

A Light-Weight Tool-Supported Method for Cyber Risk Assessment in the Planning of Cyber-Physical Smart Grids

Gencer Erdogan*, Tesfaye Amare Zerihun[†], Iver Bakken Sperstad[†] and Oddbjørn Gjerde[†]

*Sustainable Communication Technologies, SINTEF Digital, Oslo, Norway

Email: gencer.erdogan@sintef.no

[†]Energy Systems, SINTEF Energi, Trondheim, Norway

Email: {tesfaye.zerihun, iver.bakken.sperstad, oddbjorn.gjerde}@sintef.no

Abstract—A major challenge during grid planning is the identification of cybersecurity threats potentially introduced by active digital measures. This challenge arises because grid planning occurs at an early, conceptual stage, typically years ahead of realization, and often lacks concrete information about the active digital measures at this early phase. This highlights the need for simple, user-friendly cyber risk assessment methods that grid planners can use, even without detailed information about the final solutions. To address this need, we propose a lightweight, tool-supported, six-step method. This method employs the Customer Journey Modeling Language (CJML), which is comprehensible to various professional backgrounds, and which we have adapted to include the necessary cybersecurity concepts to help grid planners identify cybersecurity threats. The method is supported by our freely available, open-source risk modeling tool. Using a case based on a real-world electricity distribution grid, we demonstrate how our method supports grid planners in performing cyber-risk assessments with limited information about the final solutions and their vulnerabilities to cyber threats. Preliminary results indicate that our method is effective in enabling grid planners to assess potential cybersecurity risks during the planning phase, thereby enhancing the reliability and security of future electricity distribution systems.

Index Terms—cybersecurity, risk assessment, light-weight, tool-supported, method, cyber-physical, smart grid, planning

I. INTRODUCTION

In smart grids, the reliance on digital technology for active measures, such as self-healing technologies, introduces vulnerabilities not found in traditional distribution grids. This digital reliance exposes critical infrastructure to cybersecurity threats, like NotPetya and the more recent cyber attack on the Viasat-operated KA-SAT network resulting in the loss of remote monitoring and control of 5800 ENERCON wind turbines across Europe [1]. Grid planning aims to find solutions to enhance the grid with these active digital measures alongside passive measures such as grid expansion, reinforcement, or reinvestment. However, since grid planning analyses are carried out at an early and quite conceptual stage [2], it is challenging to identify potential cybersecurity threats. This is due to the lack of concrete information about active digital measures at this early phase, often several years before solutions are implemented. This results in uncertainties about the final solutions, which includes the physical electricity grid as well as the digital

systems, and their associated cyber risks. Given that non-cyber experts are often involved in assessing these cyber risks with limited information about the final solutions [3], there is a need for low-threshold methods to assess cyber risks during the grid planning process. Such methods would enable easier comprehension of cybersecurity risks and threats, ensuring that those responsible for the grid development can take timely and effective measures to safeguard the grid already at the planning stage. This is particularly important for grid planners, enabling them to evaluate active digital measures on equal footing with traditional (passive) measures, and to compare the costs, benefits, and risks of different alternatives.

In previous work, we identified seven needs for cyber-risk assessment in the context of cyber-physical smart grids [3]. The needs were identified by interviewing relevant companies in the electricity sector. However, the identified primary need for a risk assessment method is that it should be simple for grid planners to understand and use, even for those who are not experts in risk assessment [3].

The contribution of this paper is twofold. First, we present a light-weight tool-supported method for cyber-risk assessment tailored to the planning of cyber-physical smart grids. Second, we present a concrete example of how it can be applied and use this as a basis to discuss the extent to which the method is easy to comprehend and use in the context of the grid planning process [2]. Our aim is to provide grid planners the means to sufficiently identify potential cybersecurity risks during the grid planning phase with limited information, efforts, and cybersecurity expertise. Early identification of cybersecurity risks allows for the avoidance of plans that rely on active digital measures associated with unacceptable risks. We propose to meet this aim by providing the grid planners first with a simplified conceptual foundation for cybersecurity risk assessment and then with a light-weight, step-wise method that builds upon these concepts. The obtained preliminary results from applying the method on a real-world reference system are promising and demonstrates that the method can support grid planners for the aforementioned task.

The rest of the paper is organized as follows. Section II briefly explains our modelling tool and the main concepts

of the CJML modelling language. Section III describes our proposed method in a running example using a reference system based on a real-life Norwegian electricity grid. Section IV discusses the extent to which our method is easy to comprehend and use. Section V relates our work to other cyber risk assessment approaches. Finally, Section VI concludes the paper.

II. RISK MODELLING TOOL

Before we explain the method, we need to explain the Customer Journey Modelling Language (CJML) and the risk modelling tool that we have developed to support the method.

As already mentioned, the tool is freely available online [4]. The tool is available as an editor accessible via a web browser, where the user can create CJML models like the one illustrated in Fig. 3 by drag-and-drop functionalities. The reader is referred to the web page of the tool for further details and supporting training materials on how to use the tool [4].

Fig. 1 illustrates the basic graphical constructs of a CJML diagram. The arrows and *italic text* in Fig. 1 are included in the figure for explanatory purposes. The dashed arrows are part of the CJML language.

According to the metamodel of CJML [5], an actor is a human or a non-human entity involved in a journey. A touchpoint is a step in a customer journey, and it can either be an action or a communication point [5]. While an action is an event or activity conducted by an actor as part of the journey, a communication point is an instance of communication or interaction between two actors. A communication point always has a sender and a receiver (with the direction shown by dashed arrows). Each communication point is carried out via a communication channel, e.g., via email or a web page.

We have extended the syntax of the CJML language by adding the cyber risk concepts: asset, threat actor, threat scenario, unwanted incident, likelihood, and consequence. According to ISO 27005, an *asset* is anything that has value to the organization and which, therefore, requires protection [6]. A *threat actor* is one who may introduce a threat, as defined by ISO 27000; a potential cause of an unwanted incident, which can result in harm to a system or organization [7]. A *threat scenario* encompasses what ISO 27000 describes as an information security event; it represents a sequence of activities or circumstances within a system, service, or network that suggests a potential violation of information security policy, indicates a control failure, or identifies a novel situation with implications for security [7]. An *unwanted incident* encompasses what ISO 27000 describes as an information security incident; it is the occurrence of a single or a series of unexpected information security events that significantly threaten to compromise business operations and jeopardize information security [7]. Regarding likelihood and consequence, we have chosen to use the more easily understood definitions provided by CORAS [8]. A *likelihood* is the frequency or probability of something to occur. A *consequence* is the impact of an unwanted incident on an asset in terms of harm or reduced asset value.

Please note that in the extension of CJML, we have opted not to incorporate the concepts of *vulnerability* and *risk treatment* (security measures), which are typically used in cyber risk assessments. This decision stems from the challenges encountered in pinpointing vulnerabilities and formulating risk treatments during the grid planning stage, as these elements are generally characterized by more detailed technical specifics that are typically not available in the grid planning phase.

III. EXAMPLE-DRIVEN EXPLANATION OF THE METHOD

In the following, we provide an example-driven explanation of our six-step method, based on a reference system that has been created from a real-life Norwegian electricity grid [9].

A. Step 1: Describe the Target of Analysis in the Planned Solution

The objective of Step 1 is to describe the target of analysis in the planned solution. The target of analysis defines the scope and boundaries that will be considered in the risk assessment [6]. The output of this step is a high-level description of the target of analysis. Based on our experience and collaborations with grid planners [2], we suggest to describe the target of analysis by considering the relevant components for a specific planned solution, and accompany the description with graphical illustrations, e.g., high-level topology diagrams, like the one shown in Fig. 2.

Fig. 2 illustrates our real-world target of analysis in the planned solution, where we consider self-healing applications in addition to grid reinforcement. In our example, this planned solution is to be implemented in the CINELDI reference system, which is a radial medium voltage (22 kV) distribution system with 124 nodes (commonly referred to as "bus" in power grid models) and 123 distribution lines (commonly referred to as "branch" in power grid models) [9]. While [9] only describes the physical grid infrastructure, Fig. 2 complements this reference system with a description of a digital infrastructure.

As illustrated in Fig. 2, the target of analysis consists of elements such as sensors that collect data for detecting and locating faults, and remotely controlled breakers (or disconnectors, or switches). The sensors are physically located in the distribution substations or on the power lines. The sensors send the collected data via Remote Terminal Units (RTU) and Intelligent Electronic Devices (IED). The RTUs and IEDs are field control devices with a communication interface used to send the sensor data to the Supervisory Control and Data Acquisition (SCADA) system over a Wide Area Network (WAN). The sensor data is then processed and sent further to the Distribution Management Systems (DMS) where the self-healing application is hosted.

Based on data received from the sensors, the self-healing application is used to locate and isolate faulty lines and restore power for disconnected customers. The self-healing application achieves this in three main steps: 1) determine the exact location of the faulty line/section, 2) send a signal to open the remotely controlled breakers on the faulty line/section

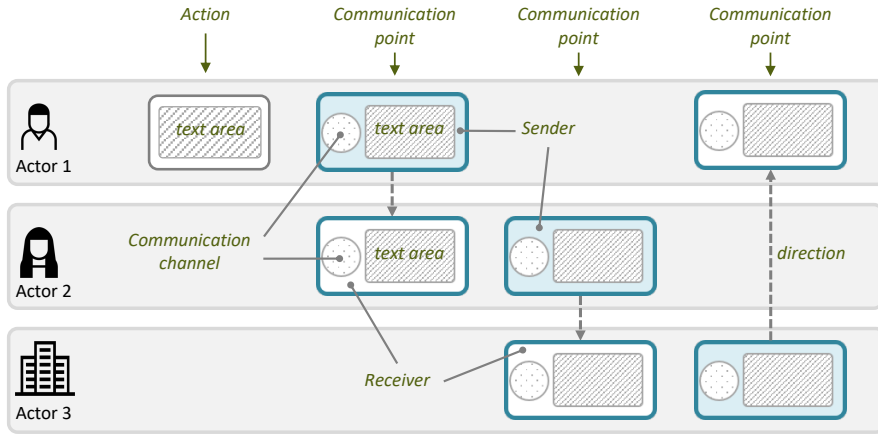


Fig. 1. The basic graphical constructs of a CJML diagram. Adopted from [5].

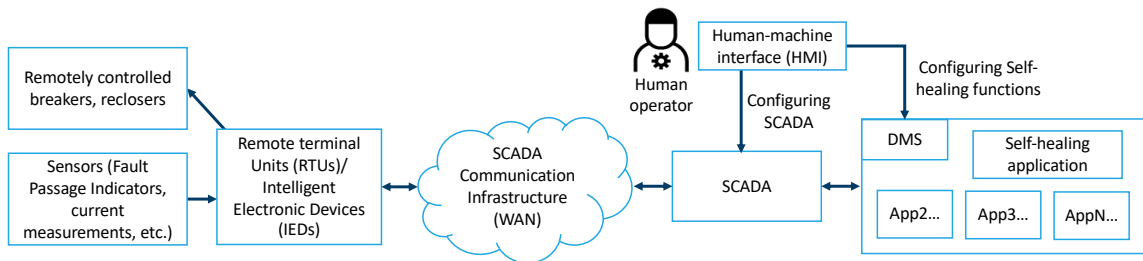


Fig. 2. Target description of self-healing application and grid reinforcement for the CINELDI reference system.

to isolate the fault, and 3) reconfigure the network to restore power to as many disconnected customers as possible. That is, the self healing application determines which of the remotely controlled breakers should be operated (closed or opened) to supply power to the disconnected customers via redundant lines (or reserve connections, labelled "backup feeders" in [9]). A user interface enables an operator to configure the self-healing application and the SCADA system.

B. Step 2: Identify Assets to Protect

In Step 2, we use the high-level target description to identify the assets that we want to protect. As the level of detail of asset identification influences the overall amount of information that needs to be collected for the risk assessment, the assets should be described at a suitable level of detail [6]. Considering the light-weight approach of our method, we recommend grid planners to concentrate on a single asset for each iteration of the method. This will frame the scope of the assessment to a suitable level given the high-level nature of the planning phase.

In the self-healing case described above, our primary concern is the cyber risks that may compromise the reliability of electricity supply in the grid with the planned solution. Thus, we want to protect the smart grid from cyber risks such that electricity supply is not disrupted or harmed. This means that our asset is *reliability of electricity supply* for which we require protection, and we want to identify cyber risks that

may impact this asset. Section III-D describes four potential cyber risks that may harm the reliability of electricity supply.

C. Step 3: Describe Likelihood and Consequence Scales

In step 3, we describe likelihood and consequence scales that are used later in the assessment (Step 5) to estimate and evaluate the identified cyber risks. Please see Section II for the definitions of likelihood and consequence.

Table I shows the likelihood scale and Table II shows the consequence scale we have identified for the running example. The likelihood scale provides likelihood values, a description for each likelihood value, and a precise definition of the likelihood value. For example, the likelihood value *Possible* means *less than twice per year*, and is expressed by the exact value five to twenty times per ten years [5,20>:10y]. Daily power grid operational risks are typically calculated using precise algorithms and probabilistic approaches [10]. However, in the grid planning phase, necessary data to calculate the probability of cybersecurity risks is not available. We therefore recommend that grid planners use a more comprehensible and practical approach by constructing frequency intervals (e.g. Table I), which are more intuitive and effective [11]. The frequency intervals can be chosen to match the relevant range of historical fault frequencies of components or they can be obtained from historical data of analogous components in similar digital systems/infrastructures. This will give the grid planners a more familiar frame of reference to use in the assessments of likelihood.

TABLE I
LIKELIHOOD SCALE

Likelihood	Description	Definition
Likely	Two to five times per year	$[20, 50 > : 10y = [2, 5 > : 1y$
Possible	Less than twice per year	$[5, 20 > : 10y = [0.5, 2 > : 1y$
Unlikely	Less than once per two years	$[0, 5 > : 10y = [0, 0.5 > : 1y$

TABLE II
CONSEQUENCE SCALE FOR RELIABILITY OF ELECTRICITY SUPPLY

Consequence	Description
Major	Severe disruption with long-term consequences.
Moderate	Significant but manageable disruption.
Minor	Minimal disruption to grid operations.

From a practical point of view, it is sufficient to define one likelihood scale that can be used in an assessment, while consequence scales should be defined for each asset that needs to be protected. This is because in practice it may be difficult to describe the damage inflicted on all assets using the same consequence scale [8]. The consequence scale in Table II is defined for the asset *reliability of electricity supply*. We see from the scale that a risk with, e.g., *Major* consequence on the asset has an impact of *severe disruption with long-term consequences*.

D. Step 4: Identify Cyber Risks

In Step 4, we identify cyber risks that the target of analysis may potentially be exposed to. This is done by first creating a high-level risk table to describe potential threat scenarios. These descriptions are then used as a basis to create graphical threat models using our web-based modelling tool [4]. The risk identification is carried out as a brainstorming session where the participants of the smart grid planning goes through the target of analysis (see Fig. 2) in a structured manner and answer the questions in the high-level risk table (see Table III). The high-level risk table shown in Table III lists four cyber risks we have identified for the self-healing application case.

Fig. 3 illustrates the threat model created for the first scenario described in the high-level risk table (first row). For each component involved in the threat scenario, we create a horizontal swimlane, i.e., one swimlane for each of the following: Sensors, SCADA Communication Infrastructure (CI), DMS, and Breakers. The threat actor, Hacker, is assumed to use a network sniffing software to monitor and capture the data sent by the sensors. Then, the hacker manipulates the sensor data and sends it to the DMS via the SCADA communication infrastructure. We assume that the DMS is not able to detect that incoming data has been manipulated and forwards it to the self-healing application. These events are labelled with

a red warning-triangle, highlighting the threat scenario. The self-healing application processes the manipulated data and provides a decision to either open or close the breakers, thus causing the unwanted incident that may directly harm the asset *reliability of electricity supply*. The unwanted incident is labelled with a yellow explosion sign. The reader is referred to the tool web page for a detailed explanation of the tool, the modelling language used (Customer Journey Modelling Language), as well as supporting training material [4].

E. Step 5: Estimate Cyber Risks

Cyber risk estimation is carried out using the the likelihood and consequence scales defined in Step 3, based on expert judgement, as well as information gathered from available resources such as annual threat reports, threat catalogues and communities, e.g., Open Worldwide Application Security Project (OWASP) [12]. The likelihood that a hacker will attempt to capture and manipulate data sent by the sensors is *Likely* because such data is typically sent to SCADA without encryption and can be susceptible to man in the middle attacks [13]. In the event that the attack is successful, then some breakers in the electricity grid will be closed or opened based on corrupted data, which in turn means that the electricity supply will be disrupted. However, the threat is still manageable in the sense that a human operator is able to locate and fix the problem via the SCADA system. We therefore assign the consequence value *Moderate* (see Fig. 3).

F. Step 6: Evaluate Cyber Risks

In Step 6, we create a risk matrix based on the likelihood and consequence scales (see Fig. 4). Each cell in the risk matrix represents a risk acceptance criteria. In our case, *Low* means that the risk is acceptable, while *Medium* and *High* means that the risk is not acceptable and should be further evaluated for possible treatment. Let us refer to the cyber risk in Fig. 3 (reliability of supply is harmed due to manipulated data) as R1. We map R1 to the risk matrix based on likelihood *Likely* and consequence *Moderate* and see that R1 has a *High* risk level and therefore not acceptable according to the risk acceptance criteria described above. This information is further used as input to the overall grid planning process [2] to provide decision support for investment in security controls as part of the grid planning.

IV. DISCUSSION

Based on the authors' own experience from the CINELDI project in which the reported method was developed [9], and according to [14], grid planners are already accustomed to conducting risk assessments in their daily work. Therefore, in terms of understanding our method for cyber risk assessment, it is reasonable to assert that grid planners are generally familiar with the steps involved, thanks to similar tasks they have undertaken. The challenge arises, however, when grid planners encounter a lack of concrete information about the planned solutions. This situation is common during grid planning, which is typically conducted at an early and

TABLE III
HIGH-LEVEL RISK TABLE DESCRIBING FOUR POTENTIAL CYBER RISKS THAT MAY HARM THE RELIABILITY OF ELECTRICITY SUPPLY

Who/what causes it?	How? What is the incident? What does it harm?	What makes it possible?	Which components are involved?
Hacker (human threat deliberate)	Hacker manages to read the sensor data and manipulate the data. This harms the integrity of sensor data, which in turn may cause a wrong decision on whether to open or close breakers.	Insufficient security on sensor or SCADA CI.	Sensors, DMS, remotely controlled breakers and reclosers, SCADA CI.
Hacker (human threat deliberate)	Hacker sends a phishing email to an operator and manages to steal the login credentials for the SCADA remote configuration capabilities. This harms the confidentiality of login credentials of the operator and gives the hacker access to SCADA.	Insufficient security filters in email server, and also insufficient security training.	Human operator, SCADA, remotely controlled breakers and reclosers.
Operator (human threat accidental)	The operator configures the SCADA or the DMS (self-healing functions) in a wrong manner which changes the value of the incoming sensor data or the outgoing data to the breakers and reclosers. This may in turn cause an open or close function by mistake.	Insufficient training for configuration.	Human operator, SCADA, DMS, remotely controlled breakers and reclosers.
SCADA (Non-human threat)	CI SCADA communication infrastructure is unavailable, which makes it impossible for the SCADA to communicate with sensors or breakers. Because of this unavailability, the self-healing functionality is not working as it should (important in critical situations).	Unstable connection, immature technology.	SCADA, SCADA CI, sensors, remotely controlled breakers and reclosers.

conceptual stage. We address this challenge both conceptually and methodologically.

From a conceptual perspective, we are using a minimum set of cybersecurity concepts generally needed to assess cyber risks, including asset, threat actor, threat scenario, unwanted incident, likelihood, and consequence (all of which are reflected in Fig. 3). These concepts are necessary to identify, estimate, and evaluate potential cyber risks, and are concepts familiar to grid planners who are not necessarily experts in cybersecurity [15].

From a methodological perspective, the steps of our method align with standard risk assessment processes, such as those outlined in ISO 27005 [6]. The first three steps of our method constitute context establishment, while steps 4 to 6 adhere to standard risk assessment practices [6]. We have deliberately omitted steps related to vulnerability identification and risk treatment. Typically, vulnerability identification is integrated into risk identification [6], and risk treatment often constitutes the final phase of any risk assessment [6]. Beyond the explanations provided in Section II for excluding these steps, our method’s outcomes are intended to feed into subsequent stages of the grid planning process [2], which involves evaluating cyber risks alongside other risk types and identifying potential mitigations for those cyber risks. Moreover, our method is designed for implementation with a minimal set of conceptual information. As demonstrated on the real-life reference system (see Section III), we utilized only high-level details about the planned solution to support the self-healing functionality in future smart grids. We recommend focusing on a single asset in each method iteration to appropriately narrow the scope of assessment. We define likelihood and consequence scales with just three levels, as a detailed assessment is unnecessary during

the grid planning phase. Risks are identified using a high-level risk table template, and graphical risk models are generated from the basic data gathered. Risks are assessed through expert opinions and information from publicly available sources. Finally, we determine the risk level by positioning each risk within a 3x3 risk matrix. These steps are designed to accommodate the challenge of limited concrete information about planned solutions.

Moreover, to ensure our method is user-friendly, we have intentionally adopted the Customer Journey Modelling Language (CJML) approach, which we expanded to include the basic set of security concepts previously mentioned. We chose CJML because it has been empirically demonstrated to be easy to understand and use by a diverse range of users, including grid planners [5], [15]. Furthermore, the symbols of a triangle with an exclamation mark and an explosion used in our threat models, as depicted in Fig. 3, draw inspiration from the CORAS risk assessment approach [8]. These symbols have also been empirically shown to be easily understandable by individuals from various professional backgrounds [16].

V. RELATED WORK

Cyber risk assessment is the industry de facto standard process to assess and mitigate potential cybersecurity risks. The most widely used standards are developed by ISO [6], [7] and NIST [17], and there exists a plethora of security risk assessment methods and approaches that are in line with existing standards. Systematic literature reviews report on, for example, general security risk assessment approaches [18], security risk assessment approaches based on specific techniques such as multi criteria decision making [19] and AI techniques [20],

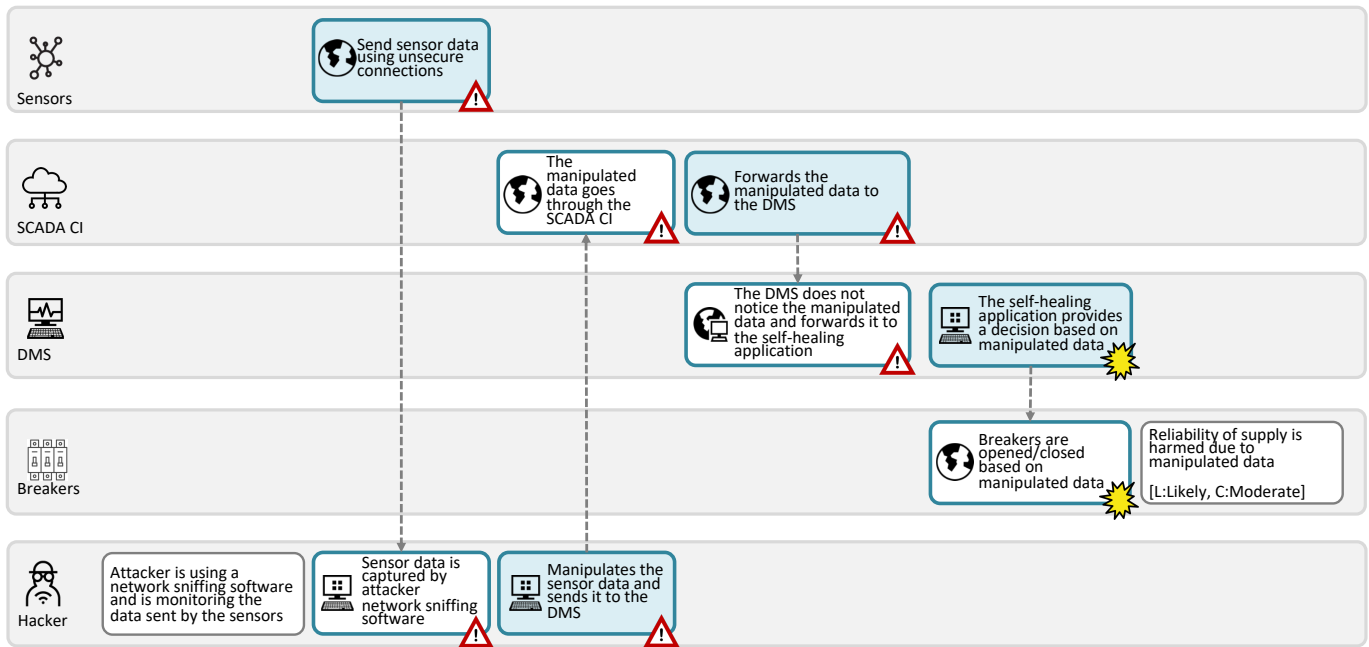


Fig. 3. Threat model for scenario where hacker manipulates sensor data and thereby harms reliability of electricity supply.

		Consequence		
		Minor	Moderate	Major
Likelihood	Unlikely	Low	Low	Medium
	Possible	Low	Medium	High
	Likely	Medium	High: R1	High

Fig. 4. Risk matrix for reliability of electricity supply.

and security risk assessment approaches for specific domains such as SCADA systems [21] and smart cities [22].

In terms of cyber risk assessment specifically for smart grids, there exists a variety of approaches, which can be roughly grouped into three categories: rigorous quantitative and probabilistic approaches, approaches based on simulation or virtualization, and high-level approaches. Most of the approaches fall in the category of rigorous quantitative and probabilistic approaches. [23] uses Fuzzy logic to calculate risk score/level. [24] and [25] applies a Markov decision process to capture the attack process in a smart grid system and calculate the probabilities of the attacks, while [26] provides a risk index calculation method based on Markov chains. [27] uses attack-defence trees to calculate quantitative risk severity levels. [28] uses Bayesian networks to calculate cyber-physical risks for circuit breakers that connect power generators to the smart grid. In contrast to our method, these approaches rely on rigorous quantitative and probabilistic assessments, which are typically not available during the smart grid planning phase.

With respect to simulation or virtualization approaches, [29] and [30] provide simulation assisted methods for performing security risk assessments based on simulated attacks on smart grid systems, [31] provides an approach to simulate attacks

based on game theory in order to identify optimal defense strategies, and [32] presents a framework to assess security risks within virtual smart grid communication networks with a specific focus on Denial of Service (DoS) attacks. We regard these approaches complementary to our approach in the sense that the simulation results produced by these approaches can be used as input to our approach during the planning phase as an additional source of information.

There are two high-level approaches that are closely related to our approach. [33] proposes an approach specifically to migrate smart grid OT services to cloud computing architectures based on security risk assessment, and [34] proposes an approach specifically to assess cybersecurity risks and vulnerabilities in smart grids with integrated solar photovoltaic. Like in our approach, [33] and [34] describe the target of analysis using high-level topology diagrams. Based on the topology diagrams, [33] identifies and assesses risks using tables only, while [34] creates data flow diagrams based on the Microsoft STRIDE approach to identify potential cyber risks. The risk models in our approach are based on CJML models and captures also the chain of events (over time) in a threat scenario in addition to data flow. Moreover, while [33] and [34] assess likelihoods qualitatively only, we make use of frequency intervals in addition to qualitative descriptions of likelihood values. In summary, the approaches provided by [33] and [34] are similar to our approach to some extent, but they are fundamentally different in the sense that the approaches address different usage areas, as explained above.

Finally, none of the related approaches mentioned above address the grid planning phase. During the grid planning process, grid planners must typically carry out cyber risk assessment when information is scarce, uncertain, and primarily

conceptual. As demonstrated in Section III, our method is designed to specifically address this challenge.

VI. CONCLUSION

Cyber-risk assessment during smart grid planning is challenging due to the absence of detailed information on potential solutions, particularly those involving active digital measures. Recognizing this, there is a clear need for straightforward, user-friendly risk assessment methods that grid planners can apply in the planning process. To address this, we propose a lightweight, tool-supported method. Our preliminary results using CINELDI's real-world reference system look promising and we believe our method is useful for grid planners to assess potential cybersecurity risks during the grid planning phase. In future work, we plan to test the method in additional case studies with grid planners.

ACKNOWLEDGMENT

This work is supported by CINELDI, an 8-year FME Research Centre (257626/E20), with funding from the Research Council of Norway and CINELDI partners.

REFERENCES

- [1] S. G. Freeman, M. A. Kress-Weitenhagen, J. P. Gentle, M. J. Culler, M. M. Egan, and R. V. Stolworthy, "Attack surface of wind energy technologies in the united states," 1 2024. [Online]. Available: <https://www.osti.gov/biblio/2297403>
- [2] I. B. Sperstad, E. Solvang, and O. Gjerde, "Framework and Methodology for Active Distribution Grid Planning in Norway," in *2020 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*. IEEE, 2020, pp. 1–6.
- [3] G. Erdogan, I. B. Sperstad, M. Garau, O. Gjerde, I. A. Tøndel, S. Tokas, and M. G. Jaatun, "Adapting Cyber-Risk Assessment for the Planning of Cyber-Physical Smart Grids Based on Industrial Needs," in *Software Technologies*. Cham: Springer Nature Switzerland, 2023, pp. 98–121.
- [4] "Human and Organisational Risk Modelling (HORM)," <https://cjml.no/horm/>, 2024, accessed April 19, 2024.
- [5] R. Halvorsrud, O. R. Sanchez, C. Boletsis, and M. Skjuve, "Involving Users in the Development of a Modeling Language for Customer Journeys," *Software and Systems Modeling*, vol. 22, no. 5, pp. 1589–1618, 2023.
- [6] "ISO/IEC 27005:2018 - Information technology - Security techniques - Information security risk management," ISO, Standard, Jul. 2018.
- [7] "ISO/IEC 27000:2018 - Information technology - Security techniques - Information security management systems - Overview and vocabulary," ISO, Standard, Jul. 2018.
- [8] M. Lund, B. Solhaug, and K. Stølen, *Model-Driven Risk Analysis: The CORAS Approach*. Springer, 2011.
- [9] I. B. Sperstad, O. B. Fosso, S. H. Jakobsen, A. O. Eggen, J. H. Evenstuen, and G. Kjølle, "Reference data set for a Norwegian medium-voltage power distribution system," *Data in Brief*, p. 109025, 2023.
- [10] O. Stover, P. Karve, and S. Mahadevan, "Reliability and risk metrics to assess operational adequacy and flexibility of power grids," *Reliability Engineering & System Safety*, vol. 231, p. 109018, 2023.
- [11] V. Giroto and M. Gonzalez, "Solving probabilistic and statistical problems: a matter of information structure and question form," *Cognition*, vol. 78, no. 3, pp. 247–276, 2001.
- [12] "Open Worldwide Application Security Project (OWASP)," <https://owasp.org/>, 2024, accessed April 7, 2024.
- [13] Ö. Sen, D. van der Velde, P. Linnartz, I. Hacker, M. Henze, M. Andres, and A. Ulbig, "Investigating man-in-the-middle-based false data injection in a smart grid laboratory environment," in *2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*. IEEE, 2021, pp. 1–6.
- [14] O. Lyulyov, I. Vakulenko, T. Pimonenko, A. Kwilinski, H. Dzwigol, and M. Dzwigol-Barosz, "Comprehensive assessment of smart grids: Is there a universal approach?" *Energies*, vol. 14, no. 12, 2021.
- [15] G. Erdogan, R. Halvorsrud, C. Boletsis, S. Tverdal, and J. B. Pickering, "Cybersecurity Awareness and Capacities of SMEs," in *Proc. 9th International Conference on Information Systems Security and Privacy (ICISSP)*. SciTePress, 2023, pp. 296–304.
- [16] B. Solhaug and K. Stølen, "The coras language-why it is designed the way it is," in *Proc. 11th International Conference on Structural Safety and Reliability (ICOSSAR'13)*. Citeseer, 2013, pp. 3155–3162.
- [17] "Special Publication 800-30 Guide for Conducting Risk Assessments," National Institute of Standards and Technology, Standard, Sep. 2012.
- [18] L. Pan and A. Tomlinson, "A systematic review of information security risk assessment," *International Journal of Safety and Security Engineering*, vol. 6, no. 2, pp. 270–281, 2016.
- [19] D. Maček, I. Magdalenić, and N. B. Redep, "A systematic literature review on the application of multicriteria decision making methods for information security risk assessment," *International Journal of Safety and Security Engineering*, vol. 10, no. 2, pp. 161–174, 2020.
- [20] G. Erdogan, E. Garcia-Ceja, Å. Hugo, P. H. Nguyen, and S. Sen, "A Systematic Mapping Study on Approaches for AI-Supported Security Risk Assessment," in *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2021, pp. 755–760.
- [21] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for scada systems," *Computers & security*, vol. 56, pp. 1–27, 2016.
- [22] J. Alshehri, A. Alhamed, and M. M. H. Rahman, "A systematic literature review on cybersecurity risk management in smart cities," in *2024 International Conference on Artificial Intelligence in Information and Communication (ICAIC)*, 2024, pp. 407–412.
- [23] S. Canbolat, G. Elbez, and V. Hagenmeyer, "A new hybrid risk assessment process for cyber security design of smart grids using fuzzy analytic hierarchy processes," *at - Automatisierungstechnik*, vol. 71, no. 9, pp. 779–788, 2023.
- [24] H. Vallant, B. Stojanović, J. Božić, and K. Hofer-Schmitz, "Threat Modelling and Beyond-Novel Approaches to Cyber Secure the Smart Energy System," *Applied Sciences*, vol. 11, no. 11, 2021.
- [25] A. Bashar, S. Muhammad, N. Mohammad, and M. Khan, "Modeling and analysis of mdp-based security risk assessment system for smart grids," in *2020 Fourth International Conference on Inventive Systems and Control (ICISC)*, 2020, pp. 25–30.
- [26] Z. Jianye, Z. Qinshun, S. Yiyang, and L. Cunbin, "Information Security Risk Assessment of Smart Grid Based on Absorbing Markov Chain and SPA," *International Journal of Emerging Electric Power Systems*, vol. 15, no. 6, pp. 527–532, 2014.
- [27] E. Rios, A. Rego, E. Iturbe, M. Higuero, and X. Larrucea, "Continuous Quantitative Risk Management in Smart Grids Using Attack Defense Trees," *Sensors*, vol. 20, no. 16, 2020.
- [28] A. AlMajali, Y. Wadhawan, M. S. Saadeh, L. Shalalfeh, and C. Neuman, "Risk assessment of smart grids under cyber-physical attacks using bayesian networks," *International Journal of Electronic Security and Digital Forensics*, vol. 12, no. 4, pp. 357–385, 2020.
- [29] S. Sierla, M. Hurkala, K. Charitoudi, C.-W. Yang, and V. Vyatkin, "Security risk analysis for smart grid automation," in *2014 IEEE 23rd International Symposium on Industrial Electronics (ISIE)*, 2014, pp. 1737–1744.
- [30] Y. Wadhawan and C. Neuman, "RI-bags: A tool for smart grid risk assessment," in *2018 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, 2018, pp. 7–14.
- [31] Q. Li, P. Lv, M. Wang, Z. Zhang, S. Wang, P. Fang, and L. Gao, "A risk assessment method of smart grid in cloud computing environment based on game theory," in *2020 IEEE 5th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA)*, 2020, pp. 67–72.
- [32] H. Maziku, S. Shetty, and D. M. Nicol, "Security risk assessment for sdn-enabled smart grids," *Computer Communications*, vol. 133, pp. 1–11, 2019.
- [33] B. Jelacic, I. Lendak, S. Stoja, M. Stanojevic, and D. Rosic, "Security risk assessment-based cloud migration methodology for smart grid ot services," *Acta Polytechnica Hungarica*, vol. 17, no. 5, pp. 113–134, 2020.
- [34] F. A. Rahim, N. A. Ahmad, P. Magalingam, N. Jamil, Z. C. Cob, and L. Salahudin, "Cybersecurity vulnerabilities in smart grids with solar photovoltaic: A threat modelling and risk assessment approach," *International Journal of Sustainable Construction Engineering and Technology*, vol. 14, no. 3, pp. 210–220, 2023.