electronics

MDPI

Article

An Approach for Analyzing Cyber Security Threats and Attacks: A Case Study of Digital Substations in Norway

Sule Yildirim Yayilgan [1,*], Filip Holik [1], Mohamed Abomhara [1] and Doney Abraham [1] and Alemayehu Gebremedhin [2]

[1] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, 2815 Gjøvik, Norway
[2] Department of Manufacturing and Civil Engineering, Norwegian University of Science and Technology, 2815 Gjøvik, Norway
* Correspondence: sule.yildirim@ntnu.no

Abstract: In this paper, we provide an approach for analyzing cyber security threats and attacks in digital substations, which is based on several steps we performed within our work on two Research Council of Norway (RCN) projects. In the literature, there are various separate or theoretical concepts to understand and follow a security analysis of smart grids in general, but none is focused specifically on digital substations. Moreover, none is showing real applicability on an existing use case, making the implementation difficult. The approach we propose here is a result of our attempts to create a comprehensive overview of the individual steps we have been taking to do the analysis. For that reason, firstly, we start with defining and explaining a digital substation and its concepts, and the security challenges related to digital substations. Afterwards, we present the main steps of the security analysis for digital substation. The first step is the security pyramid. The following steps are threat analysis, threat modeling, risk assessment and the simulation impact analysis, which are another contribution from our group presented in this paper. Considering that the main goal of a security analysis is to create awareness for the stakeholders of digital substations, such an impact simulation provides a flexible way for stakeholders to see and to understand the consequences of security threats and attacks. We summarize the paper with an illustration of the steps we are taking in the form of the approach for digital substation.

Keywords: attacks; cyber security; digital substation; smart grid; threats

Citation: Yildirim Yayilgan, S.; Holik, F.; Abomhara, M.; Abraham, D.; Gebremedhin A. An Approach for Analyzing Cyber Security Threats and Attacks: A Case Study of Digital Substations in Norway. *Electronics* **2022**, *11*, 4006. https://doi.org/10.3390/electronics11234006

Academic Editor: Ali Mehrizi-Sani

Received: 22 November 2022
Accepted: 28 November 2022
Published: 2 December 2022

1. Introduction

Digital substation (DS) is a term applied to electrical substations where operation is managed between distributed intelligent electronic devices (IEDs) interconnected by communications networks [1]. Digitalization involves introducing Information and Communication Technologies into the grid. It involves the replacement of copper wires with single fiber optic cables and the introduction of new digital devices such as IEDs. It also includes the management of measurement, control and status messages and exchange of data among devices, which takes place through digital interfaces. The main benefits of digitalization to the power grid company are reduced cost and increased reliability. The digital architecture and use of fiber optic cables greatly reduce time and effort needed to build, operate and troubleshoot any potential issues in the substation. Optical technology is also more resilient, which further decreases the chance of faults.

Digital substation development is rather new in Norway and IEC 61850 process bus technology is used for digitalization. Statnett, the grid company which owns the ECODIS project [2] funded by the Research Council of Norway is investigating new functionality advantages and associated costs with this technology. Functionality is first and foremost dependent on software.

Additional security challenges rise in the substations due to digitization. Substation control systems should be protected and preserved from cyber-attacks. Our team explores the cybersecurity related challenges in digital substation and digital secondary substation, respectively, in the ECODIS [2] and InterSecure [3] projects. Our objective is to create security awareness through the results of our work and hence stakeholders can take security protective measures accordingly.

The main contribution of this paper is to describe a complete approach for analyzing cyber security threats and attacks through a case study that has a focus on the digital substations in Norway. NIST provides a set of guidelines [4] for smart grid cyber security, where logical architecture and the interfaces of the smart grid, high level security requirements starting from security objectives, cryptography and key management issues and relevant concepts are explained in detail however a roadmap for where and how to start, how to progress with and how to complete a cyber security analysis for a smart grid is lacking in the document. In addition, NIST does not provide any specific guidelines for specifically doing cyber security analysis in digital substations which we consider as a case of smart grid grid security. IEEE provides Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems without any roadmap or an approach for cyber security analysis [5]. In the current literature, threat analysis, threat modeling and risk assessment are exploited as alternative ways of doing cyber security analysis for a critical infrastructure; however, instead of approaching and using them alternatively, we use them as complementary steps of an overall security analysis of a smart grid, e.g., digital substation in our case. Such an approach requires a starting point which is the security pyramid in our case. The pyramid is used by an U shape walk from the top to the bottom in order to define a general list of security objectives, a list of threat and attack categories and a list of threat and attack types for smart grids and given a particular smart grid, e.g., a particular digital substation, we refine a valid list of threat and attack types, a list of threat and attack categories and a list of security objectives that apply to the particular substation. The walk through from the bottom to the top of the pyramid constitutes of application of steps such as threat analysis, threat modeling, risk assessment and simulations with the aim of creating security awareness in the end for digital substation stakeholders, operators and consequently end users as well.

There are five steps in the security analysis approach. The contribution of this paper is to interpret and use each of these steps as complementary steps of an overall security analysis approach instead of using them as alternative security analysis methodologies to each other. We clearly show the outcomes of each step in the approach and how each outcome is provided as input to the next stage. In addition, each individual step provides the following contributions:

1. the security pyramid—the three-level starting point for the smart grid security analysis;
2. threat analysis—a process of identification of assets and risks;
3. threat modeling—a process to identify the most vulnerable parts of the system;
4. risk assessment—provides identification and detailed understanding of risks of threats and provides mitigation recommendations;
5. simulations for impact analysis—practical verification of identified threats and the proposed model in a high-detailed simulation model.

The rest of the paper is organized as follows: Section 2 summarizes state of the art literature and compares it to our work; Section 3 describes components used in DS; Section 4 introduces the approach; Section 5 applies the approach on the use case from Norway; and finally, Section 6 concludes the paper.

2. Related Work

The literature related to cyber security issues and challenges in digital substations, which is the scope of this work, as explained in Section 3, is still quite limited to the best of our knowledge. In [6], behavior analysis and anomaly detection for a digital substation is provided. The authors developed and implemented a cyber security testbed for the

digital substation for their use cases and analyzed potential security threats. The authors propose Network and Security Management (NSM) application and integration using a cyber–physical security testbed for assessing and monitoring risk in a digital substation environment. They also investigated IEC 61850 protocol and use generic object-oriented substation environment (GOOSE) and manufacturing message specification (MMS)-based experimental data to implement their use cases. Further, the authors test their testbed using the real network traffic data captured from both the North American and South Korean digital substation environment. However, the authors work at the networking and protocol levels and do not distinguish between attacks on specific components. In [7], problems of cyber security of digital substations are discussed. The most common attacks and their influence on the operation of digital substation is analyzed. In addition, a tree of threats and attacks to mitigate attacks and restore operation of digital substation after the occurrence of attacks is generated. Ref. [8,9] shows the performance of Secure Sampled Value (SeSV) allowed security feature packets transmitted between security and control devices by appending the extended IEC61850 packets to a message authentication code (MAC). A thorough explanation of DoS attacks and how they can be simulated in a Substation Automation Systems (SAS) in the form of four case studies is provided in [10]. In [11], SYN-Flood attack is simulated in digital substation. SYN-Flood is an attack which exploits TCP protocol vulnerabilities. In the simulation, CPU utilization, link load and TCP connection delay are used as parameters to evaluate the effect of SYN-flood attacks. These parameters are compared for attach and no attack cases. OPNET platform is used for simulations.

In [12], the authors propose cyber security proxy gateways in digital substation. An upper cyber security proxy gateway is implemented in the station layer and a lower one is implemented in the process layer such that the fragile bay layer in the middle where IEDs lay is free from cyber attacks. The main form of a process layer cyber attack is that the process layer sends false or tampered SMV (Sampled Measured Values) messages to protective relays of the bay level. The total transmission delay of star and ring network substation SMV message is 1.229 ms and 1.278 ms, respectively. Both satisfy the real-time requirement that the transmission delay is less than 4 ms.

In [13], a review of asset centric threat modelling approaches are presented. Among the reviewed threat modeling approaches, PASTA is the closest approach to our cyber security analysis methodology. Meanwhile, in [13], threat analysis and threat modeling concepts are used interchangeably and more specifically threat analysis is a component of the threat modeling process, in our approach, threat analysis precedes threat modeling. In addition, risk and impact analysis are considered as part of the threat modeling process while we separate risk assessment and impact simulations as separate components. Business impact analysis is as an important part of the PASTA process, while in our methodology, our overall starting point is the security pyramid and the security objectives at the top of the pyramid. This gives us the flexibility to have a focus right away on the cyber security challenges in DS. In addition, it is stated in [13] that the reviewed threat modeling approaches may fail to capture potential threats to a cyber-physical system due to the timing, uncertainty, and dependencies that exist between its entities. On the other hand, in our approach, the threat modeling component of our methodology provides a detailed analysis of the threats in terms of these aspects. An example of such work from our group is provided in [14].

In [15], the authors have a goal to analyze the direct cyber-physical impacts of specific cyber attacks on the power system. Cyber events are defined as both intentional acts of sabotage and random hardware or software failures. Further events are categorized into four categories according to their affect on physical equipment, communication channels, applications and data. In our approach, all of these are considered as components of digital substation. In [16], a risk analysis approach based on threat modeling where the threat modeling component provides a threat list is used. The threat list is a pre-defined list and the case study is a smart home whereas our use case is digital substation. In [17], three

types of security strategies are examined, namely network separation, communication message security, and monitoring.

In [18], the author proposes an extension of the IEC 61850 standart to enable the handling of intrusion detection. The author also develops a test bench for studying cyber vulnerabilities of IEC 61850 automation systems, including attack generation and intrusion detection. Ref. [19] discusses the challenges with IEC 62351-6 standard and proposes an authentication approach based on message authentication codes. In [20], security filters as add on devices are proposed between IEDs and communication bus. It is used to add MAC tags to the outgoing Ethernet packets. Experiments with it show that it adds only 20–60 microseconds of delay. This is in alignment with substation protection and control requirements. In [21], the authors develop an MU that complies with the IEC 61850 9-2LE standard and its guidelines. A start topology is used for simulations however there are no simulation results reported beyond the process bus design. Ref. [22] provides experiences related to employing IEC61850-based digital substation pilot project at Hydro-Québec. Protection and control architectures are explained and phases for implementing IEC61850 in a digital substation are provided. Ref. [23] investigates the timing constraints of authenticating GOOSE messages. Finally, in [24], a thread model for ABB produced IEDs is created and the functionality of it is verified using several scenarios. On the other hand, in our work, we aim at proposing an cyber security analysis approach for the full digital substation and its components.

As can be seen from the literature review, each research work has a focus on security challenges, e.g., most common attack(s) or a sole approach, e.g., threat modeling in order to identify and solve security gaps in a digital substation. In addition, our work encompasses using sole approaches to identifying and solving security gaps [25,26] of power networks namely, threat modeling [14], security pyramid [27], risk assessment [28], simulations and emulations [29], and privacy [30]. However, our work has also shown that "identifying and understanding security challenges and creating security awareness through that requires a more comprehensive approach than using a single approach or a combinations of a few approaches together". To the best of our knowledge, there is no united approach that integrates all these into a single method to do a complete security analysis for digital substations to create security awareness. In this paper, we aim at describing and demonstrating such an approach. When we started the work on analyzing the security aspects of digital substations, we did not have such a guide in hand. We applied sole steps separately for various purposes such as threat modeling to identify threats or risk assessment to identify risks; however, at some point in time, we noticed that we are using these steps in an order where we provide certain inputs from a previous step to the next step in the flow. This paper will describe the approach that we finalized in our work.

3. DS System Architecture

In Figure 1, an overall architecture of a digital substation is provided and the components in the architecture are explained below it.

A substation has the following components:

- SCADA is a centralized system used for monitoring and controlling of all substations. It is a supervisory system for gathering data about industrial processes and sending control commands. It is located in a control center outside the DS and it is therefore out of the scope of this work.
- Gateway is a network device that allows data to flow from and into the substation. It connects the substation to the WAN.
- HMI is a graphical interface between a human operator and the controller (all the physical devices) of an industrial system. It provides interaction and communication between them.
- WAN is a network which connects the substation with the control center. It is accessible through the gateway.

- LAN/Ethernet is a local network in the DS and it is used by process and station buses.
- Switch is a network device that is used for connecting devices and switching datagrams (messages) between them.
- Process and Station Buses provide communication between lower and higher layer grid components.
- IED is a microprocessor-based device that is used by the electric power industry to control and monitor power system switching devices.
- MU is a device that enables the implementation of IEC61850 process bus by converting analog signals from the conventional CT/VT into IEC61850 Sampled Values (SV) for metering, protection, and control purposes.
- CT/VT are devices that constantly interact with physical environment and communicate with the controller via a shared process bus.

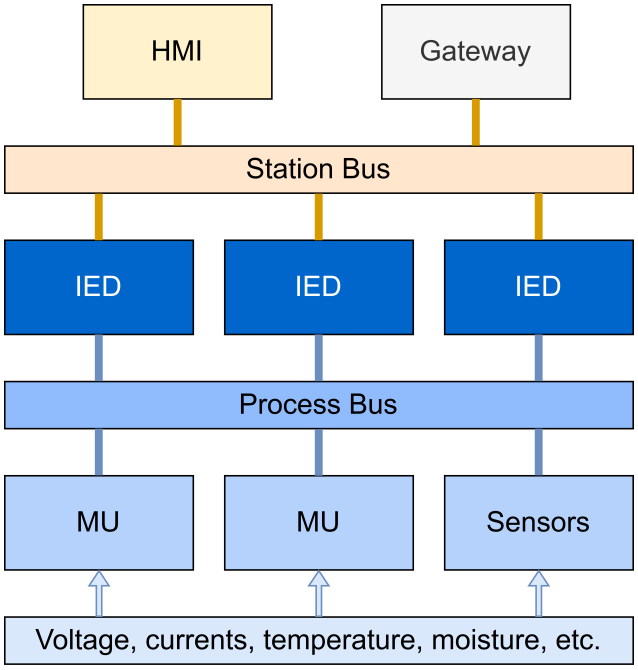

Figure 1. Digital Substation Architecture.

3.1. Communication Protocols

A digital substation uses various communication protocols as described below.

3.1.1. Analog Messages

Analog messages are sent by CTs and VTs to MUs or IEDs which converts the data into digital format.

3.1.2. IEC 61850

IEC 61850 is the main standard for communication in electrical substation and it defines abstract data models and their mapping to those protocols: GOOSE, MMS, and SV.

- GOOSE is used for communication on the process bus mainly between IEDs. Messages are embedded straight into Ethernet frames and cannot therefore exit the LAN. Protocol uses publisher-subscriber mechanism via L2 broadcasting. Messages are used mainly for delivering time-critical information [31] triggered by an event.
- MMS is used on the station bus to provide information monitoring to HMI and SCADA (via WAN). It uses TCP to deliver messages outside of the substation.
- SV is used similarly as GOOSE on the process bus. It also uses Ethernet frames, but it is used mostly for continuous streaming of measurement data.

3.1.3. IEC 60870-5-104

IEC 60870-5-104 is used mostly for communication between substations and SCADA. It uses TCP protocol and it typically encapsulates data from multiple sensors into a single message. It can send messages periodically, on upon request from SCADA.

4. An Approach for Digital Substation Cyber Security Analysis

The main security challenge in smart grid arises due to the digitalization of communication and use of common Ethernet technology. This move decreases the design complexity but makes the components more vulnerable to common attacks. Other challenges relate to improper authentication, lack of encryption, insufficient verification of data, credential management, configuration and maintenance of software, and access control. In this section, we will provide the steps and concepts of the approach we have used for security analysis of digital substation. The five main steps are listed as below:

1. the security pyramid;
2. threat analysis;
3. threat modeling;
4. risk assessment;
5. simulations for impact analysis.

4.1. The Security Pyramid

In [27], we are proposing the three-level security pyramid as an approach for analyzing smart grid security as shown in Figure 2. In this paper, the pyramid is used to set a starting point as being the first step in our approach. That is, firstly a smart grid company sets the three security objectives to initiate a security analysis as shown at the top level of the pyramid. The security objectives are Confidentiality, Integrity and Availability (CIA). Then, for the middle level, a list of general threat and attack categories is provided for smart grid security analysis. These categories do not consider concrete attacks implementations. Examples of these categories are Data Manipulation, Unauthorized Access of Data, Attacks due to Unauthorized Access of Users or Devices, and Threats on the Privacy of Customers [27]. At the bottom level, a list of more specific threat and attack types is provided for smart grid security analysis. An example can be the STRIDE model, which categorizes threats into Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege [32]. These types consider concrete attack implementations and can be very specific, for example, "RAM access". All the three layers of the pyramid are used in the threat analysis step.

Figure 2. Levels of abstraction for Smart Grid Security analysis. Adapted from [27].

4.2. Threat Analysis (How an Attacker Utilizes Component-Wise Vulnerabilities)

In general, threat analysis is a process used to determine which components of the system need to be protected and the types of security risks (threats) they should be protected from [33]. In Figure 3, an example of potential assets and relevant threats to be

analyzed is provided. In the figure, SCADA, gateway, IEDs, HMI, MUs and CT/VT are identified as assets. DoS attack, malware injection, packet transfer delay, grid messages (SV, MMS, GOOSE) and GPS spoofing, network monitoring and port scanning, man in the middle attack and intrusion from the internet are identified as potential threats to be further analyzed.

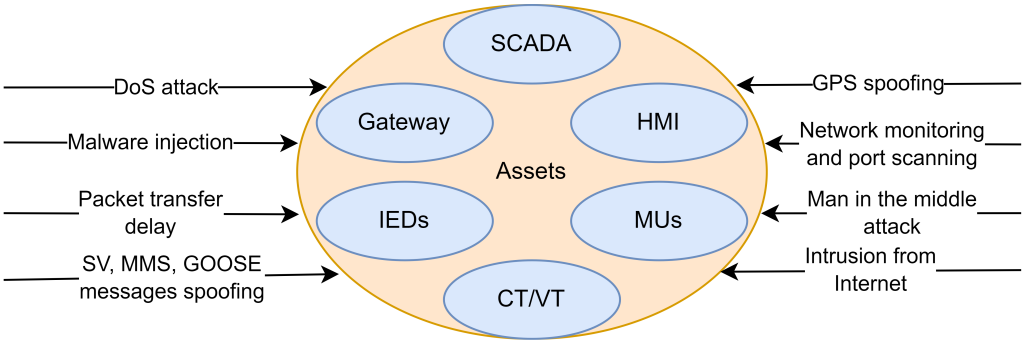

Figure 3. Potential assets and threats to be analyzed. Adapted from [33].

In our case, the threat and attack types from the security pyramid are mapped to the assets of the smart grid, hence giving an overview of what threats and attacks are possible for which components and parts in the smart grid. This output is called the security map. Threat analysis continues with linking categories from the middle level of the security pyramid to the security map which results in the security table. The security table is then used for linking security objectives from the upper level of the security pyramid and creating the threat analysis table. This table is the main output of the threat analysis and it is used as the input for the following step—treat modeling.

The results of the further analysis of the example provided in Figure 3 can be found in Table 1. The effect and likelihood pair of each potential threat on the identified assets of a specific organization is assessed. The likelihood is defined as: "How easy it is for an attacker to exploit the threat. It is a combination of required knowledge and availability of specific tools which can be used for the attack [14]." For example, malware injection to IEDs may be Destructive (A) for the substation and the likelihood of such a threat to happen is indicated as Likely (B). The effect considers consequences in terms of equipment damage, revenue and reputation loss, and consumer and operator safety [14]. The types of effects and likelihood are also listed in the table. In the context of a smart grid, the meaning of each effect type and each likelihood type is as follows.

Effects:

- A (Destructive)—causes damage to the grid equipment, which can lead to blackouts, potentially affecting lives of people.
- B (Disabling)—can lead to blackouts without permanent damage of the grid equipment.
- C (Disruptive)—affect grid observability, without affecting its functionality.
- D (No impact)—has no impact on functionality or observability.

Likelihood:

1. A (Certain)—will happen with very high probability.
2. B (Likely)—might happen with medium probability.
3. C (Unlikely)—might happen with very low probability.
4. D (Impossible)—cannot happen.

Table 1. An example of a threat analysis table. Adapted from [33].

Threats/Assets	SCADA	Gateway	HMI	IEDs	MUs	CT/VT
DoS attack	C/C	C/B	C/B	A/B	A/B	A/C
Malware injection	A/B	C/C	C/B	A/B	A/C	A/D
Packet transfer delay	C/C	C/C	C/C	A/B	A/B	A/C
SV, MMS, GOOSE spoofing	C/C	C/C	C/C	A/B	A/B	A/C
GPS spoofing	C/D	D/D	C/B	A/B	A/B	D/D
Net. monitoring and scanning	D/B	D/B	D/B	D/B	D/B	D/D
Man in the middle attack	A/B	B/B	C/B	A/B	A/B	A/C
Intrusion from Internet	B/D	B/C	B/C	A/C	A/C	A/D

Effect: A = Destructive, B = Disabling, C = Disruptive, D = No Impact. Likelihood: A = Certain, B = Likely, C = Unlikely, D = Impossible

4.3. Threat Modeling

In general, threat modeling is a process by which a view of potential threats is provided through creating an abstraction of the system, profiles of potential attackers, including their goals and methods and a catalog of potential threats that may arise [34,35]. Threat modeling is expected to answer questions such as "Where is the system most vulnerable to attack?", "What are the most relevant threats?", and "How to implement protection against these threats?".

Threat modeling uses the table from the threat analysis step (Table 1). The goal of this step is to quantify the risk. The output of the risk analysis is therefore updated with numeric evaluations of *effects* and *likelihoods*. This process can use various metrics. The most simple one is to statically assign numbers to each level. For example, effects can be rated as:

- A (Destructive) = 1
- B (Disabling) = 0.66
- C (Disruptive) = 0.33
- D (No impact) = 0.1

A similar scale can be assigned for likelihood. Finally, the risk is calculated using the following formula:

$$Risk = Effect * Likelihood \quad (1)$$

Output from the threat modeling is being used in the next step—risk assessment.

4.4. Risk Assessment

Risk assessment involves identification of security risks through the analysis of assets, threats and vulnerabilities, including their impacts and likelihood [36]. It is a process of evaluating results of the threat modeling and creating a risk assessment model, which can be used as input for the simulations for impact analysis. In practice, this means to evaluate the threat model and based on calculated risk values (from Equation (1)), assign each threat into one of the following categories:

1. Critical threats—threats for which impacts and mitigation techniques are not clear. Those threats need to be further analyzed in impact simulations.
2. Threats for which impacts and mitigation techniques are clear—those threats do not have to be analyzed in the simulation model, because their impacts are well known and mitigation techniques can be deployed.
3. Threats which can be ignored—this includes low risk threats, which does not have to be further considered.

4.5. Simulations for Impact Analysis

Simulation for impact analysis takes critical threats as classified in the risk assessment step and tests corresponding attacks in a high-detailed simulation model. The goal is to verify feasibility of such attacks and their impacts on the system. This data offers a valuable insight into the attack process and can be used in implantation of more effective mitigation methods. The simulation model should be as close as possible to the real environment, and it therefore often combines simulation with emulation techniques. In addition, the impacts of the attacks on the system is shared with user of services of the smart grid and the stakeholders.

4.6. The Approach in a Nutshell

Our approach process is shown in Figure 4. The upper left corner represents the security pyramid. Firstly, the security pyramid is traversed from top to bottom in order to define a list of security objectives, a list of security categories and a list of security types for a smart grid use. After that, given a specific type of smart grid such as a DS and its assets, the pyramid is traversed from bottom to upwards in order to link each of the layers of the pyramid to the steps of the threat analysis step. A threat analysis table is generated out of the threat analysis step which is then provided as an input to the threat modeling step. The outcome is a threat model which is further processed by the risk assessment step in order to create a risk model. The risk model is used in order to perform impact simulations through which security awareness can be created. Impact simulations have to be conducted only for threats classified as critical in order to demonstrate theirs consequences and help with providing enough data to develop effective mitigation techniques. Other threats can be simulated in order to demonstrate threats' milder consequences if required. Data from the impact simulations and risk model are then used in developing security awareness policies such as mitigation techniques, security policies, configuration of firewalls, access control lists, intrusion prevention systems, etc.

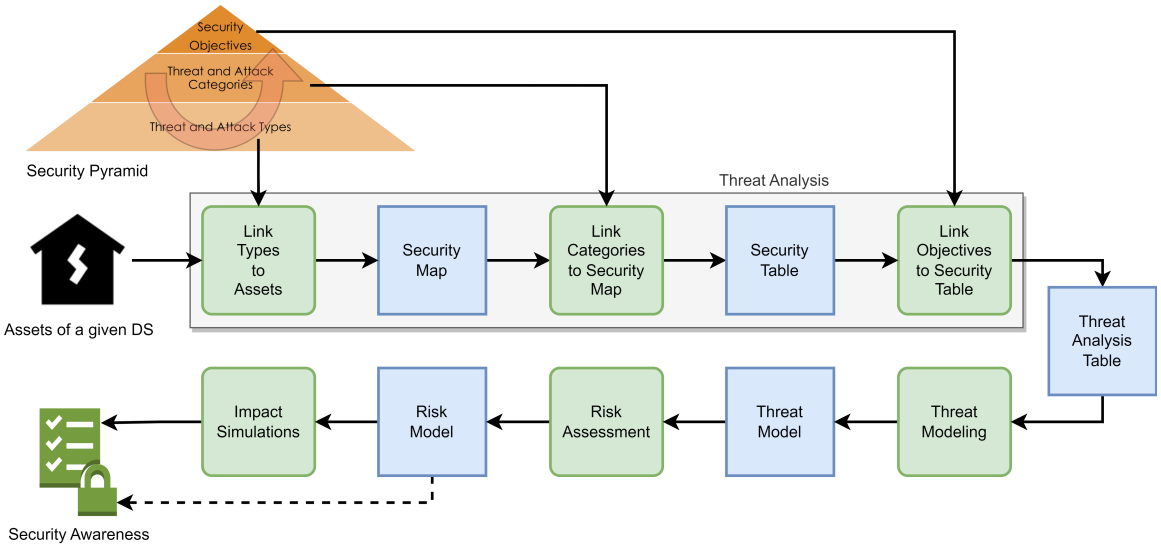

Figure 4. Digital Substation Cyber Security Analysis Approach Flow.

This awareness is based mostly on practical results from the impact simulations, which show exact steps of each analyzed attack. This gives the stakeholders an understanding of the consequences and risks of various cyber threats and attacks applicable to DS. Stakeholders can therefore take necessary measures to prevent and mitigate the threats in a timely and effective manner.

The following is a list of results that will be obtained using the analysis approach:

- Intermediary results include (1) a map of which assets are likely to be threatened or attacked by which threat and attack types (2) a list of more general categories for the

actual threat and attack types for the smart grid (3) the security objectives relevant for the particular grid (4) a threat model (5) a risk model (6) simulations for the most risky threats and attack scenarios.
- Final results include demonstrations of simulations of the most risky scenarios to the stakeholders of smart grids in order to raise security awareness which will lead to taking precautions.

5. Applying the Approach to a Smart Grid Use Case: Digital Substation

In this section, we will show how we used the approach explained in the previous section in order to promote security awareness in Digital Substations.

5.1. The Security Pyramid

In this section, in accordance with the security pyramid, we will define the security objectives, a list of threat and attack categories and a list of threat and attack types for a digital substation [27].

5.1.1. What Are Security Objectives in DS?

NIST [4] has defined principles of confidentiality, integrity, and availability (CIA) to maintain the security and privacy of smart grids [37]. This standard, however, refers only to different concepts in smart grid cyber security and does not focus on substations practically as in our work. Confidentiality is information protection from access without a proper authorization. Integrity is the assurance that information is not modified without authorization. Confidentiality and integrity are both ensured mostly outside substations by encrypted VPN connections with the control center. On the other hand, their applicability within current substations is limited. Availability guarantees that data, applications and resources are available to authorized users whenever they are needed. Availability is critical for correct operation of smart grid protections and in current scenarios has priority over security features.

5.1.2. What Are Cyber-Security Threat and Attack Categories in DS?

In general, cyber security threat and attack categories for IoT-Enabled smart grids are listed as below and we assume that the same threat and attack categories are applicable in power grids and hence in digital substation.

- Data manipulation—tampering with control and sensor data can cause damage of grid equipment and outages.
- Unauthorized access of data—can disclose sensitive information.
- Unauthorized access of devices or users
  - unauthorized access of devices—unauthorized devices in the DS network can become entry points for an attack.
  - unauthorized access of users—including insiders and former employees.
- Threats on the privacy of customers—sensitive data of power consumption which can identify customers ethnicity, habits, used appliances, presence in the house and other information.
- Disruption threats—can be life threatening (hospitals, heating during cold temperatures, etc.).

5.1.3. What Are Common Threat and Attack Types in DS?

- DoS Attack, e.g., block flow of information to intended IEDs by flooding to reduce service availability
- Malware injection, e.g., the attacker injects malicious software such as ransomware and worms into software components of DS resulting in an undesirable operation, or failure of operation
- Packet transfer delay, e.g., delay in control commands

- GPS spoofing, e.g., desynchronization
- SV, MMS and GOOSE message spoofing –, e.g., prevent legitimate IEDs from getting critical messages by modifying GOOSE header fields to hijack communication channel
- Port Scanning, Network monitoring, e.g., data theft
- MitM attack, e.g., the attacker gains unauthorized access on communication network
- Corporate network intrusion from internet –, e.g., intrusion into the local network of substation with subsequent information distortion

5.2. Threat Analysis

5.2.1. Security Map: Linking Threats and Attack Types to Assets

In this step, we link the threat and attack types to DS assets. We have already provided a list of assets and a list of threat and attack types in a DS in the previous sections. Figure 5 illustrates the resulting security map. Please note here that in reverse to presenting the results of threat analysis directly in the form of a table as in Table 1, we prefer to first generate a map form presentation in order to provide a demographic view of which attack and threat type can occur in which component of the digital substation and where in the substation.

- SCADA is located in the control center outside the DS. If an attacker gains access, it is possible to take control of the system. The attacker may manipulate the SCADA software (inject a malware), access confidential information (including data on servers and sensors from the entire grid), cause a DoS attack (potentially resulting in loss of grid observability and controllability) and send false commands resulting in control of the entire grid network with potential to damage the grid equipment.
- Gateway: an attacker may intrude to the network passing through the gateway and gain access to several components and/or flood the network via a DoS attack.
- HMI: if an attacker gains access, it is possible to take control of the system and the attacker may manipulate the HMI software (inject a malware), access confidential information on servers and sensors (within the substation) and send false commands to control the substation with potential to damage the substation equipment.
- IEDs: an attacker may gain access to an IED by obtaining login credentials. Hence, the attacker may reprogram IED, access data on IED, and/or stop/change device functionalities.
- MUs: an attacker might gain access to an MU device, manipulate analog data received from NCIT, and/or stop and/or control functionality.
- Physical Devices (CT/VT)—an attacker might gain access to sensory data, listen to measured values, and/or damage devices physically.
- Communication networks are vulnerable mostly to sniffing and DoS attacks. Sniffing can be classified to passive (monitoring and traffic capture) and active (port and vulnerability scanning). DoS attacks makes the network inaccessible to the intended users by flooding the network with traffic.
- Physical site: an engineer, technical staff, or an outsider with malicious purposes intrude into the DS as follows:

  using a mobile device with access to Internet in DS (malicious insider);
  using an infected USB flash disk or laptop in DS (insider);
  data access and modification on DS devices and communication lines interference (malicious insider and outsider);
  controlling devices manually such as turning on/off switches (malicious insider);
  controlling functionality of devices to stop, start or reverse functionality (malicious insider and outsider).

As shown in Figure 5, it is possible to attack the DS through namely, SCADA system, HMI, IED, MU, switches, process and station busses. Even though the figure visualizes the communication of the DS to other DS', the focus of the paper is attacks within a single DS. Considering these attack points, the common types of cyber-attacks in a DS include denial-

of-service (DoS), network monitoring and intrusion, malware injection, physical intrusion, spoofing and man-in-the-middle (MitM) attacks. One of the main contributions of the paper is to identify the possible attack types that can occur through each DS component.

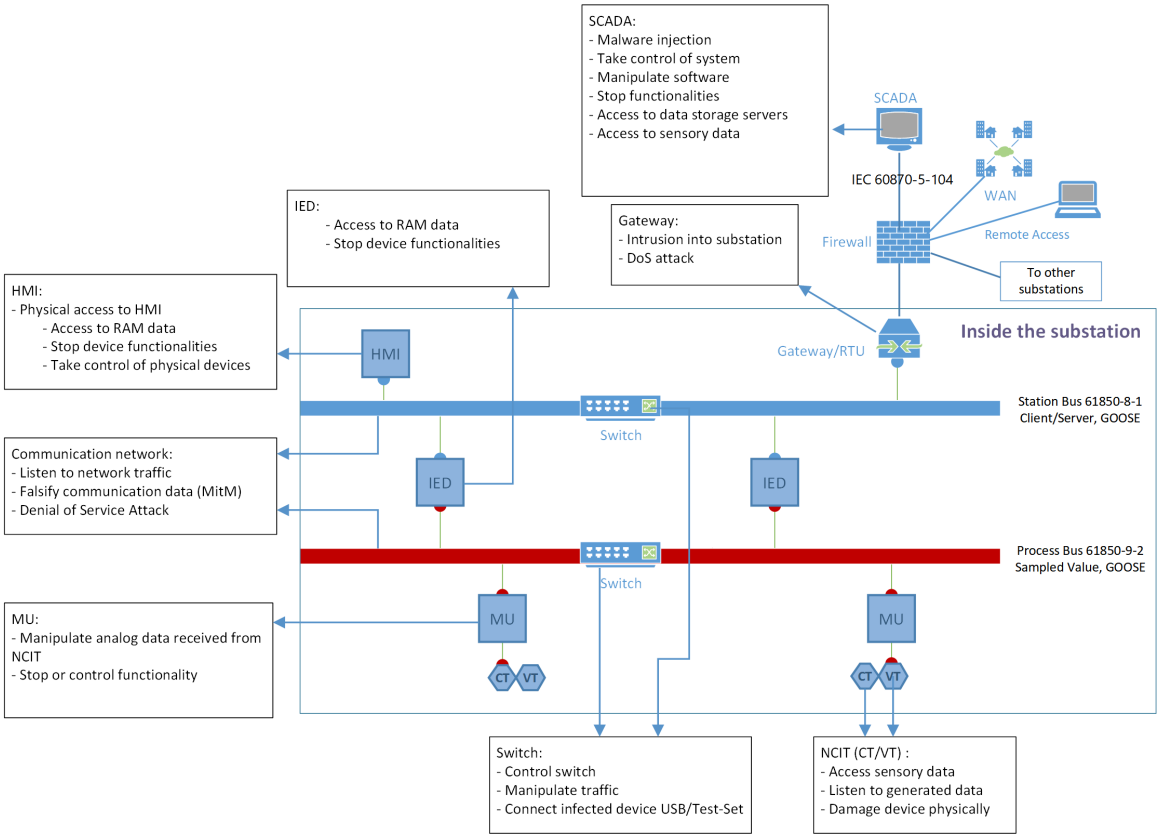

Figure 5. The security map as an initial step of threat analysis [27].

5.2.2. Security Table: Linking Threat and Attack Categories to Security Map

As we have seen in the previous step of threat analysis, in the security map, DS assets are linked to "Threat and Attack Types" which are identified to occur on them. Further in this step, we obtain a Security table (Table 2 excluding the last three columns labeled CIA) by linking the corresponding threat and attack categories of the security pyramid to the threat and attack types of the security map.

5.2.3. Threat Analysis Table: Linking Security Objectives to Security Table

Finally, the security objectives are linked to the Security Table in the last step of threat analysis as shown in Table 2 (now including the last three columns labeled CIA). The security objectives are goals and constraints that affect the CIA (defined in Section 5.1.1) of the DS data and systems. These objectives do not have to remain static and can be influenced by later design and implementation activities. While for some assets only a single security objective will hold, for others, two or more objectives may hold simultaneously. The likelihood and effects of threat and attack types are categorized in this step.

5.3. Threat Modeling

The threat modeling takes in the threat analysis table, and will map the likelihood and effect categories (A, B, C, D) into numbers in order to calculate a risk per threat and per attack. The resulting threat model will be passed onto the risk assessment step.

Table 2. The Security Table resulting from linking Threat and Attack Categories to the Security Map. Adapted from [27].

SG Threat and Attack Categories		**Data Manipulation Attacks**	**Unauthorized Access of Data**	**Unauthorized Access of Devices or Users**		**Attacks on the Privacy**	**Disruption att.**	**C**	**I**	**A**
DS Assets	Attack/Threat Types			Dev. to SG	Users to dev.					
SCADA	Malware injection	X	X	X	X	X		X	X	
	Take control of system			X	X			X	X	X
	Manipulate sw	X	X		X			X	X	
	Stop functionality	X			X		X		X	X
	Access to data storage servers	X	X			X		X	X	
	Access to sensory data		X					X	X	
Gateway	Intrusion into DS		X		X				X	
	DoS						X			X
IED	RAM access	X	X		X	X		X	X	
	Stop function.	X			X		X			X
HMI	RAM access		X		X			X	X	
	Stop functionality	X		X	X		X			X
	Take control	X	X		X	X	X	X	X	X
Communication network	Listen to network traffic		X			X		X		
	Falsify comm. data (MitM)	X	X					X	X	
	DoS						X			X
MU	Manipulate analog data	X	X		X			X	X	
	Stop/control functionality	X			X		X			X
Switch	Switch control				X			X		X
	Manipulate traffic	X	X	X		X	X	X		X
	Connect infected dev. (USB)	X	X		X	X		X	X	
NCIT (CT/VT)	Access to sensory data		X					X		
	Listen to generated data		X			X		X		
	Physical damage				X					X

5.4. Risk Model: Risk Assessment and Management

This is a work in progress; however, we have a preliminary risk assessment published in [28]. Risk assessment is the practice of identifying, assessing, controlling, and treating the DS. The main goals of risk assessment are to identify and understand the risk, prioritize the risk and treat (accept, mitigate, transfer or control) the risk. There are several structured approaches for risk assessment and management that integrates security risk assessment activities into the system development life cycle. In our work, a custom risk assessment approach based on the NIST's guidelines outlined in [38] is applied.

5.5. Impact Simulations

The goal of the impact simulation is to verify identified threats with high degree of precision. It is important to mention, that simulation model techniques, selected attack types, and explored impacts will differ from use case to use case. This section shows an

example of our approach. The results were used to demonstrate the verification of the attacks with smart grid stake holders in Norway in order to create security awareness and provide them with insight into these attacks and how they happen.

We have created a simulation model using virtual machine (VM), Mininet network emulator and IEC 61850 library for emulated communication of substation protocols. This setup allowed us to verify identified threats with high realism. Topology of the impact simulation model is shown in Figure 6. The entire smart grid topology is running within Mininet and has configured links (named *AttackDSS* 1/2 and *AttackDPS* 1/2) to VirtualBox networks. Those links can be used to connect physical or virtual machines into the model. We have used it for connecting a VM with Kali Linux to perform selected attacks.

The risk model in our use case scenario identified two critical threats—sniffing and denial of service.

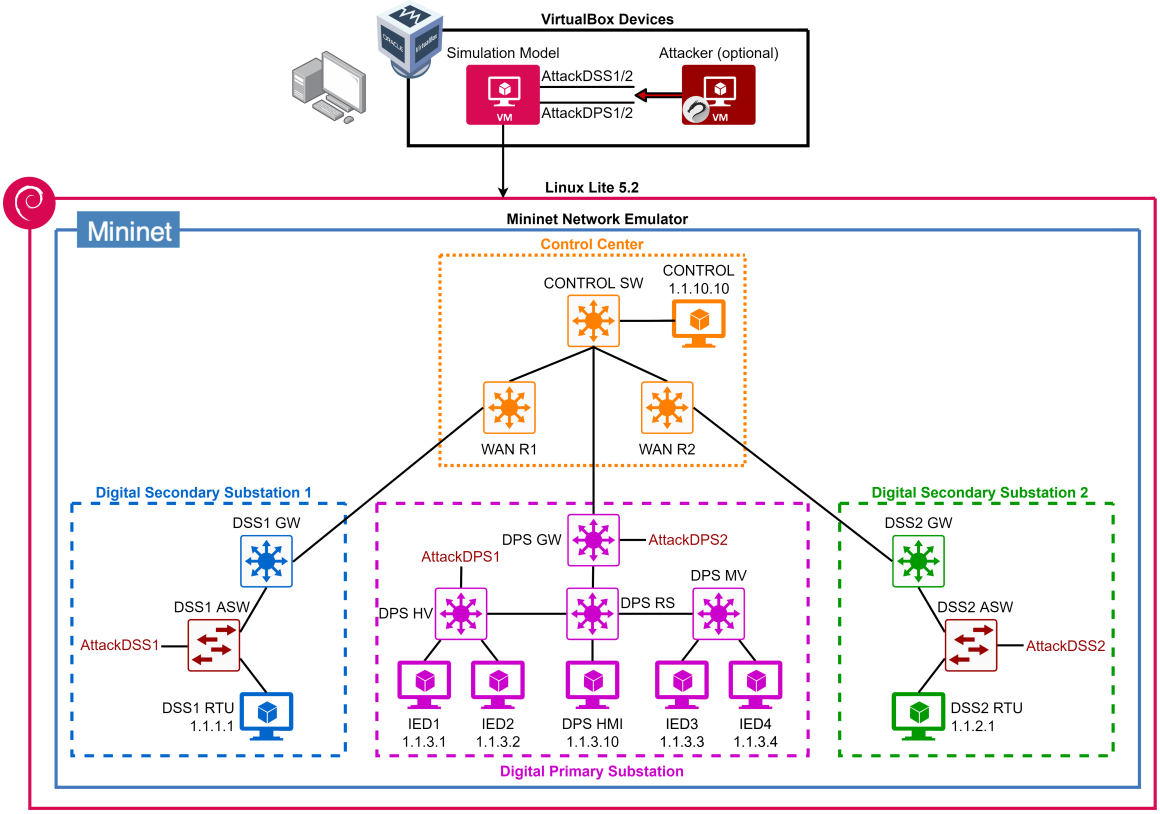

Figure 6. Impact Simulation Model.

5.5.1. Passive Sniffing Attacks Verification

The main goal of sniffing attacks was to show stakeholders, which information about the DS operation can an attacker acquire simply by gaining access to the network.

First, we used Wireshark to capture complete substation communication as this is not encrypted. All the details such as measured values, sensor IDs, or SCADA commands were plainly visible, as shown in Figure 7. Those information could be misused in spoofing, man-in-the-middle, or replay attacks. Moreover, this attack cannot be detected and it is therefore important to know, what data might be compromised.

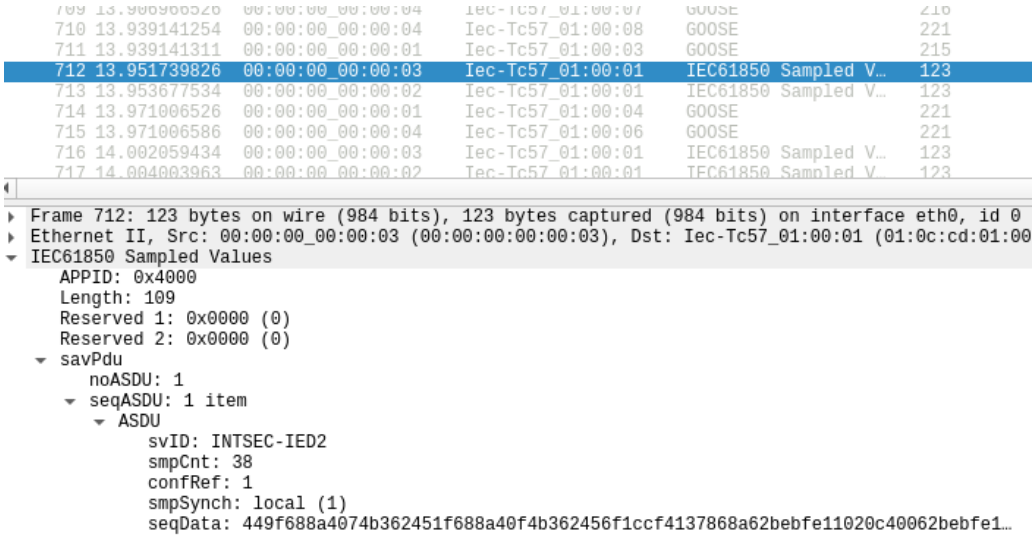

Figure 7. Captured communication.

5.5.2. Active Sniffing Attacks Verification

We then used active sniffing with the "netdiscover" tool. It uses ARP packets to probe all devices in the network and therefore locate even devices, which are not sending any traffic. It was able to detect all devices in the topology as shown in the Listing 1. Found devices correspond to IEDs, RTUs, and the control center as shown in Figure 6. IP addresses of grid equipment and SCADA can be misused by the attacker to launch more serious attacks (DoS).

Listing 1. Active sniffing by netdiscover.

```
Currently scanning: 1.1.134.0/16 | Screen View: Unique Hosts
9 Captured ARP Req/Rep packets, from 8 hosts. Total size: 540
-----------------------------------------------------------------
IP At MAC Address Count Len MAC / Host
-----------------------------------------------------------------
1.1.1.1 00:00:00:00:00:06 2 120 XEROX
1.1.2.1 00:00:00:00:00:07 1 60 XEROX
1.1.3.1 00:00:00:00:00:01 1 60 XEROX
1.1.3.2 00:00:00:00:00:02 1 60 XEROX
1.1.3.3 00:00:00:00:00:03 1 60 XEROX
1.1.3.4 00:00:00:00:00:04 1 60 XEROX
1.1.3.10 00:00:00:00:00:05 1 60 XEROX
1.1.10.10 00:00:00:00:00:08 1 60 XEROX
```

5.5.3. Denial of Service Attacks Verification

The main goal of Denial of Service (DoS) attacks was to verify functionality of substation communication protocols during high network load. For this reason, IEC 104 communication was modified to utilize timestamps and 1 second message intervals to automatically calculate delay, jitter and packet loss. A script on the receiving device (Control PC) compared sending and receiving timestamps of two consequent messages to calculate the values.

DoS was tested using seven different types of the attack: TCP SYN flood, FIN flood, SYN FIN flood, Push ACK flood, RESET flood, UDP flood, and Smurf attack using the hping3 tool. TCP SYN attack was also tested with the Metasploit tool. The attacker in form of another VM (with Kali Linux) was connected to the *AttackDSS1* port (on a switch between GW and RTU of DSS1) and the attack target was Control PC. Both VMs were set to use 4 GB of RAM and up to 6 virtual CPUs without limiting theirs maximum utilization.

These values can be modified so that performance of the model would be calibrated to performance of a real substation. As our goal was mainly to show traffic patterns and connectivity loss, this calibration was not our priority. Attacker's BW and number of PPS were measured using the *ethstats* tool and AWB between the RTU and Control PC was measured using the *iperf* tool, where the RTU was set as client and the Control PC as a server. The results of the DoS testing are shown in Table 3.

Table 3. Denial of Service Verification Results.

Attack Type	Attacker BW	Attacker PPS	ABW	AVG Delay	MAX Jitter	AVG Jitter	Loss
No attack	-	-	8.9 Mbps	1 ms	46 ms	1.3 ms	0%
SYN (hping3)	22.5 Mbps	46,894	76 Kbps	194 ms	1112 ms	230 ms	49.2%
FIN flood	25.1 Mbps	52,383	83 Kbps	188 ms	1114 ms	222 ms	51.7%
SYN FIN	27.1 Mbps	56,366	85 Kbps	254 ms	1575 ms	291 ms	54.2%
Push ACK	26.2 Mbps	54,564	81 Kbps	468 ms	1096 ms	358.3	53.7%
RESET	27.9 Mbps	58,030	84 Kbps	1.33 s	8196 ms	671 ms	67.8%
UDP flood	22.9 Mbps	47,696	75 Kbps	-	-	-	68.5%
Smurf	17.1 Mbps	35,516	4.9 Mbps	11 ms	257 ms	12.7 ms	0%
SYN (Metasploit)	1 Mbps	2113	8.9 Mbps	1.7 ms	244 ms	10.7 ms	0%

ABW—Available bandwidth for the smart grid communication; PPS—Packets Per Second.

Results show how much traffic the attacker was able to generate and its effect on the smart grid communication. Available bandwidth (ABW) shows amount of traffic available for legitimate communication (more is better). All the attacks except Smurf and SYN with Metasploit were able to severely disrupt the communication with consequences of making the RTU (and therefore the entire substation) unavailable for SCADA.

5.5.4. Other Usage

Our simulation model uses emulated communication (identical with real traffic) and can be therefore used to generate realistic traffic imprints, which can be used to configure and calibrate protection tools (such as firewalls and IPS), or for machine learning purposes. This data would be otherwise difficult to acquire in a production environment.

6. Conclusions

In this paper, we presented an approach for making smart grid networks more secure. The approach provides clear step by step guide, which can be easily used by stakeholders and each step can be clearly delegated to corresponding workers. Unlike the NIST's "Guidelines for Smart Grid Cybersecurity" [4], our approach is presented on a realistic use case and provides practical examples of implementation in Norwegian substations.

The approach starts with becoming familiar with the security pyramid and its generic sets of security objectives, threats and attack categories and threat and attack types at each of its layers in a top-down way. Next, given a specific DS and its assets, in a bottom-up way, specific threat and attack types, threat and attack categories and security objectives are identified and used in each of the steps of the approach such as threat analysis, threat modeling, risk assessment and impact simulations in order to create security awareness to the stakeholders of the specific DS through the demonstration of the simulations and classifications from the risk model. Only by following the presented approach, one can gain full security awareness from all aspects—threat analysis, threat modeling, risk assessment and impact simulation. Omitting one or more of the steps may result in an incomplete picture about the security situation, which can result in staying unaware of potential vulnerabilities and taking actions towards them.

Author Contributions: Conceptualization, S.Y.Y.; methodology, S.Y.Y.; software, F.H.; validation, M.A., A.G. and D.A.; formal analysis, M.A.; investigation, S.Y.Y, F.H., M.A., D.A. and A.G.; resources, S.Y.Y. and A.G.; data curation, F.H.; writing—original draft preparation, S.Y.Y, F.H., M.A., D.A. and A.G.; writing—review and editing, S.Y.Y. and F.H.; visualization, F.H. and S.Y.Y.; supervision, S.Y.Y.; project administration, S.Y.Y.; funding acquisition, S.Y.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the ECODIS and InterSecure projects funded by the Research Council of Norway under grant numbers RCN 296550 and RCN 296381, respectively.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ABW	Available Bandwidth
ACK	Acknowledgement
ARP	Address Resolution Protocol
CIA	Confidentiality, Integrity, Availability
CT/VT	Current/Voltage Transformer
DoS	Denial of Service
DS	Digital Substation
GPS	Global Positioning System
HMI	Human Machine Interface
HW	Hardware
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IoT	Interet of Things
IPS	Intrusion Prevention System
GOOSE	Generic Object-Oriented Substation Environment
LAN	Local Area Network
RCN	Research Council of Norway
NCIT	Non-conventional Instrument Transformers
NIST	National Institute of Standards and Technology
NSM	Network and Security Management
MAC	Message Authentication Code
MitM	Man-in-the-Middle
MMS	Manufacturing Message Specification
MU	Merging Unit
PASTA	Process of Attack Simulation and Threat Analysis
PPS	Packets Per Second
RAM	Random Access Memory
RTU	Remote Terminal Unit
SAS	Substation Automation Systems
SCADA	Supervisory Control and Data Acquisition
SeSV	Secure Sampled Values
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privilege
SG	Smart Grid
SMV	Sampled Measured Values
SV	Sampled Values
SW	Software
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VM	Virtual Machine
WAN	Wide Area Network

References

1. Csanyi, E. What Is the Digital Substation and What Makes it Digital? EEP—Electrical Engineering Portal. Available online: https://electrical-engineering-portal.com/digital-substation (accessed on 6 May 2022).
2. SINTEF, ECODIS—Engineering and Condition Monitoring in Digital Substations. Available online: https://www.sintef.no/en/projects/2019/ecodis/ (accessed on 6 May 2022).
3. Lnett, InterSecure. Available online: https://www.l-nett.no/fou-og-innovasjon/fou-prosjekter/intersecure (accessed on 6 May 2022).
4. NISTIR 7628 Rev. 1, Guidelines for Smart Grid Cybersecurity. Available online: https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final (accessed on 31 October 2022).
5. *IEEE Std C37.240-2014*; IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control System. IEEE Power and Energy Society; IEEE Press: New York, NY, USA, 2014.
6. Kwon, Y.; Lee, S.; King, R.; Lim, J.; Kim, H. Behavior Analysis and Anomaly Detection for a Digital Substation on Cyber-Physical System. *Electronics* **2019**, *8*, 326. [CrossRef]
7. Kolosok, I.; Korkina, E. Problems of Cyber Security of Digital Substations. In Proceedings of the VIth International Workshop 'Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security, Irkutsk, Russia, 17–24 March 2019; Atlantis Press: Amsterdam, The Netherlands, 2019; pp. 75–78. ISSN 1951-6851. [CrossRef]
8. Karnati, R. Security of Process Bus in Digital Substation. Master's Thesis, University of Michigan-Dearborn, Dearborn, MI, USA, 2020.
9. Hong, J.; Karnati, R.; Ten, C.W.; Lee, S.; Choi, S. Implementation of Secure Sampled Value (SeSV) Messages in Substation Automation System. *IEEE Trans. Power Deliv.* **2022**, *37*, 405–414. [CrossRef]
10. Ashraf, S.; Shawon, M.H.; Khalid, H.M.; Muyeen, S.M. Denial-of-Service Attack on IEC 61850-Based Substation Automation System: A Crucial Cyber Threat towards Smart Substation Pathways. *Sensors* **2021**, *21*, 6415. [CrossRef]
11. Hou, L.; Zhang, J.; Jin, N.; Zhu, M.; Li, Y. Digital substation cyber security analysis with SYN-flood attack as a simulation case. In Proceedings of the 2016 Chinese Control and Decision Conference (CCDC), Yinchuan, China, 28–30 May 2016; pp. 4467–4472. [CrossRef]
12. Zhang, J.; Zhang, J.; Zeng, P.; Li, Y.; Yang, C.; Jin, Y. Key Issues in Designing Cyber Security Proxy Gateways for Digital Substation Non-immune Bay Layers. In Proceedings of the 2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Honolulu, HI, USA, 31 July–4 August 2017; pp. 1309–1312. [CrossRef]
13. Nweke, L.O.; Wolthusen, S. A Review of Asset-Centric Threat Modelling Approaches. *Int. J. Adv. Comput. Sci. Appl. (IJACSA)* **2020**, *11*, 1–6. [CrossRef]
14. Holik, F.; Flå, L.H.; Jaatun, M.G.; Yayilgan, S.Y.; Foros, J. Threat Modeling of a Smart Grid Secondary Substation. *Electronics* **2021**, *11*, 850. [CrossRef]
15. Liu, R.; Vellaithurai, C.; Biswas, S.S.; Gamage, T.T.; Srivastava, A.K. Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid. *IEEE Trans. Smart Grid* **2015**, *6*, 2444–2453. [CrossRef]
16. Vallant, H.; Stojanović, B.; Božić, J.; Hofer-Schmitz, K. Threat Modelling and Beyond-Novel Approaches to Cyber Secure the Smart Energy System. *Appl. Sci.* **2021**, *11*, 5149. [CrossRef]
17. Sugwon, H. Cyber security strategies for substation automation systems and their implications. *Int. J. Smart Grid Clean Energy* **2019**, *8*, 747–756. [CrossRef]
18. Maëlle, K.Q. Cyber Security of the Smart Grid Control Systems: Intrusion Detection in IEC 61850 Communication Networks. Ph.D. Thesis, Université Grenoble Alpes, Grenoble, France, 2017.
19. Shailendra, F.; Anderson, R.J.; McGrath, K.; Hansen, K.T.; Alvarez, F. The Protection of Substation Communications. 2009. Available online: https://www.cl.cam.ac.uk/rja14/Papers/S4-2010.pdf (accessed on 7 May 2022).
20. Ishchenko, D.; Nuqui, R. Secure Communication of Intelligent Electronic Devices in Digital Substations. In Proceedings of the 2018 IEEE/PES Transmission and Distribution Conference and Exposition, Denver, CO, USA, 16–19 April 2018; pp. 1–5. [CrossRef]
21. Yuvaraj, N.; Lakpathi, M.; Mithun, T.P. Study and Analysis of Protection Scheme of Digital Substation Using IEC61850-9-2 Process Bus Technology (2019). *Int. J. Electr. Eng. Technol.* **2019**, *10*, 1–9. [CrossRef]
22. Talwar, S.; Loiselle, E.; Lambert, D.; Boutin, W.; Lavallee, M.; Sarubbi, F. Digital Transformation of Substation through IEC61850 Standard. CIGRE Canada. 2019. Available online: https://cigreconference.ca/papers/2019/CIGRE-190.pdf (accessed on 7 May 2022).
23. Elbez, G.; Keller, H.B.; Hagenmeyer, V. Authentication of GOOSE Messages under Timing Constraints in IEC 61850 Substations. In Proceedings of the 6th International Symposium for ICS and SCADA Cyber Security Research 2019 (ICS-CSR), Athens, Greece, 10–12 September 2019. [CrossRef]
24. Luyi, S.; Lang, S. *A Threat Modeling Language for Substation Automation Systems*; KTH, School of Electrical Engineering and Computer Science (EECS): Stockholm, Sweden, 2020.
25. Khodabakhsh, A.; Yayilgan, S.Y.; Houmb, S.H.; Hurzuk, N.; Foros, J.; Istad, M. Cyber-security gaps in a digital substation: From sensors to SCADA. In Proceedings of the 9th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 8–11 June 2020; pp. 1–4.

26. Dalipi, F.; Yildirim, S. Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016.
27. Abraham, D.; Yayilgan Yildirim, S.; Mohamed, A.; Gebremedhin, A.; Fisnik, D. Security and Privacy Issues in IoT-Based Smart Grids: A Case Study in a Digital Substation. In *Holistic Approach for Decision Making Towards Designing Smart Cities 2021*; Springer International Publishin: Cham, Switzerland, 2021; ISBN 978-3-030-85566-6.
28. Khodabakhsh, A.; Yayilgan, S.Y.; Abomhara, M.; Istad, M.; Hurzuk, N. Cyber-risk identification for a digital substation. In Proceedings of the 15th International Conference on Availability, Virtual, 25–28 August 2020.
29. Holik, F.; Abraham, D.; Yildirim Yayilgan, S. Emulation of IEC 60870-5-104 Communication in Digital Secondary Substations. In *Communications in Computer and Information Science*; Springer International Publishin: Cham, Switzerland, 2022; Volume 1616. [CrossRef]
30. Khodabakhsh, A.; Yayilgan, S.Y. Data Privacy in IoT Equipped Future Smart Homes. In Proceedings of the International Conference on Intelligent Technologies and Applications, Gjøvik, Norway, 28–30 September 2020; pp. 384–391. [CrossRef]
31. ScienceDirect, Manufacturing Message Specification. Available online: https://www.sciencedirect.com/topics/engineering/manufacturing-message-specification (accessed on 6 May 2022).
32. Conklin, L. Threat Modeling Process. Available online: https://owasp.org/www-community/Threat_Modeling_Process (accessed on 6 May 2022).
33. McCabe, J. *9—Security and Privacy Architecture, Network Analysis, Architecture, and Design, 3rd ed.*; Morgan Kaufmann: Saint Louis, MO, USA 2007; pp. 359–383. ISSN 18759351, ISBN 9780123704801. [CrossRef]
34. Shevchenko, N. Threat Modeling: 12 Available Methods. Software Engineering Institute Blog. Available online: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/ (accessed on 6 May 2022).
35. Shevchenko, N.; Chick, T.; O'Riordan, P.; Scanlon, T.; Woody, C. *Threat Modeling: A Summary of Available Methods*; White Paper, CMU; Software Engineering Institute: Pittsburgh, PA, USA, 2018.
36. O'Connor, A. Security Risk Assessments and Threat Modelling, and Why We Do Both—LinkedIn. Available online:https://www.linkedin.com/pulse/security-risk-assessments-threat-modelling-why-we-do-both-o-connor (accessed on 6 May 2022).
37. Harvey, M.; Long, D.; Reinhard, K. Visualizing NISTIR 7628, Guidelines for Smart Grid Cyber Security. In Proceedings of the 2014 Power and Energy Conference at Illinois (PECI), Champaign, IL, USA, 28 February–1 March 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 1–8. [CrossRef]
38. Blank, R.M.; Gallagher, P.D. *Guide for Conducting Risk Assessments*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2012. [CrossRef]