An Industrial Trial of an Approach to Identification and Modelling of Cybersecurity Risks in the Context of Digital Secondary Substations

Aida Omerovic[1], Hanne Vefsnmo[2], Oddbjørn Gjerde[2], Siri T. Ravndal[3], Are Kvinnesland[3]

[1] SINTEF Digital, Norway; [2] SINTEF Energy, Norway; [3] Lyse Elnett, Norway
{firstname.lastname}@sintef.no, {firstname.lastname}@lyse.no

Abstract. We have in an earlier study proposed a set of requirements and an approach to identification and modelling of cybersecurity risks and their impacts on safety, within the context of smart power grids. The approach, which consisted of a process and a modelling language, was a partially customized version of the existing "CORAS" risk-analysis approach. As a part of the study, feasibility of the approach was evaluated by applying it on an industrial pilot for so-called self-healing functionality of a smart power grid. The results obtained were promising, but further empirical evaluation was strongly needed in order to further assess usefulness and applicability of the approach in the context of smart power grids. This paper provides a detailed account of results of applying the same approach to cybersecurity risk identification and modelling in the context of another smart grid pilot, namely digital secondary substations. The trial was conducted in a real setting, in the form of an industrial case study, in close collaboration with the major Norwegian distribution system operator that has been running the pilot for about two years. The evaluation indicates that the approach can be applied in a re-al setting to identify and model cybersecurity risks. The experiences from the case study moreover show that the presented approach is, to a large degree, well suited for its intended purpose, but it also points to areas in need for improvement and further evaluation.

Keywords: Cybersecurity, Digital Substations, Cyber Risk, Smart Power Grids, Risk Identification, Risk Analysis, Risk modelling.

1 Introduction

Power grids are being increasingly digitalized, thanks to the evolving maturity and availability of the information and communication technologies (ICT). The digitalization of the electric power grids will include new concepts based on intelligent sensors in the grid and efficient communication between these sensors and the Supervisory Control and Data Acquisition (SCADA) system or distribution management system (DMS) [3]. The modern electric power grids adopting the technologies such as new communication networks, software, hardware, and control systems, are denoted as "Smart Grids". The goal of the energy providers and distributors is to utilize the digitalization in order to meet the needs for flexibility and efficiency of the power grid. Those needs are primarily driven by new power intensive loads due to, for example,

This is the accepted version of an article published in Lecture Notes in Computer Science, vol. 12026
http://dx.doi.org/https://doi.org/10.1007/978-3-030-41568-6_2

electric vehicle charging, thus increasing the peak power demand along with the simultaneous penetration of stochastic renewable energy sources. In this setting, it is crucial to preserve the resilience of such a critical infrastructure that the power grid represents. However, the smart grids are not only enabling better utilization of the power grids, but also increasing complexity of the systems, thus introducing new kinds of risks, including the so-called cybersecurity risks (also known as digital risks). The cybersecurity risks may also lead to risks impacting security of power supply. One example of how adversaries can exploit the new components and technologies, is the cyberattack against the Ukrainian Power Grid in December 2015, where the outages affected approximately 225 000 customers that lost power across various areas [16].

By adding functionality to the power grids, ICT systems also contribute to unwanted incidents. Tøndel et Al. [22] argue that power grid reliability will increasingly depend on ICT components and systems. They also claim that the current methods for risk analysis of power systems seem unable to take into account the full array of intentional and accidental threats. In addition, they found few methods and publications on identification of interdependencies between the ICT and power system. The objective of this research has been to provide support for cybersecurity risk analysis that takes into account the specific characteristics of smart power grids and meets the distinct needs within this domain.

A major challenge of the power domain is that the smart grid solutions have been in operation for a very limited period of time. Since the emerging solutions are at their early stages, there is a lack of historical data and operational experiences that could constitute relevant input to the risk models. This uncertainty due to lack of knowledge makes it extremely difficult to identify or predict the unwanted incidents that may occur in the future. Instead, one must focus on identification of the known vulnerabilities that are introduced due to the increasing usage of ICT technologies and their interdependencies with the physical power grid. However, the traditional risk analysis approaches often pre-assume that the nature and impact of the unwanted incidents are known, by demanding specific information on event description and risk quantification. Risk modelling, that is, the modelling of what can go wrong [17], is a technique for risk identification and assessment.

With respect to the state-of-the-art, several tree-based and graph-based notations within risk modelling exist. Fault Tree Analysis [9], Event Tree Analysis [10] and Attack Trees [21] are examples of the former and provide support for reasoning about the sources and consequences of unwanted incidents, as well as their likelihoods. Cause-Consequence Analysis [19], CORAS [17], and Bayesian networks [4] are examples of graph-based notations. CORAS is a tool-supported and model-driven approach to risk analysis that is based on the ISO 31000 risk management standard [13]. It uses diagrams as a means for communication, evaluation and assessment. Markov models [11], CRAMM [2], OCTAVE [1], Threat Modelling [18] and a number of others, have also been applied to support risk analysis. A framework for studying vulnerabilities and risk in the electricity supply, based on the bow-tie model, has been developed and is published for instance in [14, 15, 8].

From a risk analysis perspective smart power grids are characterized by their inherent uncertainties due to both the stochastic nature of generation and load as well as an increased complexity giving rise to new risks which are introduced through the ICT part of the system. Moreover, the interdisciplinary nature of such systems poses requirements on comprehensibility of the design of smart power grids and the corresponding risk models. Hence, a smart grid setting which includes a complex and critical cyber physical system, human in the loop, uncertainty due to lack of knowledge, many dependencies and interdisciplinary aspects, challenges the state-of-the-art on cybersecurity management. In an ideal setting, the risk model can be presented to human in a suitable interface, thereby serving as a useful support for decision making during design and operation. However, as they stand, none of the existing approaches provides the support that takes into account the specific characteristics of smart power grids and meets the distinct needs for cybersecurity risk analysis within this domain. This indicates a need for an approach to cybersecurity risk identification which is customized to address the following **requirements** (the ordering is arbitrary and does not express the relative importance of the requirements):

1. The approach is cost-effective and light-weight, i.e. the benefits of using it are well worth the effort. In particular, the value of gaining the decision support through applying the approach, should significantly outweigh the effort needed.
2. The cyber risk model can be developed and easily understood by the involved actors who represent varying roles and background.
3. The risk model has sufficient expressive power to capture relevant aspects of the cybersecurity risk picture in the context of smart power grids.
4. The risk model facilitates inclusion of the information that is available, while not requesting unrealistic degree of precision.
5. The risk model can visualize the cybersecurity relevant dependencies and sequence of states/events both for the whole context and for the detailed parts of the scope of analysis. This implies the ability of the modelling approach to both address a sufficiently broad scope, as well as to express the necessary details.

We have in an earlier study [20] introduced the above listed requirements to a risk analysis and modelling approach in the context of smart electric power distribution grids. Based on these requirements, this earlier study proposed a customized four-step approach to cybersecurity risk identification and modelling. The feasibility of the approach was evaluated on an industrial pilot for so-called self-healing functionality of a smart grid. The approach, which consisted of a process and a modelling language, was, to a high degree, based on parts of the previously mentioned CORAS method for model-based risk analysis. Compared to CORAS, the process and the modelling approach we have applied are simplified and partially adapted. The results obtained were promising. However, the need for more empirical evaluation in order to further assess usefulness of the approach, was evident. The original requirements to the approach and the approach itself, were therefore suggested to still be relevant and applicable for the next trial, i.e. the study reported in this paper.

This paper provides a detailed account of results of applying the abovementioned previously proposed approach to cybersecurity risk identification and modelling in the context of another smart distribution grid pilot, namely an operational pilot on digital secondary substations. The trial was conducted in a fully realistic setting, in the form of an industrial case study, in close collaboration with a major Norwegian power distribution system operator (DSO) owning the digital secondary substations, which were commissioned in the period 2016 - 2019. The evaluation indicates that the approach can be usefully applied in a realistic setting to identify and model cybersecurity risks. The experiences from the case study moreover show that the presented approach is, to a large degree, well suited for its intended purpose, but it also points to areas in need for improvement and further evaluation.

The rest of this paper is organized as follows: In Section 2 we briefly present the research strategy applied. Our approach for cybersecurity risk identification and modelling is presented in Section 3. The setup and the results from the trial of the approach are outlined in Section 4. In Section 5 we discuss the results, before concluding in Section 6.

2 Research Strategy

The research strategy applied is in line with the design science approach [23], and follows the three steps illustrated in Figure 1. Although Figure 1 illustrates sequential steps, the research strategy was followed iteratively where some of the steps were revisited during the process. In Step 1, the goal was to identify the requirements for a risk identification and modelling approach that addresses the specific characteristics of the smart grid domain. In Step 2, the goal was to develop a customized approach with respect to the requirements identified in Step 1. Based on the state-of-the-art overview and the lessons learned from the above-mentioned previous trial of the approach, the original five requirements and the approach that were identified and proposed in the previous study, were deemed to still be relevant and applicable. The requirements are listed in Section 1, while the approach containing four phases is presented in Section 3.

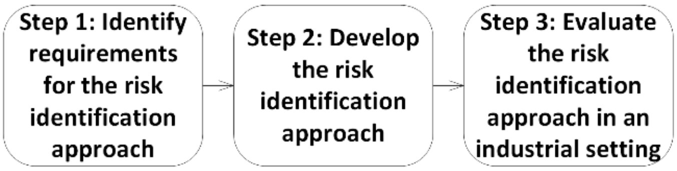

Step 1: Identify requirements for the risk identification approach
Step 2: Develop the risk identification approach
Step 3: Evaluate the risk identification approach in an industrial setting

Figure 1. Research strategy.

Finally, in Step 3 of the research strategy, we evaluated the approach in an industrial setting together with a DSO (i.e. the power distribution system operator that was the use case provider) that is currently operating a pilot on digital secondary substations in their power grid. The evaluation was carried out as follows: First, we established the context and gained a deep understanding of the digital secondary substations, based on reports on state of the practice, dialogue with domain experts who participated in the analysis group, as well as the documentation provided by the DSO. Then, the modelling approach was introduced by the analyst to the domain experts from the DSO. Thereafter, the analyst proposed a preliminary version of the risk model which focused on cybersecurity aspects of reliable energy supply. The preliminary version of the risk model was thereafter revised through several iterations, in close collaboration between the analyst and the domain experts. Once no more of the context documentation or brainstorming in the analysis group was needed for further modelling, a tool (checklist) for IoT security from ENISA [6] was proposed by the analyst and reviewed by the DSO, resulting in a new and complete version of the risk model. Lastly, a verification of the risk model was performed by the DSO putting forward a set of independently developed risk scenarios (originating from a former risk analysis of a similar context, which had been performed independently from ours). The scenarios were then exposed to the risk model in order to seek needs for updates. The model was reviewed against the scenarios during a workshop with the analysis group and two additional domain experts from the DSO who had not been involved in the previous steps of the analysis. The independence of the brought risk scenarios and the two new domain experts, were a means of strengthening the reliability of the validation step. The complete evaluation process, as well as the outcomes of it, are presented in Section 4.

3 Approach to Cybersecurity Identification and Modelling

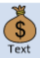
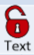
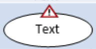
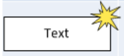
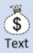
Our approach to cybersecurity risk identification and modelling has been previously proposed and presented in Omerovic et Al. [20]. The description of the approach is a core baseline for understanding contents of the trial. Hence, this section contains nearly the same generic description of the approach as the one given in the original source (i.e. the paper reporting on the aforementioned previous study), in order to enable the audience to read this paper independently from the former one. The approach consists of four main phases, inspired by the CORAS method and modelling language, but simplified and customized in order to address our specific requirements listed in Section 1. Our approach is assumed to be carried out by an analysis group, consisting of analysts and domain experts, representing competence in risk analysis, cybersecurity, and smart power grids. One individual may cover one or more roles, and several individuals may represent a similar role. Most importantly, the composition of the analysis group needs to include the relevant competence and ensure a sufficient degree of continuity (with respect to attendance of some of the participants) within the group. The four phases of the process include: 1: Context establishment; 2: Risk identification and modelling; 3: Risk model validation; and 4: Follow-up.

The objective of Phase 1 is to characterize the scope and the target of the analysis. Stakeholders that the analysis is being performed on behalf of, time perspective, relevant terminology, assumptions, roles and participants of the analysis group, as well as the information sources, are specified. Assets, that is the values that will drive the focus of the analysis, are also defined. This phase produces descriptions, insights and a common understanding of the target of analysis. The target of the analysis is, moreover, specified and modelled with respect to capabilities, structure, dataflow, workflow, etc. The existing target specifications (i.e. those which are available prior to the analysis) may be reused or referred to.

The objective of Phase 2 is to identify the relevant risk model elements and develop a risk model. The risk model elements may be of the following types: assets, vulnerabilities, threat scenarios and unwanted incidents. The unwanted incidents are the elements that may harm the assets (which are assumed to be specified during Phase 1). The very first step of this phase is to introduce the types of the model elements to the analysis group. A brief introduction to the modelling constructs and their simple explanations is illustrated in Table 1. The explanations in the last column are simplified

This is the accepted version of an article published in Lecture Notes in Computer Science, vol. 12026
http://dx.doi.org/https://doi.org/10.1007/978-3-030-41568-6_2

Table 1. Constructs of the cybersecurity risk modelling language.

Symbol	Name	Simple explaination
	Direct asset	Something of a value to the stakeholders and needs to be protected. The risks are to be identified with respect to the direct assets.
	Vulnerability	A state or a property that may be exploited.
	Threat scenario	A relevant event or a property that does not directly harm an asset.
	Unwanted incident	An event that directly harms an asset.
	Indirect asset	Something of a value to the stakeholders and can be affected by a direct asset.

wordings inspired by corresponding definitions from CORAS[1]. Thereafter, the identification of risks through a risk modelling activity using the constructs in Table 1, is initiated. The instantiated constructs are, as a part of this process, annotated with descriptive text. The relationships between the instantiated model constructs are expressed with arcs connecting the relevant elements, thus resulting in a risk model shaped as an acyclic directed graph. The analyst shall facilitate the model development by iteratively posing questions on risks that may harm the assets and the possible vulnerabilities and threat scenarios that cause those risks. The analyst shall also contribute with cybersecurity domain knowledge during the risk modelling. The analyst shall, moreover, ensure that the syntax of the risk model is consistent. The domain experts shall, during the risk modelling, contribute with the domain knowledge on power grids. Discussion is facilitated in order to align the different domains and reveal the relevant risks. At the same time, the context description from Phase 1 is actively used. Moreover, if needed, refined descriptions of selected model elements are provided. For some parts of the risk model, it may be appropriate to express uncertainties and assumptions, in form of supplementary information or within the model.

Phase 3 aims at validating the risk model developed in the preceding phase. That is, the model should be exposed to quality assurance based on various and complementing kinds of empirical input, in order to ensure an acceptable level of uncertainty. The uncertainty may origin from insufficient information or knowledge, or from variability in context, usage, etc. This is followed by adjustments of the model with respect to the structure and the individual elements. Eventually, the model is approved if the evaluation shows that the revised version is sufficiently complete, correct and certain.

The objective of Phase 4 is two-fold, namely communication and maintenance of the results. The specific tasks of this phase include summary of most critical findings, evaluations of validity and reliability of the risk model, recommendations of risk treatments, summary of uncertainties in the findings, as well as communications of the results to the relevant stakeholders. Maintenance of the risk model involves monitoring of assumptions and the context changes that may require updates of the risk model.

[1] Note that the definition of vulnerability from the energy sector is slightly different, namely "Vulnerability is an expression for the problems a system faces to maintain its function if a threat leads to an unwanted event and the problems the system faces to resume its activities after the event occurred. Vulnerability is an internal characteristic of the system" [15].

4 Trial of the Approach on an Industry Pilot on Future Digital Substations

This section outlines the process undergone during the industrial case, as well as the main properties of the risk model produced. We also summarize the lessons learned.

4.1 Setting of the Case Study

By the introduction of digital secondary substations new sensors and communication technologies provide new measurements and remotely controlled disconnectors in the medium voltage (MV) (1-35 kV) distribution grid. As a result, the digitalization of the secondary substation gives new possibilities for smarter operation and fault- and interruption handling. At the same time these technologies introduce new vulnerabilities to the system. To study these vulnerabilities a case study has been performed together with a Norwegian grid company, in order to study 31 digital secondary substations they own in the south-western part of Norway.

Digital Secondary Substations. The electrical energy must be transported from the power generators to the consumers. On the way, electric power may flow through several substations being transformed between different voltage levels. The secondary substations are the interconnection between the MV and low voltage (LV) distribution grid levels. A digital secondary substation is typically described as an electrical substation where operation is managed between distributed intelligent electronic devices (IEDs) which are interconnected by the communication network. In this specific case study, the secondary substations (31 in total) are equipped slightly differently, but with a lot of common functionality. The first digital secondary substation was commissioned in 2016 and the last one within this pilot, was commissioned in 2019. All 31 secondary substations are equipped with remotely controlled disconnectors at all incoming and outgoing cables. Every cable has also a fault current indicator, annotated with green circles in Figure 2, that detects both short-circuit fault and earth-fault, and communicates directly to the SCADA-system via remote terminal unit (RTU). For the transformers in the secondary substation, sensors are installed to monitor the oil pressure, the oil level and the transformer temperature, as indicated within the blue box in Figure 2. On the LV side of the secondary substation, indicated with orange color in Figure 2, power analyzers are installed to measure current, voltage, active/reactive power and earth fault. In addition, sensors are installed on the doors to detect whether the door is closed or open, and temperature sensors are installed to measure the room temperature within the substation building. Monitoring of the arc arrester and detection of the SF-6 pressure is, moreover, installed.

The different sensors placed in the digital secondary substation transfer the following parameters to the SCADA system in real-time through secured and encrypted fiber network: temperature (room and transformer); frequency, line voltages; phase voltages, total harmonic distortion (THD) voltages; currents; THD currents; active power (P), reactive power (Q) and apparent power (S); power factor.

Scope of the analysis. The stakeholder of this risk analysis has been the DSO, owning the 31 digital secondary substations. Their concern is the company reputation, their

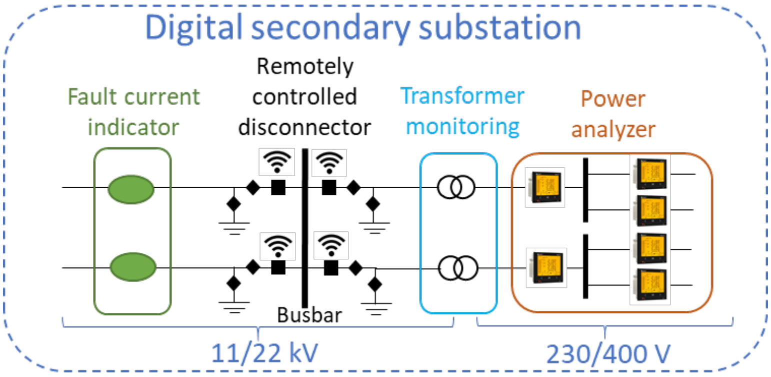


Figure 2. A sketch of the digital secondary substation indicating the different types of sensors and technologies installed.

income (economy), as well as Environment, Health and Safety (EHS). The scope of the analysis has been to protect the asset; the reliability of supply of the electric power system, defined as: "*probability that an electric power system can perform a required function under given conditions for a given time interval.*" (IEV 617-01-01) [12]. This asset may be affected (positively or negatively) by digitizing the secondary substation. On the positive side, the sensors will give warnings for instance of increasing transformer temperature, which may trigger desired maintenance and avoid transformer damage. For instance, a fault current indicator functioning correctly will contribute to localizing the fault faster which will reduce the fault localization time and by that the interruption time and cost. On the other hand, wrong signals from the sensors may lead to wrong decisions, and in worst case lead to longer interruption duration. In addition, remotely controlled disconnectors may potentially be opened by an attacker, and lead to interruption for all customers behind that substation. By adding all these sensors, the system becomes more complex and the consequences of the critical events may increase, while the introduction of the ICT-support decreases the consequences of the frequent events [7].

The scope of the analysis comprised all systems and subsystems starting from the front-end at the SCADA-systems and until the LV-side of the secondary substation. The infrastructure for the smart meters and the SCADA-system itself, are outside of the scope. The focus was on the parts within the yellow rectangle in Figure 3. The figure was developed during the context establishment and was later actively used during the analysis. The frontends are the parts of the SCADA-system which have two-ways communication with all digital secondary substation. The communication link (indicated with red lines) involves firewalls and routers. It uses encryption before sending the information over public fiber network. The routers and the firewalls are duplicated on the SCADA side of the communication link. At the secondary substation, the signals are received by a router which contains an access list. The RTU is the receiver of the information from the SCADA-system. In addition, the RTU is the unit collecting all data from the sensors within the substation. The secondary substations have battery back-up (24 V), which can, in case of interruptions, supply the required power to the RTU and the sensors.

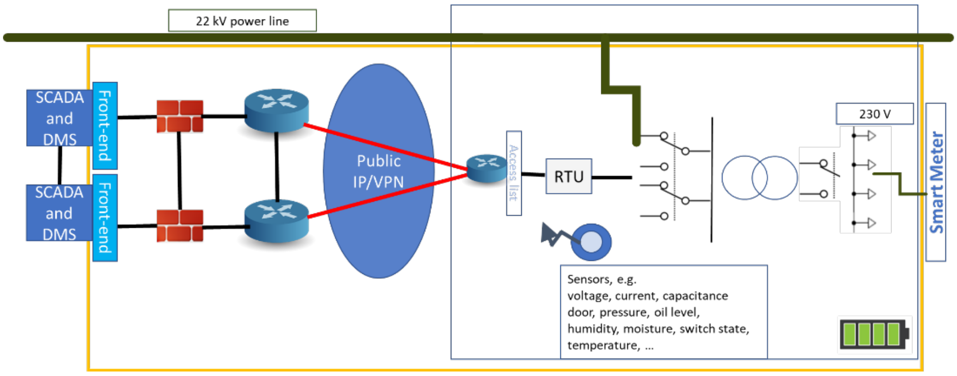


Figure 3. Sketch of what is within and outside of the analysis. The yellow rectangle shows the boundaries of what is inside the analysis.

Assumptions and delimitation of the industrial case. The following assumptions were made in the case study as part of context establishment:

- The SCADA system is outside of the scope of this analysis (as indicated in Figure 3).
- The smart meters (installed at all end-users in Norway from 1st of January 2019) and the belonging infrastructure are outside of the scope.
- Physical security of the secondary substation and human safety are outside of scope of this analysis.
- The purpose has been to carry out a qualitative risk assessment of the digital secondary substation, no quantification has been done.
- The focus is on the 31 secondary substations in south-eastern part of Norway. Any possible additional consequences resulting from an increased number of digitalized secondary substations, are not a part of the analysis.

The main focus has been on the new vulnerabilities and threats introduced by installing the new technology and sensors, especially with establishing the communication link between the SCADA-system and the disconnectors at all secondary substations. Cybersecurity, specifically related to the communication infrastructure, is of particular importance. The exclusion of the SCADA system and the smart meters from the scope was a deliberate choice, as primarily the risks introduced by the particularities and new aspects of this specific case study, were focused on.

Background of the participants involved in the analysis. The analysis was performed with a core team of seven people. The risk analysis was performed by one analyst, PhD, with about 16 years of experience in software engineering and cybersecurity risk management, and two domain experts with 6-18 years of relevant experience within power system reliability and security of electricity supply. These three participants are affiliated with the research institute. From the grid company a six people in total have been involved in this analysis. The main contributions have been given by a core group consisting of four people; one manager and three domain experts. The three domain experts have the following expertise area; one is a network communication expert; one is a SCADA system expert and one is an information security expert. They each have more than 20 years of experience in their fields. Two additional experts from the grid company participated only in the validation workshop; one expert in planning of the digital secondary substation and the other expert in risk analysis. These two had not been a part of this analysis before and gave useful input in the validation phase.

4.2 Process Outline

The case study was conducted between November 2018 and March 2019, in the form of eight videoconference meetings and one physical meeting. The setting was fully realistic in terms of the context specified, the process undergone, the risk model that was developed, and the participants that were involved. The cybersecurity risks of the secondary digital substations pilot were identified and modelled, with respect to the established context. The case study included trial of primarily the first three phases of the approach presented in Section 3.

Table 2 summarizes the process undergone. For each workshop, we list the meeting number, the date, the participants, the meeting type, the meeting length, and the activities which were conducted. Unless otherwise specified, the mentioned activities were conducted during the meeting.

Table 2. The process conducted during the case study.

Meeting number: 1**; Date:** 21.11.2018**; Participants:** analyst, 1 domain expert from the grid company, and one from the research institute, the manager from the grid company**; Meeting type:** video**; Duration:** 1,5h; **Activities:** Establishment of context, goals, scope and focus for the case study.
Meeting number: 2**; Date:** 22.11.2018**; Participants:** analyst, 2 domain experts from the research institute**; Meeting type:** video**; Duration:** 1h; **Activities:** An introduction to the digital secondary substations and their role in the power grid was given by the domain experts to the analyst.
Meeting number: 3**; Date:** 10.12.2018**; Participants:** analyst, one domain expert from the grid company and one from the research institute**; Meeting type:** video**; Duration:** 1.5h; **Activities:** Further clarifications of the context.
Meeting no. 4**; Date:** 12.12.2018**; Participants:** analyst, three domain experts from the grid company and one from the research institute, the manager from the grid company**; Meeting type:** video**; Duration:** 2 h; **Activities.** Further clarifications of the context. High level cybersecurity risk analysis.
Meeting number: 5**; Date:** 17.12.2018**; Participants:** analyst, three domain experts from the grid company and one from the research institute, the manager from the grid company**; Meeting type:** video**; Duration:** 2h; **Activities:** Terminology clarifications. Cybersecurity risk modelling, based on the context and the high level risk analysis.
Meeting number: 6**; Date:** 21.01.2019**; Participants:** analyst, three domain experts from the grid company and two from the research institute, the manager from the grid company**; Meeting type:** video**; Duration:** 3h; **Activities prior to the meeting:** the analyst updated the model remaining by covering the remaining aspects from the high-level analysis. **Activities during the meeting:** the analyst presented the new version of the model. Continued cybersecurity risk modelling.
Meeting number: 7**; Date:** 20.02.2019**; Participants:** analyst, three domain experts from the grid company and two from the research institute, the manager from the grid company**; Meeting type:** video**; Duration:** 2h; **Activities prior to the meeting:** the analyst updated the model with the relevant contents and the grid company had an internal walkthrough of the results. **Activities during the meeting:** the analyst presented the new version of the model. Continued cybersecurity risk modelling.

Meeting number: 8**; Date:** 06.03.2019**; Participants:** analyst, one domain expert from the grid company and two from the research institute, the manager from the grid company**; Meeting type:** video**; Duration:** 1.5h; **Activities prior to the meeting:** the analyst retrieved the ENISA IoT tool [6], processed the contents and annotated potentially relevant parts. The list was then processed by the domain experts from the grid company and the relevant parts were extracted. The risk model was then updated by the analyst and sent to the analysis team. The grid company prepared a set of scenarios (based on an independent earlier risk analysis) to be used for validation of the risk model. **Activities during the meeting:** the analyst presented the new version of the model. Continued cybersecurity risk modelling. A brief intro by the analyst to the ENISA IoT tool and a proposal to process it in order to complement the model with any missing aspects mentioned by the tool.
Meeting number: 9**; Date:** 11.03.2019**; Participants:** analyst, five domain experts from the grid company, the manager from the grid company**; Meeting type:** physical**; Duration:** 4h; **Activities prior to the meeting:** the analyst retrieved the ENISA IoT tool, processed the contents and annotated potentially relevant parts. The list was then processed by the domain experts from the grid company and the relevant parts were extracted. The risk model was then updated by the analyst and sent to the analysis team. The grid company prepared a set of 19 risk elements and 9 scenarios (based on an independent earlier risk analysis of digitalized secondary substations) to be used for validation of the risk model. **Activities during the meeting:** Validation of the risk model. The analyst first presented the updated model. Thereafter, each one of the scenarios were gone through and a check was made as to whether the contents were already represented by the model. During the processing of the risk elements against the risk model, five vulnerabilities were added – three of them were triggered by one risk element each, and two were triggered by a fourth risk element. During the processing of the nine scenarios, a minor model update was made for the first scenario, no updates were needed for the second and the third scenario, the fourth scenario was found to be outside the scope, one vulnerability was added to the model due to the fifth scenario, no changes were needed due to the sixth scenario, one vulnerability was added to the model due to the seventh scenario, no changes were needed due to the eighth scenario, and three vulnerabilities were added to the model due to the seventh scenario.

4.3 Results from the Case Study

A high-level view of the risk model obtained from the above summarized process, is shown on Figure 4. The figure indicates the size of the final model, and reports on some of the contents. Selected parts of the model (i.e. those model elements that miss a textual annotation) are, for confidentiality reasons, undisclosed. The disclosed details on the figure include a representative selection of the specific vulnerabilities, threat scenarios, the one unwanted incident and the asset, in order to illustrate the abstraction level and the relationships among the elements.

The risk model shown on Figure 4 contains 14 undisclosed threat scenarios (*TS_01* – *TS_14*) and 10 disclosed ones, one unwanted incident which is disclosed, and one direct asset which is disclosed. Most of the vulnerabilities are undisclosed and only annotated by a numerical value. The numbers associated with the many vulnerability symbols represent the number of distinct anonymized vulnerabilities in the actual model that lead to the specified threat scenarios. For example, one vulnerability is annotated with the digit 18 and leads to the threat scenario "Insufficient security of SCADA or DMS". This conveys that there are eighteen different vulnerabilities that in our final risk model lead to this threat scenario. Moreover, there are, for instance, two distinct vulnerabilities which in our final risk model lead to **both** threat scenarios *TS_10* and *TS_11*.

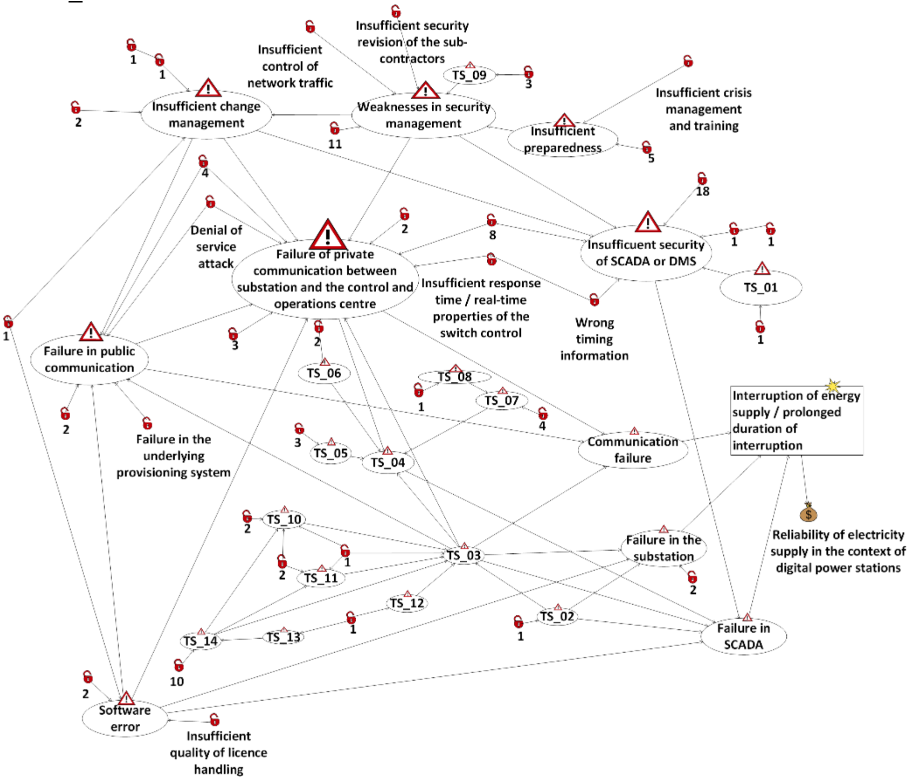

Insufficient security revision of the sub-contractors
Insufficient control of network traffic
1
1
2
TS_09
3
Insufficient change management
Weaknesses in security management
11
Insufficient crisis management and training
Insufficient preparedness
5
18
4
Denial of service attack
2
Failure of private communication between substation and the control and operations centre
8
Insufficuent security of SCADA or DMS
1
1
TS_01
1
Insufficient response time / real-time properties of the switch control
Wrong timing information
1
Failure in public communication
3
2
TS_06
TS_08
1
TS_07
4
Interruption of energy supply / prolonged duration of interruption
2
Failure in the underlying provisioning system
3
TS_05
TS_04
Communication failure
TS_10
2
1
TS_03
Failure in the substation
Reliability of electricity supply in the context of digital power stations
2
TS_11
2
TS_12
1
TS_02
1
Failure in SCADA
TS_14
TS_13
10
2
Software error
Insufficient quality of licence handling

Figure 4. High level view of the risk model. TS means Threat Scenario. The numbers underneath some of the vulnerabilities indicate the number of the distinct vulnerabilities present in the indicated parts of the model.

4.4 Experiences and Lessons Learned

Upon having completed meeting 5, the grid company wrote a feedback (without any prior request from group members) expressing that the workshop gave a good impression, and that the systematic approach and the graphical representation of the risk model, were appreciated. The second feedback was requested and received upon completion of the case study. The message was: "The process was useful and good. We were not a priori familiar with the approach applied, in particular not with the modelling approach. In addition to the improved competence on methodology for risk analysis, the work will be carried on and used as a baseline for another (specifically named) innovation project."

The group agreed that a thorough understanding of the context is crucial. In fact, a deep understanding of the digital secondary substations was gained by all analysis participants including the analyst, which also enabled the analyst to actively participate in risk modelling and development of the preliminary model. Such a deep insight into the domain is not assumed by the approach, but it was in our case experienced as an enabler of a better progress of the analysis.

Like in the previous trial of the approach, we have observed that regardless of how well the security risk analyst understands the context, it is crucial that the analyst does not develop the risk models alone. Risk identification triggers namely many useful discussions among the analysis participants, and it helps reveal knowledge, risks, inconsistencies and misunderstandings. Such information is crucial for validity of the risk model.

None of the domain experts from the grid company had prior experiences in either CORAS or graphical risk modelling in general. Still, the risk model was gradually updated into new versions through iterative and thorough discussions among all the participants. Our observation is that an adequate level of abstraction was selected, in terms of both the resulting size of the model and the level of detail provided. An important property of the risk model was that it was possible to express all information into one merged model, so that the complexity and the relevant relationships were explicitly reflected in a single comprehensive overview.

5 Discussion

Based on the results presented in Section 4, we discuss and evaluate the fulfilment of the requirements defined in Section 1. The second part of this section discusses the main threats to validity and reliability of the results.

5.1 To What Degree are the Requirements Fulfilled?

Requirement 1. To fully justify this requirement, we would have to quantify the benefits, as well as the costs. We have not attempted to do so. However, the feedback which has been received and the experiences gained, at least partially, indicate that the benefit justifies the effort, meaning that our customized approach is reasonably cost effective as well as light-weight. Moreover, our approach does not comprise risk estimation, evaluation and treatment, which are activities that many full-scale risk analysis methods include. This saved significant effort, although benefits of such activities were not realized either.

Requirement 2. As previously mentioned, the participants had rather varying background. Still, after a brief introduction of the approach, they were quickly able to actively contribute to the model development. Moreover, their involvement during the process demonstrated comprehensibility of the modelling approach.

Requirement 3. We were able to express all cybersecurity relevant risk elements and their mutual dependencies that were identified during the process. This suggests that our risk modelling approach has the expressiveness needed to capture relevant aspects of the cybersecurity risk picture in the context of smart power grids.

Requirement 4. As previously mentioned, smart grid concepts and technologies are still relatively immature, as they have not been in operation for a significantly long time. Thus, there is little experience on possible cyber risk incidents and their consequences for power system. Our approach has therefore deliberately been designed with simplicity as a goal, and with focus on vulnerabilities instead of the incidents. In the context of this case study, no unavailable information or details of unrealistic precision were demanded by the approach. In cases where such contents were possible and desired to include, the model was capable of adopting them. The analysis group was therefore free to choose the level of granularity in the risk model which is appropriate for expressing the information available.

Requirement 5. The final risk model included the high-level risk picture overview for the whole context. The needed details, such as decomposed vulnerabilities as well as dependencies among the model elements, were also explicitly expressed within the same model. This suggests scalability of the modelling approach in terms of both the ability to address a broad scope and to detail the necessary parts of it. Given its size, our model was readable when printed on a poster of A0-format.

5.2 Threats to Validity and Reliability

The results of the trial indicate feasibility of applying the approach. We have observed and received feedback suggesting that new knowledge about the target of analysis and its security risks was gained, which may suggest usefulness of the approach. However, application of the approach on a specific case such as digital secondary substations has clear limitations in terms of representativeness of the target of the analysis for the aimed smart grid domain. A generalization of the results is therefore not yet possible. For that, far more empirical evidence and multiple trials are needed.

The brainstorming-driven approach to risk modelling which significantly relies on the domain-expert knowledge is a threat in itself, due to the limited structure. Under such circumstances, the ability to ensure that all possible risk model elements have been considered, is limited. The validation step of the approach is therefore crucial.

The validation phase showed that several updates of the model were needed, upon exposure of the model to the independently retrieved risk scenario. Also, the use of the ENISA IoT tool triggered significant number of updates in terms of new model elements. All these steps were performed during some of the final meetings. Hence, we have no evidence that additional empirical sources would not have involved new changes in the risk model. This clearly represents a threat to reliability and validity.

A retrospective evaluation of the model with respect to historical risks would have been of interest, but the industry pilot has not been running for long enough in order to have sufficient empirical baseline. The fact that the analysis group was composed of experienced domain experts, did most likely balance this and contribute to validity of the input. It should be mentioned that the analyst from this case study had a main role in the original design of the customized version of the approach. This may represent a threat to validity of the evaluation of performance of the approach with respect to the five requirements (in Section 5.1). As such, it is also a threat to reliability of the evaluation results, as we cannot know to what degree another analysis group, without presence of the approach designer, would have obtained the same results.

The follow-up phase of the approach was not tried out, thus leaving another uncertainty in the evaluation. We did, however, show that the model is relatively easy to modify, as well as that if facilitates communication of the risk picture.

6 Conclusions and Future Work

This paper reports on the results of applying an earlier proposed approach to cybersecurity risk identification and modelling, on a pilot on digital secondary substations. The trial was conducted in a fully realistic setting, in the form of an industrial case study, in close collaboration with a major Norwegian distribution system operator. We argue that our approach to some extent fulfils the five pre-identified requirements and the results do indicate feasibility and usefulness of the approach. However, there are at the same time, clear limitations in terms of reliability and validity of the results.

The next step will be to perform a postmortem evaluation of both this case study, as well as the previous one that addressed the self-healing pilot. The two case studies as well as their respective postmortems will then be cross-analyzed in order to progress the evaluation. Another next step is to develop specific recommendations, templates and guidelines for cybersecurity risk identification in the smart grid domain, based on our approach.

For future studies it would be of interest also to investigate 1) the importance and possible increased risk (possible single points of failure) related to installing similar equipment in many secondary substations versus the increased complexity and possible interoperability issues if different equipment is selected and 2) the impact on the power distribution system from increased penetration of digital secondary substations (e.g. possible propagation of failure).

ACKNOWLEDGEMENTS

This paper has been funded by CINELDI - Centre for intelligent electricity distribution [5], an 8-year Research Centre under the FME-scheme (Centre for Environment-friendly Energy Research, 257626/E20). The authors gratefully acknowledge the financial support from the Research Council of Norway and the CINELDI partners. The centre gathers a significant number of the major public and private actors from the energy sector in Norway, and performs research on the future intelligent energy distribution grids.

References

1. Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2003) Introduction to the OCTAVE Approach: Carnegie Mellon University.
2. Barber, B. and Davey, J. (1992) 'The use of the CCTA risk analysis and management methodology CRAMM in health information systems', Proceedings of the 7th International Congress on Medical Informatics, pp. 1589-1593.
3. Belmans, R. (2012) Strategic Research Agenda for Europe's Electricity Networks of the Future - SmartGrids SRA 2035: European Technology Platform SmartGrids.
4. Ben-Gal, I. (2008) 'Bayesian networks', Encyclopedia of statistics in quality and reliability, 1, pp. 1-6.
5. CINELDI (2019) CINELDI. Available at: https://www.sintef.no/cineldi (Accessed: June 2, 2018).

6. ENISA (2019) ENISA Good practices for IoT and Smart Infrastructures Tool. https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool Accessed: February 22, 2019
7. Heegaard, P. E., Helvik, B. E., Nencioni, G. and Wäfler J. (2016), "Managed Dependability in Interacting Systems," in Principles of Performance and Reliability Modeling and Evaluation: Essays in Honor of Kishor Trivedi on his 70th Birthday, L. Fiondella and A. Puliafito, Eds. Cham: Springer International Publishing, 2016, pp. 197–226.
8. Hofmann, M., Kjølle, G. and Gjerde, O. (2012) 'Development of indicators to monitor vulnerabilities in power systems.', Proceedings of the 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012: Curran Associates, Inc., pp. 5869-5878.
9. IEC (1990): IEC 61025:1990 Fault tree analysis (FTA): International Electrotechnical Commission.
10. IEC (1995): IEC 60300-3-9:1995 Dependability management - Part 3: Application guide - Section 9: Risk analysis of technological systems: International Electrotechnical Commission.
11. IEC (2006): IEC 61165:2006 - Application of Markov techniques: International Electrotechnical Commission.
12. IEC (2009): IEC 60050-617:2009 - Organization/Market of electricity: International Electrotechnical Commission.
13. ISO (2009): ISO 31000: Risk Management - Principles and Guidelines: Geneva: International Organization for Standardization.
14. Kjølle, G. and Gjerde, O. (2012) 'Risk Analysis of Electricity Supply.', Risk and Interdependencies in Critical Infrastructures: A Guideline for Analysis: Springer, pp. 95-108.
15. Kjølle, G. and Gjerde, O. (2015) 'Vulnerability analysis related to extraordinary events in power systems.', Proceedings of the 2015 IEEE Eindhoven PowerTech: IEEE, pp. 1-6.
16. Lee, R. M., Assante, M. J. and Conway, T. (2016) Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case, Washington: Electricity - Information Sharing and Analysis Center.
17. Lund, M. S., Solhaug, B. and Stølen, K. (2010) Model-driven risk analysis: the CORAS approach. Springer.
18. Microsoft (2018) Security Development Lifecycle. Available at: https://www.microsoft.com/en-us/SDL (Accessed: November 2018).
19. Nielsen, D. S. (1971) The cause/consequence diagram method as a basis for quantitative accident analysis, Roskile, Denmark: Risø National Laboratory Risø-M, No. 1374.
20. Omerovic, A.; Vefsnmo, H.; Erdogan, G.; Gjerde, O.; Gramme, E. and Simonsen, S. (2019). A Feasibility Study of a Method for Identification and Modelling of Cybersecurity Risks in the Context of Smart Power Grids. In Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk - Volume 1: pp. 39-51.
21. Schneier, B. (1999) 'Attack trees: Modeling security threats', Dr. Dobb's Journal, 24(12), pp. 21-29.
22. Tøndel, I. A., Foros, J., Kilskar, S. S., Hokstad, P. and Jaatun, M. G. (2017) 'Interdependencies and reliability in the combined ICT and power system: An overview of current research', Applied Computing and Informatics, 14(1), pp. 17-27.
23. Wieringa, R. J. (2014) Design science methodology for information systems and software engineering. Springer.