University of South-Eastern Norway

Faculty of Technology, Natural Sciences and Maritime Sciences

CS5000 - Master's Thesis

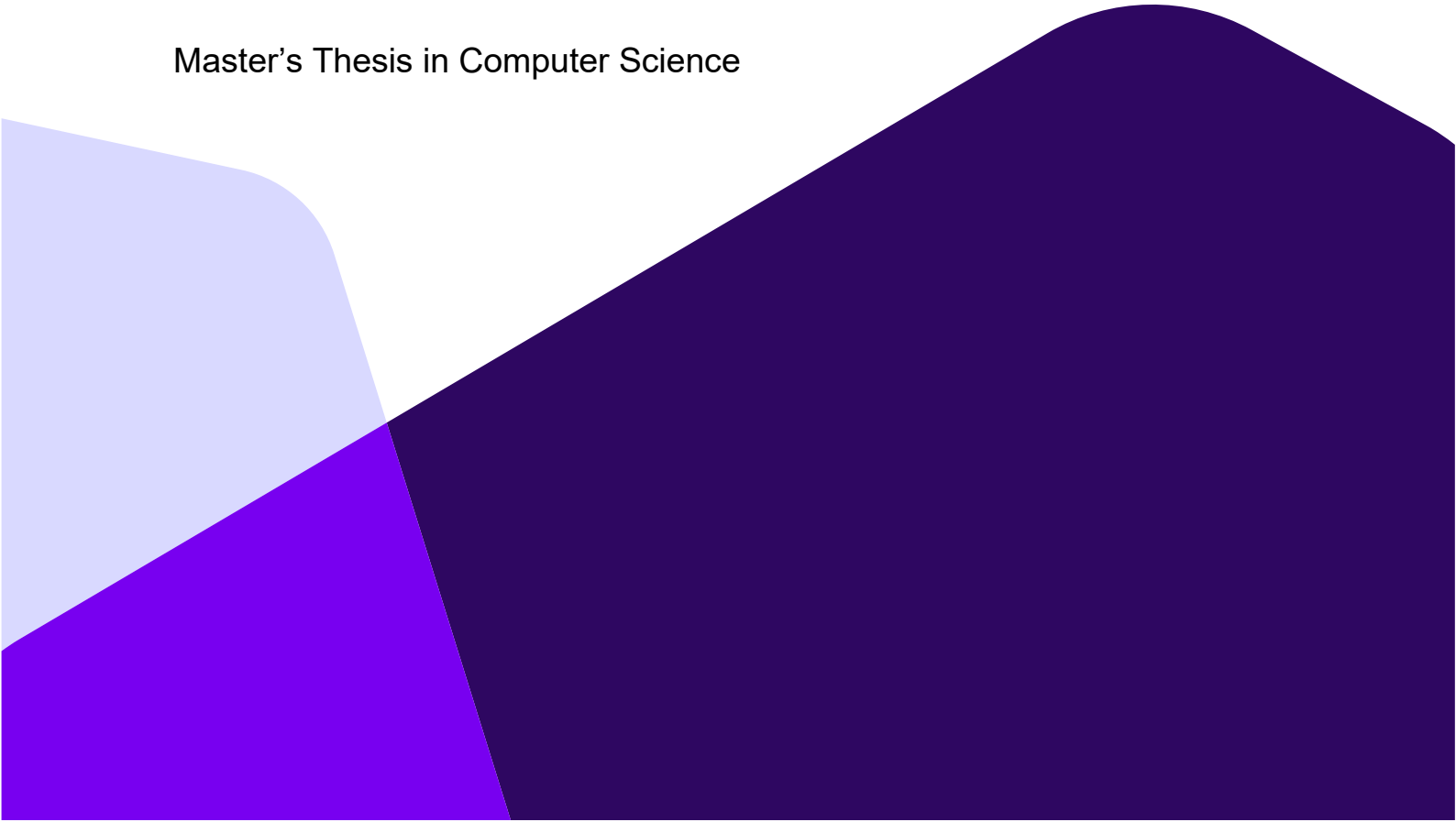
Study programme: MACSI

Spring 2024

Borgny Louise Gløersen / 8501

Developing a Cyber Security Documentation Package for Project Deliveries

Master’s Thesis in Computer Science



University of South-Eastern Norway
Faculty of Technology, Natural Sciences and Maritime Sciences
Department of Science and Industry systems
PO Box 235
NO-3603 Kongsberg, Norway.

http://www.usn.no

This thesis is worth 60 study points.

Developing a Cyber Security Documentation Package for Project Deliveries

Master's Thesis in Computer Science

Borgny Louise Gløersen

Supervisors

Academic

Joakim Kävrestad

Industry supervisor

Tor Eivind Wilhelmsen

University of South-Eastern Norway

Faculty of Technology, Natural Sciences and Maritime Sciences

Department of Science and Industry Systems

Campus Kongsberg

May 2024

Abstract

This thesis focuses on creating a flexible cyber security framework to improve compliance with cyber security requirements for oil and gas industry projects. Typical oil and gas projects have requirements and specification regarding cyber security that will vary from operator to operator and scope of supply, whether or not the installation is new or existing. However, these unique specifications from the different operators impose issues to the supplier who works with numerous clients within the industry. One of the issues emerging from the client's specification is that the specification is applicable to the entire oil and gas installation, whereas the scope for the supplier side of the project may only be a small fracture of it depending on the task. Another issue is regarding the level of cyber security knowledge the engineering on the supplier side may have in order to understand their responsibilities from the specification given by the client. Through qualitative study of a case with one of such suppliers, has reveled that the knowledge on the topic for complying with requirements from the client's specification are low, there is also a lack of specification from said supplier. To improve this situation, the study maps the recurring topics between the different clients' specifications and topics the employee of the case faces the most. Those derived topics have then been presented to a custom framework which is tailored for the used case on the supplier side. This framework allows the engineers working on the project to know what cyber security requirements are applicable to them. The framework has been reviewed by its users with positive responses regarding it as relevant and usable, and improving the understanding of cyber security responsibility for them as a supplier of their project scope.

Keywords

framework, cyber security framework, ICS security, oil industry, gas industry, compliance

Acknowledgements

I am deeply indebted to my USN supervisor, Joakim Kävrestad, and industry (external) supervisor, Tor Eivind Wilhelmsen, for their invaluable guidance throughout this thesis. Your insightful advice and constant reassurance about the direction and progress of my work have been instrumental in reaching this point. We're almost at the finish line with this!

I also would like to thank my manager at Guidant, Morten Røraas, and the rest of the team for collaborating with me in this study and always cheering me on. You guys won't get rid of me that easily, and I will probably still be a pain in your butt when the result from this study shall evolve forward.

Big thanks to my closest friend, Elin Gravningen, who has also been there with me through this process, encouraging me, spinning ideas off with, and also, but not least, helping me with some grammar (not as much fun laughing about my writing mistakes when I had to use Grammarly during your exam period). Big thanks to Even Andreas Bergan for being there for me as encouraging support during the last half of this process; even though it is not always related to this thesis, you make me smile and laugh, which keeps my spirits up.

Contents

List of Figures

List of Tables

Acronyms

CIS Center for Internet Security

CIS CSC CIS Critical Security Control

CMMI Capability Maturity Model Integration

COBIT Control Objectives for Information and Related Technologies

CPMI-IOSCO The Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO)

CVSS Common Vulnerability Scoring System

DSR Design Science Research

DSRM Design Science Research Methodology

FAIR Factor analysis of information risk

GD201 Government Decision 201

HAZOP Hazard and Operability Analysis

HEIs Higher Education Institutes

IEC International Electrotechnical Commission

ISA International Standards on Auditing

ISO International Organization of Standardization

ITIL Information Technology Infrastructure Library

N/A Not Applicable

NIST National Institute of Science and Technology

NIST CSF NIST Cyber Security Framework

PMBOK Project Management Body of Knowledge

SDL-CPPS Security Development Lifecycle for Cyber-Physical Production Systems

SPICE Software Process Improvement and Capability dEtermination

TARA Transfer, Accept, Reduce, Avoid

VDI/VDE Association of German Engineers and Association of German Electrical Engineers (Verein Deutscher Ingenieure und Verband Deutscher Elektrotechniker)

1 Introduction

Cyber threats continuously evolve, and the countermeasures have to evolve [1]. Where the focus of the research has been towards infrastructure, hardware and software [2]. Regarding infrastructure, communication and data sharing in different environments can increase the risk [3]. As companies are interested in their revenue, they look for ways to be innovative and cost-effective while complying with regulations [4]. With the concern of the increasing threats, reliable frameworks have to be developed [4]. A method for developing those could be Design Science Research Methodology (DSRM) [5–8].

This study focuses on organisations within the oil and gas industry with an increased focus on complying with cyber security requirements in their projects [9, 10]. With various standards, frameworks and/or specifications that focus on the organisational level through the background literature, where is the focus on projects, more specifically, directed towards a supplier in a project from an organisation? It is important to have standardised solutions that fit the area of work. A standardised solution for project deliveries could be cost-effective as the road towards the solution does not have to be explored again for each project.

Existing solutions and how they were obtained to improve cyber security in businesses and organisations are outlined in detail in Chapter 2 of this report. The review shows that different methods, standards, and frameworks have been used to achieve cyber security goals. Those include ISO, NIST, IEC, and others. The focus on having a custom framework in place is not new, but it can be traced back to at least 2012. In 2012 Bayuk et. al. [11] acknowledged the same as NIST [12], that there is no one-size-fits-all, and recommends setting customised design goals.

This study has been carried out as a case study, where DSRM has been used to create an artifact. The project will deliver a framework, artifact, that fits the company's needs, whether it is a large or small project. Whether the project is from scratch or just a software upgrade, The framework will be developed to address the company's clients' cyber security requirements and the common issues the employees face the most in their projects to create a standardised solution which can be used across different variants of their project deliveries.

1.1 Problem statement

Through the time spent at the company, which is the use case in this study, the employees at the company have vented their frustration with the lack of their own cyber security requirements and how to understand the clients' requirements. This study shall focus on how the method used to develop a framework on an organisational level can be used on a project level. The goal is to ease employees' frustration and confusion in the projects by defining the relevant requirements for the use case from the common topics that the employees face and the client's requirements. The other goal of creating a framework is to be as compliant with the clients' specifications as possible but also to be focused on what the company in the case study delivers in their projects, as not all of the requirements from the clients may be relevant towards what the company in the case delivers.

When developing an artifact for a solution to the case's problem, it is important to remember that it has to be appropriate to the case's customers' specifications. To do that, the customers' specifications shall be studied to find common topics occurring as one of the baselines and using the official standards and frameworks they refer to. A survey shall be performed to understand the topics that the case employees struggle the most with understanding and/or fulfilling.

1.2 Research Questions

The employees in the case used in this study have over time vented their frustration of problems faced working with clients and their requirements for cyber security in the projects delivered by the employees. This research focuses on how a framework can be developed on a project level. The goal is to provide a documentation package which contains a custom framework and a checklist to be used to document how the framework has been applied in projects. The objective is to have a flexible framework towards the case and keep the framework aligned with the official standards the clients are referring to be as compatible as possible with as many customers as possible.

RQ1: What are the commonalities between the standards from the customers in the industry and what differs between them in their requirements?
RQ2: How do the employees work to fulfil the customer's standards and requirements?
RQ3: Is the artifact perceived as useful by developers, and how can it be further improved?

1.3 Approach

To be aligned with the cyber security requirements used in the industry, the different specifications have been compared in regards to the most common topics and the most used standards referred to. To verify the topics as relevant, a survey performed has allowed focusing on the most relevant topics from the selection from the comparison to add to the custom framework. However, the selection based on the survey results and the comparison is only to create a baseline, where more relevant requirements can be added in later stages from the beginning drafts of the framework.

Peffers et. al. states that the first step of design science research methodology is "Problem identification and motivation" [13]. The goal of the artifact is to solve a defined problem, where it can help to break down the main problem definition into smaller tasks to contain the complexity of the problem. By working together with the people who are supposed to use the artifact may also help manifest the current problem [14]. This means that by collaborating with the users having a problem, defining the problem becomes easier and more natural.

1.4 Assumptions and Limitations

1.4.1 Assumptions

- It is assumed that the employees participating in the survey have a basic understanding of clients' cyber security expectations. The focus on cyber security in projects is mainly driven by the clients themselves. Therefore, they have provided their suppliers with training and workshops to support their understanding.
  The assumption is further supported by first-hand experience working alongside the surveyed employees a year before the master's thesis project commenced as part of the master's program. During this time, I have also been included in a significant part of the department's cybersecurity-related discussions.

- The second assumption is that when standards are referenced in customer documents, those references refer to the latest editions of the standards.

- It is assumed that the evaluation of the framework might reveal topics not initially considered during the first survey.

1.4.2 Limitations

- Due to time constraints, this master's project will not include real-world testing of the developed framework. Negotiating a test with a customer would require getting involved at a very early stage of contractual and project planning. Consequentially, performing a test is not deemed feasible within the thesis timeline.
- The framework is limited to the requirements from the IEC 62443 standards, as the clients mostly use these, and due to the time limitation, are then unable to explore other standards' requirements to evaluate if those are more suited or not to apply in the framework.
- The framework is limited to the common topics that the case employees face the most when working on projects.

1.5 Contributions

- Academic literature on incorporating good cyber security practices in companies has, to this point, mainly focused on the organisational viewpoint. This is relevant and appropriate as nurturing a cyber-secure culture in a company should be a structural concern and come from the top levels. However, addressing these concerns from a structural and organisational viewpoint does not necessarily make good cyber security philosophies easily converted into operation. This case study provides an example of how theory should also work in practice, which is often not easily put into practice. This study has expanded the focus area by focusing on how a custom framework could be tailored to a project level.
- This study has mapped out different topics within the scope of cyber security that the case found to be reoccurring and should be applied to a framework. Researching the case provided valuable insight into identifying common issues in projects where employees strive to comply with the client's requirements. The study also demonstrated how different clients' requirements may vary. The research project, together with close collaboration with the connected company, gave access to numerous client project specifications and requirements. Therefore, it was possible to identify relevant commonalities between them. This facilitated the development of a framework that supports compliance with the company as well as multiple clients' needs.
- This method of collaboration can also be used to create other frameworks that need to be tailored to different goals, as it is possible to move from focusing on an organisational level down to a project level. As the existing literature focuses on the organisational level, the

same methodology and way forward from existing literature are also considered applicable to a project level through this study. This contributes to the existing literature by focusing on how DSRM can create a framework fitted to a project level through the case study.

1.6 Thesis Outline

Chapter 2 presents the literature collection and the existing literature focus points regarding recommendations, existing approaches and solutions, information about the most known standard and framework, and basic information about the control system for this study's case.
Chapter 3 presents the case used in this study, and a review of the methodology approach applied which is divided into three phases.
Chapter 4 presents the results gathered from each phase of the study.
Chapter 5 focuses on discussing the results from Chapter 4 of each of the research questions.
Chapter 6 presents the possible future steps.
Chapter 7 concludes this study.

2 Background

This chapter will review relevant literature and standards that are applicable to the thesis topic. Then, relevant standards and frameworks are described. The first part will explain how articles were selected for the study, while the second part will provide an in-depth analysis of different articles. The next section will focus on the applicable standards and frameworks for further study. Before the summary, the last part will concentrate on the control system used in the study as a case, as it will help understand the requirements for the study's proposed solution.

2.1 Literature Collection

As part of the literature review process, a systematic search was conducted. Using IEEE and Google Scholar databases. The results of the search for various criteria are presented in Table 1. Due to the large number of results, only the first page of articles was considered. The titles were read, and based on their relevance, the abstract and conclusion were reviewed to determine whether to keep the article for further study or move on to the next one. The next section will cover the study of the selected articles in more detail.

Search key	IEEE		Google Scholar	
	No limit	From 2019	No limit	From 2019
Cyber security framework	4653	3046	975000	56400
Cyber security framework for project	428	316	647000	58100
Organization cyber security	2618	1582	788000	21700
Cyber hygiene	76	67	353000	16500
Cyber security documentation	72	35	240000	16400
DSRM cyber security	0	0	550	409
Design science research methodology cyber security	104	87	556000	18400
Cyber security framework industry 4.0	82	70	202000	16700

Table 1: Search Results

2.2 Previous Work

The section discuss the present state of focus regarding cyber security strategies and measures across various sectors worldwide. It will also delve into the different combinations and methods utilized by different authors to achieve their objectives. Furthermore, the authors will highlight some shortcomings in existing standards and frameworks, and suggest their recommendations for improvements.

2.2.1 Focus on weaknesses and recommendations

Government regulations in cyber security: Framework,standards and recommendations [2]
Srinivas et al. [2] have discussed the different cybersecurity strategies adopted by non-EU countries like Japan, Canada, and China, as well as the United States of America. They have focused on the threats faced by these countries and the measures and requirements associated with these strategies. For example, one of the threats they describe is a virus, and the countermeasure for it is an antivirus program. They have also elaborated on the requirements, such as confidentiality, integrity, authentication, availability, authorisation, physical theft of devices, non-repudiation, and freshness [2].

Srinivas et al. [2] discuss the various challenges related to standardisation in cybersecurity [15]. A significant challenge is the lack of agility. The process of agreeing and designing a standard can take a long time, ranging from months to years, which can make the standard partially or fully outdated by the time it is completed. To overcome this challenge, a solution could be to have good practice documents as a base for the corresponding standard. This approach can help the development of the standard to be at a comparable momentum, making it applicable in real-life environments.

Srinivas et al. [2] have brought up the issue of multiple sets of standards being defined in various domains. This can create problems for end-users who may find it difficult to determine which standard is the best fit for them or meets their requirements. Additionally, standards from different groups can be combined to achieve a particular objective.

Based on the study Srinivas et al. [2] performed in mapping cyber security strategies across nations, and focusing on threats, measures, and challenges, they propose different steps of recommendations for improvements. One of these recommendations is that the parties agree on the use of standards and to include the standards' references in the procurement procedures. Another one is that they mention organisations Srinivas et al. [2] discuss the cybersecurity strategies adopted by non-EU countries, such as the USA, Canada, Japan, and China. They focus on the threats, requirements, and measures associated with these strategies.

Srinivas et al. [2] point out that one of the significant challenges in standardising cybersecurity is the need for more agility. Agreeing on and designing a standard can take a long time, ranging from months to years, making the standard obsolete by the time it is completed. To overcome this challenge, a solution could be to use good practice documents as a base for the corresponding standard. This approach can help the development of the standard be at a comparable momentum, making it applicable in real-life environments.

Another issue raised by Srinivas et al. [2] is the existence of multiple standards being defined in various domains. This can create problems for end-users who may find it challenging to determine which standard best fits them or meets their requirements. Additionally, standards from different groups can be combined to achieve a particular objective.

Based on their mapping of cybersecurity strategies across nations and focus on threats, measures, and challenges, Srinivas et al. [2] propose several steps of recommendations for improvement. One of these recommended steps is for the parties to agree to use standards and include the standards referenced from the agreement in the procurement procedures. Another recommended step is that organisations involved in financing research and development should find compatible standards for various activities and follow them whenever appropriate, involved in the finance of research and development to find compatible standards for various activities and should be following them whenever appropriate [2].

Information security management frameworks and strategies in higher education institutions: a systematic review [16]
Merchan-Lima et al. [16] reviewed Information Security Management (ISM) in higher education. The list below contains different standards and frameworks used in the research by Merchan-Lima et al. [16]:

- ISO27000
- COBIT
- ITIL
- NIST SP 800-30
- EDUCAUSE

Following their study on the development of the ISM Framework, they provide recommendations for consideration for further implementation in an era of evolving threats. Their proposed focus list includes risk assessment [17], user awareness [18], establishing protocols, IT governance [19], and validation. They recommend that risk management should be seen in the light of the information security life cycle as a process, and once implemented it should be re-evaluated periodically.

Following one of the recommendations for protocols, they recommend having templates and guidance documents as a reference. IT governess has recommendations on two areas, vulnerabilities and cyber security. Merchan-Lima et al. [16] recommend automatic vulnerability checks and remediation; another recommendation is to establish appropriate physical and logical access control.

Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education [20]
Rajab et al. [20] study focuses on employees in higher education. They note that the users in the university lack compliance with their proposed security policies. By lack of compliance, both students and employees are putting their information at risk. Rajab et al. [20] goal with their study is to determine different factors in relationship with the intended security policy compliance.

Their paper presents a study based on models of behaviour, motivation, organisation, for predicting employees of higher education's intentions for complying to information security policies. Through their study, a survey was performed to find the predictive indicators associated with intentions for compliance among the university staff and faculty. Results from the survey by Rajab et al. [20] show the intentions for compliance are affected by the employees' perceptions of vulnerabilities. The perceptions found from the survey maps the affection on compliance were associated with risks, the ability to respond to incidents, their ability and choices if a breach of information security occurs, and the probability of getting caught violating policy compliance.

Based on their study's survey results, it suggests that employees' compliance is lower when the probability of detection goes higher. However, the study found that vulnerability has the highest effect on higher education employees, increasing their intentions to comply with security policies. The results include that employee compliance would also be high with the employees' skills, confidence, and ability to respond to different security risks such as phishing and infected files. This is reflected in the results as the Protection Motivation [21] was the best-suited model for predictive intentions of security policy compliance. The other theories covered were however not supported. The motivational model was the most relevant, which was due to perceived vulnerability, response efficacy, and cost.

A review of the current cyber hygiene in small and medium-sized businesses [22]

Ncubukezi et al. [22] focuses on the current cyber hygiene of small and medium-sized businesses in South Africa. With the increase in the range of opportunities on the Internet [23], such as using it as a library, entertainment, and social networking, the range of threats is also increasing. The increase in threats affects not only people but also businesses and devices. That is why everyone must keep up good cyber hygiene, which could be achieved by awareness and documentation that could inform about policies, standards, and rules to follow. By the lack of this, a business could be left to threat by the employees, leading to financial loss, data loss, and damage to infrastructure.

Further Ncubukezi et al. [22] focus on what cyber hygiene [24] is, and the necessity of awareness and having knowledge of potential risks and threats, and how they can be prevented. Such as having a routine promoting safety and security and focused at security on different levels, such as economic, organisational, and technical, due to the variety of potentially affected areas. Businesses should invest to ensure the security measures are up-to-date, to mitigate the such threat as data loss and cost.

A framework that Ncubukezi et al. [22] suggests that businesses could align with is NIST Cyber Security Framework. This is because the framework primarily aims to provide different cyber security-related activities. Also focusing on the need to understand the different assets at play to provide the necessary measures as policies and rules against their potential threats. NIST also provides a suggestion that it should be necessary training provided about security measures. If the five cores of the NIST framework are not being followed, the business could have a harder time handling the vulnerabilities when a threat arises. Summarised, could these factors lead to potential poor cyber hygiene, lack of awareness, policies, and measures of security activities.

Through the study by Ncubukezi et al. [22], the current cyber hygiene was mapped through the businesses across South Africa with diverse business sectors. However, the global pandemic has been an influence on the data gathered. There was a quantitative study, but there was also a qualitative study focusing on 30 participants. The results of these questionnaires in the study reveal that 83% of the participants have been open to different cyber threats. Luckily, none of the participants were reported as victims of the threats. The people in the questionnaire have stated that they do have antimalware/viruses available, but they are not sure if it is up-to-date or not, whereas 33% of them do not bother to check for potential updates to the software [22]. None of the participants mentioned a document that could help them guide them in handling incidents available; however, a structured document could help them in regards to best practices and better cyber hygiene [25].

The study then shows that overall knowledge of cybersecurity-related activities is limited, as is awareness of good cyber hygiene against potential threats. The same goes for businesses that do not prioritise risk assessment and analysis and lack formal documentation to train employees on acceptable security measures, practices, and awareness.

2.2.2 Focus on combining and proving existing approaches

Cyber-physical risks identification on industry 4.0: A methodology proposal [26]
Santos et al. [26] research focuses on risk identification where they propose an approach based on the different standards and models, ISO31000, PMBOK, Risk Model by Brocal et al. [27], HAZOP and NIST CSF. Even with existing risk identification they propose to improve the risk identification towards the cyber-physical environment.

One of the challenges that has been identified by Santos et al. [26] is regarding connected devices and services, and the risks that emerge. These risks from connected devices and services resulting from connectivity between systems. Another challenge that Santos et al. [26] mention is concerning hazard identification and disaster prevention. Where the risk emerges in response to the impact of economics, the volume of data generated that must interact within the system, and other activities.

With Santos et al. [26] focusing on risk identification, they propose an approach that uses Risk Model, ISO31000, PMBOK [28], and HAZOP [29] as a bottom-up approach for risk identification. Whereas the top-down approach is based on NIST CSF. The bottom-up approach proposed will start at the physical layer, through the interconnection layer, and up to the cyber layer, whereas the top-down approach starts at the cyber layer and goes down to the physical layer. Figure 1 illustrates the bottom-up and top-down approach, that has been described by Santos et al. [26]. In cyber-physical systems, the physical layer can consist of components such as physical components and physical measurable states, the interconnection layer can consist of programmable controllers and sensors, and the cyber layer can consist of supervisory computers.

Santos et al. [26] provides an example of how the bottom-up approach can be used in a flare gas system of an oil plant. The system comprises field instrumentation such as controllers, valves, measurement equipment, control room instrumentation, and more. They suggest following the HAZOP approach to identify plausible causes of deviations, such as "broken instrumentation" causing "no gas flow".

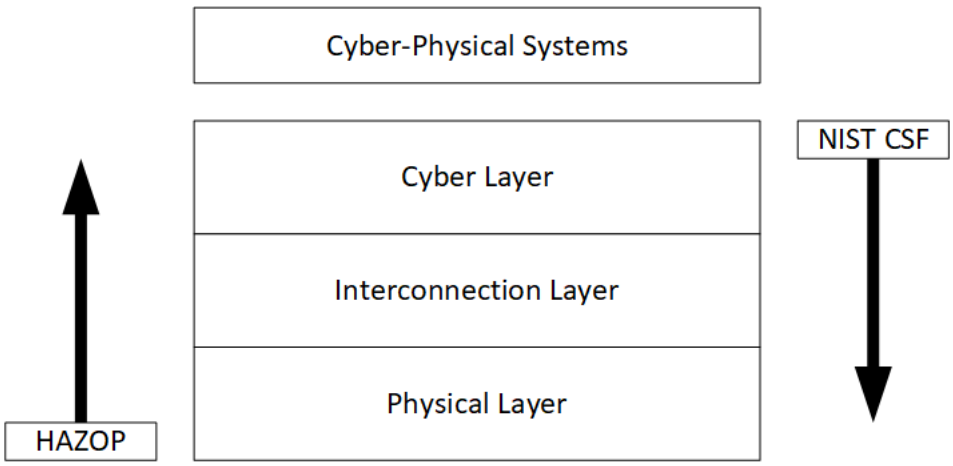


Figure 1: An illustration of the proposed model

Although HAZOP primarily focuses on the physical layer, it can be expanded to cover other layers. On the other hand, the top-down approach uses the NIST cyber security framework that starts from the opposite end of the layers. NIST CSF categorises different risks into sub-categories and benchmarks. Santos et al. [26] propose sub-categories for asset management, including physical devices and systems, and software platforms, which cover all layers of the cyber-physical system.

Santos et al. [26] combines the bottom-up and top-down approaches to optimise the detection, mitigation, and prevention of emerging risks.

Cyber security framework for the internet-of-things in industry 4.0 [4]
Radanliev et al. [4] paper presents a qualitative case study focusing on Industry 4.0. The case study goes more into depth about then-today's cyber trends [30, 31], risk frameworks and models. With today's vast amount of devices, some are bound to be connected one way or the other. The risk and concerns also increase with the increase of network-connected cyber-physical devices. That concerns all; however, for the industries, it can create trouble with their interests. Companies are interested in revenue, having it cost-effective, and complying with new regulations.

Through the Radanliev et al. [4] study, they want to offer new design principles for enabling people to adopt best cyber security practices and a quick, up-to-date overview of IoT advancements. They will achieve this by presenting the strengths and weaknesses of today's frameworks and models of different practices. Through their process of developing design principles, Radanliev et al. [4] attempt to have Industry 4.0 initiatives integrated with the academic literature. They compare cyber risk focus through national initiatives and compare existing solutions. Taking that into consideration, they also consider economics due to the interest of industries.

During the reflection of present-day models and frameworks, they compare the selected models/frameworks on the criteria of how to measure, standardise, and compute risk and disaster and recovery planning. Some of the findings of the reflection were that ISO has disaster recovery promoted by having a standard for this. In contrast, NIST has recommendations for recovery and is the most advanced framework in the area of disaster and recovery planning.

List of standards and frameworks Radanliev et al. [4] use in the comparison:

- NIST Cyber Security Framework (NIST CSF)
- FAIR
- CMMI
- CVSS
- ISO 15504 - SPICE
- ISO 27031
- ISO 27032
- ISO 27001
- Octave
- TARA

Through the qualitative study, Radanliev et al. [4] found that implementation of recovery planning has previously failed in the leading initiatives. Even when the frameworks and models have disaster and recovery planning recommended, this action has been ignored. Due to the problems, a tool, Monte Carlo simulation [32] has been suggested by Radanliev et al. [4] to help reduce risk uncertainty and to help with a cost estimation of the impact of cyber risks. Through the calculations, companies could develop and enable appropriate measures for the risk in recovery planning and the insurance to the industry for a more realistic cost.

Security development lifecycle for cyber-physical production systems [33]
Eckhart et al. [33] present that information security has become a pressing issue for product suppliers, system integrators, and asset owners. This issue occurs as digitisation reaches new heights, and new threats also arise. Neither does it help the situation that engineers lack sufficient information security knowledge, nor miss a security development lifecycle dedicated to system integrators. This is why Eckhart et al. [33] goal is to create security-related activities building on existing standards [34] and guidelines, literature [35–37], and provide pointers that could fill potential gaps in knowledge. The different standards they focus on in their study are:

- IEC 62443
- VDI/VDE 2182
- SDL-CPPS
- NIST 800-82

Through their study, they describe some key characteristics of Cyber-Physical Production Systems, such as the connectivity of devices and the continuous exchange of data. However, this has its downsides, such as increased connectivity, which also expands the attack surface area. Another issue they state is that a patch may not fix an issue completely [33, 38]. The risk of a patch not fixing an issue also results in the system being exploitable till the end of its life. Even though the software industry has well-established security activities, the automation industry does not. According to Eckhart et al. [33], the reason for that is that there is a lack of research in this area for the automation industry for applicable methods on security-related activities. The existing solutions have been designed to be generic. The flexibility affects the relevance to production systems engineering, making the existing solution less relevant for the industry by not being able to create relevant security activities.

Through Eckhart et al. [33] study, they start with some background on production systems engineering, which, on behalf of the asset's owner, is undertaken by system integrators as part of plant engineering. The production systems engineering varies on the Cyber-Pysical Production System to be developed. Through discussion with stakeholders in the study, they have described the workflow as five parts, preparation, basic and detailed engineering, integration, and installation and ramp-up. The issue still stands that security activities need to be integrated into the workflow. Further on, they asses different standards.

The first standard they study is the IEC 62443, which provides general guidelines. However, it does not adjust towards the production systems engineering regarding specifying a security development lifecycle. But, the IEC 62443 does aim to address security issues with relevant aspects for product suppliers, system integrators, and asset owners. The second, VDI/VDE 2182, which Eckhart et al. look into [33] is a risk-based approach that can apply to implementing security measures. This could be relevant for product suppliers, system integrators, and operators. The approach also provides guidelines for automation components that can be used for establishing principles, but the recommendation the model has is not tailored to production systems engineering. Even if it is not tailored, the study mentions that Security Development Lifecycle for Cyber-Physical Production Systems (SDL-CPPS) could be implemented supplementary to the guidelines as an option.

NIST 800-82 is the third that is analysed. NIST is described as having various techniques and covering a broad scope, and NIST can be used as a basis for implementing some security-enhancing measures. The downside to NIST is that it does not fully address security concerns that may arise for system integrators. Further into the topic of SDL-CPPS states Eckhart et al. [33] that SDL-CPPS must be protected against increasing threats, that it is necessary to impose requirements to include security-improving activities. These activities must be an effort until the system's end-of-life, not letting the security activities stop after installation.

Through workshops held in the study, other challenges have been discussed, such as adaptation, which arises from shifting the responsibility from asset owners to system integrators, and training and adjusting the engineering workflow could be costly. Engineers with minimum training could also create difficulty with minimum security knowledge even though the need is rising. Tools to use as implementation accelerators are also missing. Designing a resilient control system does positively affect availability; however, from the workshop conducted in the study, it still falls back on justifying the additional cost for the SDL-CPPS security activities.

2.2.3 Focus on creating a new solution towards a goal

Using design science research method to develop a cyber security framework for HEIs in Moldova [6]

Research done by A. Alexei [6] focuses on using Design Science Research (DSR) to solve their problem in the field of cyber security. In this situation, the problem arises from the lack of a comprehensive framework for Higher Education Institutes (HEIs) in Moldova. A. Alexei [6] uses DSR to create a cyber security framework to increase cyber security in HEIs.

Through the introduction of the paper, A. Alexei [6] mentions that several services are based on communication networks and that HEIs depend on the technologies for that. This results in an increase of attacks within HEIs [39, 40]. The problem of countering these attacks comes from the lack of knowledge. The lack of knowledge also increases the amount of risk and potential damage to activities in HEIs. Cyber security has as a role increased in importance [40]. Some assets for support that are necessary to consider are network devices, human resources, applications, and infrastructure, however, they need to protect the business processes, exams, information, dedicated applications, and online courses. Even with the increase of importance of cyber security, A. Alexei [6], reveals some concerns around the topic for HEIs. The concerns are in regards to there not being an explicitly applicable research solution, which could lead to a potential loss of influence. Where the potential loss of influence is in regards to the field of cyber security, A. Alexei [6] achieves the action for each step of DSR and letting the results of the study be reproducible.

Further into A. Alexei [6] study, a survey was done with the stakeholders, where the results were that none of the participants was certified with any information security standards. From researchers, there was a different view on which standards would be appropriate to follow. The standards that prevailed from the researchers were ISO27001, COBIT, and ITIL. A downside being discovered was that the standards are towards the commercial organisation [16, 41], creating a difficult problem for them to be implemented for use for HEIs. In Moldova, there exists a (Government Decision 201 (GD201)) which refers to all public organisations of approval of mandatory minimum cyber security requirements.

Using DSR [13, 42] to create a cyber security framework for HEIs, is could be seen as an opportunity for information systems research to address real-world challenges. Using DSR to create an innovative solution to the problem. Throughout the work using DSR the author's goal is to create a cyber security framework for HEIs. The artifact proposed to increase has requirements to comply with the international standard ISO27001. Whereas the ISO standard gives generic support, the Grundschutz

gives technical support to the framework as well [6]. The artifact was demonstrated before experts and stakeholders, and evaluated by the experts who then gave feedback on the framework. The artifact has been communicated to people through scientific papers and conferences. Then A. Alexei [6] concludes that using DSR was successful in achieving the goal for the research problem of creating a framework to increase cyber security in HEIs.

Developing a cybersecurity framework for the banking sector of Namibia [7]
E.-L. T. Nawa [7] conducted a research study to develop a cyber security framework for banking institutions in Namibia. The research was carried out using the DSR methodology, which involved evaluating existing frameworks, identifying gaps, and developing a framework that is tailored to the unique demands of the banking sector in Namibia. This was motivated by the lack of an official cyber security framework in the banking sector of Namibia [43], which has made it vulnerable to cyber-attacks [44].

The study involved an analysis of global cyber threats faced by the banking sector, and an assessment of the policies and strategies used in Namibia. The research found that the current cybercrime bill in Namibia leaves organisations open to more threats as they are required to lower their security standards to comply, making them liable if they fall victim to cybercrime. This puts the banking sector at risk due to the lack of adequate cyber security measures against cybercrime [45]. Therefore, developing a cyber security framework for the banking sector is crucial to protect against cyber threats.

The study focused on various existing frameworks, standards, and best practices, including NIST CSF, CPMI-IOSCO, ISO/IEC 27001:2013, CIS, and a framework for Governance of Information Security. The gaps in these frameworks were assessed, and it was found that they were unable to be generalised for the banking sector in Namibia due to the specific and unique demands of the sector. Therefore, a tailored framework was needed to suit the environment and demands of the banking sector in Namibia.

The research was carried out using a qualitative method, which involved semi-structured interviews with staff from different banks in Namibia. The interviews helped to evaluate the current status of cyber security in the banking sector and identify areas needing an improvement. The evaluation of the current status and existing frameworks was done in the design and development phase.

The results of the study indicated that the changes in strategies proposed by the framework could be positive for the banking sector, as it would greatly improve resilience against cyber threats. Therefore, the recommendations for improvements made by E.-L. T. Nawa [7] could greatly benefit the banking sector in Namibia.

A framework for cyber security awareness in small, medium and micro enterprises (SMMEs) in South Africa [8]

T. Lejaka's thesis [8] focuses on creating a cyber security framework using the DSR Methodology for small and medium-sized businesses in South Africa. The author emphasizes the limited knowledge and skill within the cyber security topic and the financial support needed to prevent threats. By creating a framework for businesses, awareness could be raised, as they have a direct impact on the infrastructure of cyber security in the country. The study's goal [8] is to address the lack of cyber security awareness [46, 47] and the absence of a suitable model and framework for increasing awareness, which was identified in the literature review.

In their study, T. Lejaka [8] discusses the global concern around cyber security, especially in developing countries like South Africa. The author emphasizes the importance of creating awareness about potential cyber threats and the need for audience analysis to tailor effective awareness campaigns. The study highlights that relying solely on technology-based solutions is not enough and can leave assets vulnerable to attacks. By educating individuals about potential risks, they can help mitigate threats. However, the study also points out that humans are the weakest link [48] in the chain and can be prone to errors, thus making them the first line of defence that needs to be strengthened [8].

To achieve the goal of T. Lejaka's study using DSR methodology, different approaches were considered. Among them, two approaches were discussed: deductive and inductive. The inductive approach was selected since it enables the researcher to focus on change during the study while providing a better understanding of the research. This approach allows for a qualitative approach and is initiated by observing and searching for patterns in data [8]. The study proposes a three-part approach for the way forward. The first part involves exploring the literature and explaining the components of the awareness framework. The second part focuses on developing the intermediate framework. Finally, the third part concentrates on validating the work by conducting interviews with experts and making necessary modifications.

The author conducted a study and successfully designed and developed an awareness framework for cyber security [8]. With increasing cyber threats, it has become crucial for businesses to tackle related challenges. However, a lack of knowledge and resources can make it difficult to stand against these challenges. The framework can help address these issues.

2.3 NIST Cyber Security Framework

In August, the NIST CSF made available a public draft of version 2.0 of the framework. The framework is meant to reduce cyber security risks in industry, governments and other organisations [49]. The feedback from NIST CSF version 1.1 being effective for addressing risk from organisations, there was also an agreement to address the current and future challenges in the framework. The framework is divided into three parts, core, profile and tiers. Figure 2 illustrates the five functions of the core of the current NIST CSF. Tiers from the framework are to clarify how they view risk and the management approach of cyber security. As for the profile, it lists an outcome of categories and subcategories based on the need and risk assessment.

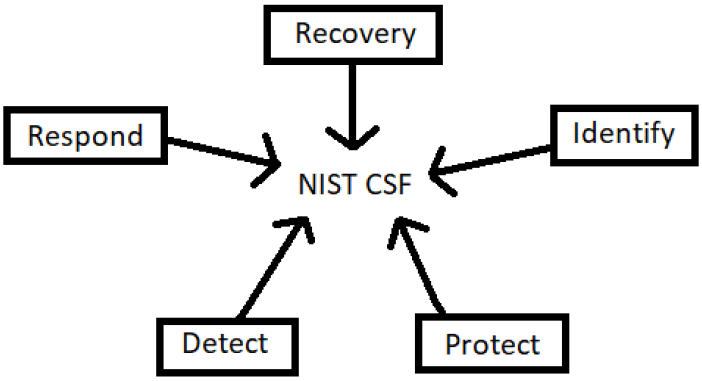


Figure 2: NIST Cyber Security Framework

The appendix of the NIST CSF version 1.1, describes common activities towards the core of the framework for critical infrastructure sectors. For these common activities for the core part of the framework, there is a column in the table of the appendix of the framework with informative references. The references for the activities in general refer to:

- CIS CSC
- COBIT
- ISA 62443
- ISO/IEC 27001
- NIST SP 800-53

Even with NIST mapping of the common activities [50], it is not intended to determine the desired outcome for the subcategories by the informative references. The framework does not suggest ways for implementation, but it does allow the user to manage their risk within cyber security.

2.4 IEC 62443 series

IEC 62443 was developed for the industrial sector, to secure automation and control systems [34]. It is designed to reduce cost and improve security, by mitigating effects and preventing cyber-attacks. The holistic approach for the IEC 62443 standards is due to not all risks being based on technologies, but also on staff. Staff must have the required training, knowledge and skills, to be able to ensure security.

The IEC 62443 series is split into four parts. The first part of the standard covers common topics. Part two focuses on methods and processes. The third part focuses on the requirements at the system level. The fourth and last part focuses on components and requirements. The four main parts are also divided into smaller parts, figure 2.

General	Policies and procedures	System	Component
IEC TS 62443-1-1	IEC 62443-2-1	IEC TR 62443-3-1	IEC 62443-4-1
IEC TR 62443-1-2	IEC 62443-2-2	IEC 62443-3-2	IEC 62443-4-2
IEC 62443-1-3	IEC TR 62443-2-3	IEC 62443-3-3	
IEC TR 62443-1-4	IEC 62443-2-4		
IEC TS 62443-1-5	IEC TR 62443-2-5		

Table 2: Division of IEC 62443 components

2.4.1 ISA/IEC

For the development of the ISA/IEC 62443, it has been done in collaboration with ISA99 committee, IEC Technical Committee 65, and the Industrial Automation and Control System Security [51]. The standard shall define cyber security requirements for robustness and resilience. The focus for the standard is towards IACS lifecycle. The naming convention between ISA and IEC is mostly similar, and the documents are identical [51]. The release of both is as simultaneous as possible.

2.5 Control system

Figure 3 is a simple illustration of components that shall communicate with each other in a metering system. An example of what could be in a control system delivery could be a mix of physical and virtual flow computers (another name for this is process machine), a server for hosting the control system program, and converters, which are just some elements of a potential delivery. However, a delivery may only include a software upgrade.

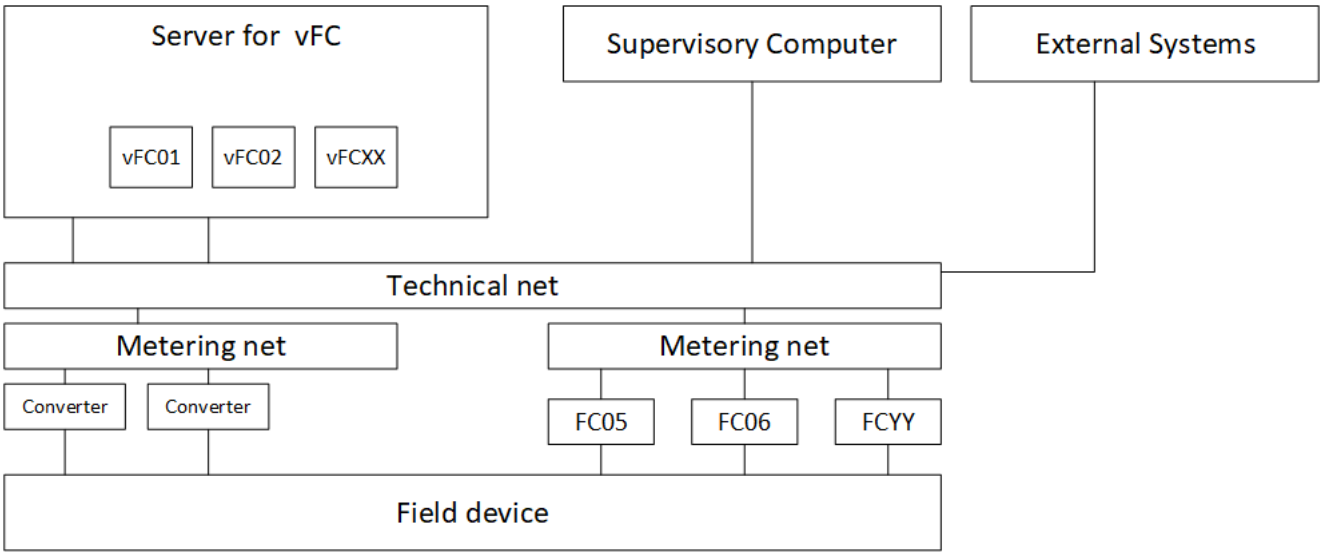


Figure 3: Basic system topology of components related to metering control system

Today, traditional control systems have evolved from purely mechanical solutions to software-based systems for the following typical applications: continuous measurements of oil and gas and batch-loading and -unloading [52]. Today's metering control system has expanded to multiphase measurements of topside and subsea. For the insurance of accurate allocation measurements, verification/-calibrations of the topside multiphase flow meter are done through a test separator.

The control system is a part of the oil and gas installation, a sub-system on the installation. The oil and gas installation operator has its own cyber security requirements to comply with. However, the requirements here are not fitted for the control system alone, as it is so wide in coverage, and the supplier, in this case, does not have a standard or framework for their delivery of the control system either.

Note: The customer will be anonymous due to the case. The customer requirements will only be used to find common topics and reference official standards.

2.6 Summary

After studying various articles, it has been found that the current focus is on national and organizational levels for cybersecurity. None of the articles specifically addresses cybersecurity for project deliveries, specifically for a product solution delivered by suppliers to customers.

The authors conducted surveys which have revealed a range of responses. However, these responses have provided valuable insights into the current state of cyber security, particularly with qualitative studies. Based on the various surveys, it has been reported that the management of cyber security is inadequate in terms of both awareness and knowledge in certain areas.

Another important factor to note is that many of the articles mention the lack of proper documentation, from focusing on rules and policies to implementation and awareness in different scenarios. However, the articles commonly recommend combining different frameworks and standards to cover gaps in a single framework or standard. They also suggest having relevant documentation available to users. The most commonly used frameworks and standards are from NIST, ISO and IEC, with different ISO and IEC standards being used (such as ISO27001 or ISO27032).

3 Methodology

This chapter describes the methodology and its application in this study. The first section takes into account different considerations for this study. The second section describes the purpose of the methodology and the intended use as an overview of the execution plan. The later sections describe the applied steps of DSRM.

Conduction of thesis work

The study follows the DSRM divided into three phases, focusing on solving the issue of the case used in this study. To understand the issues the employees face in their work, a survey will be performed to map and review the client's specifications of cyber security requirements. Together with common topics from these specifications and topics that are common through the projects the employees work on, it affects the framework's design. Reviews of the framework, along with a second survey, allow for an evaluation of whether or not it is suitable and what topics are missing that were not discovered during the first survey that may be relevant to apply.

3.1 Considerations

3.1.1 Case scenario

Guidant Measurement is the company used as the case for the development of a custom framework for the documentation package. While the company is a recent spin-off from TechnipFMC [53], the control system and equipment which the Control System department delivers are still the same with the same people and the same clients. Guidant provides a tailored made control system configured to the client's needs in the oil industry. The metering control system provides a complete picture of operations and measuring from production to storage facilities [54]. With real-time data, the operators can monitor flow, leakage detection and meter diagnostics, which also increases the safety and reliability of the system [54].

This research focuses on creating a framework and documentation package at the project level that fits the company's needs. The employees have struggled with a lack of experience and procedures of their own regarding cyber security measures, which creates problems in understanding the requirements that the clients have for their deliveries. Due to the metering control systems integration into the client's network, the cyber security requirements that the clients have are not always applicable to the control system as the requirements are for the whole system and not separated for

the specific little part which is the control system in the big picture. The main goal for the case is to develop a framework which contains cyber security requirements which apply to their deliveries but also complement the requirements of the clients to avoid issues.

3.1.2 Ethical consideration

This study includes participants in surveys and discussions. During the study, all the participants were anonymous and about that fact. The participants have also been informed about the purpose of the different surveys and discussion.

The use of the company's clients' specifications as the base for finding common topics of interest, the clients' specifications shall not be referenced but kept anonymous in this study due to confidentiality and to protect client information.

3.2 Design Science Research Methodology

Through the literature, three papers focus on the use of DSRM, whereas the other papers do not centre much on the specific methodology used in their work. The papers in the literature review that have used the DSRM, have also used it in order to create framework which would be used on the organizational level. The goal of this study is to develop a framework, which can be used in project deliveries. As the DSRM centres around developing an artifact to solve specific problems, it is deemed a good match for this study.

The Methodology

De Sordi [14] describes that there are two distinctions that needs to be understood. The natural science focuses on the physical and abstract, and the artificial which focuses on an entity to provide functionality [14]. The the artificial science are one of the core concepts of DSR [14]. From existing theories and knowledge, the artifact developed shall come forth with a solution to a defined problem [42]. It has also been emphasized that the methodology should be used for addressing relevant and important issues [42]. From the study of similar solutions, there appears to be a gap in the area of focus. The current focus areas are on the typical organisational level, and not on a product level the organisation could provide as a supplier. Through the existing work, it is clear that a standard or framework is not a one-size-fits-all, where to goal for the artifact is to create a solution that fits the product level for a supplier. A part of the artificial science, the idea of the artifact, could be used to create benefits for a third-party [14]. As long as the required functionality for the situation is in place, is valid and useful, the space of problem in DSR does not need an absolute and ample truth for all

situations [14]. There is room to focus the solution on a single location or situation, as long as the artifact is valid and useful for the selected context.

The six steps from Peffers et. al [13] is divided into three phases, to separate the main activities. These three phases are the illustration of the workflow in this study, figure 4 which is based on the methodology from Peffers et. al. [13]. The first phase focuses on the problem identification and objectives for a solution. The second focuses on the development and demonstration. The third phase focuses on the finalisation with the evaluation and communication of the artifact for its users.

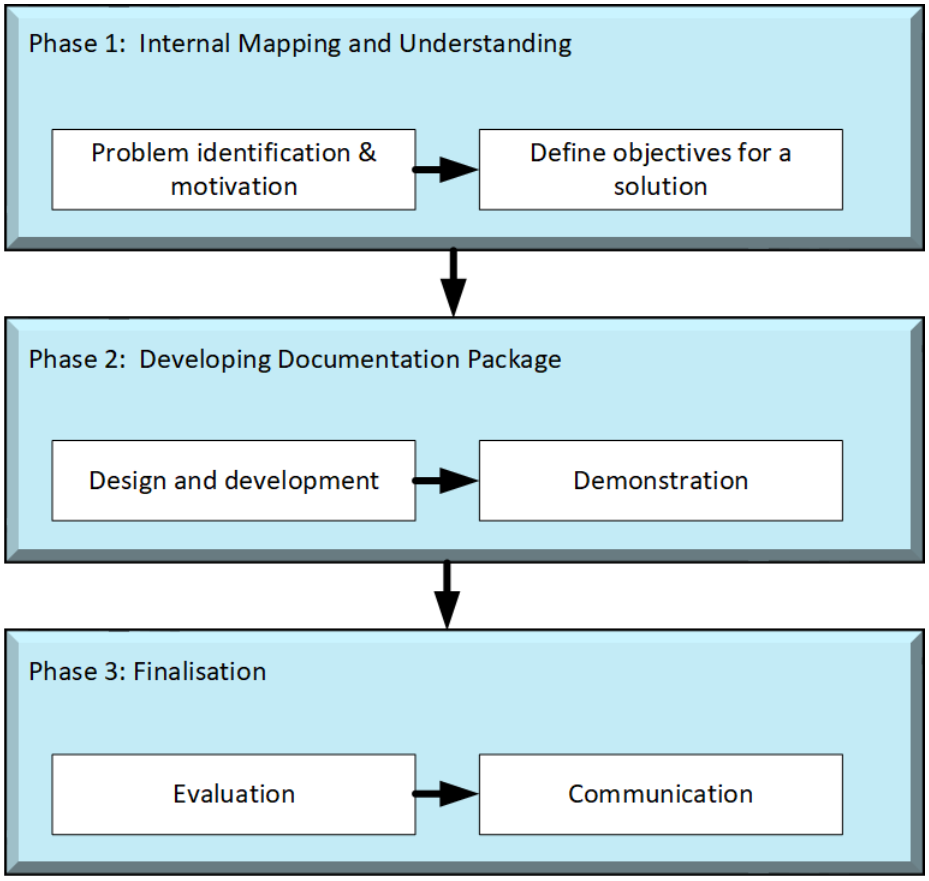


Figure 4: DRSM process model

3.3 Phase 1: Internal Mapping and Understanding

This section focuses on the first two steps of the DSRM [13, 14]. To effectively develop a solution, it is crucial to define the problem first and then create an artifact as a solution [13]. Communication with the practitioners who will use the artifact to solve their problems could help improve the manifestation of the problem of its perception [14]. As for the motivation part of the first step of DSRM, including the current status of the problem's knowledge applies context to the motivation of the problem [14] [13].

From problem definition, the definition of objects for a solution shall rise from knowledge, and the solution needs to be both possible and feasible to achieve [13] as well as avoiding the unachievable parts [14]. This is why it is important to know of the current problems and solutions to the topic [13].

3.3.1 Problem Identification and Motivation

Through studying existing literature focusing on customizing a framework for the fitted need, the studies performed show that the existing focus area lies on the organizational and national levels. Some of the previous work uses the same methodology approach towards small and medium-sized businesses [8], and the banking sector [7], however, these solutions are still on the organisational level. The current literature leaves a gap in the product level an organization can supply. To focus the work further, a single case situation will be used to develop and test the proposed artefact's functionality. As other solutions have fitted solutions to their cases, this study follows the same direction, only at a different level than the others, down at the product/project delivery level where existing literature lacks information on the topic.

As clients usually have their own specifications to follow in a project, it does not mean that all the requirements fit all the suppliers the clients use. The following work in this study is collecting different client specifications to compare for common topics. Following the specification collection and comparison, a survey issued shall give guidance to where the common issues arise when working with cyber security in projects, as well as the common topics that the employees faces the most.

Survey: The purpose of the survey of the company's employees was to get a qualitative understanding of the current cyber security picture in their project deliveries, which includes taking into account their products.

1. In your opinion, to what degree is cyber security made a priority in project deliveries?
2. What steps do you personally take to ensure good cyber security in project deliveries?
3. Can you list what cyber security requirements and standards that customers request that *company* adhere to?
4. What type of cyber security related issues do you find in the interfacing between *company* and their customers?
5. Which of the cyber security related requests and issues are more challenging to follow up from the perspective of *company*?
6. In your opinion, what cyber security related actions and initiatives is it appropriate that we to perform in our projects? (e.g. hardening, firewall configuration, documentation et cetera)
7. What type of resources such as automation scripts, templates, checklist and so forth, would you find helpful in your efforts to comply with cyber security requirements?

Participation and data collection: The survey was handed to participants through their manager. The participants either have extended knowledge working in project deliveries or are quite new employees who are just starting to learn the area of work with the routines. With a few newer employees, their judgment could have some bias towards their mentors in the department. Another factor which could also provide bias is the fact that the company the department is in is also the employer of this study's researcher.

Survey analysis: This part of the survey consists of manually analysing the results, by highlighting the most common issues and wishes suggested for a possible solution to the problem. The main steps to follow in the analysis are to first review the results, then organise the results, and finally interpret the results.

3.3.2 Definition of the Objectives for a Solution

Through the study of existing solutions, some of the papers have already achieved creating their desired solution for organisations using DSRM [6] [7] [8]. Whereas the other papers creating their solutions does not mention the use of DSRM, but they were also able to achieve their goals. With interviews and surveys, those papers covered in the previous chapter were able to get a visualisation of their current situation, which also applies for this study, as well as identifying requested solutions.

Based on the results of the survey conducted for this study with the presented case situation, the clear view was there is no great solution for handling cyber security requests in projects, and that there is a need to have a framework that is fitted for project deliveries of their products. As well as relevant document templates where applicable and solutions for automation of the practical part of the framework.

In order to be able to achieve the goal, the clients standards and official standards they refers to has to be collected in order to get an overview of topics that can be relevant to consider feasible to apply in the framework for the supplier side, as the clients framework may be applicable to their entire project and not only for the specific supplier, resulting in much content not being applicable. By studying the different client standards, to find official standards that they refers to, comparing common topics through the different client standards. Where the topics that occurs the most will be highest on the list to evaluate if it fits the delivery part, if so, then included in the new framework with reference to the official standard.

Based on the resulting framework, the framework can be used as a base to creating a checklist for documentation of execution especially for the practical parts, and for the creation of an automation script to ease the time used on the practical parts that needs to be executed in projects. Where possible, also create templates, which could be used to e.g. documentation of the product. This template could include the standard ports and protocols being used in the project, what sort of protection provided for ports not in use. Where this template could include the standard equipment being used, with possibility to be multiplied for the amount of the equipment.

3.4 Phase 2: Developing Documentation Package

This phase of the study focuses on the third and forth part of the DSRM. For designing and development of the artifact shall follow the objective from the previous step [14]. To construct a solution, it is need to have actions and resources available in order to create a design to a realistic problem [42]. As the solution as an artifact can be anything as long as it has the desired functionality [13], the design concept being communicated can take different forms of diagrams, models and/or procedures with its users [14].

The part of demonstration, the purpose is to have all of the components and concepts being tested as the goal is to get the artifact evaluated to see if it solves the problem as a proof-of-concept [14]. Hevner et. al. [42] covers different methods to test a proposed concept, the most promising method is controlled experiment due to the artifact being tested in a controlled environment for its qualities and usability.

3.4.1 Design and Development

Based on the results from the survey, the wishes for the artifact is to include a checklist and automation script for the practical part of a custom framework, as well as designing a custom framework fitted towards project deliveries. With the collection of the different client standards and the official standards they refer to, the clients standards gives a pinpoint to topic important for consideration for inclusion in the custom framework. The topics of importance from the client standards and official standards shall be included in the custom framework shall be referring to the official standards and not the client standard, to avoid second-hand information. The custom framework shall have a reference list between the different topics and which standard they refer to, to make it easier to give specific updates whenever the official standard has a new update to different topics.

Based on the result of the designed custom framework, a checklist shall be developed to comply to the practical execution of the framework to add towards documentation purposes. A script developed towards the execution of the framework shall be to automate the execution where possible from the framework, to help decreasing execution time of the framework.

The documentation package shall also include other documentation templates. One of the documentation templates shall include standard/common equipment usually used in projects, where commonly used ports and protocols can be prepared in advance, and can be multiplied and/or modified based on the number of equipment in the project and its usage if deviating from standard. The

document shall also include different protection mechanisms possible, such as disabled in software and/or physical port blocks, and so on. Another documentation template shall include a network topology template of standard/common equipment in project deliveries at their respective security levels.

3.4.2 Demonstration

With a part of the demonstration process being a demonstration of proof-of-concept [14], the demonstration of the concept shall be done through an internal design review with a few selected employees with the most experience from projects including cyber security. Design review of the custom framework allows these employees to give direct feedback on the concept. This part of the process can give the first part of feedback for whether parts is missing, irrelevant for their projects, and/or needs adjustments.

3.5 Phase 3: Finalising

The last phase focuses on evaluation and communication. The artifact must have good quality and design being both pleasing for the designer and user [42]. A part of the evaluation of the artifact includes a discussion of concerns and deficiencies the proposed artifact has [14]. By including the practitioners who will use the artifact, their feedback on the evaluation could be natural [14]. The different methods for evaluation from Hevner et. al. [42] could be applied for evaluation. Based on the results of evaluation, it may be necessary to make adjustments resulting in iterating back to the design and development part [13].

It is important to utilize the most effective media in order to inform the practitioners of the potential of the artifact [14]. In the communication, it shall be communicated of the problem and its solution, the artifact, and its design and effectiveness [13].

3.5.1 Evaluation

This part will include responses in a larger scale than the design review since this part can include feedback from more people who will evaluate the functionality and usability of the artifact. This part builds on the previous step of demonstrating the concept, where the user can be able to test for themselves in a controlled environment. The feedback can be provided through a survey.

Survey: The purpose of this survey is to get an evaluation from the employees who have experience from working with projects, and get an evaluation of whether the framework is reasonable or not to apply to their scope of work. The evaluation also takes into account any confusion and topics that might be missing, which the participants did not consider themselves during the previous survey

1. What is your opinion of using the new framework as the baseline for cyber security requirements in projects?
2. Do you understand the responsibilities you get regarding complying with the framework? If not, please explain what you find unclear?
3. Are there any areas that are unclear in the framework?
4. Are there any topics that you think are missing in the framework?
5. What kinds of difficulties do you think might arise from applying the framework in projects?
6. What steps do you feel appropriate to take as a next step to further improve cyber security in projects?

3.5.2 Communication

There are a few ways the artifact can be communicated to the users for this case scenario. An option is to demonstrate and inform through a meeting such as a department meeting. An other option is to provide the information regarding the artifact of its usage and purposes to a manager to distribute to relevant employees needing the artifact in their work. The third option is to inform project leaders of the new solution to deploy in their projects, and inform relevant employee working on the project to utilise the new solution. Where in this situation, a combination of all three is preferred due to the information being available to all necessary parties that can deploy the artifact in their projects.

4 Results

This chapter focuses on the different results achieved during the different phases of progress in this study. Where each section phase follows the sections from the previous chapter. The appendix contains the framework result after the last phase of this study.

4.1 Phase 1: Internal Mapping and Understanding

This section focuses on the gathered results from section 3.3, which focuses on problem identification and motivation, and definitions of the objectives for a solution. These two areas of Phase 1 focus on gathering qualitative data on the current situation in project deliveries, different kinds of issues that arise in projects and what sort of solutions are preferable to have. The other part is comparing the different client specifications to locate common official standards used as well as common topics mentioned between the specifications. With the combination of these results, creating objectives for what the documentation package shall include to provide improvements to the current status in future project deliveries.

4.1.1 Survey

The survey was handed to 15 possible participants through their manager, who either works with product development or project deliveries. The survey was answered by 13 participants. Throughout the survey, the answers vary throughout the different questions. Some answers are Not Applicable (N/A) due to participants not having answers from their side of work in the company, those answers for the questions are excluded, whereas their answers not being N/A are included.

1. **In your opinion, to what degree is cyber security made a priority in project deliveries?**

   The overall results show that the prioritisation lies with high priority from the client side, and even that does differ based on the project type. Project type means that there is a brand new project or an addition/upgrade to an existing one. However, the increase in focus applies to the existing ones as well, even if not as much as the new projects. Other than the pressure of prioritisation from the client side, without that, the prioritisation internally is too low.

   The survey also includes that from the client side to the supplier side, that the client's requirements are far more time-consuming than planned to achieve satisfactory performance.

2. **What steps do you personally take to ensure good cyber security in project deliveries?**

   Two of the responses state that they want to include a cyber security resource in this area of their projects, whereas five of the others mention the use of self-assessment and other documentation templates being filled out during the projects where one of these participants mentions special document developed for them as supplier to fill out. As for six of the other responses, mentioning either security for network traffic such as encryption and preventing leakage of IP addresses and passwords to the wrong person/s. With different types of experiences, the results are visible in what different areas have been noticed as notable to remember.

   Another point of note is that most of the responses mention that the employees only do what is required from them by the clients with the most mentioning of documentation.

3. **Can you list what cyber security requirements and standards that customers request that *company* adhere to?**

   Six of the responses state that they do not know any specific standards or requirements the clients request them to adhere to. Where three of the responses point to IEC 62443 from the client's requirement document, two to the client's documents, and the other two point to specific actions. Where these actions are passwords, firewalls, encryption, virus protection, and data handling practices.

4. **What type of cyber security related issues do you find in the interfacing between *company* and their customers?**

   One of the answers to this question was that they did not find any issues or have had involvement in projects where issues could have arrived, and another did not have such involvement in projects. Four others mention one or more issues regarding documentation, wishing for templates/"standards" for delivery of typical equipment in projects, and the lateness of the mention of cyber security in projects. Whereas the lateness has been improved.

   Seven of the answers mention either one or more of the following; their trouble regarding networks, passwords, firewalls, interfaces between hardware according to requirements and others mentioned below.

5. **Which of the cyber security related requests and issues are more challenging to follow up from the perspective of *company*?**

   Documentation appears to be one of the problems three of the answered employees face as challenging requests to follow up. As well as three others either meet the challenge of limited time for performance or lack of knowledge on the topic. Seven of the responses meet challenges for one or more regarding password management/access control, firewalls, fixing vulnerabilities in older systems/hardware, hardening and firewalls, and proper training.

6. **In your opinion, what cyber security related actions and initiatives is it appropriate that we to perform in our projects? (e.g. hardening, firewall configuration, documentation et cetera)**

   From the responses, seven of the responses were in regards to documentation, however, the responses in regards to what kind of documentation differed. Some just mention documentation in general, whereas three of them mean either appropriate documentation such as system and network topology, analysis of zones and conduit and self-assessment. Six of the answers focus more on either one or more of the following; secure setup, incident response plan, use of certificates and encryption, audits, password vault, firewalls, backup and hardening. And some on having a list of who is expected to be responsible for what in a project, like what the supplier and client are supposed to be responsible for, such as the client being responsible for the virtual machine.

7. **What type of resources such as automation scripts, templates, checklist and so forth, would you find helpful in your efforts to comply with cyber security requirements?**

   12 out of 13 of the answers to this question want documentation templates, that take into account commonly used equipment, the second-ranking answer is a wish for a checklist for documentation, and then automation of the different necessary actions. Three answers want either network topology with conduits, knowledge of firewall requirements and security solutions for servers and network communication. Whereas five of the answers want automation towards execution, one also wants a script for regularly checking for threats.

Notable areas from survey question two and four

- Secure network communication/ encryption
- Communication on different VLANs
- Firewalls
- Documents/templates
- Participate in meetings/ discussions
- Requirements to specific hardware
- Access control/ authentication methods/ password management
- Awareness towards fishing
- Software updates
- Training
- Backup solutions
- Patch management
- Hardening (both in software and hardware with port blockers)
- Secure protocols

4.1.2 Study of standards

Through this study, four client specifications were gathered to study. By studying the specifications the goals were to identify the common standards referenced to as well as the common topics between the specifications. As there is a different variety of standards being referenced through the different specifications, table 3 shows the most commonly referenced standards and the number of occurrences between them.

Standard	Client occurrence
IEC 62443-3-3	4/4
IEC 62443-2-1	3/4
IEC 62443-2-4	3/4
IEC 62443-3-2	3/4
IEC 62443-3-1	2/4

Table 3: Most common standards referenced

Further into studying the different topics in the different client specifications, table 4 shows the most common topics across the specifications as well as the number of occurrences in them.

Topic	Client occurrence
Firewall	4/4
Backup and recovery	4/4
Network segregation	3/4
Antivirus	2/4
Account management	3/4
Hardening	3/4
Updates and Patching	4/4
Malware	3/4
Remote access	4/4
Time sync	4/4
Traffic	3/4
A@P	4/4
Topology	4/4
Equipment List	4/4
IEC 61850	4/4
Port & Protocols	4/4

Table 4: Common topics

4.1.3 Objectives for the package

The objectives for the documentation package were derived from the survey responses and the review of the clients' specifications. With the repetition of documentation in project deliveries regarding cyber security will be the main goal for improving the current state. The package shall include templates for:

- Custom framework fitted for projects
- Checklist for execution of framework for documentation
- Template for equipment list with typical/standard equipment listed
- Templates for network topology, zones and conduits

The framework shall include the common topics between the common issues faced in projects and common topics between the client's specifications. The custom framework shall include specific references between the framework chapters and section, and the official IEC 62443 chapters and section, to allow easier update whenever an update arrives. As for the content of the framework, it shall minimum include:

- Ports and protocols
- Backup and recovery
- Network (segregation, zones and conduits)
- Antivirus and antimalware
- Account management
- Hardening
- Updates and patching
- Firewalls
- Equipment list

4.2 Phase 2: Developing the Documentation Package

The second phase of this study focuses on the design and development, and demonstration of the artifact. The design and development build on the results of the previous phase and the demonstration will be done as a proof-of-concept.

4.2.1 Designing and Developing the Artifact

The design of the custom framework follows a document template used in this study. The framework template shall include general information, terms, definitions and abbreviations, references, the framework and a checklist. A clear difference in the design of the reference list in the framework document is that there is a cross-reference table which links the different sections in the custom framework with the specific sections that have been used for reference, whereas the clients' frameworks only reference to the standard used with no more specifics. This enables the framework's users to find and read the original source more easily, as well as enabling the possibility to update the framework easier whenever an update to the original standards arrives. As for the framework, it contains the minimum listed in Section 4.1.3, and the checklist is designed to document the execution.

The custom framework's section that are based on IEC, which states that information shall be in procedures for execution, example backup, the framework therefor states also that it shall be mention in procedures such as installation procedure. The checklist has then points for the user to remember to make sure that the necessary information for execution is described in the procedure. The framework is not meant for contain other information than what should be applicable and documentation for the framework has been followed. Meaning the different procedures needed to be followed shall be described in the corresponding documentation for different procedures and manuals for the execution of the different requirements.

One of the experiences that some of the employees has from cyber security in their projects are that they have to define zones and conduit, identify security levels for equipment delivered. The framework has a section that follows up on information for the requirements regarding how this shall be done. It contains the reference model for IEC [55] as well as an example of which level typical equipment of a project shall be placed, Figure 5. It also states that topology templates shall be used, and have the requirements for placement of zones, conduits and security level applied.

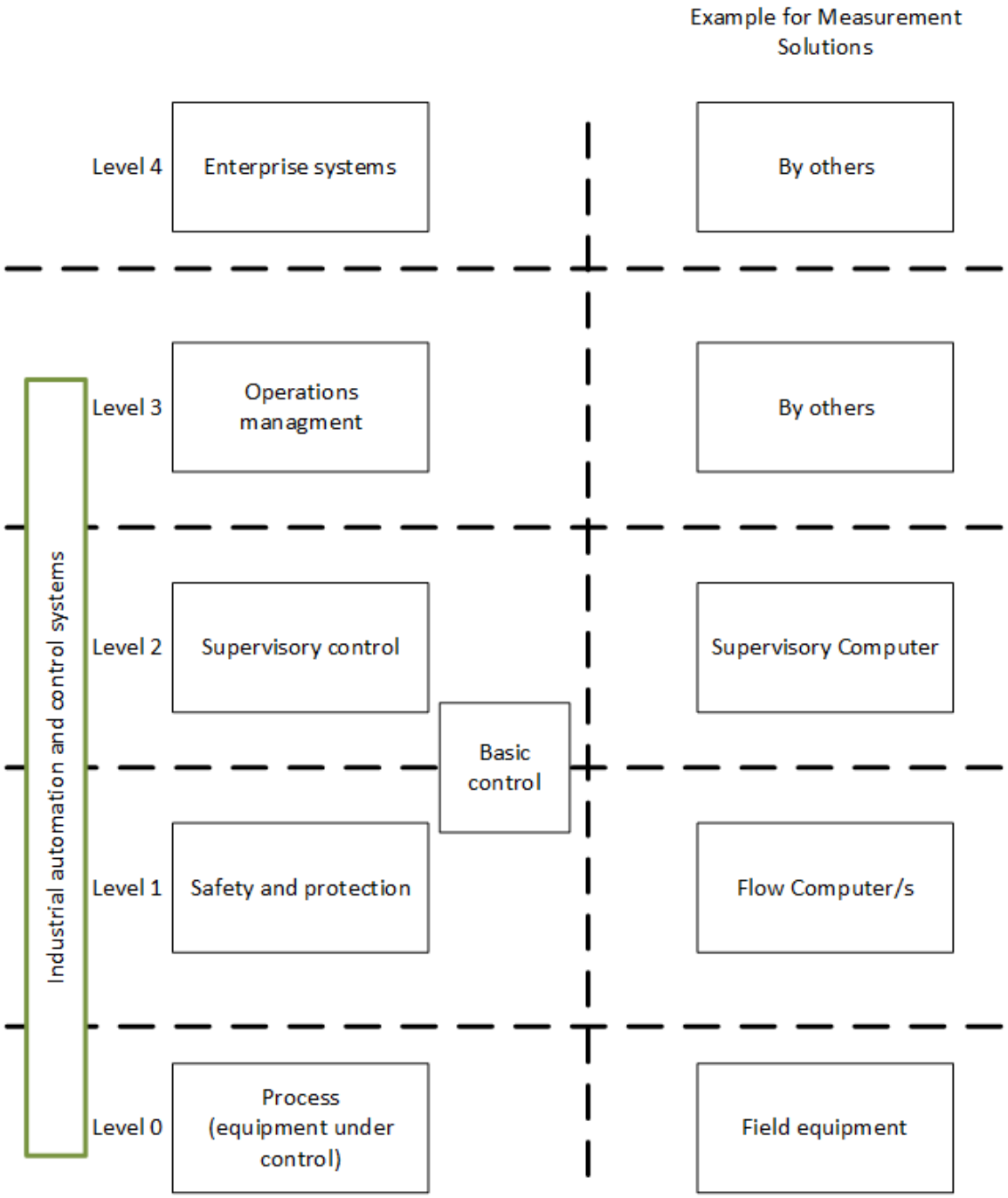


Figure 5: Reference model for IEC 62443 to the left, example for applying for Measurement Solutions to the right

Regarding the requirements for accounts (user groups, authenticator, password and sessions), the framework is mixed of recommendation from both IEC and NIST. That is with regards to what is possible to achieve and not. The framework contains what is achievable. IEC recommend that passwords shall have a time limit [56], whereas NIST [57] does not recommend it as changing password as it can create user frustration and the passwords can be more predictable to guess. In the case for password, the recommendation from NIST has been the preferred choice to follow. However, checking passwords towards a blacklist as NIST [57] recommends is not something that is possible to perform

for the case used, but the passwords shall be changed by the client upon a project delivery, and the client is free to apply their own requirements as they see fit if they want to apply stricter policies and requirements than delivered in the project as it can be integrated into their system.

Other consideration in the framework are that the where the IEC standard opens for the either the supplier or client as asset owner to be the responsible party for the following of a requirement, the custom framework puts the responsibility for that requirement to the client, however, it is describe an option for whenever the client are too insistent that the supplier shall be the one responsible. Firewall is an example of this, where IEC 62443-2-4 [58] notes that the responsibility can be transferred to the asset owner either prior to or at project turnover, where the framework leaves the responsibility to the asset owner (client), but supplier can be the responsible if client insists. Else, the framework has the requirements based on the IEC 62443 standard for the different sections.

Internal discussion with employees in the design phase

During the design phase of the framework document, there have been three small discussions with a few of the employees of the study's case. Where there has been a discussion with one of the employees with the most experience of participating in projects with a focus on cyber security in regards to what is possible to achieve and not, with the focus lying on users and passwords, with the results as stated above. Another employee was clear that the framework cannot open up for self-thinking, and that it has to be stated clearly what shall be done in the framework, but have the option to modify the responsibility only if the client is insisting.

Other than that, there has been positive feedback from three project engineers and one project manager to the design of the framework document. They were most positive to the cross-reference table between the framework's content and the specific sections in the standards for easy look-up if the need occurs to look into the original source, as well for future updates.

4.2.2 Demonstration

Results from Design Review

Review 1

This has been documented with the draft before review, a draft with the comments from review, and the document being applied with the necessary changes to track the progress before, from and after the review.

Four out of seven attended the design review for the custom framework. Based on the responses from the meeting, the attendees were positive to the results of the framework. However, there was a few places that the attendees felt that needed to be modified due to them being unclear, and missing information. The necessary changes discussed are as followed:

- Make the text clear to leave no room for doubt about who is responsible for what, as this has occurred in a few of the sections
- Add "By others" to the example with the reference model
- Rename the Equipment List to Self-Assessment
- Add sub-suppliers to the requirements where appropriate, such as the Self-Assessment
- Even though NIST suggest minimum 8 characters for password, the employees wants a minimum 12 characters long password
- Specify that the requirement for follow-up on updates and patching applies through a maintenance contract
- Backup - Remove the reference to the installation procedure, and add reference to the operation and maintenance manual instead. Also add the manual to the recovery section
- Make the Antivirus/malware section clear on the responsibility part
- Add requirement regarding protection of equipment being shipped against tampering
- Update the checklist according to the changes in the framework

It was also discussed that the "Read for shipment" document has not been updated for some time, and that it needs an update, where that document needs a check-point confirming that the cyber security checklist has been completed before equipment shall be shipped to client.

Review 2

In the second round of review where five out of seven participants present. The purpose of the second review were to review the changes in the framework which is based on the feedback from the previous review. The overall response from the review was that the document now looks good, with a few minor changes needed without the need for a new review.

- Only use blue text for information and text to be changed in project, do not use multiple colors to differ between information and editable, since that is not how a document template usually are
- Just have a general description in definitions for sup-suppliers
- Add references to the documents in the checklist

After the review of the framework, the discussion when towards other documents, that different procedures and documents needs to be updated according the framework. That there is a need for more templates for system and network topology, self-assessment, and "Ready for shipping", as well as the offer phase for projects needs to be clear on what requirements in cyber security shall be followed, if following the framework or the requirements clients have, as well as who is responsible for what concerning equipment and requirement to them.

4.3 Phase 3: Finalising

The third and last phase focuses on the evaluation of the framework through a survey with the same group of employees who participated in the first survey.

4.3.1 Evaluation

Results from survey:
13 out of 16 participants in this survey has answered. One of the participants has answered they do not have any experience in regards to cyber security on all questions and is therefore not in results below. One participant called for a one-to-one meeting with questions and comments to the framework, where the overall comments were regarding the formatting of the document, such as font size and headings, as well as wondering if the checklist should be a separate document. With a discussion with document control, the conclusion to that question is yes, the checklist shall be a separate document. This is because the framework works as a procedure and the checklist as a report.

1. **What is your opinion of using the new framework as the baseline for cyber security requirements in projects?**
   Four of the participants answered that they view the framework positively. Two think this could be a good tool to use for the work regarding cyber security, and two of them assume it will be updated regularly through the years and when gained experience. Four answered that the framework is good, that it is a good idea to have, one stated that it looks useful. One answered that the framework is a good guideline to follow, understands that it is to follow when evaluating cyber security implementation to the devices, Two wondered if the document shall be sent to client or not.

2. **Do you understand the responsibilities you get regarding complying with the framework? If not, please explain what you find unclear?**
   Nine of the answers were "yes" for understanding, but that one pointed out a section they think would need technical expertise to understand fully. Four of the participants answered that they think they understand the responsibilities regarding complying with the framework, where one asked if it could be used to document compliance to client requirements, one of them mentioned that mostly in projects they do not have any responsibility other than supporting clients to achieve theirs, and one answered no and asked where the responsibilities have been written. One answered that it is unclear who should be responsible if it is the software engineer or a dedicated cyber security responsible, but that it looks like the software engineer is responsible for ensuring the checklist is completed.

3. **Are there any areas that are unclear in the framework?**

   To this question, one of the participants did not answer, another answered N/A due to not working on projects. One answered they needed information on how the requirements could be implemented, and one requested a more specific description of what sort of action is required in the checklist. Three answered no. One wonders what the self-assessment sheet would look like and how it would be completed. Another thinks the requirements for sub-suppliers look unclear, and there are possible difficulties in having the sub-suppliers fill out their parts of the self-assessment. One asks what an authenticator is. One answered that it is not clear what the checklist is for if it is for the individual types of equipment that are usually a part of their delivery due to some requirements not being achievable for all types of equipment. One answered how to verify only documented communication is allowed and how to verify unnecessary functions, ports etc are disabled.

4. **Are there any topics that you think are missing in the framework?**

   Five of the participants answered no to this question, and one of them mentioned that using the framework in projects could reveal missing topics. One has answered that they miss information about emerging threats and industry-specific regulations. One answered encryption. Two answered self-assessment sheet, where one of them mentioned that it has a short description of it and that all devices shall be assessed for specific IEC requirements. One answered how to properly handle sensitive information/documentation in the transmittal. One answered CSNE IAT/FAT requirements and typicals, as well as requirements for sub-suppliers. One asked if OPC UA should be mentioned and may be configured with private keys.

5. **What kinds of difficulties do you think might arise from applying the framework in projects?**

   One of the participants answered setting and documenting policies, which could create difficulties using different operative systems and versions if using scripts, as well as document handling from project to project (such as storage of checklist, having design review or verification of execution). One answered whose responsibility it is to comply. One answered resource constraints, interpretation and implementation. One answered firewalls as for them the topic is new. Three answered that issues may arise due to client specifications containing different information than the new custom framework, one mentioned collecting specifications from sub-suppliers to the self-assessment, and another focused on the framework not being capable of covering the clients' requirements. Where one says no, another sees the problem not having the checklist as a separate document. One answered being accountable to follow requirements and guidelines from the clients. One answered if they comply to client requirements or not. One answered they do not know.

6. **What steps do you feel appropriate to take as a next step to further improve cyber security in projects?**

   One of the answers was starting to implement the use into projects, as well as updating the relevant procedures and manuals to be according to the framework. Two of the answers included automation where possible according to the policies of the framework, and to other answered having design reviews to incorporate feedback into the framework. One also included in their answer providing training and fostering a continuous improvement for cyber security practices. Four answers focused on document templates, where one specifies such as for network topology and self-assessment, and one of them also asked about management requirements. One answered they did not know due to not working on projects. Another answered training, due to the need for a change of mindset to understand threats and action for mitigation. One answered automation of the processes. One answered implementing strong passwords.

Based on results from the second survey focusing on the created framework, the feedback on the framework for use in projects was very positive. As some answered it looks like a good idea and looks useful, others are prepared for updates to come when experience has been gained through use in projects. Most of the participant either understand their responsibility or think that they, except one. As most participants understand their responsibility, some areas in the framework are unclear. The most common topic that is unclear is regarding the self-assessment with a lack of information on the execution of completing it. Other sections that look unclear also regard a more specific description of information. Following the request for more information on the self-assessment, templates and document handling are information missing in the framework and the package.

The most common answer regarding expected difficulties from applying the framework in projects is whether or not it covers the requirements that the clients have. Other participants focus on following and executing the different necessary actions.

For the next step, most of the participants want the framework to be used in projects and the necessary documents to be updated and actions in the framework to be automated for execution. Where the framework shall be updated concerning experience gained through using it. One answered the need for training.

Design Review after Survey Modifications

The new revision of the framework has modifications based on the survey results. The feedback from the survey that has been considered into the new revision were:

- Separating the different specific actions in the checklist from bullet points into separate action row
- Be more specific on requirements for sub-suppliers
- Add a description of authenticator in definitions
- Add a deeper description for the usage of the checklist
- Document handling described
- CSNE IAT/FAT procedure described

Based on the review with four employees, the participants were content with the new changes, which were based on the feedback incorporated into this framework revision. Once the framework is ready for use, the next step in their eyes will be for documents to be updated according to this framework and for other document templates to be created.

4.4 Documentation Package content

Through surveys, discussions, and design reviews regarding the documentation package, not only do several documents need to be updated regarding different procedures to comply with the requirements gained from the IEC 62443 standard and NIST publications, but new document templates need to be created to comply with the rest based on the lack of document templates from the used case. Even though these new document templates shall be project-specific when used, they shall be general and use commonly used equipment. As these documents are aligned towards complying with the framework, the documentation package shall include the following documents based on this study's findings from the used case:

- Framework
- Network topology (physical and logical)
- Self-assessment
- CSNE IAT/FAT procedure

5 Discussion

This chapter focuses on the discussion between the research question in this study and the results from the previous chapter with results.

5.1 Research question 1

What are the commonalities between the standards from the customers in the industry and what differs between them in their requirements?

Eckhart et al. [33] view that responsibility from one asset owner to another can cause different challenges, and this is confirmed in this study based on the different levels of knowledge the case employees have when working on projects. However, the requirements from different asset owners in the used case are confirmed to differ as there is not a one-size-fits-all [11] [12]. It confirms that the different clients as asset owners have their own unique set of requirements. When the framework was created in this study, it was important to be aware of the clients' requirements to be as cooperative as possible with as many of them as possible. Being able to meet what they actually need [59].

This research question was a part of the first phase of this study. Where the point was to collect different clients' specifications to compare. The results were illustrated in two tables, see table 3 and 4, which show how common the different standards used are and how common the different topics are. The results show that IEC 62443-3-3 is the most common standard used as it is used across all of the specifications from the clients, whereas the IEC 62443-3-1 is less commonly used as it is referenced by only half the specifications in this study. Regarding the topics, firewalls and backup and recovery are topics that are common across all the specifications, whereas antivirus is a less common topic in the specifications. The difference in how common topics and referenced standards are brought forth how important certain topics and standards are over each other.

This comparison is, however, not an exact solution to which topics are to be prioritised for the custom framework. The results also depending the topics the employees come across as more common when they interact with the clients, even though this gives a perspective of which may be relevant. Additionally, the results from the first survey in this study show that topics like network topology, antivirus, firewalls, and more topics have been viewed as important from both the clients' specifications and through the employee's experience when they have worked on projects.

It also has to be noted that even though the participants in the survey are from the same company, the experience of cyber security does vary based on how the clients have previously initiated the focus in their projects. The results from the survey are then biased towards the clients the different employees have worked with, which may differ from employee to employee. Where a few employees may have worked with a client who focuses more on a specific topic than others with a different client. This may result in some topics being mentioned as more common even if it is from one client that is common across projects for multiple employees, whereas then other topics are viewed as less common due to not as many employees working with that client compared to other clients.

5.2 Research question 2

How do the employees work to fulfil the customer's standards and requirements?

Eckhart et al. [33] study has focused on automation systems for cyber-physical systems, where it was made clear that security-related methods and activities are designed generally. However, as the study focuses on designing a solution that shall improve security-related activities, it also focuses on the area where there is a lack of knowledge in the area they are to fill. Eckhart et al. [33] do point to the fact that challenges do arise when responsibilities are shifted from the asset owner to the system integrator, which is why it is important for training, tools, and methods for the engineers to gain the necessary knowledge that they need.

Based on the literature review, the article from Eckhart et al. [33] is closer to the project level than an organisational level than the other articles from the review. However, as it focuses on methods to improve the situation of responsibility shifting, it does not focus on how different actors, other than the asset owner, face their problems and how to meet the expectations of asset owners.

This research focuses on how such expectations are being met in the current situation in which they are used. Based on the results from the first survey, the employees find it difficult to work with cyber security in projects due to a lack of knowledge, especially regarding the requirements which shall apply to them as suppliers from the client's specifications. So far, the internal prioritisation of the company has been too low on the topic, and cyber security is quite time-consuming to achieve a satisfactory level of performance, which is why some employees wish for a dedicated resource who knows the topic. At the minimum, the employees have done what the clients have asked of them.

Even though the employees' different knowledge of cyber security mirrors the responses in both surveys. Some answers provide specific actions and topics to prioritise, while others focus more on the lack of time and resources to support their projects. For those participants who have participated in projects where cyber security occurs, the answers to the questions vary in depth based on their experience, as some gave short answers. Others gave longer ones with different focus areas based on their experience.

The first survey noted that the topics of lack of knowledge and cyber security being time-consuming should be management issues. Those leading the projects should prioritise the time needed in the project scope for cyber security and have a resource familiar with cyber security. This way, the cyber security in each project could be more satisfactory than the bare minimum of what the client requests and not become an afterthought due to the amount of work in the rest of the project.

However, the participants in the first survey indicated different areas such as backup, hardening, and more, which they feel are appropriate actions that should be performed within cyber security in a project. They do wish for document templates and programs/scripts that could make the task of cyber security less time-consuming. This could allow the project engineer to perform as much as they possibly can with their level of knowledge for both project components and cyber security. Templates for documentation for known components that are regularly used in projects that the employees fill out themselves may also allow for less use of a dedicated resource to perform all of the cyber security self-assessment, where the cyber security resource may perform where there is no common equipment in the delivery as well as checking that the documentation that the project engineer has prepared is correct.

5.3 Research question 3

Is the artifact perceived as useful by developers, and how can it be further improved?

The overall responses from the employees regarding the custom framework for the documentation package were positive. The employees thought the framework could be a good idea; however, as most thought the framework was clear regarding who had the responsibility, some answered it was unclear. This response was improved for the document review following the survey. It must also be a part of the work process once the package is used in projects regarding who is responsible for what internally.

Regarding applying the framework in projects, some employees think issues may arise from the point that the framework does not match the specifications of each client. However, the framework does not match the specifications completely because it focuses on common topics the employees face in their projects, along with the topics from the different specifications used in this study. This means that at this stage, not all relevant topics that may be applicable have been included, but they should be applied if deemed applicable at a later stage. This is mostly due to variations in the different clients' specifications. The framework has to, in the end, cover the base of what the employees in this study deliver, where some topics in the client's specification may not be relevant, which is why it started with what is common.

This document shall evolve with experience from applying in projects when a new version of the standards referenced occurs and other standards and frameworks deemed fit. It may also evolve when the clients have new versions of their specifications to be as compatible as possible but still be unique towards what the case can deliver [59]. The continued development plan corresponds well to what Hevner et al. [42] describes for an artifact: the work is not done. The artifact can be consciously evaluated towards the new specification from the clients, and evaluate whether or not there is a need for changes in the artifact's design [42].

5.4 Method and process

In this study, the DRSM methodology was followed. A survey was performed to map the current issues in the case of the problem identification. As the first survey focuses on problem identification, have a few interviews with some of the more experienced employees from the case, which could have focused more on the work process internally and how the results became as they did in the survey. Which could be useful for planning how the artifact will be applied in their future projects. The interview could also have included more detailed information regarding what would be possible regarding the different topics of the cyber security requirement against the common equipment in a project, whereas this would be more relevant towards a self-assessment of the equipment as a template in the documentation package.

The development and evaluation of the framework revealed that multiple documents in the case needed information updates, as well as new document templates, such as testing templates, which were discovered during the evaluation. As these documents need an update, the requirement has been made as an action in the checklist, which may be removed as the document templates have been updated. Still, it should also be present in the checklist as long as the documents may not be

updated to future templates for existing projects. However, those points in the checklist could also be useful whenever standards used to have updates, resulting in the framework needing an update. This can be considered when a new revision of the framework is needed.

As for the demonstration and evaluation, there was good feedback during the design reviews, and a few selected employees with experience from projects with some cyber security attended the review. That way, it was possible to show the result of the development of the framework and for them to give feedback. That also allowed the employees to give an opinion in the review for where there could be a misunderstanding in the framework and topics that were not considered earlier when the objectives were defined to be added into the framework. The second survey also allowed a larger group of employees to give input on topics they might not have considered during the first survey.

As the methodology gave positive results based on employee feedback through the design review and survey, there is room for a different approach, such as interviews, as discussed earlier. Interviews could provide a different view of understanding, which could impact the artifact created. The methodology is then suited to be used with other types of approaches. In contrast, this study mainly focused on a strategy that used surveys and reviews of the artifact, as some of the articles from the literature review also used surveys to map organisations. Both surveys and interviews may be followed for problem identification and objective definition of the DSRM. This is a recommendation to get a deeper understanding of the issue at hand and to create specific objectives for when other companies may follow the same method for creating their frameworks and/or documentation on a project level.

6 Future Work

Future work may consist of applying other relevant topics that were less common from the client specification into the custom framework. It may also include other topics from the IEC 62443 standard that the client specifications do not focus on, as well as looking into other standards that were uncovered in the literature review such as ISO and deeper into NIST.

Regarding the documentation package, the next step for the development should be designing templates for the self-assessment and the two parts of the network topology, where the standard equipment in projects that is known is pre-filled out and easy to apply in the different projects where it is needed. The checklist in the document with the framework is for information to the client at the beginning of the project, so there should be a separate document containing the checklist as a report at a later stage. Developing a script or a program which can execute specific actions such as setting different password policies, hardening in the operating system, and more, could increase in efficiency for time used for configuring according to the framework.

Another step forward in the future is applying the documentation package in projects, to uncover issues and missing topics in the framework, and continuously improve the package with time and regular updates to be aligned with the latest revision of the different standards and framework which is included in the custom framework in the package.

7 Conclusion

This study focused on designing a framework for a documentation package for use in the industry. The focus was on the framework's practical use, depending on where it shall be used, giving theoretical and practical value to this research. Based on the response from the employees who will use the artifact, they were content with the development progress for use on a project level that is fitted towards use in project deliveries. When working on the framework for the documentation package, it was concluded that new document templates must be developed and included in the documentation package.

Following the development of the artifact, this study has closely collaborated with the employees regarding the framework covering the base needs. The base consists of requirements that commonly occur across different projects they deliver, where the framework is created to be universal for use across the other projects with various clients as far as possible, regarding what kind of equipment is also familiar to the deliveries. To create a framework containing the expected requirements, comparing clients' specifications, design reviews, discussions, and surveys with the case employees was performed to pinpoint the most relevant topic. The topics were then located in the IEC 62443 standard, and their requirements were pulled into the custom framework alongside some of the recommendations from NIST publications. While developing the framework, which is the artifact, the process includes the discovery of different documents within the company of the used case, as well as a need for new documents, which shall then be a part of the documentation package as templates for use in the case's project deliveries.

The existing literature focuses on cyber security measures that may be taken in different industry sectors. The methods used in the literature are composed of surveys to understand the current cyber security measures' current status for the different cases they focus on. The results gained are a framework for use on an organisational level. The same goes for the articles from the literature review that focus on using the DSRM to solve their problems. The articles from the literature have their solution to their cases, where their solutions differ in terms of what kinds of standards and frameworks they have used and how they have built their solution. Based on the literature review, the DSRM is deemed a suitable methodology due to the purpose of creating an artifact for solving a specific problem, and this has been combined with the method of performing surveys to map the current status and most common issues this study's case faces the most. This allows for the creation of a fitted framework that can take the employees' struggles and concerns into consideration of the artifact. The positive responses from the employees from the second survey during this research show promise that the

artifact created for use on a project level shows promise, where the next steps would be continuing the development and deploying it in projects to get real usability feedback.

However, due to the feedback from the survey, it is also important to consider that the artifact users will need some competence development on the subject, as well as management and project leaders' being able to allocate time for training and project execution. This is because some feedback has focused on the lack of prioritisation of cyber security in the projects the employees have been working on. As other articles from the literature review show, a lack of knowledge is not uncommon and can be improved by sharing knowledge, training, and communication.

References

[1] M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, "Exploring the top five evolving threats in cybersecurity: An in-depth overview," *Mesopotamian Journal of CyberSecurity*, vol. 2023, p. 57–63, Mar. 2023.

[2] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Future generation computer systems*, vol. 92, pp. 178–188, 2019.

[3] M. Fassnacht, C. Benz, D. Heinz, J. Leimstoll, and G. Satzger, "Barriers to data sharing among private sector organizations." `https://scholarspace.manoa.hawaii.edu/items/6dc8079f-1c91-46c5-ab94-bab8a4d4ed98`, 01 2023. Proceedings of the 56th Hawaii International Conference on System Sciences | 2023.

[4] P. Radanliev, R. Mantilla Montalvo, S. Cannady, R. Nicolescu, D. Roure, J. Nurse, and M. Huth, "Cyber security framework for the internet-of-things in industry 4.0," *Preprints*, p. 2019030111.

[5] A. Dennis, R. Jones, D. Kildare, and C. Barclay, "Design science approach to developing and evaluating a national cybersecurity framework for jamaica," *THE ELECTRONIC JOURNAL OF INFORMATION SYSTEMS IN DEVELOPING COUNTRIES*, vol. 62, no. 1, pp. 1–18, 2014.

[6] A. Alexei, "Using design science research method to develop a cyber security framework for heis in moldova," in *Electronics, Communications and Computing*, pp. 62–62, 2021.

[7] E.-L. T. Nawa, *Developing a cybersecurity framework for the banking sector of Namibia*. PhD thesis, Namibia University of Science and Technology, 2021.

[8] T. Lejaka, *A framework for cyber security awareness in small, medium and micro enterprises (SMMEs) in South Africa*. PhD thesis, 2021.

[9] H. Afzaal, H. Imran, M. Salama, and C. Turner, "Oil and gas sector: A systematic literature review of digitalization, cybersecurity, and human factors in the post covid world," 01 2024.

[10] A. S. Mohammed, P. Reinecke, P. Burnap, O. Rana, and E. Anthi, "Cybersecurity challenges in the offshore oil and gas industry: An industrial cyber-physical systems (icps) perspective," *ACM Trans. Cyber-Phys. Syst.*, vol. 6, sep 2022.

[11] J. L. Bayuk, J. Healey, P. Rohmeyer, M. H. Sachs, J. Schmidt, and J. Weiss, *Cyber Security Policy Guidebook*. United States: John Wiley Sons, Incorporated, 2012.

[12] "NIST Cybersecurity Framework getting started." https://www.nist.gov/cyberframework/getting-started. Accessed: 2023-08-10.

[13] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of management information systems*, vol. 24, no. 3, pp. 45–77, 2007.

[14] J. O. De Sordi, *Design science research methodology : theory development from artifacts*. Palgrave pivot, Cham, Switzerland: Palgrave Macmillan, 2021.

[15] S. Purser, "Standards for cyber security.," 2014.

[16] J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, G. Lopez-Fonseca, and D. Quiroz, "Information security management frameworks and strategies in higher education institutions: a systematic review," *Annals of Telecommunications*, vol. 76, pp. 255–270, 2021.

[17] M. Jufri, M. Hendayun, and T. Suharto, "Risk-assessment based academic information system security policy using octave allegro and iso 27002," *2017 Second International Conference on Informatics and Computing (ICIC)*, pp. 1–6, 2017.

[18] A. Asosheh, P. Hajinazari, and H. Khodkari, "A practical implementation of isms," vol. 11, pp. 1–17, 04 2013.

[19] M. Sharbaf, "A new perspective to information security: Total quality information security management," *ACM International Conference Proceeding Series*, vol. 2014, pp. 56–60, 09 2014.

[20] M. Rajab and A. Eydgahi, "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education," *Computers & Security*, vol. 80, pp. 211–223, 2019.

[21] R. Rogers, J. Cacioppo, and R. Petty, *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*, pp. 153–177. 01 1983.

[22] T. Ncubukezi, L. Mwansa, and F. Rocaries, "A review of the current cyber hygiene in small and medium-sized businesses," in *2020 15th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 1–6, 2020.

[23] T. Lejaka, A. Veiga, and M. Loock, "Cyber security awareness for small, medium and micro enterprises (smmes) in south africa," pp. 1–6, 03 2019.

[24] D. Hadjizenonos, "How to have strong cyber hygiene." https://www.bizcommunity.com/article/196/661/204326.html, 2014. Accessed: 20.05.2024.

[25] E. Kritzinger and S. Solms, "A framework for cyber security in africa," *Journal of Information Assurance Cybersecurity*, pp. 1–10, 01 2013.

[26] M. F. O. Santos, W. S. Melo, and R. Machado, "Cyber-physical risks identification on industry 4.0: A methodology proposal," in *2022 IEEE International Workshop on Metrology for Industry 4.0 IoT (MetroInd4.0IoT)*, pp. 300–305, 2022.

[27] F. Brocal, C. González, D. Komljenovic, P. F. Katina, and M. A. Sebastián, "Emerging risk management in industry 4.0: An approach to improve organizational and human performance in the complex systems," *Complexity*, vol. 2019, 2019.

[28] C. Piney, "Risk identification: combining the tools to deliver the goods," in *PMI® Global Congress 2003—EMEA, The Hague*, South Holland, The Netherlands. Newtown Square, PA: Project Management Institute.

[29] M. Mansoori, I. Welch, K.-K. R. Choo, and R. Maxion, "Application of hazop to the design of cyber security experiments," pp. 790–799, 03 2016.

[30] Y. Liao, F. Deschamps, E. Rocha Loures, and L. Ramos, "Past, present and future of industry 4.0 - a systematic literature review and research agenda proposal," *International Journal of Production Research*, vol. 55, 03 2017.

[31] S. Weyer, M. Schmitt, M. Ohmer, and D. Gorecky, "Towards industry 4.0 - standardization as the crucial challenge for highly modular, multi-vendor production systems," vol. 48, pp. 579–584, 12 2015.

[32] K. Ruan, "Introducing cybernomics: A unifying economic framework for measuring cyber risk," *Computers Security*, vol. 65, pp. 77–89, 2017.

[33] M. Eckhart, A. Ekelhart, A. Lüder, S. Biffl, and E. Weippl, "Security development lifecycle for cyber-physical production systems," in *IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society*, vol. 1, pp. 3004–3011, 2019.

[34] "Editorial Team *Understanding IEC 62443*." `https://www.iec.ch/blog/understanding-iec-62443`, 02 2021. Accessed: 2023-12-08.

[35] C. Schmittner, Z. Ma, and E. Schoitsch, "Combined safety and security development lifecylce," in *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*, p. 1408–1415, 07 2015.

[36] M. Faruque, F. Regazzoni, and M. Pajic, "Design methodologies for securing cyber-physical systems," in *Proceedings of the 10th International Conference on Hardware/Software Codesign and System Synthesis, ser. CODES '15*, (Piscataway, NJ, USA), p. 30–36, IEEE Press, 2015.

[37] C. Sun, J. Ma, and Q. Yao, "On the architecture and development life cycle of secure cyber-physical systems," *Journal of Communications and Information Networks*, vol. 1, p. 1–21, 12 2016.

[38] I. Dragos, "Industrial control vulnerabilities: 2017 in review," *Dragos, Inc.*

[39] A. Alexei and A. Alexei, "Cyber security threat analysis in higher education institutions as a result of distance learning," *International Journal of Scientific Technology Research*, vol. Volume 10, pp. 128–133, 03 2021.

[40] A. Alexei, "Network security threats to higher education institutions," vol. 341, 07 2021.

[41] S. Donaldson, S. Siegel, C. Williams, and A. Aslam, *Cybersecurity Frameworks*, pp. 297–309. 01 2015.

[42] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS quarterly*, vol. 28, no. 1, pp. 75–105, 2004.

[43] "Bank of namibia annual report." `https://www.bon.com.na/CMSTemplates/Bon/Files/bon.com.na/92/92d106b2-a920-4168-be80-ec1645e42e95.pdf`, 2017.

[44] M. Bhasin, "Menace of frauds in the indian banking industry: An empirical study," *Australian Journal of Business and Management Research*, vol. 4, pp. 1–13, 04 2015.

[45] I. Fachruddin, D. Mayasari, R. Kurniawan, N. Agustin, R. Ganefwati, P. Daulay, A. Meifilina, T. Alamin, R. Fitriana, S. Sutomo, A. Sulton, I. Noor, R. Ahmad Imron, T. George, R. Hallatu, and M. C. B. Umanailo, "Cybercrime case as impact development of communication technology that troubling society," *International Journal of Scientific Technology Research*, vol. 8, pp. 1224–1228, 09 2019.

[46] Z. Dlamini and M. Modise, "Cyber security awareness initiatives in south africa: A synergy approach," in *7th International Conference on Information Warfare and Security: Iciw 2012*, pp. 98–107, Academic Conferences Limited, 2012.

[47] M. T. Siponen, "A conceptual foundation for organizational information security awareness," *Inf. Manage. Comput. Secur.*, vol. 8, pp. 31–41, Mar. 2000.

[48] J. Abawajy, K. Thatcher, and T.-h. Kim, "Investigation of stakeholders commitment to information security awareness programs," in *2008 International Conference on Information Security and Assurance (isa 2008)*, pp. 472–476, 2008.

[49] NIST, "The nist cybersecurity framework 2.0." https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd, 11 2023. Accessed: 2023-12-08.

[50] NIST, "Framework for improving critical infrastructure cybersecurity, version 1.1." https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, 2018.

[51] ISA Standards and Publications, "Isa/iec 62443 series of standards." https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. Accessed: 2023-12-08.

[52] D. Olaussen, "Metering kontrollsystemer et tilbakeblikk, status i dag og noen tanker om veien videre." https://nfogm.no/wp-content/uploads/2018/03/3-Olaussen-David-Metering-kontrollsystem-sett-bakover-og-fremover-i-tid.pdf. Accessed: 2023-12-11.

[53] Guidant Measurement, "Guidant - about us." https://guidantmeasurement.com/contact-us/. Accessed: 2024-04-17.

[54] Guidant Measurement, "Guidant - system and automation." https://guidantmeasurement.com/control-solutions/. Accessed: 2024-04-17.

[55] International Electrotechnical Commission, "IEC TS 62443-1-1, industrial communication networks – network and system security – part 1-1: Terminology, concepts and models," 07 2009.

[56] International Electrotechnical Commission, "IEC 62443-3-3:2013, industrial communication networks – network and system security – part 3-3: System security requirements and security levels," 08 2013.

[57] NIST, "Nist special publication 800-63b, digital identity guidelines - authentication and lifecycle management." https://doi.org/10.6028/NIST.SP.800-63b, 06 2017.

[58] International Electrotechnical Commission, "IEC 62443-2-4:2015+AMD1:2017 CSV, security for industrial automation and control systems – part 2-4: Security program requirements for iacs service providers," 08 2017.

[59] I. Corradini, *Building a Cybersecurity Culture*, pp. 63–86. Cham: Springer International Publishing, 2020.

Appendices

Appendix A Framework

The framework for the documentation package developed for this study's use case is included in the appendix.

Cyber Security Template

Document type	Doc.no :	SPC-0000037277		
Specification	Page :	1 of 15		
Status	**Change no.**	**Date**	**Version**	**Revision**
In preparation		##	00	##

NOTE: Text marked like this is in blue supposed to be removed as it is as supplement information/ text to be edited

Table of Contents

1 GENERAL

The purpose of this document is to give clear requirements to what shall be followed regarding cyber security in the *ProjectName* delivery for the supplier-side, and potential sub-suppliers.

Chapter 5 Framework contains information related to the requirements, and the requirements for the different topics of relevance for the metering control system.

Chapter 7 Checklist shall be the documentation of execution of chapter 4. Covering all the requirements from the framework. The checklist shall be completed before "Ready for shipment".

2 ABBREVIATIONS AND DEFINITIONS

2.1 ABBREVIATIONS

CSNE	Cyber Security Network and Engineering
ERD	Embedded device requirement
FAT	Factory Acceptance Test
NIST	National Institute of Standards and Technology
Req.ID.	Requirement Identification
SAT	Site Acceptance Test
SL	Security Level
SL-C	Capability Security Level
SL-T	Target Security Level
SP	[US NIST] Special Publication
SR	System requirement
ZCR	Zones and conduits requirement

2.2 DEFINITIONS

Authenticator – something used to confirm the user's identity, such as password
Client – *Name of client in project*
Conduit – grouping of communication channel that connects two or more zones with shared security requirements
Interface - communication between two entities, such as between device A and device B
SL-C – measure configured and integrated with no need for additional compensation of measures later
SL-T – the desired level of security that is needed to ensure correct operation
Sub-supplier – Supplier providing equipment/service to another supplier
Supplier – Guidant Measurement
Zones – Grouping of assets based on either risk, criticality, operational function, location or required access

3 REFERENCES

3.1 PROJECT DOCUMENTS

Ref. No.	Document Title / Drawing Title	Client Doc. No.:	TechnipFMC Doc. No.:
[1]	Functional Design Specification	???	???
[2]	Self-assessment	???	???
[3]	Network Topology	???	???
[4]	Operation and Maintenance Manual	???	???
[5]	CSNE FAT procedure	???	???
[6]	Installation procedure	???	???
[7]	CSNE SAT Procedure	???	???
[8]	Ready for shipment	???	???

3.2 STANDARDS

Ref. No.	Document Number	Document Title
[9]	IEC 62443-3-2:2020	Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design
[10]	IEC 62443-1-1:2009	Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models
[11]	IEC 62443-2-4:2017	Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers
[12]	IEC 62443-3-3:2013	Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels
[13]	IEC 62443-2-3:2015	Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment
[14]	NIST SP 800-63B	Digital Identity Guidelines: Authentication & Lifecycle Management
[15]	IEC 62443-4-2:2019	Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components

3.3 CROSS-REFERENCE BETWEEN SECTION AND STANDARDS

Ref. Section This document	Standard used	Standard section/s
5.1 Network	[9] IEC 62443-3-2:2020 [11] IEC 62443-2-4:2017	ZCR 3.1 ZCR 6.4 SP 06.01
5.1.2 Firewalls	[11] IEC 62443-2-4:2017	Req.ID. SP.03.02 note 1
5.1.3 Security Level	[9] IEC 62443-3-2:2020 [10] IEC 62443-1-1:2009	ZCR 5.6 6.2.1
5.2 Self-Assessment	[11] IEC 62443-2-4:2017	Req.ID. SP.06.01 Req.ID. SP.06.02
5.2.1 Ports and Protocols	[11] IEC 62443-2-4:2017	Req.ID. SP.03.05
5.3.1 Account Management	[12] IEC 62443-3-3:2013	SR 1.3
5.3.2 Authenticator	[12] IEC 62443-3-3:2013	SR 1.5
5.3.2.1 Passwords	[12] IEC 62443-3-3:2013 [14] NIST SP 800-63B	SR 1.5 & SR 1.7 Appendix A & 5.1.1.1 & 5.1.1.2
5.3.3 Login attempts	[12] IEC 62443-3-3:2013 [14] NIST SP 800-63B	SR 1.11 5.2.2 10.3 (table 10-1)
5.3.4 Session Lock	[12] IEC 62443-3-3:2013 [14] NIST SP 800-63B	SR 2.5 4.3.3
5.4 Updates and Patching	[13] IEC 62443-2-3:2015	4.1
5.5.1 Backup	[12] IEC 62443-3-3:2013	SR 7.3
5.5.2 Recovery	[12] IEC 62443-3-3:2013	SR 7.4
5.6 Antivirus and antimalware	[11] IEC 62443-2-4:2017 [12] IEC 62443-3-3:2013	Req.ID. SP.10.01 SR 3.3 & SR 7.2
5.7 Hardening	[12] IEC 62443-3-3:2013	SR 7.7
5.8 Physical tampering	[15] IEC 62443-4-2:2019	ERD 3.11

4 DOCUMENT HANDLING

Documents shall have the capability to protect confidential information. The information shall support explicit read authorization whether it is at rest or in transit. Information protection can be achieved through encryption, physical means, or other solutions.

SR 4.1 states that network configuration may be considered as confidential in some situations. Documents that contain network information shall be considered confidential and shall be encrypted with a password where possible, and be password protected at the minimum at rest and in transmittal.

5 FRAMEWORK

5.1 NETWORK

The following subsection applies to creating Network Topology [3] documentation. The topology shall consist of two parts, one physical and one logical. It shall include network devices, internal and external interfaces, and logical access points.
Existing system topology shall be used for input of needed equipment to be added.

System topology template shall be used and apply the sub-sections to gain the network topology.

5.1.1 Zones and Conduits

To ensure that security is being enforced, zones shall be created to provide network segregation. The zones must be separated by firewalls to work as a conduit between them.

Some examples of devices and networks should be categorised into groups and segregated into separate zones.:

- Trusted from untrusted networks
- Temporarily connected devices
- Servers from workstations
- Embedded devices
- Wireless devices

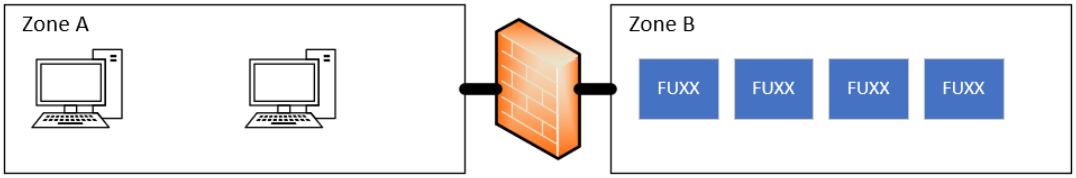


Figure 1: Simple illustration of segregation into different zones with firewall (conduit) between them

5.1.2 Firewalls

According to IEC 62443-2-4:2017 [11], Appendix A requirement ID SP.03.02 note 1, the responsibility for maintaining firewall rules and documentation may be transferred to the asset owner before or at a turnover of the project. In that case, the supplier shall provide support for verification and documentation for the rules to be up-to-date.

*NOTE: This paragraph can be switched out with the one above **IF** the client is insisting that supplier configure the firewalls.* With regards to IEC 62443-2-4:2017 [11], Appendix A requirement ID SP.03.02 note 1, firewalls shall be configured and maintained by the client, but the supplier shall provide the necessary information. This shall include the Equipment List that details the components that will need to connect and communicate with each other, together with the zone categories they belong to. Relevant ports and protocols will also be included.

The recommendation for firewall configuration is Deny-All, with only necessary and documented connections to be allowed through.

5.1.3 Security Level

Following the IEC 62443-3-2:2020 [9], a security level shall be established for each zone, which shall be according to the reference model for the IEC 62443 standard in ref. IEC 62443-1-1:2009 [10]. The reference model is illustrated in Figure 2.

Each zone shall have a defined Target Security Level (SL-T), which shall be present on the Network Topology [3] that has detailed zones and their conduits. For each zone, the SL-T is the desired level of security, which shall be a part of the drawing containing zones and conduits.

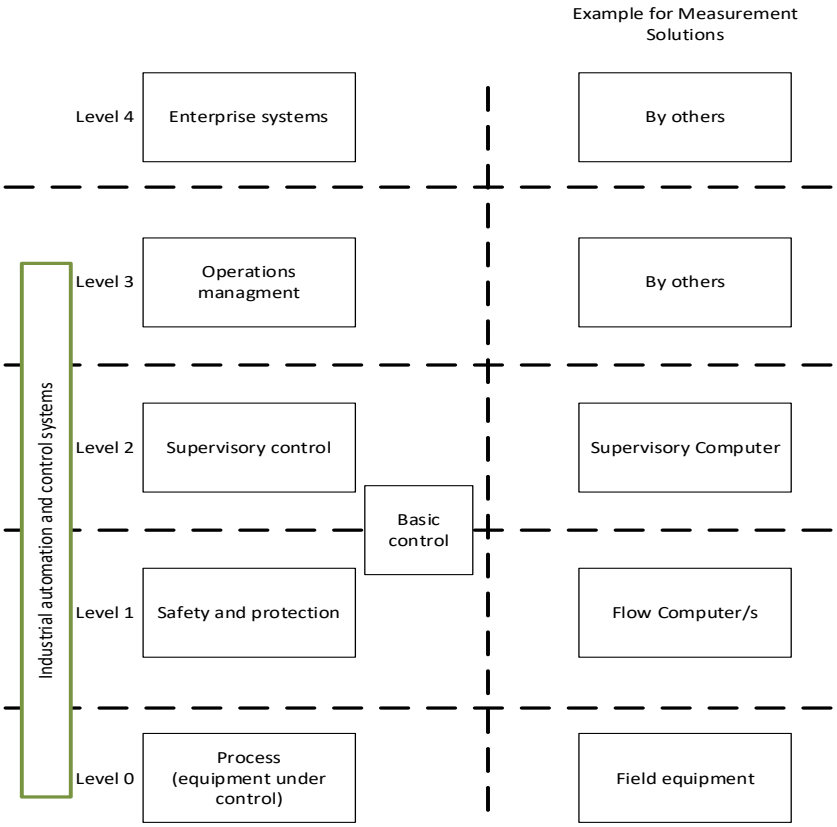


Figure 2: Reference model for IEC 62443 to the left, example for applying for Measurement Solutions to the right

Security Levels:

- SL 0: No defined measures
- SL 1: Protection against casual/coincidental transgression
- SL 2: Protection against intentional transgression with the use of low resources, skills and motivation
- SL 3: Protection against intentional transgression with the use of moderate resources, skills and motivation
- SL 4: Protection against intentional transgression with the use of knowledgeable resources, skills and motivation

Placement of levels for project scope:

- SL 0: Field equipment
- SL 1: Controllers/real-time control
- SL 2: Operator/Engineering stations

More information about the SL can be found in Annex A in IEC 62443-3-2:2020 [9].

5.2 SELF-ASSESSMENT

The supplier shall be able to document the connection and configuration of the network during the project. This means that the document describes how the devices are connected to each segment in the network. For example, an Ethernet device's documentation shall include the address, switch to which device it is connected, and copy of the file used for configuration of the device. All network interfaces in the project scope shall be identified. The self-assessment shall include the version and serial number of all devices and software components. A part of the self-assessment is to ensure that all equipment delivered in the project follows the cyber security requirement, and where they do not, they shall have a description of measure taken to ensure how it shall be achieved.

Sub-suppliers shall provide the supplier with the necessary information regarding their delivery, for the completion of the self-assessment.

5.2.1 Ports and Protocols

With regards to section 5.1.2, only documented communication shall be allowed, as well as documenting unused physical ports that shall be configured to prevent unauthorized access.

5.3 MANAGEMENT CONTROL

5.3.1 Account Management

Account management may include a grouping of accounts based on conditions established for membership and assignments. There may be individual groups, role-based, device-based, and control systems. Unused default accounts shall be removed.

Client shall be responsible for configuring relevant user accounts and groups on the server for their needs as they are the asset owner after project handover. This is due to a supplier not having all the relevant information to administrate all necessary accounts and groups.

5.3.2 Authenticator

The authenticator shall be changed upon installation by the client. Control system shall be capable of changing/refreshing authenticators and protect from unauthorized disclosure and modifications when stored and transmitted. An authenticator can be tokens, symmetric/private keys, biometrics, passwords, physical keys and key cards.

The requirement for applying hardware mechanisms applies to SL-C 3 and 4. Other measures for authenticators apply to lower levels.

5.3.2.1 Passwords

Utilizing password-based authentication in the control system shall enforce configurable password strength based on minimum length and variety of characters.

NIST [14] states that the length and complexity of passwords increase the difficulty of guessing the password, however, it can also increase the frustration of creating a password. NIST [14] recommend therefore that the user shall be encouraged to make their passwords as lengthy as they want within reason. Highly complex passwords shall be avoided due to the potential vulnerability of being written down or stored electronically in an unsafe

manner. Instead of applying complexity, passwords shall be checked towards a blacklist to avoid insecure passwords.

With switching passwords periodically, the motivation for creating strong passwords decreases, and new passwords can be easier to guess, as well as easier guessable based on previous if compromised.

With limitations to what the supplier can provide based on the information and recommendations of requirements, the supplier shall follow these recommendations for policy settings:

- Minimum length of passwords shall be 12 characters long
- Force complexity: No, but encouraged
- Password expiration time: No

Equipment handed over to the asset owner during project turn-over, which the asset owner then has responsibility for maintaining, may implement their password policies as they see fit for integration into their systems.

5.3.3 Login attempts

The control system shall enforce the limit of a configurable number of login attempts. Access shall be denied for a certain period before the counter of login attempts is reset to zero. Following Table 10-1 [14], passwords shall have a minimum of 10 attempts allowed. Supplier follows the minimum allowed attempts as the max.

- Max 10 login attempts before the user is locked and needs admin to unlock

5.3.4 Session Lock

To prevent further access, a session lock shall be initiated after some time of inactivity or manual initiation. NIST [14] suggests a session lock of 15 minutes or longer. Supplier follows the minimum suggestion time as the maximum time of inactivity before logout.

- Session locks after 15 minutes of inactivity

5.4 UPDATES AND PATCHING

Backups need to be performed before starting any updates and/or patching due to the risk of the update/patch changes resulting in negative effects, to be able to roll back to the last secure version. It is recommended to perform updates/patching during other routine maintenance outages and not during normal operations due to potential disruption in operations.

If the asset owner takes over the responsibility for equipment after delivery, they shall take over the responsibility for patching and updates for the server's operative system.

The supplier can be responsible for their equipment and software through a separate maintenance contract.

5.5 BACKUP AND RECOVERY

5.5.1 Backup

In case of misconfiguration and/or system failure, it is important to have up-to-date backups for recovery. It is important to conduct backups on user-level and system level without

disrupting normal operations. Whereas SL-C 1 follows SR 7.3, SL-C 2 follows the enhancement of SR 7.3 (provides the capability to verify the reliability of backup mechanisms).

The control system has procedures in place for performing backups. Whenever a project is upgraded and/or modified, a backup shall be performed before and after the installation of changes [6]. For a new project, a backup shall be taken as left, due to no existing system in place beforehand.

Procedure to perform backup shall be described in Operation and Maintenance Manual [4], and shall be performed at the beginning of a scheduled maintenance to avoid disrupting normal operations in order to have an up-to-date back-up.

5.5.2 Recovery

After a failure or disruption, the control system shall be able to recover to a known secure state. Known secure backups are loaded, tested and functional. Having necessary system documentation and operating procedures available. Operation and Maintenance Manual [4] shall have recovery procedure included.

5.6 ANTIVIRUS AND ANTIMALWARE

The party responsible for providing the operating system is also responsible for providing documentation for malware protection such as anti-virus. The responsible party shall have the anti-malware/virus installed and configured. If the supplier is responsible, it shall be installed and configured before shipment. Else by other, they are responsible for installing and configuring and providing to the supplier to test and verify during FAT/SAT if requested by the client.

The control system shall provide support verification of intended operation and security functions, and report abnormalities when discovered during FAT, SAT and maintenance. However, antivirus scans shall not be done during normal operations as they can disrupt the operation.

5.7 HARDENING

Unnecessary functions, ports, protocols and/or services shall be prohibited and/or restricted, to apply the least functionality. Everything beyond baseline configuration shall be disabled by default.

5.8 PHYSICAL TAMPERING

Mechanisms to protect embedded devices shall be in place against unauthorized access. Tampering-resistant measures can be locks, hardened enclosures, security screws and so on. A simple means to detect physical tampering is removing/breaking the seal on the equipment.

Protection mechanisms used against physical tampering shall be described in Ready for ship [8].

6 CSNE FAT

A CSNE test shall be performed in order to verify that the different cyber security requirements have been met. It shall test the design of the security control with measures to compensate where equipment cannot fulfil the requirement alone, as described in the self-assessment.

The test procedure shall be described to give guidance on how the different tests shall be performed in order to verify that all the security requirements in this framework and self-assessment have been met. The test shall be performed with the equipment of the final design.

If compensated methods are provided by others, then there shall be a collaboration in order to test the complete design by the supplier. One method of example is firewall provided by others.

7 CHECKLIST

The purpose of this checklist is to document that the necessary action has been taken according to the framework.

Actions regarding policy setting is regarding supervisory computer, other equipment shall be covered in the self-assessment. *The last sentence regarding setting policy, in the future those points in the checklist shall be switched out with running script on the SC….*

This checklist shall be complete by the time of Ready for ship [8] is to be completed. Ready for ship document shall have a checkpoint to confirm that this checklist has been completed.

Topic	Requirement	Executed (Yes/No)	If "No", why? /what has been set differently from the requirement?
5.1 Network	Physical Network topology[3] contains: • Zones and conduits • Equipment placed in security levels		
5.1 Network	Logical Network topology[3] contains: • Conduits • Equipment and communication link		
5.2 Self-Assessment	Filled out, [2]		
5.3.1 Account Management	Unused default accounts removed		
5.3.1 Account Management	Verify that procedure [4] has described user groups and how to add users to the control system		
5.3.2.1 Passwords	Set policy to no complexity		
5.3.2.1 Passwords	Set policy for minimum length to 12 characters		
5.3.3 Login attempts	Set policy to max 10 attempts		
5.3.4 Session Lock	Set policy to max 15 min inactivity		
5.4 Updates and Patching	Executed before shipping		
Updates and Patching	Disable automatic updates		
5.5.1 Backup	Verify that backup is described in procedure/s /manual [4][6]		
5.5.1 Backup	Backup is performed before shipment		

Topic	Requirement	Executed (Yes/No)	If "No", why? /what has been set differently from the requirement?
5.5.2 Recovery	Verify Recovery is described in procedure/s /manual [4]		
5.6 Antivirus and antimalware	Verify that antivirus and antimalware is described in procedure/s [5][7][8]		
5.7 Hardening	Disable unused ports, protocols, services		
5.7 Hardening	Verify that port blockers are in place where applicable		
5.8 Physical tampering	Verify that physical tampering protection is described in procedure [8]		