Needs and Challenges Concerning Cyber-risk Assessment in the Cyber-physical Smart Grid

Gencer Erdogan[1][a], Inger Anne Tøndel[2][b], Shukun Tokas[1][c], Michele Garau[3][d] and Martin Gilje Jaatun[2][e]

[1]*Sustainable Communication Technologies, SINTEF Digital, Oslo, Norway*

[2]*Software Engineering, Safety and Security, SINTEF Digital, Trondheim, Norway*

[3]*Energy Systems, SINTEF Energy, Trondheim, Norway*

{Gencer.Erdogan, IngerAnne.Tondel, Shukun.Tokas, Michele.Garau, Martin.G.Jaatun}@sintef.no

Keywords: Cyber-risk, Cybersecurity, Cyber-physical, Smart Grid, IoT, Needs, Challenges, Success Criteria.

Abstract: Cyber-risk assessment methods are used by energy companies to manage security risks in smart grids. However, current standards, methods and tools do not adequately provide the support needed in practice and the industry is struggling to adopt and carry out cyber-risk assessments. The contribution of this paper is twofold. First, we interview six companies from the energy sector to better understand their needs and challenges. Based on the interviews, we identify seven success criteria cyber-risk assessment methods for the energy sector need to fulfill to provide adequate support. Second, we present the methods CORAS, VAF, TM-STRIDE, and DA-SAN and evaluate the extent to which they fulfill the identified success criteria. Based on the evaluation, we provide lessons learned in terms of gaps that need to be addressed in general to improve cyber-risk assessment in the context of smart grids. Our results indicate the need for the following improvements: 1) ease of use and comprehensible methods, 2) support to determine whether a method is a good match for a given context, 3) adequate preparation to conduct cyber-risk assessment, 4) manage complexity, 5) adequate support for risk estimation, 6) support for trustworthiness and uncertainty handling, and 7) support for maintaining risk assessments.

1 INTRODUCTION

The ongoing digitalization of the electric power grid is resulting in complex cyber-physical smart grid systems. In such systems, it is no longer possible to separate the digital part of the system from the more traditional power part of the system, as these technologies are becoming deeply integrated. From a cybersecurity perspective, this tight integration exposes the power grid to many cyber-risks introduced by digitalization, e.g., via IoT systems that are increasingly used in the context of smart power grids (Tøndel et al., 2018).

Cyber-risk assessment is the de facto approach used by large organizations to manage cybersecurity risks, but current standards, methods and tools do not adequately provide the support needed in practice for smart grid systems. For example, on the one hand we have widely used cyber-risk assessment approaches such as ISO 27005 (ISO/IEC 27005:2018, 2018) and NIST 800-39 (NIST 800-39:2011, 2011), while on the other hand we have risk assessment approaches that are specific for power systems (Jakobsen et al., 2021; Li, 2014). Although risk assessment approaches from the cybersecurity and the power domains share some overall characteristics, the industry is struggling to adopt and carry out risk assessments considering cyber-risks, and has limited knowledge on how to best use existing approaches to carry out a holistic cyber-risk assessment considering the merged cyber-physical aspect of the future power grid systems. Moreover, there is a lack of knowledge for combining an assessment of specific types of threats (e.g., cyber) with a more overarching assessment to obtain a more concrete picture of the overall risk.

This paper explores the industry's challenges and needs for carrying out cyber-risk assessment in complex and integrated cyber-physical systems, with focus on smart grids. Moreover, it explores strategies

[a] https://orcid.org/0000-0001-9407-5748
[b] https://orcid.org/0000-0001-7599-0342
[c] https://orcid.org/0000-0001-9893-6613
[d] https://orcid.org/0000-0002-9803-9944
[e] https://orcid.org/0000-0001-7127-6694

Erdogan, G., Tøndel, I., Tokas, S., Garau, M. and Jaatun, M.
Needs and Challenges Concerning Cyber-risk Assessment in the Cyber-physical Smart Grid.
In *Proceedings of the 17th International Conference on Software Technologies (ICSOFT 2022)*, pages 21-32
ISBN: 978-989-758-588-3; ISSN: 2184-2833

for moving towards more integrated risk assessment that includes both cybersecurity and power system threats, as well as ICT dependability issues. Thus, the contribution of this paper is twofold. First, we carry out interviews with representatives from the industry to better understand the current and envisioned needs when it comes to cyber-risk assessment related to smart grids. These interviews lead to the identification of success criteria for risk assessment methods in the context of smart grids. Second, we describe four different methods for risk assessment we have used in previous work to assess cyber-risks in smart grids. For each of these methods, we provide a description and evaluate the extent to which they meet the success criteria identified from the interviews. Based on the evaluation, we map the four methods to a qualitative scale representing the level of fulfillment of criteria. We also provide lessons learned in terms of identified gaps that need to be addressed to improve cyber-risk assessment in the context of smart grids.

The rest of the paper is organized as follows. Section 2 describes the background and related work. Section 3 describes our research method. Section 4 describes the findings from the interviews and the identified success criteria. Section 5 describes the four risk assessment methods used in previous work, while Section 6 evaluates the extent to which the methods fulfill the identified success criteria. Finally, Section 7 concludes the paper and summarizes lessons learned in terms of identified gaps.

2 BACKGROUND AND RELATED WORK

According to ISO 27005, "a risk is a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event" (ISO/IEC 27005:2018, 2018). As indicated in Section 1, there are many standards and specialized approaches for cyber-risk assessment. The most widely used standards are developed by ISO and NIST. The literature offers a wide variety of modelling techniques for risk identification and assessment. Fault tree analysis (FTA) (IEC 61025:2006, 2006), event tree analysis (ETA) (IEC, 1995) and attack trees (Schneier, 1999) are examples of tree-based approaches and provide support for reasoning about the sources and consequences of unwanted incidents, as well as their likelihoods. Cause-consequence analysis (CCA) (Nielsen, 1971) and Bayesian networks (Ben-Gal, 2008) are examples of graph-based notations. Cause-consequence analysis employs diagrams that combine the features of both fault trees and event trees, whereas the latter two serves as mathematical models for probabilistic and statistical calculations, respectively. Moreover, whereas alternative approaches such as CRAMM (Barber and Davey, 1992) and OCTAVE (Alberts et al., 2003) rely on text and tables, graph and tree-based approaches use diagrams as an important means for communication, evaluation, and assessment.

In the context of smart grids, risk assessment is the process of identifying, estimating and prioritizing risks to the grid's operations and assets. The aforementioned steps are part of the standard risk assessment processes (ISO/IEC 27005:2018, 2018; NIST 800-30, 2012). The technological trends underlying the smart grid suggests a broad spectrum of the ICT being deployed for more effective grid operations. This integrated digital-power grid shift also brings growing attack risks to the smart grid. The energy industry faces significant challenges in managing such risks. When analyzing risks in today's power systems, traditional risk assessment methods should be integrated with an assessment of cyber-physical interdependencies, in order to highlight potential vulnerabilities that can represent a source of hazard. While traditional risk assessment focuses on hazards with relatively high probability that come from inherent properties of the system (e.g., component aging), vulnerability assessment can be seen as a method that aims at identifying hidden vulnerabilities in infrastructure systems that can bring to disruptive events, such as blackouts, economic or social turmoil, etc. (Kröger et al., 2011). These high-impact and low-probability events can be too complex to be described with traditional risk-assessment approaches. Typical examples of cases where risk-based approaches may be insufficient for a proper analysis of hidden vulnerabilities are the cases of emergent behaviors, intricate rules of interaction, system of systems, broad spectrum of hazard and threats (Kröger et al., 2011). A framework for studying vulnerabilities and risk in the electricity supply, based on the bow-tie model, is proposed in (Hofmann et al., 2012; Kjølle et al., 2012; Hofmann et al., 2015). Among the vulnerabilities, a specific case is represented by cyber-security risks, which can be defined as the potential of loss as a result of cyberattack resulting from the operations of an information system.

A fundamental work on risks related to the digitalization process in power systems has been proposed by the Task Force on Reliability Consideration for Emerging Cyber-Physical Energy Systems (Aravinthan et al., 2018). The authors emphasize the necessity of modernizing the reliability and risk

assessment methods traditionally adopted in power systems. A multi-layer modelling approach is suggested, where the power layer, communication and coupling layer and decision layer interact in order to enable the power system operation. Each of these layers are characterized by vulnerabilities that should be singularly addressed. Conventional risk assessment techniques are primarily focused on the power layer, and can be primarily classified into two categories: analytical methods and simulation methods (e.g., Monte Carlo simulation) (Billinton and Allan, 1996). In order to include in the power system risk assessment possible failure states in the ICT infrastructures, novel approaches have been introduced, which adopt complex network theory (Zhu et al., 2018), cyber-physical interface matrix (Lei et al., 2015), co-simulation (Garau et al., 2015), and traditional event trees (Liu et al., 2019) and reliability block diagrams (Ding et al., 2018). These works adopt approaches that are strongly related with the concept of probability of failure occurrence, therefore they find a difficult application to scenarios where the threat is deliberate and there are few statistics available to be included in probabilistic approaches. As a consequence, in order to model the effect of successful exploitation of vulnerabilities, risk modelling is performed using high-level conceptual models, such as ISO/IEC Common Criteria standard (Aravinthan et al., 2018), stochastic Petri net models (Ten et al., 2008), Markov processes (Zhang et al., 2016) and Bayesian attack graphs (Zhang et al., 2015).

3 RESEARCH METHOD

Figure 1 illustrates our research method, which consists of six steps. In Step 1, we conducted four interviews with four companies in the energy sector and two interviews with two sectorial organizations. The two sectorial organizations are the Computer Emergency Response Team for the electric power sector (KraftCERT) and the Norwegian Water Resources and Energy Directorate (NVE). The energy companies are not named due to confidentiality. Thus, we carried out in total six interviews. Table 1 lists the interviews we carried out, including date, duration, participants, and the type of company/organization interviewed. The interview team consisted of two participants; one taking the role as interviewer and one taking the role as secretary. The interviews were semi-structured, covering the following topics:

- Current practice in cybersecurity and risk management in the energy sector.
- Risk management and cybersecurity approaches that work well based on the interviewee's experience.
- Needs and challenges within risk management and cybersecurity in the energy sector.

The main task of the secretary was to note the questions asked by the interviewer, as well as the answers provided by the interviewee. However, we did allow for the secretary to also come with questions sporadically, in which case the interviewer would take notes. In addition to the time spent on conducting the interviews, the interviewer and the secretary spent approximately 1 hour after each interview to tidy up the transcribed interview draft.

All interviewed companies/organizations are Norwegian. We recruited the interviewees by asking them directly through our own network, but also asking companies and organizations from the Centre for Intelligent Electricity Distribution project (CINELDI, 2022), which is the project in which this work was carried out. The interviewees were people with different roles, including Chief Information Security Officer (CISO), Cybersecurity expert, and Senior Project Manager.

The output of Step 1 was a set of interview notes. The interview notes were used as input to Step 2, in which the interview team coded the collected data using the MAXQDA tool. The coding was mainly inductive, but with some high level organizing codes to structure the material (current practice; works well; challenges; needs). In Step 3, the interview team went through all the codes and highlighted the notes that indicated a need or a challenge the energy sector was experiencing with respect to risk assessment. For this, we used memos in MAXQDA that were linked to the coded segments.

In Step 4, we identified a set of success criteria based on the needs and challenges indicated by the interviews. The success criteria represent criteria for risk assessment approaches to successfully assess cyber risks in (the future) cyber-physical smart grids (according to the needs indicated by the interviewees). In Step 5, we described four risk assessment approaches we have used in industrial cases within the energy sector to assess risks in smart grids. The approaches we describe are CORAS, the Vulnerability Analysis Framework, Threat Modeling with STRIDE, and Stochastic Activity Network. These approaches were selected because of two main reasons: 1) the authors have years of experience in applying these methods in the energy sector as well as other industrial context, and 2) these approaches support risk assessment from different yet complementary perspectives, and we wanted to assess the feasibility of the approaches with respect to the identified

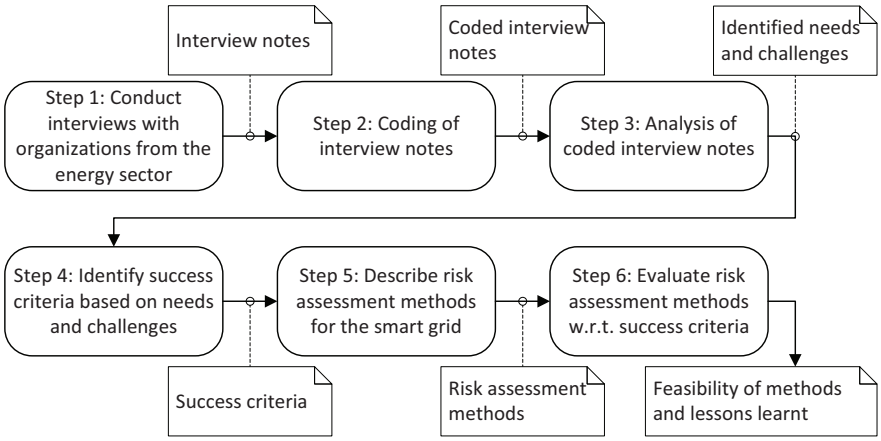

Figure 1: Research method.

success criteria.

Finally, in Step 6, we evaluate the four risk assessment approaches with respect to the identified success criteria; we discuss the extent to which the risk assessment approaches fulfill the success criteria and the gaps that need to be addressed. This evaluation also acts as a basis for lessons learned, summarized in Section 7.

4 IDENTIFIED SUCCESS CRITERIA

This section describes the success criteria identified based on the interviews, as explained in Section 3. In total, we identified seven success criteria (SC) for risk assessment approaches, addressing needs and challenges in the industry pointed out by the interviewees. In the following, we present each success criterion and describe their motivation based on the interviews.

SC1 Be easy to comprehend and use by people who are not experts in risk assessment. Interviewees state that it is essential that risk assessments are easy to do also by people who are not experts in cybersecurity and risk assessment. Several interviewees express that quantitative methods are not currently an option for them, and that there is a need to start with very easy methods. One interviewee even states that it is more important that a method is easy to use than the quality of the results of the analysis, because if the method is too complex and requires too much effort it will meet resistance and the risk assessment will probably not be carried out. Currently, many of the companies seem to opt for using the same methods for cyber risk as for other risk. In the companies, there is a limited number of people that have the competence to do risk assessments related to cyber risk, and information security experts become a bottleneck if they have to be involved in all such assessments. Thus, there is a push towards system owners taking on more responsibility for assessing risk, and at least one of the companies are training project managers in performing risk assessments that include information security. Note also that we talked with relatively large companies within this sector. However, one interviewee explains that more than half of the Distribution System Operators (DSO) are small companies with less than 50 employees. And such companies are unlikely to have dedicated in-house cybersecurity experts. If the risk analyst does not have the necessary competence, support, or training, interviewees explain that one risk is that the analyst just ticks that a risk assessment has been performed without the risks being properly assessed.

SC2 Provide support to determine whether the method is a good match for a given context. There is a large variety in current practice and current ability to perform cybersecurity risk assessments among the companies in the energy sector. A method that is suitable for a larger company with dedicated information security experts may not be suitable for a smaller company without such experts. Based on the interviews, it seems that especially for those with limited competence, it is difficult to know how to start analyzing cyber risk and what questions to consider in the assessment. Further, there are different types of risk assessments that are performed in the companies, ranging from yearly risk assessments to smaller assessments as part of procurement or changes. There is a clearly stated need to start with simple assessment approaches, but at the same time the complexity of the target of analysis may point to a need to move towards more complex assessment approaches in some cases, including when companies have become more mature in their approach to cybersecurity risk assessments.

Table 1: Interviews conducted. CISO = Chief Information Security Officer. PM = Project Manager.

No.	Date	Duration	Interview team	interviewee	Organization
1	28.09.2021	1 hour	1 Interviewer 1 Secretary	1 Cybersecurity Expert	KraftCERT
2	15.10.2021	1 hour	1 Interviewer 1 Secretary	1 CISO	Energy company
3	19.10.2021	1 hour	1 Interviewer 1 Secretary	1 CISO	Energy company
4	04.11.2021	1 hour	1 Interviewer 1 Secretary	1 CISO 1 Senior PM	Energy company
5	05.11.2021	1 hour	1 Interviewer 1 Secretary	1 CISO	Energy company
6	22.11.2021	1 hour	1 Interviewer 1 Secretary	1 Cybersecurity Expert	NVE

SC3 Support preparation for risk assessment, including establishing a common understanding of concepts and build necessary knowledge of participants from IT and OT. When cybersecurity is considered in the more traditional risk assessments, it is experienced as being abstract. Interviewees tell of experiences where cybersecurity is represented with only one scenario in combination with other types of threats, e.g., technical failures, extreme weather conditions. In many of the companies there seem to be a division between IT and OT, though some explain that understanding across IT and OT has improved, e.g., through participating in workshops. One of the interviewees explains that there commonly is a lack of training of people that become involved in a risk assessment. One example pointed out is that individuals from OT are involved (which is encouraged) in risk assessments without any prior understanding of cyber risk and the risk assessment process, thus leading to misunderstandings and challenges during assessment. IT and OT people may, e.g., disagree on the interpretation of key concepts such as likelihood and consequence and have a different understanding of criticality. In the sector, there is some support material available from sectorial organizations. However, there is a need for more support – concrete examples and lists of scenarios are highlighted in the interviews – to motivate for risk assessments, help understand what may happen, and improve quality. It is difficult to contribute meaningfully to a risk assessment without some basic understanding of a potential attack, what techniques can be used, and how such attacks can be mitigated. Furthermore, though people from OT are experts in their domain they might not have the knowledge needed to evaluate cyber risk, e.g., know the architecture of the OT systems.

SC4 Manage complexity in the risk assessment, considering the target of analysis. The analysis target is complex, and the complexity is increasing, which makes it difficult to do good risk assessments. There are several reasons for these challenges. There are ongoing changes in work processes and in systems and their use, and some of these changes happen gradually. Often, manual systems are seen as backups, but eventually the organization looses experience in using these manual backup systems, and thus they lose much of their value. This gradual change can be difficult to capture in risk assessments. For example, if an assessment uses a previous analysis as a starting point, it is easy to become influenced of the previous conclusions and not see what has changed and the assumptions that may no longer be valid. Furthermore, there are connections and dependencies between systems that may be difficult to capture in an assessment. Interviewees provide examples that though OT systems are clearly mission-critical, other systems like Advanced Metering Infrastructure (AMI) may also be critical as they are necessary for other key functions, such as being able to bill customers. However, these other systems may not get enough attention. It is challenging to understand how one risk affects other risks. Assessments are often done for single systems or for single types of incidents, but it is challenging to understand any relations between these and combine analysis results to get a more holistic view of the risk.

SC5 Support risk estimation, e.g., likelihood and consequence estimation, as well as ranking of assets considered in the risk assessment. There is a need to know what are the most critical assets and work processes to protect. Risk estimation is often done through estimation of the likelihood and consequence of certain incidents. However, the criteria that are used to estimate likelihood and consequence in assessments of other types of risk may not be relevant when assessing cyber risk. Moreover, interviewees tell that disagreements between different professions often happen related to likelihood and consequence estimation. When it comes to consequence, the main challenges are related to estimation of indirect consequences (e.g., reputation). One interviewee points to security economy as important moving forward, to make the economic costs of secu-

rity incidents clearer to the decision makers. When it comes to likelihood estimation, this is considered particularly difficult as one is dealing with malicious threats. Several interviewees consider replacing likelihood estimates with evaluations of threat actors and their capacity and intention, and the vulnerabilities present. However, changing the method into something that is different from what is used for assessments of other types of risks in the company is not without challenges. For example, this makes it difficult to aggregate results from different analysis to support decision-making. Furthermore, interviewees explain that there is not enough data to use for estimating likelihood, and point to the risk of underestimating the likelihood for things that have not yet happened. One interviewee explains that support for reuse of likelihood estimates would be highly useful. Support for reuse would reduce the need to involve key experts in every analysis. Many of the assessments are of objects that have similar characteristics. Moreover, many aspects about the threats are similar for other companies of the same type.

SC6 Provide support for increasing trustworthiness of the risk assessment results, as well as manage and represent uncertainty. Criticism of current risk assessments is that they are subjective and that they are not able to identify all important issues to consider, to improve cybersecurity. Due to challenges related to risk estimation (SC5), a few interviewees point to the need to consider uncertainty in the risk estimates. Trustworthiness in risk estimation is important, to be confident in what to report to management, and in providing arguments for how security investments are important for the business. Several of the interviewees move towards more pentesting and system monitoring, as these are considered more effective than risk assessments in identifying vulnerabilities. Thus, this brings up possibilities for combining risk assessments with pentesting and monitoring, in ways that increase trustworthiness in assessment and effectiveness in testing and monitoring. Some interviewees envision a future with more real time risk assessments, and wish for more tool support that can help them in the risk assessments and that are able to bring in data as support, e.g., to identify relevant threat scenarios.

SC7 Facilitate risk management through documentation, maintenance of assessments, and expression of risk treatments. As pointed out by one interviewee, risk assessment does not necessarily imply risk management. Though an analysis identify many risks, it may not be straight forward to know what to do about these risks. Another interviewee points out that the more traditional way of thinking within this sector, that everything should be secure, may not work moving forward, and that there will be a need to build resilience into the system so that they can tolerate some cyber-incidents taking place. Regarding documentation, one interviewee explained about a lack of culture for documenting risk analysis. Moreover, interviewees point to the importance of having updated risk assessments. However, it is challenging to ensure such updates are made whenever there are changes made in the systems. Furthermore, with increasing number of systems, scalability of the assessment approach is also an issue, especially if information security experts need to be involved or even responsible for such assessments. Another challenge is communicating the results of the risk assessment in a way that is comprehensible to management and that puts the cyber-risk topic on their agenda. On the positive side, one interviewee tells about regular reporting of cyber risk to the board, and another tells about using threat modeling in the management group at a high level, to discuss why attacks are possible and what can be done. On the other hand, one interviewee points to the risk assessment as difficult to communicate to the management.

5 RISK ASSESSMENT METHODS

This section describes the four risk assessment approaches we have used in industrial cases within the energy sector: CORAS, the Vulnerability Analysis Framework (VAF), Threat Modeling with STRIDE (TM-STRIDE), and Dependability analysis with Stochastic Activity Network (SAN). Because of space restrictions, we provide a brief description of each approach and refer to other sources for further details.

5.1 CORAS

CORAS is a method for conducting security risk assessment (Lund et al., 2011). In the CORAS method, a security risk assessment is conducted in eight steps: 1) preparations for the analysis, 2) customer presentation of the target, 3) refining the target description using asset diagrams, 4) approval of the target description, 5) risk identification using threat diagrams, 6) risk estimation using threat diagrams, 7) risk evaluation using risk diagrams, and 8) risk treatment using treatment diagrams.

CORAS provides a customized language for threat and risk modelling, and comes with detailed guidelines explaining how the language should be used to capture and model relevant information during the various steps of security risk assessment. The

CORAS method provides a web-based tool (CORAS Tool, 2022) designed to support documenting, maintaining and reporting assessment results through risk modelling.

CORAS is a general approach to cybersecurity risk assessment and has been applied to a large variety of risk assessment targets and concerns within numerous domains, including security, safety, law, civil protection, emergency planning, defense, health, and energy (Lund et al., 2011; Omerovic et al., 2019; Omerovic et al., 2020).

5.2 The Vulnerability Analysis Framework (VAF)

The Vulnerability Analysis Framework (VAF) (Gjerde et al., 2011; Hofmann et al., 2015) is an analysis approach aimed at identifying and analyzing extraordinary events that can impact power system security. The key concepts in VAF are *susceptibility* (i.e., the extent to which a system is susceptible to a threat), and *coping capacity* (i.e., the extent to which a system is able to cope with the negative consequences of a potential threat). These are concepts used in bow-tie diagrams, and VAF can utilize bow-tie diagrams for some of its six analysis steps: 1) identify critical consequences, 2) identify outages leading to critical consequences, 3) identify threats that can cause the critical outages, 4) identify vulnerabilities, susceptibility and coping capacity, 5) identify factors influencing coping capacity, and 6) vulnerability evaluation, identify existing and missing barriers against critical outages.

The VAF has been used for analysis focusing on the more traditional threats experienced in power systems, such as meteorological events and technical failures. However, it has also been successfully used for analysis of a cyber-physical power system where cyber threats were included in the analysis (Tøndel et al., 2021). This resulted in the recommendation that interdependencies were identified and documented from Step 3 and onwards, e.g., using the interdependence types identified by Rinaldi et al. (Rinaldi et al., 2001); physical, cyber, geographical, and logical.

5.3 Threat Modeling with STRIDE (TM-STRIDE)

Threat modeling is a process that reviews the security of any connected system, identifies problem areas, and determines the risk associated with each area. We refer to the result as a threat model, even though it might not necessarily satisfy the formal requirements of a "model". Incidentally, threat modelling is part of what McGraw refers to as Architectural Risk Analysis (McGraw, 2006).

The STRIDE mnemonic (**S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, **E**levation of privilege) was introduced by Microsoft, and gained prominence through Swidersky & Snyder's (Swiderski and Snyder, 2004) book on threat modeling and Howard & Lipner's (Howard and Lipner, 2006) book on the Microsoft Security Development Lifecycle. A later book by Shostack (Shostack, 2014) also covers a number of compatible software tools, including the Microsoft Threat Modeling tool (Bygdås et al., 2021), which conforms to the methodology presented by Swidersky & Snyder.

The first step in this threat modeling approach is to draw a data flow diagram (DeMarco, 1979) which helps to understand the system's attack surface by providing an overview of entities, processes and data stores, identifying trust boundaries and sketching how data flows in the system. The resulting threat model is thus a visual representation of four main elements: the assets within a system, the system's attack surface, a description of how the components and assets interact, and threat actors who could attack the system and how the attack could occur.

5.4 Dependability Analysis with SAN (DA-SAN)

A novel approach for dependability analysis of power systems is proposed by Zerihun, Garau, and Helvik (Zerihun et al., 2020) based on Stochastic Activity Network (SAN) modelling. SAN is a variant of Petri Nets (Sanders and Meyer, 2000) and provides a flexible formalism which is particularly suitable for complex interacting entities, through the input and output ports that allow representing interaction with simple conditional statements. The approach provides an efficient method to analyze the impact of ICT vulnerabilities on power system operation.

Major events such as failure and repair within power system and ICT systems are modelled along with the ICT infrastructure management (MANO system, VM redundancy, etc.) with the SAN formalism. The power flow and power system operation calculations are performed with numerical solvers, included in the SAN model with external C++ libraries purposely developed. The tool implemented exploits and enhances the inherent advantages of the SAN formalism: efficient computation simulation, structured modelling, and modularity and flexibility.

In (Zerihun et al., 2020), the SAN method is evaluated on a test distribution network, where the impact of ICT internal and external vulnerabilities on the per-

formances of a state estimation calculation is quantitatively analysed. Among internal vulnerabilities, radio link failures, server failures, measuring devices, etc. have been considered. Among external vulnerabilities, the impact of signal fading due to rain precipitation has been inspected.

6 EVALUATION OF RISK ASSESSMENT METHODS

Figure 2 illustrates a comparison of the risk assessment methods CORAS, the Vulnerability Analysis Framework (VAF), Threat Modeling with STRIDE (TM-STRIDE), and Dependability Analysis with SAN (DA-SAN) in a scale reflecting their fulfillment of the success criteria described in Section 4. The placement of each method in the scale in Figure 2 is based on the authors' expert knowledge and experience in using the methods as outlined in Section 5.

Companies within the energy sector need risk assessment approaches that are easy to comprehend and use (SC1). The methods VAF and CORAS have empirically been shown to be easy to comprehend and use by people with different backgrounds (Solhaug and Stølen, 2013; Lewis and Smith, 2010). However, we believe VAF is slightly easier to comprehend by personnel of the energy sector companies because VAF uses concepts and constructs that are commonly used in the energy sector. CORAS has also been used in many industrial risk assessments for the energy sector (Omerovic et al., 2019; Omerovic et al., 2020). Threat modelling using Data Flow Diagrams is a widely used approach, and it is therefore reasonable to argue that it is easy to use, in particular considering cyber risks. The approach DA-SAN needs specialized expertise and may not be easy to use unless one has the specific competence and skills. Although VAF, CORAS, and TM-STRIDE may be easier to comprehend and use compared to DA-SAN, none of the methods fully meet the SC1 criterion. Based on the interviews and our experiences, we argue that not many of the existing risk assessment approaches are easy to comprehend and use for non-experts in the energy sector because most approaches do not have domain-specific support for the energy sector (see Section 2).

Considering the criterion SC1, and the fact that all the identified criteria described in Section 4 points out the need for some kind of support to more easily carry out risk assessment, indicates that comprehensibility and ease of use is the most important success criterion. One way of addressing this challenge would be to make the existing approaches more light-weight, but this would come at the cost of expressiveness and the methods' ability to handle complexity. Thus, to successfully achieve criterion SC1, it is necessary to develop risk assessment methods that are easy for the energy sector to use, as well as providing guidelines to select from a variety of approaches that balances between ease of use and the need for assessing complex scenarios. According to the interviews, such guidelines would pave the way for a faster uptake of cyber-risk assessment knowledge in the energy sector.

With respect to support to determine whether the method is a good match for a given context (SC2), all the methods do provide general guidelines for the analyst to understand the context in which the method may be applied. However, these general guidelines are meant for security experts and are not an adequate support for non security experts in the energy sector as they are struggling to answer questions like: "how can I carry out a simple high-level risk assessment even if I don't have cyber-risk expertise?", "what questions should I consider when assessing risks?", "which method should I use if I have a complex target of analysis?", and so on. Thus, the energy sector needs guidelines to select appropriate risk assessment methods considering the competence of those who will carry out the assessment, as well as the objectives of the planned risk assessment. For example, the VAF method may be used to identify and explore the most critical unwanted incidents. These incidents may be used as input to the CORAS method, which may help identify the chain of events that may cause the unwanted incidents, including exploited vulnerabilities. The threat scenarios and vulnerabilities identified using CORAS may in turn be used as input to the TM-STRIDE method to analyze how the vulnerabilities are exploited from a data-flow perspective. Finally, the DA-SAN method may be used to identify the consequences of the identified vulnerabilities and unwanted incidents on a power-grid system using simulation techniques.

Regarding SC3, among the methods we have considered, CORAS and TM-STRIDE have thorough steps to prepare a risk assessment in terms of establishing the context and making sure that all involved stakeholders have a common understanding of the context, concepts, and objectives of the risk assessment. The VAF method also has the necessary steps to prepare an assessment, but is slightly easier to use in the context of the energy sector because it does not require any vocabulary specific to power system security or cybersecurity. The DA-SAN method has preparation steps in terms of modelling the target. Though it is important to obtain a common understanding of the context, concepts, and objectives,

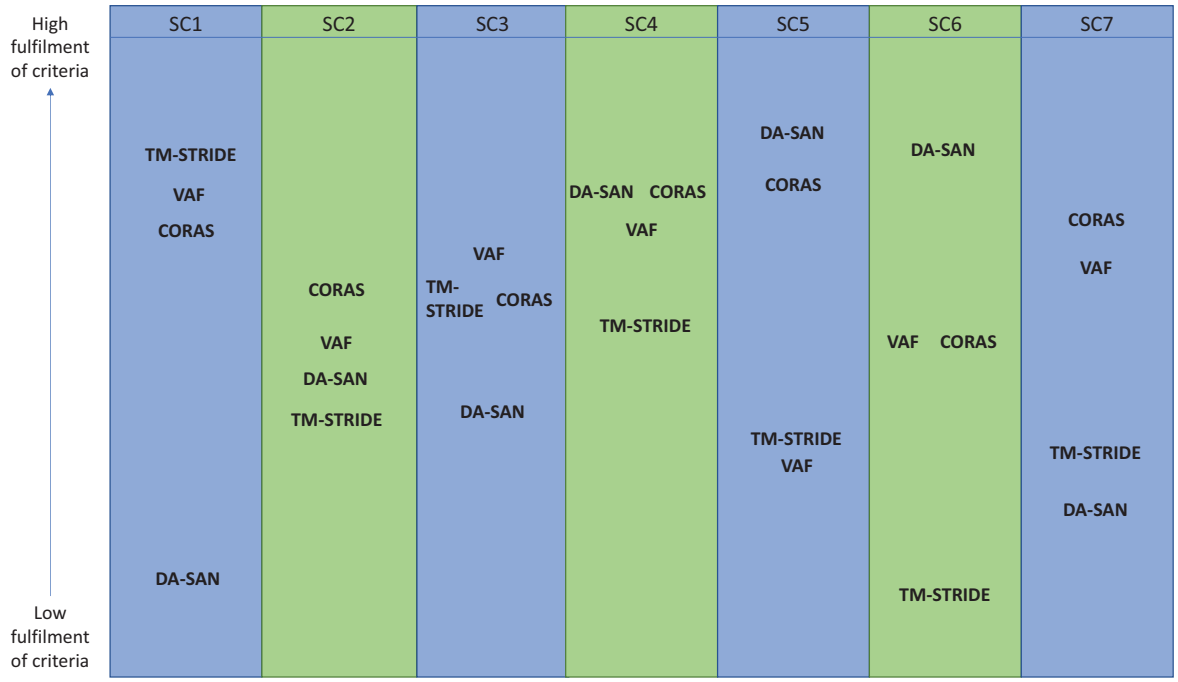

Figure 2: Comparison of methods with respect to fulfillment of the success criteria described in Section 4.

the energy sector needs support in terms of domain-specific cyber-risk example scenarios as well as training material about cyber-risk assessment to properly prepare participants of risk assessment and help contribute meaningfully during an assessment. These aspects may be included as part of a method, for example during the preparation of an assessment participants can be introduced to risk assessment with example scenarios specific to the energy sector. However, a proper educational support would be to train the relevant people using facilities such as cyber ranges that are capable of simulating cyber-attacks on energy infrastructure. Our previous work shows that cyber-risk training using cyber ranges are effective for a variety of domains such as energy distribution, railroad transport, and education (university) (Erdogan et al., 2020; Erdogan et al., 2021).

The infrastructure of energy systems are becoming increasingly complex, and it is therefore necessary to manage the complexity of the target of analysis (SC4). The methods we consider in this paper have mechanisms in place to address complexity. However, while the methods DA-SAN and TM-STRIDE lack the capability to express risks the target of analysis is exposed to as part of the target models, the methods VAF and CORAS lack the expressiveness to represent the target of analysis as part of the risk models. Each aforementioned method have of course been developed for their specific purpose, but it is reasonable to argue that a method capable of capturing both the target of analysis and risks could be beneficial when assessing risks in the context of the energy sector because of its cyber-physical aspects. According to the interviews, one aspect that is especially important to consider in the context of complexity, is the ability to maintain risk assessments over time. With the digitalization of the energy systems, changes (both from a cyber perspective and from a physical perspective) may happen frequently. Whenever an update is introduced in the energy systems, then it is important to consider this change in the risk assessment as well. The CORAS method has explicit support to consider a risk picture before a change is introduced, and after a change is introduced in the target system.

The success criterion SC5 points out the need for support for risk estimation and ranking of assets. The methods VAF and TM-STRIDE do not provide support in estimating risks, but rather rely on external methods to estimate risks. DA-SAN supports risk estimation in terms of quantification of the consequence of failure states in the Cyber Physical Power System (CPPS), while CORAS mainly supports likelihood estimation using the CORAS calculus. Ideally, according to the interviews, a risk assessment method should provide guidelines for both likelihood and consequence estimation. One possible approach is to combine different methods to fully achieve SC5. For example, DA-SAN can support CORAS with consequence estimates, while CORAS can support DA-SAN with likelihood estimates. Another option is to

develop method-independent support for risk estimation for the energy sector to support risk estimation in a broader set of methods.

For all risk assessments, it is important that the assessments are trustworthy and that the uncertainty of the results are considered as part of the assessment (SC6). The methods CORAS and VAF actively involve people with different backgrounds in the risk assessment process to obtain information from relevant experts, and thereby increase the trustworthiness of the risk assessment. TM-STRIDE offers no direct support in relation to trustworthiness and uncertainty assessment. Among the four methods considered in this paper, DA-SAN is the only method that provides mechanisms (and tools) to quantitatively assess the uncertainty of the risk assessment to increase the trustworthiness. DA-SAN does this as part of the simulation. Trustworthiness and uncertainty are in general very important factors for decision support when evaluating whether to invest in new security mechanisms, either for physical security (security of supply) or software security.

Regarding SC7, the methods CORAS and VAF use the diagrams produced in the risk assessment as a basis for documentation and communication with the stakeholders. These methods also support the identification of risk treatments and may therefore help decision makers to identify and select appropriate risk treatments. CORAS also supports change management of assessment results, as described above related to maintenance of risk assessments. The methods TM-STRIDE and DA-SAN mainly create and use models to identify risks, but also to document the findings. Maintenance of risk assessment results and treatment identification are not supported by TM-STRIDE and DA-SAN. One important challenge none of the methods are able to support is continuous updated risk assessments. Based on our experience, we believe this challenge is not supported by current risk assessment methods for the energy sector in general, but it is something that must eventually be supported to cope with the tsunami of data produced by the IoT devices that will be integrated in the energy systems. Dynamic and real-time risk assessment must inevitably be addressed and properly supported, but the current state of risk assessment in the energy sector shows that basic needs and challenges (as described in this section) must be addressed before the dynamic/real-time aspects can be supported.

7 CONCLUSIONS AND LESSONS LEARNED

The energy sector is struggling to adopt and carry out risk assessments considering cyber risks in the context of smart grids. In this paper, we have interviewed representatives from the energy sector to better understand the current and envisioned needs and challenges of risk assessment methods for smart grids. Based on the needs and challenges, we identify a set of success criteria that should be fulfilled for the energy sector to successfully carry out cyber-risk assessment. Then we evaluate the methods CORAS, TM-STRIDE, VAF, and DA-SAN with respect to the identified success criteria. The methods CORAS, TM-STRIDE, VAF, and DA-SAN are methods the authors have used in previous work to carry out risk assessment of energy systems and smart grids. Based on the evaluation, we discuss the extent to which the aforementioned methods fulfill the success criteria and discuss gaps that need to be addressed in general.

We interviewed four Norwegian energy companies and two sectorial organizations. The two sectorial organizations are the Computer Emergency Response Team for the electric power sector (KraftCERT) and the Norwegian Water Resources and Energy Directorate (NVE). The energy companies are not named due to confidentiality. Based on the needs and challenges described by the interviewees, we identified seven success criteria cyber-risk assessment methods for the energy sector need to fulfill. In short, these are related to: ease of use and comprehensible methods (SC1), support to determine whether a method is a good match for a given context (SC2), adequate preparation to conduct cyber-risk assessment (SC3), manage complexity (SC4), adequate support for risk estimation (SC5), adequate support for trustworthiness and uncertainty handling (SC6), and support for documenting and maintaining risk assessments and identifying appropriate risk treatments (SC7). The reader is referred to Section 4 for a detailed description of the success criteria.

Although the number of interviewees are only seven (four CISOs, two cybersecurity experts, and one senior project manager), all interviewees are people with years of experience in cybersecurity within the energy sector. Moreover, in the case of KraftCERT and NVE, the interviewees are experts who are aware of the general needs and challenges in the industry and critical infrastructure sector in general. It is therefore reasonable to argue that the abovementioned success criteria need to be addressed for the critical infrastructure sectors in general.

The methods we evaluated in this paper (CORAS,

TM-STRIDE, VAF and DA-SAN) fulfill the above success criteria to a certain extent, but none of the methods fulfill all the success criteria. The reader is referred to Section 6 for a detailed discussion about the gaps that need to be addressed. In summary, we conclude with the following lessons learned.

1. Considering the fact that all success criteria (SC1-SC7) point to the need for some kind of support to more easily carry out risk assessment, we see that there is especially a need to improve the comprehensibility and ease of use of risk assessment methods for the energy sector in general.
2. There is a need for support in helping risk analysts in the energy sector, including people both from IT and OT, in selecting the right risk assessment method for the right context. There is also a need for domain-specific training material and example scenarios to help participants contribute meaningfully during an assessment (SC2 and SC3).
3. There is a need for improving comprehensibility and ease of use of methods, but on the other hand, there is also a need for managing complexity of risk assessments to consider complex target of analyses. These may be two conflicting needs, but they indicate that risk assessment methods for the energy sector need to be easy to comprehend and use, but also able to sufficiently consider a complex target of analysis (SC4).
4. Risk assessment methods for the energy sector need to support risk quantification, trustworthiness and uncertainty handling (SC5 and SC6).
5. The risk assessment needs to be easy to maintain, and the risk assessment results need to better provide decision support (SC7).

ACKNOWLEDGEMENTS

This work has been conducted as part of the CINELDI project (257626) funded by the Research Council of Norway.

REFERENCES

Alberts, C., Dorofee, A., Stevens, J., and Woody, C. (2003). Introduction to the octave approach. Technical report, Carnegie-Mellon University.

Aravinthan, V., Balachandran, T., Ben-Idris, M., Fei, W., Heidari-Kapourchali, M., Hettiarachchige-Don, A., Jiang, J. N., Lei, H., Liu, C.-C., Mitra, J., Ni, M., Papic, M., Parvania, M., Sephary, M., Singh, C., Srivastava, A., Stefanov, A., Sun, H., and Tindemans, S. (2018). Reliability modeling considerations for emerging cyber-physical power systems. In *Proc. 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS'18)*, pages 1–7. IEEE.

Barber, B. and Davey, J. (1992). The use of the CCTA risk analysis and management methodology CRAMM in health information systems. *Medinfo*, 92:1589–1593.

Ben-Gal, I. (2008). Bayesian networks. *Encyclopedia of Statistics in Quality and Reliability*, 1.

Billinton, R. and Allan, R. N. (1996). *Reliability Evaluation of Power Systems*. Plenum Press, New York, 2 edition.

Bygdås, E., Jaatun, L. A., Antonsen, S. B., Ringen, A., and Eiring, E. (2021). Evaluating threat modeling tools: Microsoft TMT versus OWASP Threat Dragon. In *Proc. 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA'21)*, pages 1–7. IEEE.

CINELDI (2022). Centre for Intelligent Electricity Distribution (CINELDI). https://www.sintef.no/projectweb/cineldi/. Accessed February 28, 2022.

CORAS Tool (2022). CORAS Risk Modelling Tool. https://stverdal.github.io/. Accessed February 28, 2022.

DeMarco, T. (1979). *Structure Analysis and System Specification*, pages 255–288. Springer Berlin Heidelberg.

Ding, Z., Xiang, Y., and Wang, L. (2018). Incorporating Unidentifiable Cyberattacks into Power System Reliability Assessment. In *2018 IEEE Power Energy Society General Meeting (PESGM'18)*, pages 1–5. IEEE.

Erdogan, G., Hugo, Å., Romero, A., Varano, D., Zazzeri, N., and Žitnik, A. (2020). An approach to train and evaluate the cybersecurity skills of participants in cyber ranges based on cyber-risk models. In *Proc. 15th International Conference on Software Technologies (ICSOFT'20)*, pages 509–520. SciTePress.

Erdogan, G., Romero, A., Zazzeri, N., Žitnik, A., Basile, M., Aprile, G., Osório, M., Pani, C., and Kechaoglou, I. (2021). Developing cyber-risk centric courses and training material for cyber ranges: A systematic approach. In *Proc. 7th International Conference on Information Systems Security and Privacy (ICISSP'21)*, pages 702–713. SciTePress.

Garau, M., Celli, G., Ghiani, E., Soma, G. G., Pilo, F., and Corti, S. (2015). ICT reliability modelling in co-simulation of smart distribution networks. In *Proc. 1st International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI'15)*, pages 365–370. IEEE.

Gjerde, O., Kjølle, G. H., Detlefsen, N. K., and Brønmo, G. (2011). Risk and vulnerability analysis of power systems including extraordinary events. In *Proc. 2011 IEEE Trondheim PowerTech*, pages 1–5. IEEE.

Hofmann, M., Kjølle, G., and Gjerde, O. (2012). Development of indicators to monitor vulnerabilities in power systems. In *Proc. 11th International Probabilistic Safety Assessment and Management Conference (PSAM'11)*, pages 1–10. Curran Associates, Inc.

Hofmann, M., Kjølle, G. H., and Gjerde, O. (2015). Vulnerability analysis related to extraordinary events in power systems. In *Proc. 2015 IEEE Eindhoven PowerTech*, pages 1–6. IEEE.

Howard, M. and Lipner, S. (2006). *The Security Development Lifecycle*. Microsoft Press, Redmond, WA.

IEC (1995). Dependability management–part 3: Application guide–section 9: Risk analysis of technological systems.

IEC 61025:2006 (2006). IEC 61025:2006 Fault tree analysis (FTA). International Standard, International Electrotechnical Commission.

ISO/IEC 27005:2018 (2018). ISO/IEC 27005:2018 - Information technology - Security techniques - Information security risk management. Standard, International Organization for Standardization.

Jakobsen, S. H., Garau, M., and Mo, O. (2021). An open-source tool for reliability analysis in radial distribution grids. In *Proc. 2021 International Conference on Smart Energy Systems and Technologies (SEST'21)*, pages 1–6. IEEE.

Kjølle, G. H., Utne, I. B., and Gjerde, O. (2012). Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. *Reliability Engineering & System Safety*, 105:80–89.

Kröger, W., Zio, E., and Schläpfer, M. (2011). *Vulnerable systems*. Springer, London.

Lei, H., Singh, C., and Sprintson, A. (2015). Reliability analysis of modern substations considering cyber link failures. In *Proc. 2015 IEEE Innovative Smart Grid Technologies - Asia (ISGT'15)*, pages 1–5. IEEE.

Lewis, S. and Smith, K. (2010). Lessons learned from real world application of the bow-tie method. In *Proc. 6th Global Congress on Process Safety*, pages 22–24. OnePetro.

Li, W. (2014). *Risk Assessment of Power Systems: Models, Methods, and Applications*. John Wiley & Sons.

Liu, Y., Deng, L., Gao, N., and Sun, X. (2019). A Reliability Assessment Method of Cyber Physical Distribution System. *Energy Procedia*, 158:2915–2921.

Lund, M., Solhaug, B., and Stølen, K. (2011). *Model-Driven Risk Analysis: The CORAS Approach*. Springer.

McGraw, G. (2006). *Software Security: Building Security In*. Addison-Wesley.

Nielsen, D. S. (1971). *The cause/consequence diagram method as a basis for quantitative accident analysis*. Risø National Laboratory.

NIST 800-30 (2012). Special Publication 800-30 Guide for Conducting Risk Assessments. Standard, National Institute of Standards and Technology.

NIST 800-39:2011 (2011). NIST Special Publication 800-39 - managing information security risk organization, mission, and information system view. Standard, NIST. Accessed: 2021-10-25.

Omerovic, A., Vefsnmo, H., Erdogan, G., Gjerde, O., Gramme, E., and Simonsen, S. (2019). A feasibility study of a method for identification and modelling of cybersecurity risks in the context of smart power grid. In *Proc. 4th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS'19)*, pages 39–51. SciTePress.

Omerovic, A., Vefsnmo, H., Gjerde, O., Ravndal, S., and Kvinnesland, A. (2020). An industrial trial of an approach to identification and modelling of cybersecurity risks in the context of digital secondary substations. In *Proc. 14th International Conference on Risks and Security of Internet and Systems (CRISiS'19)*, pages 17–33. Springer.

Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6):11–25.

Sanders, W. H. and Meyer, J. F. (2000). Stochastic activity networks: Formal definitions and concepts. In *School organized by the European Educational Forum*, pages 315–343. Springer.

Schneier, B. (1999). Modeling security threats. *Dr. Dobb's journal*, 24(12).

Shostack, A. (2014). *Threat modeling: Designing for security*. John Wiley & Sons.

Solhaug, B. and Stølen, K. (2013). The coras language-why it is designed the way it is. In *Proc. 11th International Conference on Structural Safety and Reliability (ICOSSAR'13)*, pages 3155–3162. Citeseer.

Swiderski, F. and Snyder, W. (2004). *Threat Modeling*. Microsoft Press, Redmond, WA.

Ten, C.-W., Liu, C.-C., and Manimaran, G. (2008). Vulnerability Assessment of Cybersecurity for SCADA Systems. *IEEE Transactions on Power Systems*, 23(4):1836–1846.

Tøndel, I. A., Foros, J., Kilskar, S. S., Hokstad, P., and Jaatun, M. G. (2018). Interdependencies and reliability in the combined ICT and power system: An overview of current research. *Applied computing and informatics*, 14(1):17–27.

Tøndel, I. A., Vefsnmo, H., Gjerde, O., Johannessen, F., and Frøystad, C. (2021). Hunting dependencies: Using bow-tie for combined analysis of power and cyber security. In *Proc. 2020 2nd International Conference on Societal Automation (SA'20)*, pages 1–8.

Zerihun, T. A., Garau, M., and Helvik, B. E. (2020). Effect of Communication Failures on State Estimation of 5G-Enabled Smart Grid. *IEEE Access*, 8:112642–112658.

Zhang, Y., Wang, L., Xiang, Y., and Ten, C.-W. (2015). Power System Reliability Evaluation With SCADA Cybersecurity Considerations. *IEEE Transactions on Smart Grid*, 6(4):1707–1721.

Zhang, Y., Wang, L., Xiang, Y., and Ten, C.-W. (2016). Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation. *IEEE Transactions on Power Systems*, 31(6):4379–4394.

Zhu, W., Panteli, M., and Milanović, J. V. (2018). Reliability and Vulnerability Assessment of Interconnected ICT and Power Networks Using Complex Network Theory. In *Proc. 2018 IEEE Power Energy Society General Meeting (PESGM'18)*, pages 1–5. IEEE.