds in those processes. This ensures that the incident is handled as 'normal operations' without panic and ad hoc decisions. Analysis of incidents identifies points that need improvement in a learning organization.Event logs are used for mandatory reporting to authorities and for sharing in information sharing platforms like ISACs.	**DE.AE-3:** Event data are collected and correlated from multiple sources and sensors	• **CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 • **COBIT 5** BAI08.02 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
				DE.AE-4: Impact of events is determined	• **CIS CSC** 4, 6 • **COBIT 5** APO12.06, DSS03.01 • **ISO/IEC 27001:2013** A.16.1.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
				DE.AE-5: Incident alert thresholds are established	• **CIS CSC** 6, 19 • **COBIT 5** APO12.06, DSS03.01 • **ISA 62443-2-1:2009** 4.2.3.10 • **ISO/IEC 27001:2013** A.16.1.4 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**The decomposition and definition phase**: roles and responsibilities regarding detection are defined, e.g. who is responsible for monitoring of what components. The procedures for scanning and monitoring are formalized, because of their possible impact on normal operations of the asset. E.g. the organization is allowed to scan, but after consultation with the asset manager and an impact analysis. (Sub) contractors agree to waivers that personnel activity can be monitored (both digital and physically). Relevant legal requirements like the GDPR are referenced and agreements are legally sound. Contracts stipulate what is monitored and to what purpose. A process for changing requirements for monitoring is agreed upon. What data is fed back to the asset owner organization is defined (e.g. for analysis in a central SOC).	**For resilience/reliability**, the SOC and SSB operations both monitor the SSB for unwanted and/or unexpected behavior, so possible incidents are detected early in the attack process, increasing the chance of preventing an incident. Attacker activity is detected in a much earlier phase with monitoring and well-defined baseline operations. Network traffic is a prime candidate that can yield information on the normal operations of an SSB. Monitoring based on network traffic must not impact normal operations of the SSB. Transgressions (not always malicious or intentional!) by personnel are detected and can be addressed. Monitoring an SSB for (cyber)security events gives insight into the likeliness the SSB will perform its function. Monitoring a SSB and controlling which code and devices have access gives a strong signal to attackers and personnel by raising the cost of a successful attack. **In case of a threat**, logs can be analyzed more closely,	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	• **CIS CSC** 1, 7, 8, 12, 13, 15, 16 • **COBIT 5** DSS01.03, DSS03.05, DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
				DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	• **COBIT 5** DSS01.04, DSS01.05 • **ISA 62443-2-1:2009** 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 • **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
				DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	• **CIS CSC** 5, 7, 14, 16 • **COBIT 5** DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
				DE.CM-4: Malicious code is detected	• **CIS CSC** 4, 7, 8, 12

		The implementation phase: monitoring is implemented, both logically (software, AV scanners, network sensors, access logs) and physically (camera placement, door alarms, room sensors). During implementation, the personnel implementing the measures are aware of the sensitive nature of their activities and protect the information (manuals, procedures, configurations) accordingly. Segmentation of networks and physical spaces is implemented, and zone boundaries are monitored. Lists of authorized personnel, software code, applications, devices, etc. are compiled and maintained in the AMS (see: ID.AM). Relevant personnel is trained in all monitoring measures implemented (both operating the monitoring equipment, and performing detective activities). **Integration & Recomposition phase**: during testing, monitoring is verified during test scenarios that represent normal and expected abnormal scenarios. Procedures for responding to unknown events are practiced. The operating baseline is established so a 'known good' situation is agreed upon. This baseline is the reference for detecting anomalies. Integration with organization wide monitoring (e.g. a organizational SOC) is verified. **Operations & Maintenance phase**: the asset is monitored, and events are processed according to agreed upon processes. New developments and events that lead to alterations in the monitoring of the asset are processed according to agreed change management procedures. Periodical testing is performed to evaluate the correct functioning of the monitoring function.	based on the specific threat, e.g. if a threat targets a specific PLC, that PLC can be monitored more closely by analyzing its logs and defining detectors for indicators-of-compromise. Allowed actions, both digital and physical can be managed and verified through monitoring. Adding capacity for monitoring and analysis can reduce the chance of a threat manifesting itself into an incident by increasing early detection. Specific scanning for vulnerabilities used in the threat are used to assess exposure to that threat (e.g. scanning for vulnerable SMB implementations to assess exposure to NotPetya malware). **In case of an incident**, monitoring increases the chance of early detection and analysis of incidents, including its cause. The corrects actions can be taken quickly and effectiveness of actions can be assessed based on monitoring (e.g. did the anomalous network traffic stop after the isolation of a PLC? Did the malfunctions stop after denying access to the server room to certain personnel?). Analysis of incident logs identifies points that need improvement in a learning organization. Detection of unknown code or devices can quickly identify if proper change procedures were followed.		· **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.3.4.3.8 · **ISA 62443-3-3:2013** SR 3.2 · **ISO/IEC 27001:2013** A.12.2.1 · **NIST SP 800-53 Rev. 4** SI-3, SI-8
			DE.CM-5: Unauthorized mobile code is detected	· **CIS CSC** 7, 8 · **COBIT 5** DSS05.01 · **ISA 62443-3-3:2013** SR 2.4 · **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 · **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
			DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	· **COBIT 5** APO07.06, APO10.05 · **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
			DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	· **CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 · **COBIT 5** DSS05.02, DSS05.05 · **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
			DE.CM-8: Vulnerability scans are performed	· **CIS CSC** 4, 20 · **COBIT 5** BAI03.10, DSS05.01 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**The decomposition and definition phase**: the bid and contract define the responsibilities for detection and processes involved. Integration with organization internal detection roles, processes and procedures are part of the design. In the design of all levels, attention is given to evaluating what detection activities will be relevant. The process description includes the confidentiality aspect of detection information	**For resilience/reliability**, detection of anomalous events is key to early mitigation or prevention of possible incidents. Detection is not limited to active malicious actions by 'hackers', but can also signal misconfigurations, not following procedures or faulty equipment. Early detection of anomalies lower the chance of an SSB malfunctioning by enabling quick response and return to normal operations. Detection also helps to quickly identify the source of possible	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	· **CIS CSC** 19 · **COBIT 5** APO01.02**,** DSS05.01, DSS06.03 · **ISA 62443-2-1:2009** 4.4.3.1 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
			DE.DP-2: Detection activities comply with all applicable requirements	· **COBIT 5** DSS06.01, MEA03.03, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3

		to ensure proper handling of sensitive event information. **The implementation phase**: The designed detection activities are implemented, and during development the developers know how to route detection alerts to relevant systems (e.g. a SIEM or logserver). **Integration & Recomposition phase**: detection activities are defined, and during scenario based testing, the completeness of the detection design is validated (do we detect the right alerts, and are relevant activities detected in a proper and timely manner). **Operations & Maintenance phase**: detection activities are performed as specified in the contract, and contract management verifies this. Incident evaluations include an analysis of the detection process, and creates a feedback loop to adjust the detection processes and activities to the changing risk environment.	faulty behavior, reducing the time needed to troubleshoot a (possible) incident. **In case of a threat**, detection can be adjusted to flag activities that are associated with a threat. This enables the quick detection of a threat manifesting itself in an SSB. **In case of an incident**, detection enables the quick detection of the offending (sub) system in an SSB, enabling isolation of the attacker or malfunction. This prevents of degrades the escalation of an incident, reducing the impact. In incident evaluation, improvements on detection are addressed.		• **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
				DE.DP-3: Detection processes are tested	• **COBIT 5** APO13.02, DSS05.02 • **ISA 62443-2-1:2009** 4.4.3.2 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.14.2.8 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
				DE.DP-4: Event detection information is communicated	• **CIS CSC** 19 • **COBIT 5** APO08.04, APO12.06, DSS02.05 • **ISA 62443-2-1:2009** 4.3.4.5.9 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 • **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
				DE.DP-5: Detection processes are continuously improved	• **COBIT 5** APO11.06, APO12.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Function	Category	Relevance In Systems Engineering	Threat states of Storm Surge Barriers	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**The decomposition and definition phase**: reference internal organizational crisis and response plans as requirement for process integration. **The implementation phase**: integration with organizational response planning is finalized. **Integration & Recomposition phase**: response plans are tested, both for the asset as including organization wide response. **Operations & Maintenance phase**: responses are handled in accordance with the defined process and procedures. Incident analysis processes assess the adequacy of the response process and will improve if necessary.	**For resilience/reliability**, a good response plan will prepare operators and cyber responders to respond to SSB incidents in a correct and timely manner, reducing possible downtime and operational impact. **In case of a threat**, response plans can be reviewed to further increase readiness for an incident. The response can be evaluated against the specific threat for effectiveness. Plans are prepared for immediate use. **In case of an incident**, the response plan ensures a correct and timely reaction to the cybersecurity incident by all SSB staff. E.g. when an incident occurs, the SSB operator opens the response plan (printed in a binder of electronically) and executes it.	**RS.RP-1:** Response plan is executed during or after an incident	• **CIS CSC** 19 • **COBIT 5** APO12.06, BAI01.10 • **ISA 62443-2-1:2009** 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**The decomposition and definition phase**: clear requirements are defined for the interaction between the asset and the asset owner organization. E.g. when (and who) to inform a SOC, crisis manager, asset owner, etc. Legal requirements for incident reporting (like the EU NIS directive) are defined in contracts.	**For resilience/reliability**, information sharing within I-STORM helps to increase resilience in the communicate as a whole because participants learn from each other (one incident can benefit resilience in the whole community). The SSB itself is more resilient, because personnel	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	• **CIS CSC** 19 • **COBIT 5** EDM03.02, APO01.02, APO12.03 • **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
					• **CIS CSC** 19 • **COBIT 5** DSS01.03

		The implementation phase: incidents during development are reported, but due to limited operational impact may be handled in a less urgent matter. Best practices for implementation of cybersecurity are explored at information sharing communities. Personnel is instructed/trained in incident response so they know their role and how to act. **Integration & Recomposition phase**: response processes and procedures are tested to validate all personnel know their role and how to act. Integration of the response procedures and processes are validated. Findings/experiences may be presented in information sharing communities to gather advise and to share experience. **Operations & Maintenance phase**: policy for continued awareness and training for proper response are performed. During incidents, the response activities are according to the plans. In incident evaluation, response communication is addressed.	know how to act and share information when a response is needed. This improves the assurance that if an incident occurs, the return to normal operations is as efficient and effective as possible. **In case of a threat**, experience with similar threats within I-STORM will help a proper response. Because it's defined in PR.DS what information can be shared with what parties in the response plan, sharing that information internally and externally can be more easily be performed. Incidents at one SSB can be input for a threat warning to other SSBs (within a community). **In case of an incident**, the processes and procedures for communicating during a response leave little room for unclarity, resulting in an efficient and effective response to (cyber) incidents. E.g. the SOC advises a plan of action to mitigate the incident, the SSB operator is part of the evaluation of that action plan and advises on its execution. The SSB manager directs a subcontractor to implement the response action plan. This process is pre-defined and therefore can be executed quickly because all parties know their role and responsibilities.	**RS.CO-2:** Incidents are reported consistent with established criteria	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
				RS.CO-3: Information is shared consistent with response plans	• **CIS CSC** 19 • **COBIT 5** DSS03.04 • **ISA 62443-2-1:2009** 4.3.4.5.2 • **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
				RS.CO-4: Coordination with stakeholders occurs consistent with response plans	• **CIS CSC** 19 • **COBIT 5** DSS03.04 • **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** Clause 7.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
				RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	• **CIS CSC** 19 • **COBIT 5** BAI08.04 • **ISO/IEC 27001:2013** A.6.1.4 • **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**The decomposition and definition phase**: responsibilities for analysis of events are defined. Analysis of events takes specific knowledge, so agreements must be reached in case of outsourcing. The organizational SOC may play a leading role in defining the analysis goals, process and procedures. The risk appetite of the organization influences to what extend analysis must be performed. Forensics and analysis cost valuable resources, so a strict definition is advised on what aspects, assets and events are to be analyzed in detail (response categories). The analysis requirements are formalized in thresholds, asset characteristics, etc. in the contract. **The implementation phase**: requirements for detection and monitoring are translated to design specifications for e.g. logs. Personnel is trained for the tasks of detection and analysis. Processes are designed for detection and analysis, including integration with	**For resilience/reliability**, analysis of security events detected by monitoring will give a very good view on the possible incidents that can impact SSB operations. This enables a proactive stance towards cyber incidents making the SSB more resilient to attackers. The return to normal operations is supported if it is precisely known wheat the cause of the incident was. Analysis will support a high level of assurance that normal operations is resumed by the absence of security events. **In case of a threat**, if a good forensics function is known to exist for a SSB, this can be a deterrent for attackers because they know the chance is high the attack is mitigated and legal prosecution against the attacker is successful. Detection and analysis threat indicators can be shared with national information sharing organizations like the NCSC of international partners like select I-STORM participants. Sharing indicators of compromise between organizations is a proven method of sharing threat intelligence. **In case of an incident**, the analysis function helps to	**RS.AN-1:** Notifications from detection systems are investigated	• **CIS CSC** 4, 6, 8, 19 • **COBIT 5** DSS02.04, DSS02.07 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
				RS.AN-2: The impact of the incident is understood	• **COBIT 5** DSS02.02 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4
				RS.AN-3: Forensics are performed	• **COBIT 5** APO12.06, DSS03.02, DSS05.07 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 • **ISO/IEC 27001:2013** A.16.1.7 • **NIST SP 800-53 Rev. 4** AU-7, IR-4
				RS.AN-4: Incidents are categorized consistent with response plans	• **CIS CSC** 19 • **COBIT 5** DSS02.02 • **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISO/IEC 27001:2013** A.16.1.4

		organizational processes and procedures. Software and other means to perform analysis (like a forensic workstation) are developed or purchased. **Integration & Recomposition phase**: using scenario's, the skills, roles, processes and procedures are tested for the analysis function of the asset. Results are assessed against the defined goals in the contract. **Operations & Maintenance phase**: analysis and detection is evaluated regularly. Incidents are supported by the analysis function, and in evaluation of an incident, the performance of the analysis function is part of the assessment (RS.IM).	identify the cause of the incident, supporting the mitigation. E.g. the presence of malware in a PLC software image will lead to a quick restore of that PLC software to a known good configuration (PR.IP). Forensics help to identify the cause, supporting the taking of legal action.		• **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
				RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	• **CIS CSC** 4, 19 • **COBIT 5** EDM03.02, DSS05.07 • **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**The decomposition and definition phase**: requirements for the return of normal operations after an incident must be translated to requirements for mitigation of cyber incidents. If the downtime of an asset is 10 hours, the downtime and mitigation of cyber incidents must fit into this time window. Next to these requirements, the roles and responsibilities must be made explicit, so it is known who is responsible for meeting the recovery deadline. **The implementation phase**: the principle of least-privilege is used to guide implementation. This ensures that all components only have the necessary connections to other components, which reduces the chance of the impact of an incident. Correct documentation of implementations is created to safeguard retention of knowledge about each component. **Integration & Recomposition phase**: incident mitigation is tested by reviewing documentation and simulating incidents. Both the process/procedures and documentation is assessed on enabling the correct mitigation in the event of an incident. **Operations & Maintenance phase**: documentation and procedures support incident mitigation. Processes give insight into the mitigation and results of incident mitigation are assessed to verify all incidents are known and treated according to the formal requirements.	**For resilience/reliability**, the assurance that all incidents are mitigated and containment of incidents is feasible, will lead to a more resilient system. The right incident mitigation will lead to a higher assurance level that SSB operations can meet the specified levels. **In case of a threat**, the list of known and accepted vulnerabilities can be evaluated against the threat and mitigated if it will lead to an incident given the new threat. The SSB manager knows what the incident mitigation capabilities are, giving assurance on continued operations in the face of the threat. **In case of an incident**, incident handling is embedded in processes and procedures (RS.RP), that will support the mitigation of incidents. If least-privilege is implemented correctly, the expansion of an incident (like malware or a hacker) will be slower, giving more time and ability to isolate the incident. Isolation of incidents will decrease the impact on SSB operations. By mitigating all incidents, SSB operations can be guaranteed to the specified level of confidence (assurance).	**RS.MI-1:** Incidents are contained	• **CIS CSC** 19 • **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 • **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
				RS.MI-2: Incidents are mitigated	• **CIS CSC** 4, 19 • **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 • **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
				RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	• **CIS CSC** 4 • **COBIT 5** APO12.06 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
					• **COBIT 5** BAI01.13

	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**The decomposition and definition phase**: the organizational learning process is referenced, so asset processes utilize and extend existing processes. Responsibilities for communicating and safeguarding lessons learned are defined. **The implementation phase**: lessons learned from other assets are used to improve the current implementation. **Integration & Recomposition phase**: lessons learned from validation at other assets are used to improve the current implementation. E.g. scenarios are reused. **Operations & Maintenance phase**: lessons learned and best practices form the core of operations, not only ensuring efficiency/effectiveness, but also to provide a baseline of operations for all assets. This supports a uniform way of working between assets.	**For resilience/reliability**, creating a learning feedback loop will help to improve SSB resilience by learning from incidents at other SSB (internally or externally). I-STORM is a community in which this learning aspect is possible. Based on experiences, shared challenges can be explored and addressed, increasing not only the SSB resiliency, but also that of other SSBs operated within the community. **In case of a threat**, experiences of past threat response help to formulate an approach. Basing an approach on proven actions helps to create confidence on the approach with all stakeholders. **In case of an incident**, past experiences help to act more efficient and effective for a new incident. Lessons learned that are shared within or outside the organization help to optimize response to incidents at other SSBs in the future.	**RS.IM-1:** Response plans incorporate lessons learned	• **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6, Clause 10 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
				RS.IM-2: Response strategies are updated	• **COBIT 5** BAI01.13, DSS04.08 • **ISO/IEC 27001:2013** A.16.1.6, Clause 10 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
Function	**Category**	**Relevance In Systems Engineering**	**Threat states of Storm Surge Barriers**	**Subcategory**	**Informative References**
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**The decomposition and definition phase**: roles, responsibilities and procedures for recovery are defined and formalized. Acceptable recovery times are based on asset performance requirements. **The implementation phase**: recovery plans are compiled for each component and integration level. **Integration & Recomposition phase**: recovery plans are tested using scenarios. **Operations & Maintenance phase**: recovery plans are known and accessible for use in case of an incident.	**For resilience/reliability**, recovery plans ensure a controlled approach to restoring normal operations. Because a response is formalized, the quality of actions is increased through the efficient and effective response. Ensuring the recovery plan is in place and ready for use reduces the time needed for restoring operations **In case of a threat**, recovery plans can be reviewed and made ready for execution. **In case of an incident**, the recovery plan is executed by the correct personnel. E.g. in case of a hack of an SSB system, the operations manager executes the recovery plan instead of ad hoc responses to the incident.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	• **CIS CSC** 10 • **COBIT 5** APO12.06, DSS02.05, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**The decomposition and definition phase**: the lifecycle of procedures and processes like the recovery plans, are defined in the requirements phase, ensuring the correct responsibility and tasks are performed for maintaining a correct recovery plan during the asset lifecycle.	**For resilience/reliability**, by incorporating lessons learned in a structural way into recovery plans, every incident (both inside and outside the organization), will improve the resilience. Recovery plan execution at other SSBs can teach other organizations on how to improve their own recovery plans. Sharing lessons learned within I-STORM can be evaluated, based on	**RC.IM-1:** Recovery plans incorporate lessons learned	• **COBIT 5** APO12.06, BAI05.07, DSS04.08 • **ISA 62443-2-1:2009** 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6, Clause 10 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
				RC.IM-2: Recovery strategies are updated	• **COBIT 5** APO12.06, BAI07.08 • **ISO/IEC 27001:2013** A.16.1.6, Clause 10

		The implementation phase: the recovery plan is developed, incorporating lessons learned from other assets and past experience, both inside and outside the organization. **Integration & Recomposition phase**: the feedback of lessons learned into recovery processes and procedures is validated, e.g. in incident response scenario testing. **Operations & Maintenance phase**: recovery plans are updated in response to organizational en environmental changes (like new operating standards or changing organizational structure). After every incident, the lessons learned are processed into a new version of the recovery plan.	the sensitivity of data and other aspects influencing information sharing. **In case of a threat**, an assessment can be made of how other organizations have handled the threat, which feeds back into the organization's own recovery plan. E.g. if an I-STORM member is faced with the threat of flooding of a control room, other members that have dealt with that threat as an incident can help to improve the recovery plan. **In case of an incident**, the recovery plan is executed, and in the analysis afterwards, lessons learned are identified and processed into a new version of the recovery plan. E.g. during the incident, there was confusion on who can give the OK to replace a component. In the next version of the recovery plan, these roles are more explicitly defined.		· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**The decomposition and definition phase**: the coordinating roles in case of recovery are defined, preventing any uncertainty when it needs to be executed. This role will coordinate who communicates with whom and when. Communication professionals (e.g. a PR department or crisis communications) have a role in the recovery process. The communication aspects of the asset recovery	**For resilience/reliability**, including all relevant stakeholders in the recovery process acknowledges the interdependent nature of SSB operations. E.g. when the power or internet is down, this has an effect on the SSB, but a misfunctioning SSB has effects on society as well. By supporting the good communication during recovery, the cascade effects can be managed better, increasing the resiliency of both the SSB as dependent systems. The public trust in the resiliency can be impacted in case of an incident, so managing the correct public image of a SSB is important to the trust	**RC.CO-1:** Public relations are managed	· **COBIT 5** EDM03.02 · **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
				RC.CO-2: Reputation is repaired after an incident	· **COBIT 5** MEA03.02 · **ISO/IEC 27001:2013** Clause 7.4
				RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	· **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** Clause 7.4

		plan interface with organizational processes like crisis communications, social media teams, etc. **The implementation phase**: process design includes communication professionals to ensure the interfacing with broader communication processes. Dependencies on other organizations and departments are included in the design of the processes. These references might include roles, contact information, what asset systems are dependent, etc. E.g. a stakeholder and dependency map is made for the asset, giving overview of all roles and organizations relevant in a recovery process. Attention is given to keeping these details current during the lifecycle of the asset. **Integration & Recomposition phase**: communications are tested, e.g. response times and contact information of other organizations are validated by calling the contact numbers and validating their correctness and if the other party knows what role they have in the recovery process. **Operations & Maintenance phase**: contact details and roles are maintained as organizations change (personnel changes, numbers change, etc.). During the execution of recovery plans, the communication between the parties proceeds according to the recovery plan, there is coordination (responsible role is detailed in the plan as well) on not deviating from the plan. The PR aspects are addressed to manage the public trust in the asset.	of the public. **In case of a threat**, notifying partners defined in the recovery plan to be alert, will improve response times in the supply chain. E.g. when the threat of the hacking of a certain system is increased, the SSB operator may inform partners downstream (like a port of local water management authority) of this fact and what actions are taken by the SSB. Thus ensuring that those parties can respond quicker if the threat leads to an incident, and maintaining the image of dependability and predictability of SSB operations. **In case of an incident**, the recovery plan correctly addresses all SSB partners that need to be notified. The impact on the public image of the SSB is evaluated, and PR actively plays a role in shaping the public image of the incident. This task may be part of the crisis management process of the organization. If not. the managing of the public image must be implemented for the SSB within the SSB organization		• **NIST SP 800-53 Rev. 4** CP-2, IR-4

9.5 Confidential Appendix 5; Interview results

This appendix is confidential and therefore not included in this document. This appendix is available as separate document to need-to-know readers.

9.5.1 Interviewee 1, exploratory interview

Confidential

9.5.2 Interviewee 2, exploratory interview

Confidential

9.5.3 Interviewee 1, validation interview

Confidential

9.5.4 Interviewee 2, validation interview

Confidential

9.5.5 Interviewee 3, validation interview

Confidential

9.5.6 Interviewee 4, validation interview

Confidential