Adapting Cyber-Risk Assessment for the Planning of Cyber-Physical Smart Grids Based on Industrial Needs

Gencer Erdogan[1][0000−0001−9407−5748], Iver Bakken Sperstad[2][0000−0002−4827−6431], Michele Garau[2][0000−0002−9803−9944], Oddbjørn Gjerde[2][0000−0002−7978−747X], Inger Anne Tøndel[3][0000−0001−7599−0342], Shukun Tokas[1][0000−0001−9893−6613], and Martin Gilje Jaatun[3][0000−0001−7127−6694]

[1] Sustainable Communication Technologies, SINTEF Digital, Oslo, Norway
[2] Energy Systems, SINTEF Energy Research, Trondheim, Norway
[3] Software Engineering, Safety and Security, SINTEF Digital, Trondheim, Norway
{gencer.erdogan, iver.bakken.sperstad, michele.garau, oddbjorn.gjerde, ingeranne.tondel, shukun.tokas, martin.g.jaatun}@sintef.no

Abstract. During the grid planning process, electric power grid companies evaluate different options for the long-term grid development to address the expected future demands. The options can be passive measures, e.g., traditional reinforcement or building new lines, or active measures, e.g., support from ICT-solutions during operation to increase the power transfer capability. The ongoing digitalization of the electric power grid inevitably push the grid companies to assess potential cyber risks as part of the grid planning process. This applies especially for active measures which to a greater extent rely on support from ICT-solutions to operate the system closer to its limits. However, current grid planning approaches do not adequately provide the support needed in practice, and the industry is struggling to adopt and execute cyber-risk assessments. The contribution of this paper is threefold. First, we interview six companies from the energy sector, and based on the interviews we identify seven success criteria that cyber-risk assessment methods for the electric power sector need to fulfil to provide adequate support. Second, we present four risk assessment methods and evaluate the extent to which they fulfil the identified success criteria. Third, we address the specific need for approaches that are easy to use and comprehend, especially for grid planning purposes, and propose a low-threshold approach to support high-level cyber-risk assessment in an electric power grid planning process. Based on our findings, we provide lessons learned in terms of gaps that need to be addressed to improve cyber-risk assessment in the context of smart grids.

Keywords: Cyber Risk · Cybersecurity · Cyber Physical · Smart Grid · Cyber-Risk Assessment · Grid Planning · Challenges · Success Criteria.

1 Introduction

Grid planning is a process that electric power grid companies carry out to change power transfer capability through decisions about the construction, upgrading, replacement, retrofitting or decommissioning of assets [16]. Long-term grid planning is typically carried out on a time horizon of decades, and aims to develop the system optimally to meet future demands. Grid planning can rely on passive measures such as traditional reinforcement or building new lines, or active measures such as support from ICT-solutions during operation to increase the power transfer capability or facilitate other kinds of optimizations. The ongoing digitalization of the electric power grid is resulting in complex cyber-physical smart grid systems that may be highly exposed to cyber risks. Electric power grid companies are therefore pushed to assess potential cyber risks as part of the grid planning process. This is difficult because most available information about the target power grid at the planning stage is at a conceptual level.

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. Widely used cyber-risk assessment approaches such as ISO 27005 [25] and NIST 800-39 [37] are not easily aligned with risk assessment approaches that are specific for power systems [26, 31]. 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. This is becoming increasingly important when 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 an 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 power systems and smart grids. Moreover, it explores strategies for moving towards integrated risk assessment that includes both cybersecurity and power system threats, ICT dependability issues, as well as the consideration of cyber risks in the grid planning process. Thus, the contribution of this paper is threefold. 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 of 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. Third, we address the need for approaches that are easy to use and comprehend, especially for grid planning purposes, and propose a low-threshold approach to support high-level cyber-risk assessment. 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, while Sect. 3 describes related work. Section 4 describes our research method. Section 5 describes the findings from the interviews and the identified success criteria. Section 6 describes the four risk assessment methods used in previous work, while Sect. 7 evaluates the extent to which the methods fulfill the identified success criteria. In Sect. 8, we turn our focus on adapting a low-threshold cyber-risk assessment method for a grid planning process. Finally, Sect. 9 concludes the paper and summarizes lessons learned in terms of identified gaps. This paper is an extended version of the paper by Erdogan et al. [13]. The new content in this extended version is related to cyber-risk assessment for grid planning based on industrial needs we identified in the first version of the paper. This extension led to updated contents in Sections 1, 2, 3, 4, and 9. Moreover, most of the contents in Sections 2 and 3 are new, while Section 8 is completely new considering the adaptation of cyber-risk assessment for grid planning.

2 Background

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" [25]. 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 [25, 38]. 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 increasing attack risks to the smart grid. The energy industry faces significant challenges in managing such risks.

Assessment of traditional, physical risks is an important part of grid companies' activities on all time horizons, from operation to long-term planning. Cyber risks, on the other hand, are typically assessed based on existing cyber-physical systems; they are usually not considered as part of planning activities for the long-term development of the system, which should be in place to promote security-by-design. Grid planning, or grid development, is traditionally dealing with "decisions that change power transfer capability through decisions about the construction, upgrading, replacement, retrofitting or decommissioning of assets" [16]. A simple example of such a decision is whether the grid company should a) upgrade a distribution line to meet the expected increase in electricity demand in an area, or b) defer the investment and take the risk of operational challenges in case it turns out that the existing system becomes insufficient to ensure the security of electricity supply. For such decisions, cyber-risk assessments are unlikely to influence the grid company's choice between the alternatives (a and b).

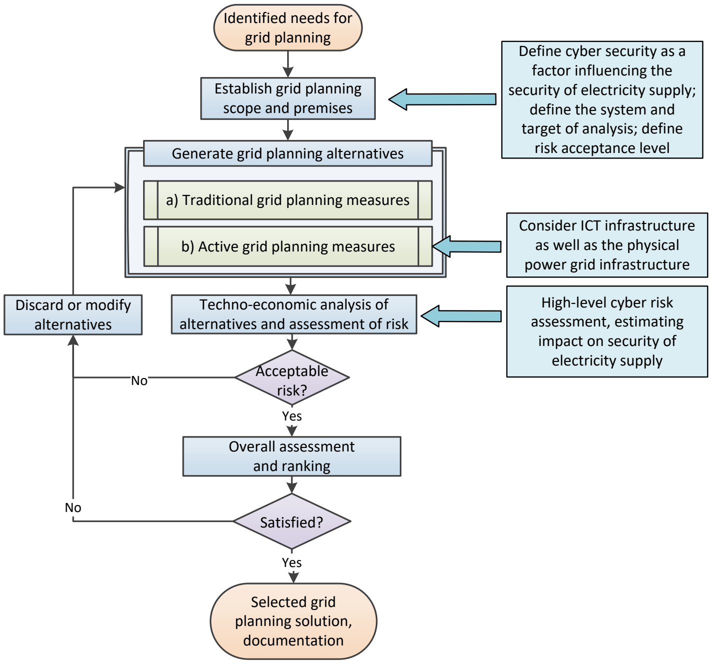
Identified needs for grid planning
Establish grid planning scope and premises
Define cyber security as a factor influencing the security of electricity supply; define the system and target of analysis; define risk acceptance level
Generate grid planning alternatives
a) Traditional grid planning measures
b) Active grid planning measures
Consider ICT infrastructure as well as the physical power grid infrastructure
Discard or modify alternatives
Techno-economic analysis of alternatives and assessment of risk
High-level cyber risk assessment, estimating impact on security of electricity supply
No
Acceptable risk?
Yes
Overall assessment and ranking
No
Satisfied?
Yes
Selected grid planning solution, documentation

Fig. 1. Framework for planning of active distribution grids, adapted from [47]. Text boxes on the right indicates the adaptations needed to consider cyber risk.

However, smart grids introduce the option of implementing so-called active grid planning measures that involve active utilization of resources in the grid during grid operation. A general framework for the planning of active distribution grids was proposed in [47]. Figure 1 gives a high-level illustration of a grid planning process according to this framework.

Figure 1 illustrates how active measures are considered on equal footing as traditional (passive) measures when generating the set of grid planning alternatives to choose from. Passive measures involve installing physical power grid infrastructure in the system. Active measures to a much larger extent also involves ICT infrastructure. For example, alternative (b) in the example above could involve installing dynamic grid reconfiguration and self-healing functionality and plan for utilizing these new resources to manage potential operational risks during the operational phase. Since this alternative (b) to a much larger extent than alternative (a) relies on ICT for operating with these active distribution grid functionalities, it is important to also consider cyber risks in the planning phase. This should be defined as a part of the grid planning study already in the initial step ("Establish grid planning scope and premises"). The remainder of this paper will however focus on assessment of cyber risk as part of the step for techno-economic analysis that includes assessment of risk in general.

3 Related Work

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) [24], event tree analysis (ETA) [23] and attack trees [43] 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) [36] and Bayesian networks [4] 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 [3] and OCTAVE [1] rely on text and tables, graph and tree-based approaches use diagrams as an important means for communication, evaluation, and assessment.

Traditional risk assessment focuses on hazards with relatively high probability that come from inherent properties of the system (e.g., component aging). 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. Vulnerability assessment can be seen as a method that aims to identify hidden vulnerabilities in infrastructure systems that can lead to severe consequences, such as blackouts, economic or social turmoil, etc. [28]. These high-impact and low-probability events can be too complex to be considered in 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 [28]. A framework for studying vulnerabilities and risk in the electricity supply, based on the bow-tie model, is proposed in [19, 27, 20, 46].

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 [2]. 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) [5]. 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 [58], cyber-physical interface matrix [29], co-simulation [15], and traditional event trees [33] and reliability block diagrams [10]. 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 [2], stochastic Petri net models [49], Markov processes [57] and Bayesian attack graphs [56].

The above presented works propose approaches that address the problem of assessing cyber-risk in the operation of the smart grid that, despite being a relatively young research area, is converging towards a consensus regarding approaches and standards. On the other side, cyber-risk assessment in the context of smart grid planning, or in the more general context of cyber-physical critical infrastructures, represents a novel research field that is mostly unexplored. For this reason, the scientific literature presents just a few works in this research field, that only border on the main research problem of finding the optimal planning solution properly taking into account cyber-risks (see Section 2). Wang et al. in [51] propose an optimisation model for distributed generation and grid expansion planning taking into account substations failures due to cyber failures. The authors model the cyber failures events with random parameters characterized by a constant failure rate, and aim at minimizing the investments taking into account the costs of energy not supplied due to cyber failures. A more accurate mathematical description of human dynamics for cyber attacks is proposed in [52], which proposes the adoption of power law distribution instead of the Poisson distribution to simulate the cyber attack occurrence pattern in the reliability evaluation of electric power grid considering cyber vulnerabilities.

Instead of considering the probability of occurrence of cyber attacks to critical infrastructures, other works focus more on the resilience properties of the infrastructure, which can be defined as the ability of the system to mitigate any residual risk, as well as address unknown or emerging threats [32, 53]. Huang et al. in [22] propose an optimal planning policy to enhance resilience and security of interdependent critical infrastructures (ICI), represented by communication networks, power grid and subway networks. The interdependencies between infrastructure components are modelled through holistic probabilistic networks, where the failure and recovery dynamics are modelled through Markov decision processes (MDP). An agent-based modelling approach is presented by Foglietta et al. [14], aiming at simulating interdependences between cyber-physical layers in critical infrastructures, and cascading effects in fault propagation.

4 Research Method

Figure 2 illustrates our research method, which consists of eight steps. In Step 1, we conducted four interviews with four companies in the energy sector and

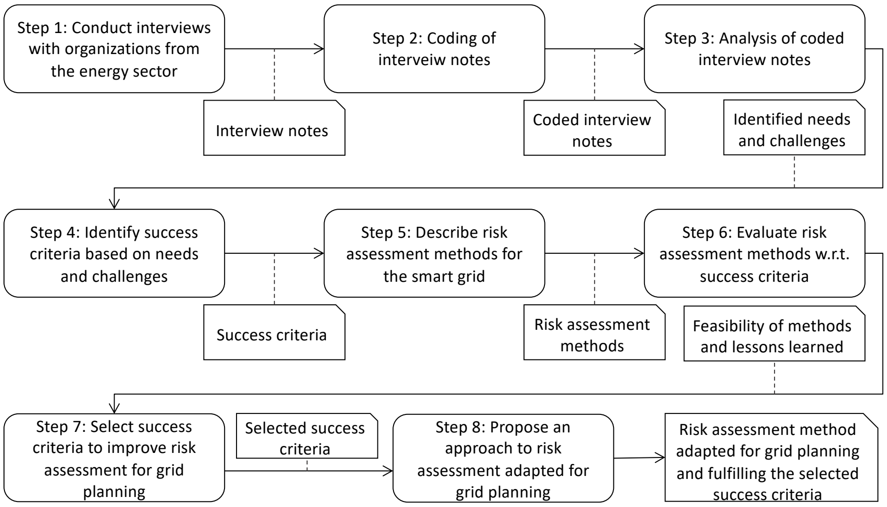
Step 1: Conduct interviews with organizations from the energy sector
Interview notes
Step 2: Coding of interveiw notes
Coded interview notes
Step 3: Analysis of coded interview notes
Identified needs and challenges
Step 4: Identify success criteria based on needs and challenges
Success criteria
Step 5: Describe risk assessment methods for the smart grid
Risk assessment methods
Step 6: Evaluate risk assessment methods w.r.t. success criteria
Feasibility of methods and lessons learned
Step 7: Select success criteria to improve risk assessment for grid planning
Selected success criteria
Step 8: Propose an approach to risk assessment adapted for grid planning
Risk assessment method adapted for grid planning and fulfilling the selected success criteria

Fig. 2. Research method.

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 through our own network, but also asking companies and organizations from the CINELDI (Centre for Intelligent Electricity Distribution) project [7], which is the project in which this work was carried out. The inter-

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

Table 1. Interviews conducted. CISO = Chief Information Security Officer. PM = Project Manager. Table adapted from [13].

viewees 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 success criteria.

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 9.

Based on the identified success criteria and lessons learned, we selected, in Step 7, one success criterion to focus on in order to adapt risk assessment for grid planning. The selected success criterion is related to ease of comprehension and use by people who are not experts in cyber-risk assessment (Criterion SC1 in Section 5).

Finally, in Step 8 we propose an approach to risk assessment, based on existing methods, adapted for grid planning and fulfilling the selected success criterion in Step 7 (SC1).

5 Identified Success Criteria

This section describes the success criteria identified based on the interviews, as explained in Section 4. 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 risks. 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 grid companies 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 electric power distribution 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.

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 security 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 high-level threat modeling in the management group, 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.

6 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). It is beyond this paper to describe each method in detail, we therefore provide a brief description of each approach and refer to other sources for further details.

6.1 CORAS

CORAS is a method for conducting security risk assessment [34]. 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 [8] 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 [34, 39, 40].

6.2 The Vulnerability Analysis Framework (VAF)

The Vulnerability Analysis Framework (VAF) [17, 20, 46] is an analysis approach aimed at identifying and analyzing vulnerabilities related to extraordinary events with respect to the security of electricity supply. 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 component outages leading to critical consequences, 3) identify threats that can cause the critical outages, 4) identify vulnerabilities associated with the power system's 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 [50]. 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. [41]; physical, cyber, geographical, and logical.

6.3 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 [35].

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 [48] book on threat modeling and Howard & Lipner's [21] book on the Microsoft Security Development Lifecycle. A later book by Shostack [44] also covers a number of compatible software tools, including the Microsoft Threat Modeling tool [6], which conforms to the methodology presented by Swidersky & Snyder.

The first step in this threat modeling approach is to draw a data flow diagram [9] 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.

6.4 Dependability Analysis with SAN (DA-SAN)

A novel approach for dependability analysis of power systems is proposed by Zerihun, Garau, and Helvik [55] based on Stochastic Activity Network (SAN) modelling. SAN is a variant of Petri Nets [42] 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 [55], the SAN method is evaluated on a test distribution network, where the impact of ICT internal and external vulnerabilities on the performances 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.

7 Evaluation of Risk Assessment Methods

Figure 3 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 Sect. 5. The placement of each method in the scale in Figure 3 is based on the authors' expert knowledge and experience in using the methods as outlined in Sect. 6.

Companies within the electric power 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 [45, 30]. However, we believe VAF is slightly easier to comprehend by personnel of the electric power sector companies because VAF uses concepts and constructs that are commonly used in the power sector. CORAS has also been used in many industrial risk assessments for the power sector [39,

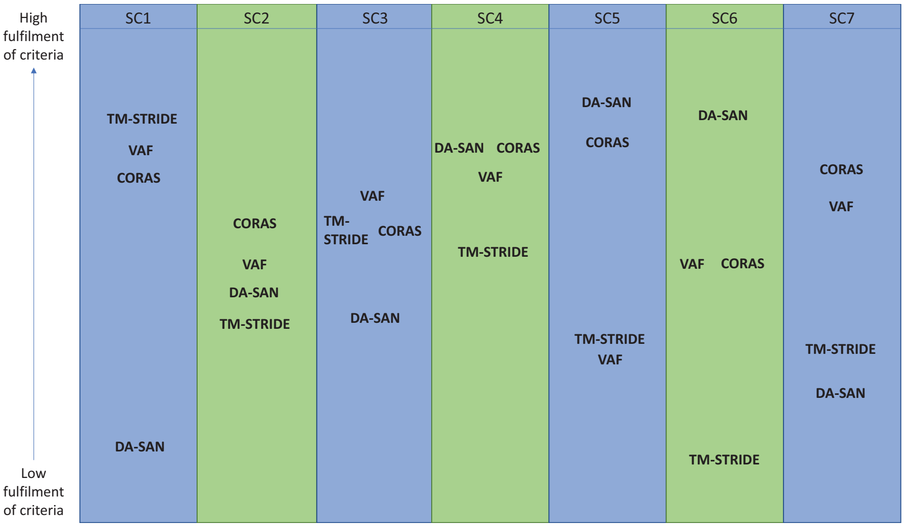

Fig. 3. Comparison of methods with respect to fulfillment of the success criteria described in Section 5. Figure adapted from [13].

40]. 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 electric power sector because most approaches do not have domain-specific support for the electric power sector (see Section 2).

Considering the criterion SC1, and the fact that all the identified criteria described in Section 5 points out the need for some kind of support to more easily carry out risk assessment, comprehensibility and ease of use seems to be 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 electric power 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 electric power 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 electric power 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 power 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 electric power 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, the power 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 electric power 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 electric power distribution, railroad transport, and education (university) [11, 12].

The infrastructure of electric energy systems is 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 electric power 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 power systems, changes (both from a cyber perspective and from a physical perspective) may happen frequently. Whenever an update is introduced in the power 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 electric power 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 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 electric power 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 power systems. Dynamic and real-time risk assessment must inevitably be addressed and properly supported, but the current state of risk assessment in the power sector shows that basic needs and challenges (as described in this section) must be addressed before the dynamic/real-time aspects can be supported.

8 Adaptation of Cyber-Risk Assessment for Grid Planning

In the context of grid planning, the target of analysis is a system that has not yet been implemented. Because the goal of planning is to identify and select a grid planning solution to implement (see Figure 1), most available information about the target of analysis is at a conceptual level. There is therefore little certain information about the final system in the planning phase. Moreover, as the planning phase may produce several alternatives of grid solutions to implement, there may be multiple potential future systems to assess. Even though the planning phase may span weeks to years (depending on the grid level), there is too little time to assess all alternatives in detail with respect to cyber risks. Thus, there is a need for high-level cyber-risk assessment methods in the planning phase that are easy to comprehend and use without having the need to go into technical details or having risk assessment expertise (SC1).

As explained in Sect. 7, VAF, CORAS, and TM-STRIDE are to some extent easy to comprehend, but none of the methods fully meet the Success Criterion SC1. According to the interviews (see Sect. 5), we see that there is a need for easier methods that do not consider quantitative aspects as a required input to the risk assessment, and that are sufficiently high-level so it is easy to carry out by people who are not experts in cyber-risk assessment. Based on these points, we propose to adopt a low-threshold approach specifically developed to facilitate ease of use for people who are not necessarily experts in cyber-risk assessment. Moreover, we propose an approach to be used in the step "Techno-economic analysis of alternatives and assessment of risk" of the grid planning framework illustrated in Figure 1. The approach we propose is named Human and Organizational Risk Modelling (HORM), co-developed by one of the authors of this paper, and it is based on Customer Journey Modelling Language (CJML) [18]. Moreover, the main target group of HORM is SMEs, which means that the approach is also suitable for grid companies since more than half of the distribution grid companies are small companies with less than 50 people who typically do not have dedicated in-house cybersecurity experts.

In the following we briefly explain HORM, and then we provide an example in context of self-healing grids based on our previous work [39]. As mentioned, HORM is based on CJML. Figure 4 illustrates the basic elements of CJML. All actors in a scenario have their own swimlane as illustrated by the three actors in Figure 4. An actor can perform an action, or there may be a communication point between two actors. An action element is used for non-communicating events, while a communication point has a sender and a receiver that must be positioned in the corresponding swimlanes of the actors. The arrow on a communication point illustrates that the information flows from the sender to the receiver of that information. A communication happens via communication channels, for example email, chat, or SMS. All actions and communication points have textual descriptions in the diagrams. Finally, all actions and communication points follow a timeline, as illustrated in Figure 4.

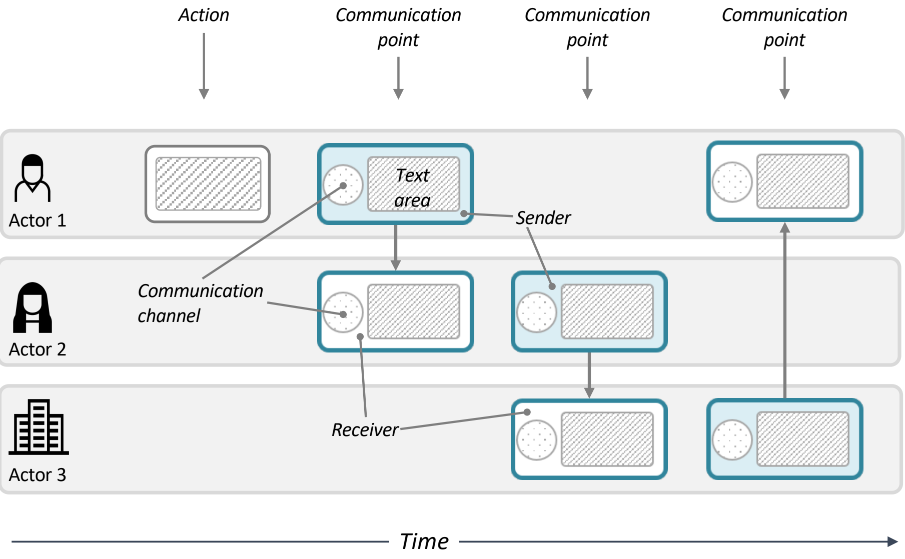

Fig. 4. The basic elements in Customer Journey Modelling Language (CJML).

HORM is based on CJML and is freely available[4]. HORM provides a method, an extension of the graphical modelling language of CJML with cyber-risk concepts and notations, and supporting tools. With respect to cyber-risk concepts, HORM includes malicious actors (such as hackers), threat scenarios, and unwanted incidents. HORM may be used to identify and analyze potential cyber risks, but it is intentionally not developed to estimate risks as this requires domain expertise and detailed information about the target of analysis, which is scarce in the context of grid planning, as pointed out above. We refer to the sources of HORM and CJML for further detailed explanation [18].

[4] https://cjml.no/horm/

Having covered the basics of HORM and CJML, let us consider a self-healing grid example we will use as a basis to identify potential cyber risks as part of grid planning. Self-healing grids are electric power grids where sensing, control, and communication technology is used for automatic reconfiguration and power restoration [39]. Assume the following context: a grid company is considering to implement a self-healing grid with centralized control as one of several alternatives during the grid planning phase. Although a self-healing grid functionality introduces benefits, it does come with potential cyber-risks. The grid company is especially worried about protecting the reliability of electric supply (security of supply) and wants to investigate potential threat scenarios that may cause prolonged duration of interruption of electric supply. Thus, as part of the planning process, the grid company wants to carry out a high-level cyber-risk assessment to identify potential threat scenarios that may cause the unwanted incident of interruption of electric supply.

A potential unwanted incident may occur if a hacker tries to access the Supervisory Control and Data Acquisition (SCADA) system using the default username and passwords for access control, which is a fairly common vulnerability in most of SCADA systems [54]. Thus, a hacker may exploit this security misconfiguration and gain access to the SCADA system, which in turn may provide access to the software in charge of controlling switches in the grid that facilitates the self-healing functionality. The hacker may then inject inadequate or misleading information into the software controlling the switches, which in turn will produce inadequate or misleading info for the switches. When the switches receive this information, they may become erroneous or delayed in their operation. This will lead to the unwanted incident that the self healing functionality (sectioning of areas in the grid) is delayed or prevented, which in turn causes prolonged duration of interruption of electric supply. Figure 5 illustrates the resulting HORM model based on the above self-healing grid example.

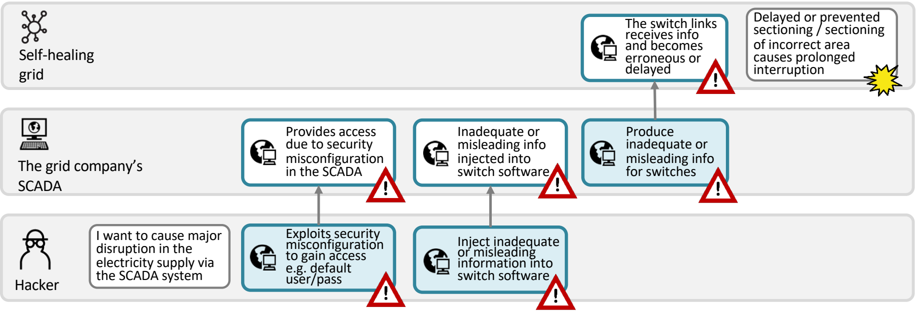
Self-healing grid
The switch links receives info and becomes erroneous or delayed
Delayed or prevented sectioning / sectioning of incorrect area causes prolonged interruption
The grid company's SCADA
Provides access due to security misconfiguration in the SCADA
Inadequate or misleading info injected into switch software
Produce inadequate or misleading info for switches
Hacker
I want to cause major disruption in the electricity supply via the SCADA system
Exploits security misconfiguration to gain access e.g. default user/pass
Inject inadequate or misleading information into switch software

Fig. 5. Hacker causes prolonged duration of interruption of electric supply.

The above example illustrates that it is possible to create high-level cyber-risk model with little information about the context of the planned grid. Given the level of abstraction of HORM models, it is reasonable to argue that models such as Figure 5 is a good starting point to support decision making in the grid planning, and to decide whether detailed cyber-risk assessment is needed.

9 Conclusions and Lessons Learned

The electric power sector is struggling to adopt and carry out risk assessments considering cyber risks in the context of smart grids, and in particular in context of grid planning. In this paper, we have interviewed representatives from the power 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 electric power 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. Finally, we turned our focus on a process used for grid planning and proposed a high-level cyber-risk assessment approach that may be used within the grid planning process.

We interviewed six companies from the energy sector to better understand their needs and challenges for cyber-risk assessment. Based on the needs and challenges described by the interviewees, we identified seven success criteria cyber-risk assessment methods for the electric power 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 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 7 for a detailed discussion about the gaps that need to be addressed.

With respect to electric power grid planning and the adoption of cyber-risk assessment for the grid planning process, we argued why there is a need for methods that are easy to use and comprehensible by non-experts (SC1), and proposed to use the Human and Organizational Risk Modelling (HORM) approach to carry our high-level cyber-risk assessment in the grid planning step "techno-economic analysis of alternatives and assessment of risk" (see Figure 1). 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 electric power sector in general.

2. There is a need for support in helping risk analysts in the power 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 electric power 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 power 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 provide better decision support (SC7).
6. There is especially a need for high-level cyber-risk assessment methods in the planning phase that are easy to comprehend and use without having the need to go into technical details or having risk assessment expertise (SC1). To this end, we propose in this paper to adopt HORM for cyber-risk assessment in the planning phase, as mentioned above.

The proposal of using HORM in grid planning is our initial step towards addressing the needs of the industry for cyber-risk assessment in context of smart-grid. We believe HORM is a reasonable approach to address SC1. However, in future work, we will try out HORM in a real-world grid planning case and investigate its feasibility.

Acknowledgements This work has been carried out as part of the CINELDI project (257626/E20) funded by the Research Council of Norway, as well as the CyberKit4SME project (883188) funded by the European Union's Horizon 2020 Research and Innovation Programme.

References

1. Alberts, C., Dorofee, A., Stevens, J., Woody, C.: Introduction to the octave approach. Tech. rep., Carnegie-Mellon University (2003)
2. 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., Tindemans, S.: Reliability modeling considerations for emerging cyber-physical power systems. In: Proc. 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS'18). pp. 1–7. IEEE (2018)
3. Barber, B., Davey, J.: The use of the CCTA risk analysis and management methodology CRAMM in health information systems. Medinfo **92**, 1589–1593 (1992)

4. Ben-Gal, I.: Bayesian networks. Encyclopedia of Statistics in Quality and Reliability **1** (2008)
5. Billinton, R., Allan, R.N.: Reliability Evaluation of Power Systems. Plenum Press, New York, 2 edn. (1996)
6. Bygdås, E., Jaatun, L.A., Antonsen, S.B., Ringen, A., Eiring, E.: 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). pp. 1–7. IEEE (2021)
7. Centre for Intelligent Electricity Distribution (CINELDI). `https://www.sintef.no/projectweb/cineldi/` (2022), accessed November 2, 2022
8. CORAS Risk Modelling Tool. `https://coras.tools/` (2022), accessed November 2, 2022
9. DeMarco, T.: Structure analysis and system specification. In: Pioneers and Their Contributions to Software Engineering, pp. 255–288. Springer (1979)
10. Ding, Z., Xiang, Y., Wang, L.: Incorporating unidentifiable cyberattacks into power system reliability assessment. In: Proc. 2018 IEEE Power Energy Society General Meeting (PESGM'18). pp. 1–5. IEEE (2018)
11. Erdogan, G., Hugo, Å., Romero, A., Varano, D., Zazzeri, N., Žitnik, A.: 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). pp. 509–520. SciTePress (2020)
12. Erdogan, G., Romero, A., Zazzeri, N., Žitnik, A., Basile, M., Aprile, G., Osório, M., Pani, C., Kechaoglou, I.: 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). pp. 702–713. SciTePress (2021)
13. Erdogan, G., Tøndel, I.A., Tokas, S., Garau, M., Jaatun, M.G.: Needs and challenges concerning cyber-risk assessment in the cyber-physical smart grid. In: Proc. 17th International Conference on Software Technologies (ICSOFT'22). pp. 21–32. SciTePress (2022)
14. Foglietta, C., Panzieri, S.: Resilience in critical infrastructures: The role of modelling and simulation. In: Issues on Risk Analysis for Critical Infrastructure Protection. IntechOpen (2020)
15. Garau, M., Celli, G., Ghiani, E., Soma, G.G., Pilo, F., Corti, S.: 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). pp. 365–370. IEEE (2015)
16. GARPUR Consortium: D3.1: Quantification method in the absence of market response and with market response taken into account. Tech. rep., GARPUR (2016), accessed November 2, 2022
17. Gjerde, O., Kjølle, G.H., Detlefsen, N.K., Brønmo, G.: Risk and vulnerability analysis of power systems including extraordinary events. In: Proc. 2011 IEEE Trondheim PowerTech. pp. 1–5. IEEE (2011)
18. Halvorsrud, R., Boletsis, C., Garcia-Ceja, E.: Designing a modeling language for customer journeys: Lessons learned from user involvement. In: 2021 ACM/IEEE 24th International Conference on Model Driven Engineering Languages and Systems (MODELS'21). pp. 239–249 (2021)
19. Hofmann, M., Kjølle, G.H., Gjerde, O.: Development of indicators to monitor vulnerabilities in power systems. In: Proc. 11th International Probabilistic Safety Assessment and Management Conference (PSAM'11). pp. 1–10. Curran Associates, Inc. (2012)

20. Hofmann, M., Kjølle, G.H., Gjerde, O.: Vulnerability analysis related to extraordinary events in power systems. In: Proc. 2015 IEEE Eindhoven PowerTech. pp. 1–6. IEEE (2015)
21. Howard, M., Lipner, S.: The Security Development Lifecycle. Microsoft Press, Redmond, WA (2006)
22. Huang, L., Chen, J., Zhu, Q.: Distributed and optimal resilient planning of large-scale independent critical infrastructures. In: 2018 Winter Simulation Conference (WSC'18). pp. 1096–1107. IEEE (2018)
23. IEC: Dependability management–part 3: Application guide–section 9: Risk analysis of technological systems (1995)
24. IEC: IEC 61025:2006 Fault tree analysis (FTA). Standard, IEC (2006)
25. ISO: ISO/IEC 27005:2018 - Information technology - Security techniques - Information security risk management. Standard, ISO (2018)
26. Jakobsen, S.H., Garau, M., Mo, O.: An open-source tool for reliability analysis in radial distribution grids. In: Proc. 2021 International Conference on Smart Energy Systems and Technologies (SEST'21). pp. 1–6. IEEE (2021)
27. Kjølle, G.H., Utne, I.B., Gjerde, O.: Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. Reliability Engineering & System Safety **105**, 80–89 (2012)
28. Kröger, W., Zio, E., Schläpfer, M.: Vulnerable systems. Springer (2011)
29. Lei, H., Singh, C., Sprintson, A.: Reliability analysis of modern substations considering cyber link failures. In: Proc. 2015 IEEE Innovative Smart Grid Technologies - Asia (ISGT'15). pp. 1–5. IEEE (2015)
30. Lewis, S., Smith, K.: Lessons learned from real world application of the bow-tie method. In: Proc. 6th Global Congress on Process Safety. pp. 22–24. OnePetro (2010)
31. Li, W.: Risk Assessment of Power Systems: Models, Methods, and Applications. John Wiley & Sons (2014)
32. Linkov, I., Kott, A.: Fundamental concepts of cyber resilience: Introduction and overview. In: Cyber Resilience of Systems and Networks, pp. 1–25. Springer (2019)
33. Liu, Y., Deng, L., Gao, N., Sun, X.: A reliability assessment method of cyber physical distribution system. Energy Procedia **158**, 2915–2921 (2019)
34. Lund, M., Solhaug, B., Stølen, K.: Model-Driven Risk Analysis: The CORAS Approach. Springer (2011)
35. McGraw, G.: Software Security: Building Security In. Addison-Wesley (2006)
36. Nielsen, D.S.: The cause/consequence diagram method as a basis for quantitative accident analysis. Risø National Laboratory (1971)
37. NIST: Nist special publication 800-39 - managing information security risk organization, mission, and information system view. Standard, NIST (2011)
38. NIST: Special publication 800-30 guide for conducting risk assessments. Standard, NIST (2012)
39. Omerovic, A., Vefsnmo, H., Erdogan, G., Gjerde, O., Gramme, E., Simonsen, S.: 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). pp. 39–51. SciTePress (2019)
40. Omerovic, A., Vefsnmo, H., Gjerde, O., Ravndal, S., Kvinnesland, A.: 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). pp. 17–33. Springer (2020)

41. Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K.: Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine **21**(6), 11–25 (2001)
42. Sanders, W.H., Meyer, J.F.: Stochastic activity networks: Formal definitions and concepts. In: School organized by the European Educational Forum. pp. 315–343. Springer (2000)
43. Schneier, B.: Modeling security threats. Dr. Dobb's journal **24**(12) (1999)
44. Shostack, A.: Threat modeling: Designing for security. John Wiley & Sons (2014)
45. Solhaug, B., Stølen, K.: The coras language - why it is designed the way it is. In: Proc. 11th International Conference on Structural Safety and Reliability (ICOSSAR'13). pp. 3155–3162. Citeseer (2013)
46. Sperstad, I.B., Kjølle, G.H., Gjerde, O.: A comprehensive framework for vulnerability analysis of extraordinary events in power systems. Reliability Engineering & System Safety **196**, 106788 (2020)
47. Sperstad, I.B., Solvang, E., Gjerde, O.: Framework and methodology for active distribution grid planning in norway. In: Proc. 2020 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS'20). pp. 1–6. IEEE (2020)
48. Swiderski, F., Snyder, W.: Threat Modeling. Microsoft Press (2004)
49. Ten, C.W., Liu, C.C., Manimaran, G.: Vulnerability assessment of cybersecurity for SCADA systems. IEEE Transactions on Power Systems **23**(4), 1836–1846 (2008)
50. Tøndel, I.A., Vefsnmo, H., Gjerde, O., Johannessen, F., Frøystad, C.: Hunting dependencies: Using bow-tie for combined analysis of power and cyber security. In: Proc. 2020 2nd International Conference on Societal Automation (SA'20). pp. 1–8. IEEE (2021)
51. Wang, H.H., Shi, L., Ni, Y.: Distribution system planning incorporating distributed generation and cyber system vulnerability. The Journal of Engineering **2017**(13), 2198–2202 (2017)
52. Xiang, Y., Wang, L., Zhang, Y.: Adequacy evaluation of electric power grids considering substation cyber vulnerabilities. International Journal of Electrical Power & Energy Systems **96**, 368–379 (2018)
53. Xu, L., Guo, Q., Sheng, Y., Muyeen, S.M., Sun, H.: On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective. Renewable and Sustainable Energy Reviews **152**, 111642 (2021)
54. Yadav, G., Paul, K.: Assessment of scada system vulnerabilities. In: Proc. 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'19). pp. 1737–1744. IEEE (2019)
55. Zerihun, T.A., Garau, M., Helvik, B.E.: Effect of communication failures on state estimation of 5G-enabled smart grid. IEEE Access **8**, 112642–112658 (2020)
56. Zhang, Y., Wang, L., Xiang, Y., Ten, C.W.: Power system reliability evaluation with SCADA cybersecurity considerations. IEEE Transactions on Smart Grid **6**(4), 1707–1721 (2015)
57. Zhang, Y., Wang, L., Xiang, Y., Ten, C.W.: Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation. IEEE Transactions on Power Systems **31**(6), 4379–4394 (2016)
58. Zhu, W., Panteli, M., Milanović, J.V.: 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). pp. 1–5. IEEE (2018)