Cybersecurity Challenges in Industrial Control Systems: An Interview Study with Asset Owners in Norway

Lars Halvdan Flå[0000-0002-3069-6788], Christoph Alexander Thieme[0000-0003-1853-0950], Martin Gilje Jaatun[0000-0001-7127-6694] and Geir Kjetil Hanssen[0000-0003-2718-6637]

SINTEF Digital, Trondheim, Norway
lars.flaa@sintef.no

Abstract. This paper presents cybersecurity challenges related to industrial control systems (ICSs), identified through interviews with ICS asset owners. We interviewed participants from 10 companies within the oil and gas, food and beverage, and electricity generation and distribution industries in Norway. The interviews focused on cybersecurity challenges related to the three topics of supply chain, handling of vulnerabilities, and testbeds and digital twins. Thematic analysis of the interviews resulted in identification of 7 challenges, which can serve as inspiration and motivation for future research efforts in the field of ICS and Operational Technology (OT) cybersecurity.

Keywords: Cybersecurity Challenges, Interview Study, Operational Technology (OT), Industrial Control System (ICS)

1 Introduction

The widespread existence of ICSs in different industries and critical infrastructures necessitates the protection of these assets against cyberattacks. The development and operation of ICSs have traditionally focused on safety and availability, and only to a lesser degree on cybersecurity. Recent trends in digitalization have however caused these systems to become more interconnected and exposed, making them more vulnerable to cyberattacks.

The motivation for this work is to explore the challenges to securing ICSs, and ultimately contribute to overcoming these challenges. The task of securing an ICS is influenced by various aspects, among them, potentially competing interests such as availability and safety, the ICS owner's risk appetite, available security solutions, available competence, and knowledge of the current threat landscape.

In order to identify the challenges and the context surrounding them, we conducted interviews with representatives of 10 companies, within 3 different industries. These industries were oil and gas, food and beverage, and electricity generation and distribution. The companies can be referred to as ICS asset owners as they all owned and operated ICSs in operation. Through analysis of the interviews, we seek to answer the

following research question: *What are the challenges with regards to cybersecurity for ICS asset owners?*

In this work, we identified 7 challenges related to cybersecurity for ICS asset owners. In this paper our primary goal is not to suggest solutions, but we rather intend to provide inspiration and motivation for future research efforts in the field.

The structure of the paper is as follows: In section 2, we give an overview of some of the previous works on interviews with ICS stakeholders. In section 3, we present the methodology of our study. In section 4, we present challenges identified from the interviews. Section 5 briefly discusses these challenges, along with some solutions. Section 6 concludes the paper.

2 Background

In this section we provide a non-exhaustive overview of existing works identifying challenges and needs for ICS security. Most of the works presented in this section refer to Operational Technology (OT), a term we argue can have a wider scope than just ICSs. However, in this case we believe that the presented works primarily refer to ICSs, and throughout the paper, these terms are used interchangeably. We prefer the term ICS, but use the term OT when used by the participants and included in quotes or when this term is used in other works which we refer to.

As part of a larger study commissioned by the Petroleum Safety Authority Norway (PSA) in 2019, Jaatun et al. performed interviews with petroleum sector stakeholders regarding Computer Emergency Response Team (CERT) capacity in the North Sea with an aim to determine the need for a separate CERT for the Norwegian petroleum industry [1]. The conclusion was that there did not seem to be grounds for establishing a separate petroleum CERT, but that the petroleum industry actors rather should join up with one of the existing CERTs such as KraftCERT. This recommendation was later adopted by PSA.

In another study for the PSA, Hanssen et al. interviewed stakeholders regarding increased integration of Information Technology (IT) and OT in the petroleum industry [2] and made several recommendations to the industry. These recommendations included an increased focus on data quality and integrity, since many of the data-intensive services being introduced in the industry are impacted directly by poor-quality data, which clearly has implications for cyber security.

In a similar study for the PSA, Jaatun et al. interviewed petroleum sector representatives to assess the applicability of Norwegian National Security Authority's (NSM) guidelines for IT security in OT-systems [3]. They found that these good-practice guidelines for IT-systems are mostly applicable also for OT-systems, but that allowances must be made for the critical nature of these systems and the priority of availability over confidentiality, implying that, e.g., security patches generally cannot be applied "immediately", and systems that are suspected of being compromised cannot simply be shut down (as in the IT world).

Within the same domain of petroleum, Onshus et al. performed interviews with petroleum industry stakeholders regarding the need for independence between IT and OT

systems [4]. They identified 15 challenges for the industry, among them how equipment and working methods can be certified in a cost-effective way. Finally, they provided recommendations to regulatory bodies and the industry, including an increased focus on cybersecurity barrier management.

Specifically targeting the topic of supply chain security, Jaatun and Sæle performed a limited set of interviews on behalf of The Norwegian Energy Regulatory Authority (NVE) to establish how particularly smaller Distribution System Operators (DSOs) in Norway could improve supply chain security [5]. Based on this work they created a checklist for use in procurement processes, where many of the recommendations are related to ensuring that suppliers are located in appropriate geographic locations, and that expectations for suppliers regarding, e.g., participation in exercises are clearly stated in contracts. They also recommend that principles for software security are observed when developing software.

On the topic of security culture in OT, Evripidou et al. conducted 33 interviews with representatives from 25 organizations and as a result identified three barriers to development of a security culture [6]. The first and second of the identified barriers was governance structure and lack of communication. The common denominator for these barriers seemed to be the traditional divide and cultural differences between IT and OT, where operations has resided with the OT/engineering department, while security has resided with the IT department on the enterprise side. The final barrier was lack of expertise, where the authors point to cybersecurity simply being added to existing job descriptions without being accompanied by competence building as one of the factors for this barrier.

Jamail et al. interviewed eleven representatives of nine organizations to explore the use of threat modelling in cyber physical systems (CPS) [7]. Among other, they found that the variety of CPS domains posed a challenge, as several of the participants working in multiple domains found it difficult to have broad knowledge of CPS threats and components.

Lastly, Nüßer et al. performed a study of the state of cybersecurity in 25 manufacturing companies, either through online questionnaires or through interviews [8]. Based on this they present what percentages of their participants perform certain activities, such as performing regular risk assessments, or what percentages experience certain challenges, such as lacking asset inventory.

Most of the work we have summarized in this section has typically focused on one particular domain, e.g., petroleum, or a particular area of cyber security, e.g., security culture. Motivated by an interest in various topics across different industries operating ICSs, we select a wider scope for our study. This is presented in section 3.

3 Methodology

In this section we describe the methodology used to answer the following research question: *What are the challenges with regards to cybersecurity for ICS asset owners?*

We collected data through interviews with ten representatives from ten companies in Norway, all operating ICSs. The companies were distributed across three industries

(oil and gas, food and beverage, and electricity generation and distribution). Interviews were performed using Microsoft Teams, with two of the authors as interviewers and one participant from the company. The interviews were recorded for analysis purposes. One of the interviewers had the role as lead, while the second asked complementary questions and took notes. The interviews lasted between 48 and 68 minutes and focused on ICS cybersecurity challenges related to the three topics of supply chain, handling of vulnerabilities, and testbeds and digital twins. The topics were chosen based on the authors' interests.

The interviews were semi-structured, meaning that they allowed the interviewers to deviate from the prepared questions in the interview guide. This format was chosen to allow interviewers to pursue interesting topics, and for the participants to have the freedom to highlight what they perceived as important. Consequently, this contributed to the interviews containing information outside of the three main topics listed earlier. The interview guide is included in the appendix. Due to the semi structured format and limited time, we did not cover all questions in all the interviews.

To enable a detailed analysis of the data, the interviews were recorded and transcribed using a locally executed instance of OpenAI's Whisper[1] software for speech recognition. The transcripts generated by Whisper were then checked against the recorded interview and corrected. These corrected transcriptions of the interviews formed the input to the subsequent analysis.

For the detailed analysis of the interviews, we based our approach on the method for thematic analysis, as outlined by Braun and Clarke [9] and later revisited in Braun and Clarke [10]. We chose this approach as it is claimed to be, among other things, flexible, relatively easy to learn and perform, and accessible to researchers with little experience of qualitative research. The method consists of six steps, as listed below. The steps are named in accordance with Braun and Clarke [10], and the description indicated how we have adapted and performed each step. Although the steps are listed sequentially, it was in practice an iterative process.

1. **Data familiarisation and writing familiarisation notes.** This step was mainly carried out by listening to the recorded interviews and correcting any mistakes made in the transcription process by the Whisper software. The transcriptions were split between two people, who listened through them in parallel and made corrections. A few high-level topics/codes were noted down in this step.

2. **Systematic data coding.** In this step, we assigned codes to data extracts interesting for our analysis, i.e., data extracts relevant for challenges related to ICS cybersecurity. The set of codes were refined and expanded as we went through the process of coding all the interview.

3. **Generating initial themes from coded and collated data.** In this step, we proposed preliminary themes based on the codes, and grouped the codes into themes. Some codes were excluded, either because they did not fit any theme,

[1] https://github.com/openai/whisper

because we considered the coded information too sensitive, or because they did not contain enough data.

4. **Developing and reviewing themes.** In this step we re-read the interviews to see if the identified themes worked and coded any overlooked segments.

5. **Refining, defining and naming themes.** In this step we renamed themes, changed the mapping of codes to themes, and split and merged themes. As a result, we converged on the themes included as subsections in section 4.

6. **Writing the report.** In this step we identified what we consider to be the main findings related to the research question. This is presented in section 4, structured according to the themes defined in the previous step.

The participants were sent a complete draft of the paper to have the opportunity to check quotes and provide feedback on the content.

4 Results

In this section we present the challenges we identified from the interviews. As we discuss further in section 5, these results should not be interpreted to mean that the following challenges were relevant to all the participants, or that all participants expressed support for all challenges. What is presented is the breadth of challenges identified in the interview material and their relevance may therefore vary among industries and companies.

4.1 Challenge: Limited insight into cybersecurity risks in the supply chain

A first challenge for ICS asset owners was a limited ability to verify the state of cybersecurity in their supply chain, both regarding the supplier companies themselves and the products and services they deliver. Most of the participants reported that they trust their suppliers on topics such as installing patches or using the system and equipment provided by the supplier. The factors underpinning this trust relation seemed to differ, but in many cases, it appeared to be the result of an inability to verify patches, systems, and equipment, typically caused by a lack of specific competence and resources.

Instead of verifying the actual products from suppliers, several of the participants stated that they resort to some sort of assessment of the supplier, either performed by a third party, the supplier themselves, or the ICS asset owner. In addition to these methods of verification, some also stated that aspects such as size and reputation influence their confidence in a supplier.

While assessments of suppliers can give insight into the first level of the overall supply chain, it can be challenging to maintain an overview of who they in turn bring in as their suppliers. Several of the participants expressed that it is challenging to acquire an overview of the companies that make up their supply chain, and they were not

aware of good tools for estimating the supply chain risk. Some examples of challenges related to supply chain risk mentioned were situations where suppliers changed cloud providers, often triggering a new risk assessment, and the challenge of estimating and following up security culture in a supplier company.

4.2 Challenge: Lack of cybersecurity awareness in the procurement process

A second challenge was a lack of cybersecurity awareness in procurement processes, both on the part of the suppliers and ICS asset owners. Several participants reported challenges related to most phases of the procurement and supplier requirements process. The very first aspect highlighted by several participants was to get involved in the procurement process. As one participant put it: *"That's been a process that's been mainly done, you know, at the plant, and they're not used to involving IT at all in the procurement process."*

The subsequent stage, formulating or determining requirements for suppliers, was also something several participants found to be a challenge. One participant highlighted the challenge of how requirements are understood by suppliers: *"[…] we can define it, cyber security, what we need but it's kind of a challenging task to give it to the vendors and that they actually understand it so and how they understand it"*.

On the topic of whether suppliers were able to meet requirements, responses included that the suppliers were immature, that larger suppliers were typically better than smaller, but also that requirements from the industry had caused a positive trend. Still, several participants also stated that they had experienced that suppliers had been reluctant to comply with requirements, for various reasons.

4.3 Challenge: Establishing asset inventory

A third challenge was to establish an inventory of the ICS assets. This topic was one that a majority of the participants highlighted as important but also as challenging. As one participant put it, "*[…] it's not one of the most important, it's the one important task to do […]*", while at the same time noting that *"[…] it's kind of challenging to actually establish it in a good practice way"*. Adding to this, another participant noted that while their current asset inventory might be up to date, maintaining it and keeping it up to date is a challenge.

Regarding the challenges of establishing and maintaining an asset inventory, it seemed to be harder on the lower levels of the Purdue model (i.e., the part of the ICS closer to the physical process). While several participants reported the use of automated solutions for asset management on servers, routers or components running general operating systems, equipment on lower levels such as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) seemed to be more challenging and by one of the participants claimed to rely more on manual input. However, while asset overview seemed to be a challenge, several participants expressed satisfaction with network-based monitoring tools and intrusion detection systems and claimed that these had improved the situation. In some cases we were also of the impression that a significant part of the value added by these solutions came from their ability to aid in asset

discovery/management. As one of the participants stated: *"So, it identifies all equipment, and it identifies all the communication that's between all equipment, and that is a great tool for us. It gives us insights, which is, before we got that tool, it was like a blur".*

A step beyond obtaining an overview of the components and software running in an ICS is to establish Software/Hardware Bill Of Materials (SBOM/HBOM) to get the full overview of the components and libraries a supplier includes in their products. While several of the participants regarded it as a useful concept, we got the impression that it was not perceived as the most urgent one. As one of the participants put it: *"[…] but of all challenges it is perhaps not be the biggest one right now"*. Another noted that one had to consider how this information would improve security.

4.4 Challenge: A need for practical cybersecurity approaches and guidance

A fourth challenge was the need or desire for more practical approaches and guidance on how cybersecurity could be implemented and managed. Several of the participants touched on how concrete guidelines or templates could be useful. Specifically, the participants mentioned a template for formulating supplier requirement, examples of security goals for common ICS architectures, list of approved providers of various services, ICS security self-assessments, ICS security dilemma training for engineers and managers, and guidance on how to do risk assessments of a supplier's country of origin. One participant also raised the challenge of knowing whether one is in compliance with laws and regulations.

The interviews revealed that there is a fair amount of variety in the standards and guidelines in use, including Center for Internet Security (CIS) Controls, the IEC 62443 family of standards, in-house made frameworks, the NSM's guidelines for IT security, and guidelines from suppliers. The desire for practical guidelines and templates can further be seen in light of some of the comments regarding some of these standards and guidelines. One participant commended the work the NSM has done for IT: " *So make it easily comprehensible, and that is what NSM, I feel, has made the foundational principles a success is that it is so concrete and easy to understand, and something everyone can start working with from one end. Something similar for ICS would have been golden*". And another clearly preferred the more practically oriented CIS control: *"The CIS controls framework is specific and prescriptive in the way that it states what to do. I have used it for quite some years, and I am very happy with it."*. At the same time, the same participant found material from ISO too focused on procedures: "*If you look at ISO, it's more procedure oriented. To exaggerate: You can have a thousand procedures and still have terrible security"*, while also stating that *"One easily gets lost paying too much attention to procedure compliance vs. focusing on the underlying controls and objectives. The tradeoff is less flexibility"*.

However, here we also saw differences between the companies and participants, as illustrated by the following comments on the IEC 62443 standard. While one participant stated that "*I would say that related to OT security, this is the standard which we focus the most on*", another argued that " *[…] I wonder how up to date those standards are […]. It seems like they try to do what the ISO 27000 series, among others, have*

done already" and a third stated that "*I think it will be extremely hard to verify supplier compliance against that standard*".

4.5 Challenge: Obtaining resources and ensuring awareness of cybersecurity

A fifth challenge was to obtain resources and ensure awareness of cyber security. As two of the participants stated, "*In a small company […], one has to achieve a lot with quite limited effort"*, and *"But there are of course those who dream of it [implementing a particular solution/feature], but are we to get our work done, many such things disappear in between everyday tasks"*. On top of this, another participant predicted that the competition for resources would harden in the time to come: *"You will have to prove the risk reducing effect, and security controls will be an economic investment just like any other*".

Two ways in which this seemed to materialize was limited abilities for in-house testing or for realization of a particular solution. Another was the challenge of monitoring requirements over time. Related to the latter, one of the participants noted that performing cyber security revisions of all their suppliers was challenging, and that it required a certain set of competence. Consequently, the participant had on several occasions communicated internally the benefit of establishing a shared cyber security revision service for the whole organization.

Cybersecurity incidents, or the potential for incidents, seemed in some cases to play a role in attracting attention and resources. As examples, one participant commended others in the industry who had publicly stated that they had been victim of an attack, as it made the job of cybersecurity personnel in other companies easier. Another participant actively used questions such as "what if this goes down for x number of hours" when interacting with plant owners in the company.

4.6 Challenge: Barriers to testbed and digital twin applicability for cyber security

A sixth challenge was related to barriers to testbed and digital twin applicability for cyber security. Most of the participants were positive to having some sort of replica of the ICS, either as a digital twin or some type of test bed. But the degree to which it was used, if at all, varied. For test beds, several of the interviews expressed that either they themselves or the supplier had some sort of testing facilities. These seemed to vary in their degree of realistic representation and could be both physical and virtualized. The degree to which testbeds were used seemed to differ between the three industries represented in the interviews, and in many cases ensuring availability was the main motivation for their use. Digital twins were less widespread, with only one of the participants expressing that this was something they worked on, while simultaneously adding that the technology was immature.

Two aspects of digital twins and test beds reoccurred. The first was that these technologies were perceived as most relevant for testing directed towards reassuring availability and to some degree for maintenance. There seemed to be less interest in building up these capabilities primarily with security in mind. Testing for security seemed

instead to be more of a complementary/secondary use case. This is likely due to the consequences of downtime in an ICS. One of the participants argued that *"[…] it is a lot easier for us to acquire resources for testing that the functionality of an ICS works as indented, compared to testing the security. This is likely related to both that I believe it would require less resources to test operational functionality, and that there is a lot more understanding for testing operational functionality in the OT community. So it becomes easier to acquire money for it."*. The second aspect was related to whether it would be possible to create a realistic enough representation of the ICS, exemplified by this response when asked if the participant saw a need for a simple and externally developed test bed: *" No, because I think it will be very difficult to make, like something that is generally applicable. Because I think it will be very supplier specific and production specific"*.

Several participants were also somewhat skeptical of test beds or digital twins for various other reasons. One questioned what good use cases for the digital twin would be, and another believed trust in the supplier should be established in other ways than the ICS asset owner performing verification in a test bed.

4.7 Challenge: Establishing vulnerability context

A seventh challenge was related to establishing the context of a vulnerability. Several participants highlighted the need for understanding the context of a vulnerability, as exemplified by the following statement: *"Our first action is to understand context […] do we have the possibility of doing something about it? Is it possible to patch, or should we just accept it, or should we apply some mitigating measures?"*. When establishing such a vulnerability context, the location of the vulnerability in the architecture seemed to be of particular importance. As one of the participants stated: "*We have a need for contextualizing the vulnerabilities to a much larger degree. With regards to where they are placed and what they are a part of. There is nothing wrong with the information, but a CVSS [Common Vulnerability Scoring System] of 9.8 is not a CVSS of 9.8. Being on a sealed off network which is very hard to reach is very different from a software running on an internet exposed server"*. A potential approach to contextualizing such vulnerabilities better, mentioned by several participants, was to construct paths or graphs to reason about potential ways for an attacker to reach certain areas/assets of an ICS.

After establishing context, a more informed decision can be taken as to whether the vulnerability should be patched. The loss of availability was not surprisingly a concern for the patching decision, and this was something that most of the participants explicitly stated.

4.8 Additional challenges

In this section we present a set of additional challenges, for which we collected less data than is the case for the challenges described above.

Several of the participants bought Security Operation Centre (SOC) services from an external provider, although it was unclear to us what parts of the ICSs and/or IT

networks these services covered. With regards to challenges related to SOC services, one participant expressed that the SOC did not understand the ICS context to a sufficient degree. As a result, the task of evaluating and contextualizing an event reported by the SOC fell to the participant. Another participant expressed skepticism regarding the quality of SOCs, mentioning long incident report times as an example.

The majority of participants indicated that they get their information on new vulnerabilities from a combination of sources, where the sources can be the suppliers themselves, CERTs, third party security providers, and government bodies, both national and international. All these various sources did not appear to be merged, and hence the ICS asset owner often has to take more than one source into account, a process that at least in some cases did not appear to be very automized. One of the participants expressed that this process suffered from information overload and a lack of support for extracting vulnerability information from supplier platforms.

Additional topics touched upon to some degree were usage of cloud services and AI. Several participants were skeptical of storing security related information in the cloud. Although we touched on AI in several of the interviews, none of the participants seemed to be heavily invested in AI for cyber security, although they all saw it as an area with potential.

5 Discussion

As shown in section 4, the set of cybersecurity challenges are quite diverse. Furthermore, none of the challenges are supported by all interviews, and we emphasize that we cannot conclude that these challenges will be equally relevant to all ICS asset owners. Aspects such as company size, industry and experience of the security team are likely to affect to what degree the identified challenges are perceived as relevant. Additionally, our methodology likely also contributes to the variety of identified challenges. Because of these aspects, we do not attempt to prioritize them with regards to importance or relevance.

Regardless, it is still interesting to observe the variety in the findings. They indicate that the challenges faced by ICS asset owners are quite diverse, and that there might be slightly varying cybersecurity foci across industries, and across companies within the same industry. An observation which further underlines this point is the answers to a question we asked at the very end of the interviews. The participants were asked to highlight one challenge or problem of particular importance, and hardly any of the participants gave the same answer.

We do however see similarities between some of our findings and the findings of earlier studies, as briefly introduced in section 2. Related to the challenge of cybersecurity awareness in the procurement process, there seems to be room for improving the cybersecurity dimension of the procurement process, a process where both ICS asset owners and suppliers must be included. Asset owners can benefit from establishing procurement processes where cyber security considerations are explicitly included, recognizing the implications cyber security incidents may have on ICS availability and business objectives. At the center of this lies the formulation of cyber security

requirements for suppliers. We are of the impression that cyber security maturity among suppliers vary, with supplier size as one of the indicators of maturity. It is however important that both suppliers and relevant personnel at the ICS asset owners (e.g. plant owners or management) both see the mutual benefits of considering cyber security in the procurement and delivery of ICS systems.

The challenge of establishing an asset inventory presents itself as particularly relevant as we found support for it in a majority of the interviews, and especially since asset overview/management was not specifically asked for in the interview guide. We suspect that a reason for its relevance independent of this is the foundational and enabling role an updated asset inventory has. We also note that this finding can be confirmed by the study of security culture in OT by Evripidou et al., where they claim that […] *asset discovery is a substantial challenge for OT companies […]* [6]. Having an overview of the assets in an ICS as one of two prerequisites for generating value from an SBOM, since it allows ICS asset owners to know where in their architecture a potential third-party vulnerability is located. The second prerequisite is to have a method for estimating the consequences of a vulnerability, i.e., contextualizing the vulnerability. Our results in this paper indicate that there is generally room for improvement when it comes to both of these prerequisites.

For our identified challenge on the need for practical cybersecurity approaches and guidance, we note that one of the participants in the work by Jamil et al. believed it could be useful for the industry as a whole to have a set of quality threat model patterns [7].

Regarding the challenge of obtaining resources and ensuring awareness of cybersecurity, this can also be related to previous findings in literature. Evripidou et al. found that *"[…] the budget and resources for OT are typically owned by the operations function, which has different priorities on how they should be spent"* [6].

Related to the challenge of barriers to testbed and digital twin applicability for cybersecurity, we should emphasize that we include it as a challenge because some of the participants believed it could be useful in a security context, and that it did not see much use in this context. However, we were of the opinion that those participants saw it more as an opportunity than a currently pressing challenge. There are probably several reasons for these technologies seeing limited use towards cybersecurity, but we present two possible reasons. The first is a matter of resources, as the quote in section 4.6 underlines. It is simply easier to get resources for testing functionality as opposed to security. The second potential reason is that other aspects are seen as more important.

When it comes to our identified challenge on contextualizing vulnerabilities, one method for doing this is through attack graphs, a topic covered among others by Kaynar [11]. In an attack graph, an attacker's privileges can be expressed as a node, and exploitation of a vulnerability can be expressed as an edge. Based on the results in our paper, we are left with the impression that such graphs have not been adapted by the industry. While reasons for this would be speculations form our side, it is evident from the work done by Kaynar that attack graphs rely on very detailed asset inventories (hosts, applications, and associated vulnerabilities), as well as their configurations (which hosts and applications can reach which other hosts and applications), which our results indicate could be a challenge. However, in addition to a need for a detailed asset inventory,

Kaynar identifies a number of additional challenges for attack graphs which may also be relevant.

Specifically related to simulating the discovery of new vulnerabilities, as mentioned in section 4.7, some of the existing works appears to have contributed to such an approach. For instance, Wang et al. [12], has, according to Kaynar, defined a metric indicating how many zero-day vulnerabilities an attacker would have to exploit to reach an asset.

Further related to the challenge of contextualizing vulnerabilities, we also note that contextualization is already a part of the CVSS framework. However, the CVSS score found in databases such as the National Vulnerability Database (NVD) is what is referred to as the base score, which in turn should be adjusted with a temporal and environmental aspect. During our interviews, we did not investigate further how the participants viewed this method, and whether it was in use or not.

When it comes to section 4.8, we use this to list additional challenges which we identified. They are grouped together as we did not find enough data for them to be included in separate sections.

5.1 Limitations

A major limitation of our work is that we only performed one interview with every participant, thereby being unable to ask clarifying and follow-up questions once we had done a preliminary analysis of the interviews.

Another limitation of our work is that we only interviewed ICS asset owners, as opposed to also interviewing product developers, system integrators, and other cybersecurity related service providers (e.g., CERT or SOC representatives). As a result, we do in some cases only get one side of the story, for instance with regards to the relationship between ICS asset owners and suppliers.

Finally, we repeat that the results are inevitably influenced by the interview guide, which focused on cybersecurity challenges related to the three topics of supply chain, handling of vulnerabilities, and testbeds and digital twins. The focus of our questions, together with the semi-structured form of the interviews, limit us to only drawing conclusions on what was said, as opposed to what was not said. As an example, while one of the participants questioned the ability the SOC to contextualize vulnerabilities, we cannot be certain what the remaining nine think of this topic.

6 Conclusion

In this paper, we present cybersecurity challenges faced by ICS asset owners, based on ten interviews with representatives from ten companies within the oil and gas, food and beverage, and electricity generation and distribution industries in Norway. Our interview guide focused on cybersecurity challenges related to the three topics of supply chain, handling of vulnerabilities, and testbeds and digital twins. The interviews were performed in a semi-structured manner, and each interview was transcribed, coded, and the combined material was analyzed using thematic analysis. We identified seven

challenges, related to limited insight into cybersecurity risk in the supply chain, lack of cybersecurity awareness in the procurement process, establishing asset inventory, a need for practical cybersecurity approached and guidelines, obtaining resources and ensuring awareness of cybersecurity, barriers to testbed and digital twin applicability for cybersecurity, and to establishing vulnerability context. The results further furthermore indicate heterogeneity in the challenges faced by the different companies, a finding we attribute to differences in size, industries, but also to our methodology. We briefly discuss the challenges but make no attempt to prioritize them in terms of importance or relevance.

Acknowledgements

We would like to thank the ten participants and express our gratitude for their participation and for openly sharing their ICS cybersecurity views, experiences, and challenges with us.

References

1. Jaatun, M.G., Bodsberg, L., Grøtan, T.O., Moe, M.E.G.: An empirical study of CERT capacity in the North Sea. In: 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, Dublin, Ireland (2020)
2. Hanssen, G.K., Onshus, T., Jaatun, M.G., Myklebust, T., Ottermo, M., Lundteigen, M.A.: Principles of digitalisation and IT-OT integration. SINTEF
3. Jaatun, M.G., Wille, E., Bernsmed, K., Kilskar, S.S.: Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer. SINTEF (2021)
4. Onshus, T., Bodsberg, L., Hauge, S., Gilje Jaatun, M., Lundteigen, M.A., Myklebust, T., Ottermo, M.V., Petersen, S., Wille, E.: Security and independence of process safety and control systems in the petroleum industry. Journal of Cybersecurity and Privacy. 2, 20–41 (2022)
5. Jaatun, M.G., Sæle, H.: A Checklist for Supply Chain Security for Critical Infrastructure Operators. Presented at the Cyber Science 2023 , Copenhagen, Denmark July 3 (2023)
6. Evripidou, S., Ani, U.D., Hailes, S., Watson, J.D.McK.: Exploring the Security Culture of Operational Technology (OT) Organisations: the Role of External Consultancy in Overcoming Organisational Barriers. In: Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023). pp. 113–129. USENIX Association (2023)
7. Jamil, A.-M., ben Othmane, L., Valani, A.: Threat Modeling of Cyber-Physical Systems in Practice. In: International Conference on Risks and Security of Internet and Systems. pp. 3–19. Springer International Publishing (2021)
8. Nußer, W., Koch, E., Trsek, H., Schumann, R., Mahrenholz, D.: Cyber Security in Production Networks – An Empirical Study about the Current Status. In: 2017

22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). IEEE (2017)
9. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative Research in Psychology. 3, 77–101 (2006)
10. Braun, V., Clarke, V.: One size fits all? What counts as quality practice in (reflexive) thematic analysis? Qualitative research in psychology. 18, 328–352 (2021)
11. Kaynar, K.: A taxonomy for attack graph generation and usage in network security. Journal of Information Security and Applications. 29, 27–56 (2016)
12. Wang, L., Singhal, A., Cheng, P., Noel, S.: K-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities. IEEE Transactions on Dependable and Secure Computing. 11, 30–44 (2014)

Appendix: Interview Guide

What is your role and department within the company?
- What is the size of the organization?

Can you tell us a little about your production environment?
- Do you have one or several factories/plants, do you use safety instrumented systems, what cyber consequences are you most afraid of?
- Do you use or plan to use IoT or AI in any way, and for what purpose?

Do you experience challenges with defining cyber security requirements for suppliers?
- Do you have adequate tools and methods for defining appropriate cyber security requirement for suppliers?
- What standards/guidelines do you use for this (e.g. IEC 62443)

Do you perceive complex supply chains as a risk, and do you feel you have adequate methods for treating this risk?
- Is supply chain risk affected by the country of origin (domestic, foreign)?
- Do you rely on system integrators for maintenance and changes?

Do you experience challenges with following up requirements on suppliers?
- Do you follow up on suppliers to suppliers?
- Do you have the necessary tools and methods for doing so?

Do you experience challenges with estimating the risk to your operations/integration work/product development stemming from the supply chain?
- Both when selecting integrators and later in the operations phase?

Do you perceive patching of your ICS environment as a security challenge? Are you worried about the integrity and safety of patches?

- Do you have adequate tools and methods to assess and ensure the integrity of patches?
- What tools do you normally use?
- When and how often do you patch?

How do you communicate when it comes to vulnerabilities in your ICS?

- Do you experience any challenges with this? (Lack of trust, lack of technical solutions,…)

On a high level, what are your current approaches to secure ICS / integration phase/ product development phase?

- Do you see a need for an ICS testbed (for instance when it comes to verifying integrity of patches, the safety of new patches, testing effects of countermeasures, testing effects of new configurations)?
- Do you see other needs for a digital replica of your ICS or parts of your ICS

Could ICS test beds be relevant in order to run training scenarios for staff?

What would be your main requirements to ICS Test beds? What do you perceive as hurdles for ICS test beds (cost, availability,..)?

Are you familiar with the Asset Administration Shell concept?

- If not, is the concept interesting for you?
- Is this something you think will become important?
- Are you concerned about the cyber security aspects of this?

Anything else you want to add that we might have forgotten to ask you about?

What are your main challenges related to security?

- Which of them is in your opinion the most important to solve?
- How do you see these changing in the future?
- Any challenges we forgot to ask you about?

Based on the topics we have discussed, do you see a need for ICS-related security research?