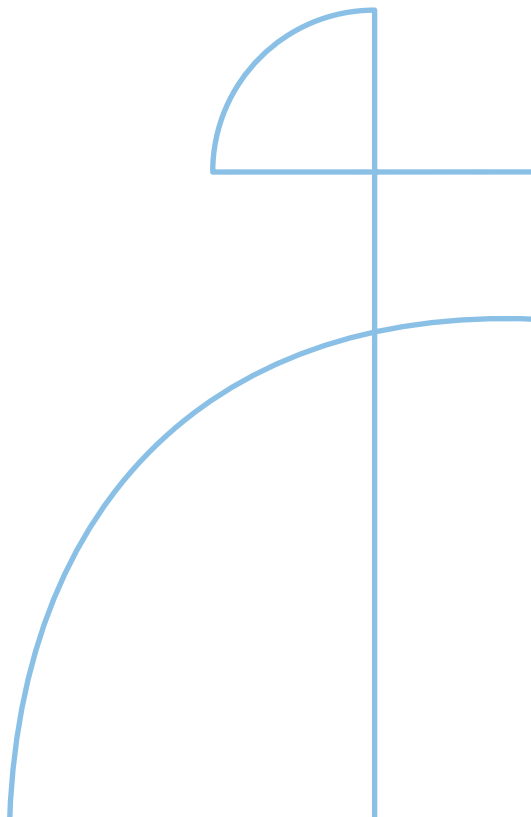
Doctoral Thesis in Electrical Engineering

Cyber Security Threat Modeling of Power Grid Substation Automation Systems

ENGLA RENCELJ LING

KTH ROYAL INSTITUTE OF TECHNOLOGY



Cyber Security Threat Modeling of Power Grid Substation Automation Systems

ENGLA RENCELJ LING

Academic Dissertation which, with due permission of the KTH Royal Institute of Technology, is submitted for public defence for the Degree of Doctor of Philosophy on Thursday the 5th of June 2025, at 9:30 a.m. in U1, Brinellvägen 26, Stockholm.

Doctoral Thesis in Electrical Engineering
KTH Royal Institute of Technology
Stockholm, Sweden 2025

ISBN: 978-91-8106-286-1
TRITA-EECS-AVL-2025:53

Printed by: Universitetsservice US-AB, Sweden 2025

I Abstract

The substation is a vital part of the power grid and serves to aid in the distribution of electricity by, for example, transforming from high to low voltage. It is essential to protect the substation as a loss of electricity would cause severe consequences for our society. The Substation Automation System (SAS) allows for remote management and automation of substations but also creates possibilities for cybersecurity threats. In this thesis efforts towards using threat modeling to assess the cybersecurity of SAS are presented. Threat modeling entails creating a model of the system that shows the possible cybersecurity threats against it. To reach this goal, previously used information sources for threat modeling in the power systems domain are found. The thesis also includes the creation of a Time-To-Compromise (TTC) estimate for cyber attacks against Industrial Control Systems. By estimating the TTC, it is possible to prioritize which attacks to defend against. One method of creating threat models is by using threat modeling languages in which the assets, associations, attacks, and defenses have been defined. In this thesis, a threat modeling language for creating threat models of SAS is presented. The threat models in this thesis are used to create attack graphs to show the possible paths an attacker could take throughout the system. The work of this thesis also consists of evaluation of threat modeling languages that have been created or used. As a result, accurate assessment of cybersecurity for SAS can be made that helps in the efforts to keep them secure against cyber attacks.

Keywords
Threat Modeling, Cybersecurity, Power systems, Substation Automation Systems, Attack graphs, Industrial Control Systems

II Sammanfattning

Transformatorstationen är en viktig del av elkraftnätet och dess roll är att hjälpa till med distributionen av el genom att som dess namn beskriver transformera om spänningen. Det är nödvändigt att skydda transformatorstationen eftersom ett elavbrott skulle skapa stora konsekvenser för vårt samhälle. Ett automatiserat transformatorstationssystem gör det möjligt att hantera den externt men det öppnar även upp möjligheterna för cybersäkerhetshot. I den här avhandlingen presenteras forskning kring användning av hotmodellering för att utvärdera cybersäkerheter för SAS. Hotmodellering innebär att man skapar en modell av systemet som visar möjliga cybersäkerhetshot mot det. För att nå det målet har informationskällor för hotmodeller inom kraftnätsdomänen sammanställts genom en systematisk litteraturstudie. I avhandlingen tas det också fram ett sätt att räkna ut tiden det tar för att framgångsrikt genomföra en cyberattack mot industriella kontrollsystem. Hotmodeller kan skapas genom att använda hotmodelleringsspråk inom vilket komponenterna, relationerna, attacker och försvar är definierade. I den här avhandlingen skapas ett hotmodelleringsspråk för att skapa hotmodeller av SAS. Hotmodellerna i detta arbete kan användas för att skapa attackgrafer som visar möjliga vägarna som en attackerare skulle kunna ta genom systemet. Arbetet utvärderar även hotmodelleringsspråken som har använts eller skapats. Som ett resultat av denna avhandling kan korrekta utvärderingar av cybersäkerhet för SAS göras vilket hjälper i arbetet av att hålla dom säkra mot cyberattacker.

Nyckelord
Hotmodellering, Cybersäkerhet, Energisystem, Automatiserade transformatorstationssystem, Attackgraf, Industriella kontrollsystem

III Acknowledgments

Thank you to my excellent supervisor Mathias Ekstedt for helping me slow down and dig deeper into the research challenges of this thesis. We have had many long discussions and without these, this thesis would not have been possible. Thank you also to my second supervisor Lars Nordström for teaching me the basics of the intricate world of energy systems and for helping me with contacts and information within the field. Thank you to Robert Lagerström for the support in the very beginning of my thesis.

Thank you to Pontus Johnson for introducing me to the world of hacking and for trusting me with responsibilities within your course. Thank you Patrik Hilber for your advance review and helpful comments. Sotirios Katsikeas, Jakob Nyberg and Viktor Engström, thank you for all the interesting discussions and I have truly enjoyed working with you in the hacking course. Thank you also to the people who I could look at as great examples, Simon Hacks, Wenjun Xiong and Andrei Butun. To my research colleagues and experts in the industry, thank you for your valuable insights.

Thank you to my friends and family who have listened to me talk about this "security stuff" over the years and for reminding me why I am doing it. Thank you mum and dad, you are an inspiration and seeing your passion in your individual fields motivated me to find my own. I am grateful to you and my siblings for your support, it means the world to me. Last but most importantly, thank you to my amazing wife and beautiful kids. You have been a welcomed distraction and a wonderful support! I love you all immensely.

IV List of publications

Papers included in this thesis:

Paper A: Engla Ling, Robert Lagerström and Mathias Ekstedt, A systematic literature review of information sources for threat modeling in the power systems domain, in Critical Information Infrastructures Security, CRITIS 2020, Lecture Notes in Computer Science, vol. 12332, Springer, Cham, pp. 47-58.

Paper B: Engla Rencelj Ling and Mathias Ekstedt, "Estimating the Time-To-Compromise of Exploiting Industrial Control System Vulnerabilities," in Proceedings of the 8th International Conference on Information Systems Security and Privacy - ICISSP, 2022, pp. 96-107.

Paper C: Engla Rencelj Ling and Mathias Ekstedt, Estimating Time-To-Compromise for Industrial Control System Attack Techniques Through Vulnerability Data, SN Computer Science, vol. 4, no. 318, 2023.

Paper D: Engla Rencelj Ling and Mathias Ekstedt, A threat modeling language for generating attack graphs of substation automation systems, International Journal of Critical Infrastructure Protection, vol. 41, no. 100601, 2023.

Paper E: Sotirios Katsikeas, Engla Rencelj Ling, Pontus Johnsson and Mathias Ekstedt, Empirical evaluation of a threat modeling language as a cybersecurity assessment tool, Computers & Security, vol. 140, no. 103743, 2024.

Paper F: Engla Rencelj Ling and Mathias Ekstedt, “Application and Evaluation of a Substation Threat Modeling Language for Automatic Attack Graph Generation”, Camera-ready submission, accepted to IEEE International Conference on Cyber Security and Resilience (CSR), 2025.

CRediT author statements:

Paper A*:* Engla Ling: Conceptualization, Methodology, Formal analysis, Investigation, Data Curation, Writing - Original Draft, Writing - Review & Editing, Visualization. Robert Lagerström: Methodology, Resources, Writing - Review & Editing, Supervision. Mathias Ekstedt: Supervision, Funding acquisition.

Papers B, C, D and F: Engla Rencelj Ling: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Data Curation, Writing - Original Draft, Writing - Review & Editing, Visualization. Mathias Ekstedt: Conceptualization, Methodology, Writing - Review & Editing, Supervision, Funding acquisition.

Paper E: Sotirios Katsikeas: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Writing - Original Draft, Writing - Review & Editing, Visualization. Engla Rencelj Ling: Conceptualization, Methodology, Software, Validation, Investigation, Writing - Original Draft. Pontus Johnson: Conceptualization, Methodology, Validation, Writing - Review & Editing, Supervision, Project administration, Funding acquisition. Mathias Ekstedt: Conceptualization, Methodology, Validation, Writing - Review & Editing, Supervision, Project administration.

Papers not included in this thesis:

Paper G: Engla Rencelj Ling, Jose Eduardo Urrea Cabus, Ismail Butun and Robert Lagerström, "Securing Communication and Identifying Threats in RTUs: A Vulnerability Analysis," in ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security, 2022.

Paper H: Engla Rencelj Ling and Mathias Ekstedt, "Generating Threat Models and Attack Graphs based on the IEC 61850 System Configuration description Language," in Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, 2021.

Paper I: Simon Hacks, Sotirios Katsikeas, Engla Ling, Robert Lagerström, "powerLang: a probabilistic attack simulation language for the power domain," Energy Informatics, vol. 3, no. 1, 2020.

Paper J: Simon Hacks, Sotirios Katsikeas, Engla Rencelj Ling and Wenjun Xiong, "Towards a Systematic Method for Developing Meta Attack Language Instances," in Enterprise, Business-Process and Information Systems Modeling 23rd International Conference, BPMDS 2022 and 27th International Conference,

EMMSAD 2022, Held at CAiSE 2022, Leuven, Belgium, June 6–7, 2022, Proceedings, 2022, pp. 139-154.

Paper K: Xinyue Mao, Mathias Ekstedt, Engla Ling, Erik Ringdahl and Robert Lagerström “Conceptual Abstraction of Attack Graphs - A Use Case of securiCAD”, Graphical Models for Security, GraMSec 2019, Lecture Notes in Computer Science, vol 11720, pp. 186-202.

V List of abbreviations

CB	Circuit Breaker
CPS	Cyber-Physical System
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DoS	Denial of Service
DSL	Domain-Specific Language
FDI	False Data Injection
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
ICS	Industrial Control System
ICT	Information and Communications Technology
IT	Information Technology
HMI	Human-Machine Interface
LD	Logical Device
LN	Logical Node

MAL	Meta Attack Language
MITM	Man-In-The-Middle
MMS	Manufacturing Message Specification
MTTC	Mean Time-To-Compromise
MU	Merging Unit
OT	Operational Technology
PLC	Programmable Logic Circuit
RTU	Remote Terminal Unit
SAS	Substation Automation System
SCD	Substation Configuration Description
SCL	Systems Configuration Language
SLR	Systematic Literature Review
SMV	Sampled Measured Value
SV	Sampled Value
TTC	Time-To-Compromise

CONTENTS

List of Figures

1 Introduction

In this thesis, research towards using threat modeling to assess the cybersecurity of the Substation Automation System (SAS) is presented. As seen in Figure 1, this thesis combines research in the three, somewhat overlapping, domains of cybersecurity, industrial control systems and threat modeling. In threat modeling, the knowledge that is learnt about the cybersecurity of a system is used to assess the threats against it. Threats in cybersecurity are intended to maliciously compromise a system, often to disrupt or steal information. The different contributions of this thesis focus on several topics within these domains.

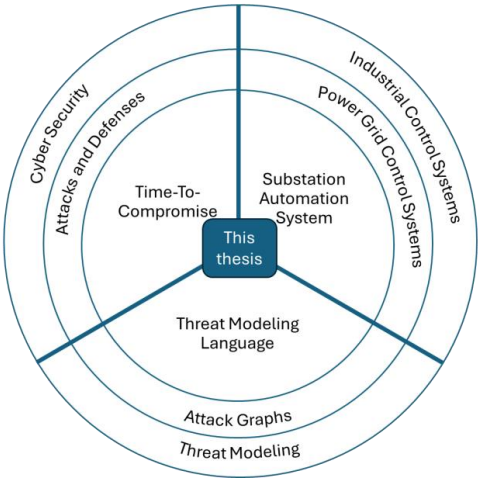


Figure 1: The three domains that this thesis combines, from broad to more specific topic.

This section will give motivation to why it is crucial to protect the SAS against cyber attacks and why this thesis focuses on the SAS. The reasons why the assessment method of threat modeling is used are also motivated. The introduction will thereafter outline the research questions and give a summary of the included papers of this thesis. Lastly, the outline for the remaining part of the thesis is given.

1.1 Motivation

In today's society we are reliant on electricity for all basic needs and necessities. Without a functioning electric grid, we cannot distribute electricity to run our hospitals and clean our water, among other critical infrastructures that are important for our sustainability. Before digitalization, the only way to maliciously shut down the electric grid would be to gain access and physically damage it. The electric grid consists of many substations and these substations can both transform voltage and include protection mechanisms in case of malicious or operational faults. There is a pressing need to protect the electric grid against cyber attacks because the modern substation has been digitalized, and many cybersecurity vulnerabilities exist for the power supply domain [1]. The energy sector appears to be an especially vulnerable target to cyber terrorism [2] and have been subjected to several attacks [3], [4]. In 2015, substations in Ukraine were attacked and around 225,000 customer lost electricity in the winter for several hours [5]. There are types of attacks against the energy sector that do not cause disruption of electricity, but instead these are data theft or ransomware attacks [6]. This thesis focus on research in the domain of Industrial Control Systems (ICS) because of the large number of threats against it and because of its large threat landscape [7], [8]. There are many reported number of vulnerabilities of ICS [9], [10] and the vulnerabilities exist in every domain within ICS [11].

Within the domain of ICS, power systems are arguably the most important critical infrastructures since they in many ways support other critical infrastructures. Substations are essential parts of the electric grid and there are different types of substations that serve different roles, such as distribution or transmission. The substations can be located in geographically difficult to reach locations, which is one reason for the need to automate and remotely manage them. With the digitalization of substations, it becomes more difficult to protect them against cybersecurity threats as they are often connected to an external network. SAS is a broad term, but the research in this thesis aligns to

the widely adapted standard IEC 61850, which defines the communication of the Intelligent Electric Devices (IEDs) that enables automation of substations.

The motivation to focus specifically on ICS compared to traditional enterprise networks implies that there is indeed a difference between the two in terms of cybersecurity. ICS is a category within Operational Technology (OT) whereas enterprise networks are categorized as Information Technology (IT). These different technologies often consist of different protocols and architectures. OT is increasingly becoming more similar to IT, but there are still many differences, for instance when considering different requirements and constraints [12]. For example, OT systems are time-critical and have high requirements on availability. They may also consist of components with limited processing power and exist in remote locations. During this transition towards systems more similar to IT there is often a combination of legacy and new equipment, which poses challenges in assessing overall security.

Threat modeling is a proactive way of assessing cybersecurity by creating a model of the different possible threats against a system. One main task of the method is to gather information regarding the assets and associations of these. Another task is to find the different cyber attacks and defenses that exist for each of the assets of the system. Even though threat modeling has been around for many years, it is still immature in many ways and has many challenges, such as a more structural approach [13]. To have a more structural approach, in this thesis the choice was made to create threat models by using threat modeling languages based on the Meta Attack Language (MAL) framework [14]. This allows for a more systematic and scalable approach that enables many threat models to be created with the same threat modeling language. In this research the focus is also on evaluation of the threat modeling languages to improve their trustworthiness and to show that they can produce accurate threat models. In the field of threat modeling there is a lack of evaluations [13]. It can be difficult to prioritize which threats to defend against by knowing which attack would be the fastest for an attacker to succeed with. This is why this thesis introduces an estimate of Time-To-Compromise for the ICS domain. Considering that resources are limited when it comes to cybersecurity defenses, it helps to know the more imminent attacks so that priorities can be set, and one can focus on assigning resources there first.

1.2 Research Questions

This thesis studies the following three research questions:

RQ1: What are the possible cyber attacks against digital substations and how can this information be included in threat models and attack graphs for cybersecurity assessment of substations?

RQ2: How can already existing configuration information of digital substations be used to automatically create threat models and generate attack graphs for cybersecurity assessment?

RQ3: Is the threat modeling language, which is used to generate attack graphs based on system models, correct?

By performing literature reviews and by creating a method of estimating the TTC of Industrial Control System attack techniques as well as a threat modeling language, Papers A, B, C and D include work to answer the first question. The second question is the focus on answering in Papers D and F. In Paper D a threat modeling language for SAS is developed, called sasLang. sasLang is an extension of the threat modeling language coreLang. In Paper F sasLang is applied by automatically creating threat models based on configuration files. The third question of evaluation is the focus on Papers E and F where coreLang and sasLang are evaluated.

1.3 Summary of the Included Papers

This thesis is a compilation of six research papers, three of which have been accepted to conferences and three that have been published in journals. Figure 2 shows an overview of the included papers and how they are related. Paper A is a systematic literature review where different information sources that have been used to create threat models in the power systems domain are found. In this paper the different options are discussed and the knowledge gained is used when continuing the research in the next papers. In Paper B, one part of threat modeling is the focus, which is the time that it takes to succeed with an attack, the Time-To-Compromise (TTC). The estimation of TTC is created for the Industrial Control Systems (ICSs) instead of aligning it to the narrower domain of power systems. In Paper C, TTC_{ICS} is applied by presenting a method of estimating the TTC per attack technique. The core contribution of this thesis, the threat modeling language sasLang, is presented in Paper D. In Paper E the threat modeling language coreLang is evaluated, which is a foundational language that sasLang is built on. The evaluation of threat modeling languages is continued in Paper F where sasLang is applied and evaluated.

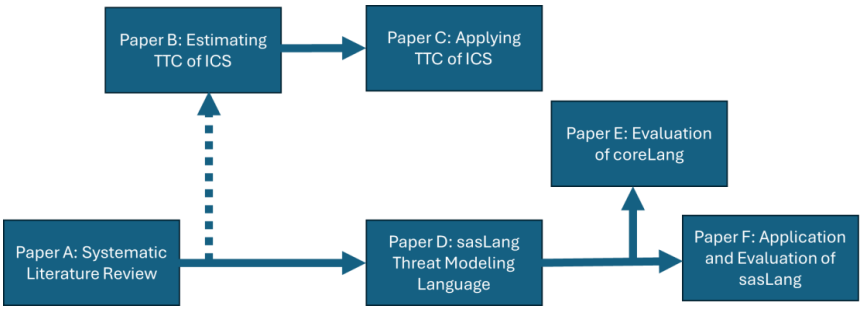


Figure 2: Overview of how the included papers of this thesis are related.

1.4 Thesis Outline

In the first part of this thesis, the introduction, background, method, contributions, conclusions and future work of the included papers are given. The second part consists of the six papers that are included in this thesis.

2 Background

In this chapter the necessary background for the included papers is described. The thesis touches on three domains: cybersecurity, threat modeling and industrial control systems with specific focus on the substation automation system. The last section of this chapter gives an overview of the related work.

2.1 Electrical Substations

The electric grid distributes electricity across large geographical locations with high voltage power lines. In this thesis the focus is not on a specific type of electric substation as there are not many differences between them in terms of cybersecurity because their main differences lie with the primary equipment [15]. An electric substation includes several types of primary equipment which is physically located in what is called the switch yard of the substation. This primary equipment is, for example, the transformer that transforms voltage from high to low, or vice versa. There are also circuit breakers that can be opened to prevent the current, or closed to allow the flow. The flow can be controlled in both normal operations and for protection purposes if there is, for instance, an overcurrent.

2.2 Substation Automation Systems

A Substation Automation System (SAS) includes cyber physical components and several different communication protocols. These components and protocols are the Operational Technology (OT) of the substation, in contrast to the Information Technology (IT) of enterprise networks. SAS is created by adding Intelligent Electronic Devices (IEDs) to the electric substation that can

provide input and output to enable digitalization [16]. It is possible to structure a SAS in numerous ways and one of these ways is shown in Figure 3. Common to all topologies are the distinct levels of substation, bay and process. It is also common to place management, Human-Machine-Interaction (HMI) and data logging processes on the substation level. Generally, the gateway to a centralized Control Center (CC) would be placed on the station level. For example, SCADA (Supervisory Control And Data Acquisition) can control a substation or send data for collection to either a microSCADA residing within the substation or to a centralized SCADA, which is placed externally in a CC. A CC can control multiple substations in a region. SCADA is a system that is commonly used to remotely manage industrial processes. There are also cases where a gateway is placed on the bay level, and this allows the bay level to directly send data to the CC. On the bay level, the Intelligent Electronic Devices (IEDs) that protect and automate the substation are placed. Depending on the level of digitalization, the process level can vary. In some cases, as seen in Figure 3, the process level consists of the sensors, actuators, and Merging Units (MUs). The sensors pick up on changes, for example in temperature and the actuators can receive digital instructions to perform physical changes, such as opening a circuit breaker. The MUs can be used for collecting and summarizing data to be sent up to the IEDs.

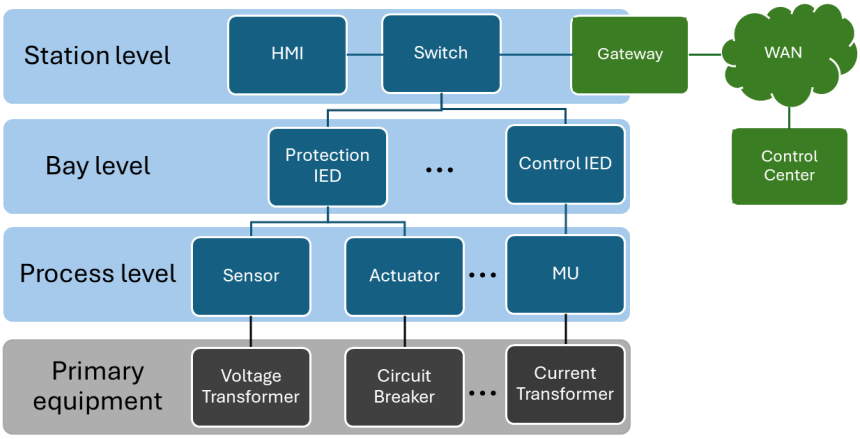


Figure 3: A simplified and typical topology of a digital substation.

In other topologies, there are Input/Output (I/O) IEDs on the process level connected directly to the primary equipment. There may also be primary equipment placed on the process level. The functionality is the same, but the

topology varies depending on where the functionality is placed considering, for example, how digital the primary equipment is.

This thesis focuses on digital substations according to the widely adapted standard IEC 61850 [17]. The protocol defines the communication protocols of the substation IEDs. The standard includes the Systems Configuration description Language (SCL) that is designed to describe the configuration of the IEDs. There are six types of SCL files and one of these, where a substation is defined, is the Substation Configuration Description (SCD) file. Before the standard was introduced in 2003, there were several efforts to digitalize the substation but without a standard it was challenging to combine different vendor products in the same substation and to share information regarding the configuration of the substation.

The IEDs are a main component of a SAS and they are configured to communicate between themselves and share information to automate processes. For instance, the process to trip a circuit breaker to protect the equipment from damage can be automate. The IEDs communicate by sending data via Logical Nodes (LNs). LNs can be combined into Logical Devices (LDs) to represent functions or equipment in the substation. The LDs are hosted on Servers on the IEDs to allow for communication outside of its local subnetwork. Figure 4 shows how the architecture of the IED is set up according to IEC 61850.

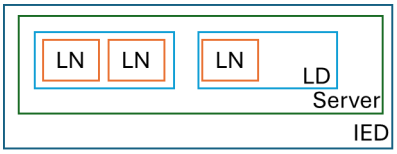


Figure 4: Logical Nodes residing in the IED.

IEC 61850 defines three different communication protocols. MMS (Manufacturing Message Specification) protocol is used for communication between the IEDs and also to communicate upwards to the HMI. GOOSE (Generic Object Oriented Substation Event) is used also used for communication between the IEDs, but is a faster publisher/subscriber type protocol that is used for sending status or control signals. Lastly, SV (Sampled Values) is used for communicating current and voltage samples to the IED.

2.3 Cybersecurity of Digitalized Substations

According to IEC, IT standards are not appropriate for defining cybersecurity in the OT domain and this was the motivation for the creation of the IEC 62443 standards [18]. Two of the reasons IT cybersecurity standards are not applicable is that the ICS devices may be limited to only serving their intended tasks so they cannot also perform security tasks and latency introduced by firewalls may be too high [19]. The IEC 62443 series of standards include best practices both from a technical perspective, but also other topics, such as training of employees.

The standard IEC 61850, which defines the communication of IEDs of electric substations, does not include security measurements but instead these have been defined in the standard IEC 62351 [20]. IEC 62351 extends IEC 61850 by adding security measures, such as, encryption and authentication of the communication protocols. There are, however, challenges in these since the encryption system suggested increases the execution time over the maximum, which also stated in the standard, so other approaches may be required [21]. Without such security measures, the digital substation is vulnerable to, for instance, False Data Injection (FDI), Man-In-The-Middle (MITM) or replay attacks [22]. The substation is also vulnerable to Denial of Service (DoS), password cracking and eavesdropping attacks [23]. It is also evident that more sophisticated advanced persistent threat (APT) attacks, that may combine multiple of these types of attacks, are increasing [24]. Another type of attack that can be used to gain access to substations is social engineering attacks where people are targeted and exploited to, for instance, trick them into clicking on a malicious link or providing their login credentials. This is the case of a substation web server phishing attack [25]. In this attack, a malicious website mimicking the substation web server is set up, which tricks the user to attempt to login. By attempting to login, the attacker gains access to the login credentials and can use these on the real website.

An attacker's main goal, according to the work by Hussain et. al., is to disrupt the substation by either attacking the communication within the substation or the HMI controlling it [26]. The substation can be accessible externally via a network to allow for remote management and control. This connection would typically be over a Virtual Private Network (VPN) tunnel to provide a secure connection over the Internet, or over a private WAN. In some cases, the substation OT network is connected to the business IT network. A substation

can also be subjected to external threats because an engineer uses an external laptop within the substation.

2.4 Threat Modeling

Threat Modeling is the process of modeling the potential threats against a system but there are many variations of the method and there is no common definition [27]. Common to all methods is, however, to proactively define the threats to gain knowledge to secure the system. Two of the most common approaches of threat modeling is STRIDE [28] [29] and PASTA [30] [31]. STRIDE stands for Spoofing, Tampering, Repudiation, Information Closure, Denial of Service and Elevation of Privilege. These are the categories of threats that are considered, and the division helps to both identify the threats and to discuss them. PASTA stands for Process for Attack Simulation and Threat Analysis. With PASTA, seven steps are followed to also include the aspect of business impact of the threats. Some of these steps are often found in other types of threat modeling methods, such as defining the object and scope of the threat model and performing a threat analysis.

To identify the threats of a system one first needs to model the system. The model of the system is often a small part or simplified version of the entire system. This is because systems, such as the Substation Automation Systems of this thesis, are often complex and it can help to focus on different parts at a time. This system model can be graphical and described with a Data Flow Diagram (DFD). This is the method used in the STRIDE threat modeling approach. The systems model can, in comparison, also be described mathematically or in text form. DFDs are often used because they are simple to work with and easy to understand, but there are several shortcomings to consider when using solely DFDs in threat modeling [32]. Sion et. al. finds that the DFD is not sufficient for threat modeling as they cannot sufficiently express security concepts, data types, dependencies of security properties and deployment information. The authors instead suggest using a modeling language to include information regarding the security and threats aspects of the system that cannot be described by a DFD, which is also the approach used in this thesis.

Another way of illustrating a system is with a Unified Modeling Language (UML) diagram as seen in Figure 5. In this example, the model includes **Network** that can be connected to **Computer**. **Computer** stores **Secret**. Each box represents an asset, and the arrows represent the association

between these. The associations follow the UML class diagram notation [33] and here they are bi-directional. The "*" indicates that there can be many assets. The same example is used to describe the threat model, attack graph and threat modeling language further on in this chapter.

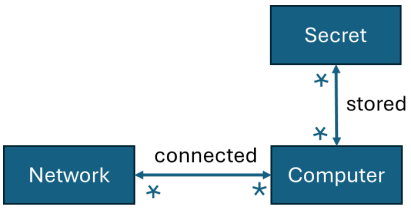


Figure 5: An example of a UML diagram.

Figure 6 shows an example of a system threat model. In this example, there are **SecretY** stored on **ComputerC** and **SecretX** stored on **ComputerD**. **ComputerA** and **ComputerB** are connected to **Network1**. **ComputerB**, **ComputerC and Computer D** are connected to **Network2.**

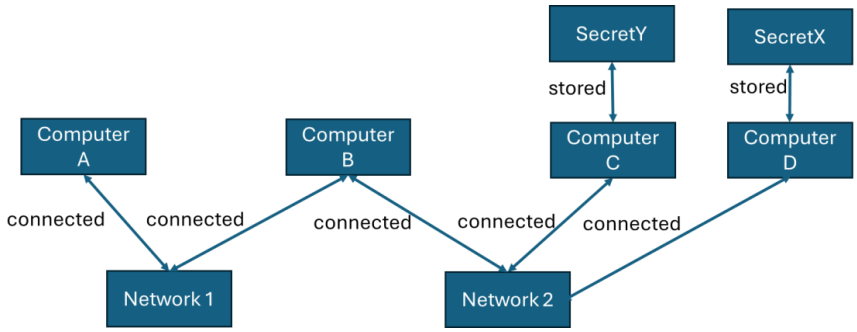


Figure 6: An example of a threat model.

2.5 Attack Graphs

An attack graph shows possible attack paths that an attacker could take throughout a system. The attack graph was first introduced by Philips and Painton Swiler as an approach to network vulnerability analysis [34]. A simpler version of an attack graph is the attack tree [35]. The nodes of the attack graph represent different attacks, and they are connected to show the relation between them. The root node of the tree is the goal of an attacker, and the attack steps are illustrated as the leaf nodes. If an attack step is reached by an "AND" attack step, it means that all the previous attack steps leading to the "AND" attack step must have been successfully reached. If the attack is reached

by an “OR“ attack step, only one of the previous attack steps leading to the “OR” attack step must have been performed successfully. According to Schneider, the nodes of the tree can be assigned with values to provide insights into, for example, how expensive the attack steps are. The addition of defenses to the attack tree was added by Kordy et. al. [36] and there have been many contributions in creating cyclic attack trees, called attack graphs [37]. An example of an attack graph is shown in Figure 7. This example is the same as the threat model shown in Figure 6. The attacker can after using the starting point *compromise* on **ComputerA** *find* **SecretX** since the *login* defense is not enabled on **ComputerB** and **ComputerD**.

Attack graphs can be added with further information, such as the probability that an attack step is successful, the probability that a defense is implemented or the time taken for an attack. In this thesis the research is on the Time-To-Compromise (TTC). TTC is defined as “time needed for an attacker to gain some level of privilege *p* on some system component *i*.” (McQueen et. al., 2006). In the MAL framework, that is used in this thesis to define the threat modeling language, the TTC can be specified per attack step and is not necessarily related to privileges. Estimating the TTC requires knowledge regarding how to score vulnerabilities [38], which includes the question regarding the exploitability of the vulnerabilities [39].

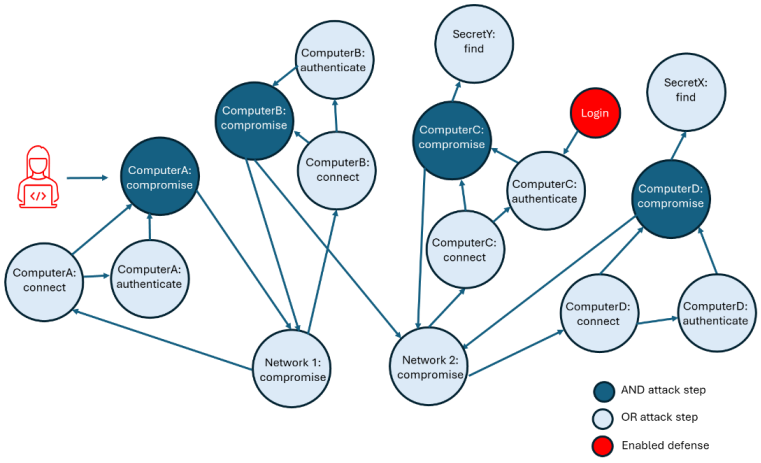


Figure 7: An example of an attack graph.

There are numerous works with attack graphs that can be generated automatically since creating accurate attack graphs by hand can be time consuming and challenging [40] [41]. There is also works that use a model

based approach, which solves the issue of attack graphs where any existing vulnerability is assumed to be exploitable [42] [43]. This is the approach that is used in this thesis by using the MAL framework [14].

Once the attack graph has been created or generated, one can run simulations and graph algorithms to further analyze it. For example, it is possible to find the shortest path or to compare the likelihood of different paths. For this purpose, different probability distributions can be used[1].

2.6 Meta Attack Language

A threat modeling language is used to describe the assets, association between the assets, attack steps and defenses that exist for a system. By defining the constraints of how any system could look like in the language, it is easier to create threat models without having to define the system again. This would allow a user that is not familiar with the details regarding attacks and defenses to create a threat model of their system. In this thesis, the research on threat modeling languages is based on a framework to write threat modeling languages called the Meta Attack Language, MAL [14], [44]. A metalanguage is a language that describes another language. In the MAL framework, the syntax and semantics used to create threat modeling languages are defined. The MAL formalism also allows for the generation of attack graphs. There are several languages that has been written within the framework, for instance: vehicleLang [45], SCL-Lang [46], coreLang [47] and powerLang [48]. These threat modeling languages can be extended following the object-oriented design paradigm, which makes it possible to use previous work to build new languages [49]. The languages can be extended in the sense of re-using a previously defined language and adding additional assets, associations, attacks and defenses to it. In the extension, it is possible to override previously defined attack steps if it is required.

In Figure 8 an example of a MAL specification of a language is shown to describe the UML diagram in Figure 5. The attacker needs to both *connect* and *authenticate* on **Computer** to *compromise* it. *Authenticate* is protected by the *login* defense and if the defense, the attacker is unable to *authenticate*. Once

[1] Supported distribution functions, https://github.com/mal-lang/malcompiler/wiki/Supported-distribution-functions, Accessed 27 March 2025

Computer is compromised, the attacker can *connect* to the **Network** to move to **Computer** and *find* ***Secret*.**

```
asset Secret {
    | find
}
asset Computer {
    | connect
        -> authenticate,
           compromise
    | authenticate
        -> compromise
    # login
        -> authenticate
    & compromise
        -> computerNetwork.compromise,
           storedSecret.find
}
asset Network {
    | compromise
        -> participant.connect
}
associations {
    Secret [storedSecret] * <-- stored --> * [computerStorage] Computer
    Network [computerNetwork] * <-- connected --> * [participant] Computer
}
```

Figure 8: An example of a MAL specification.

This MAL specification includes three assets and two associations. The attack steps in this example are either of type "OR" or "AND" as indicated by the "|" and "&" symbols. If there is an arrow "->" below an attack step, this indicates the next attack step. There are attack steps that exist between assets. For example, the attack step *compromise* on **Network** leads to the attack step *connect* as part of the **Computer** asset. Defenses, "#", can have Boolean values of true or false. A Bernoulli distribution can be assigned for the likelihood of this value. More details regarding the syntax of MAL can be found in the MAL documentation[2]

Figure 9 gives an overview of how the language described in the MAL specification is used to create an instance model of a system. The MAL specification contains a description of the entire system in terms of assets, associations, defenses and attack steps. The instance model is created to illustrate a specific scenario. The instance model is used as input to generate an

[2]MAL Syntax, https://github.com/mal-lang/mal-documentation/wiki/MAL-Syntax, Accessed 27 March 2025

attack graph showing the possible paths that an attacker may take in that specific system.

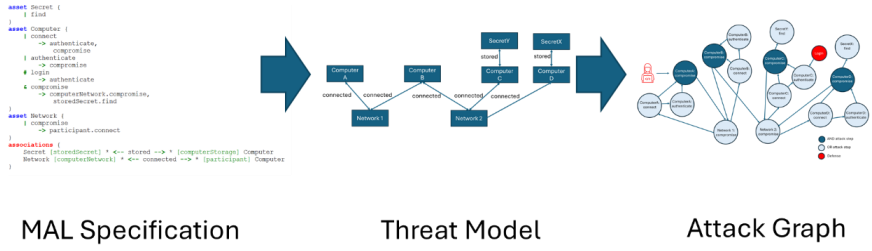


Figure 9: The MAL specification is used for creating a threat model, which can be used as input to create an attack graph.

2.7 Related Work

The related work for the overall research topic of this thesis is summarized in this section. Further related work is described in each of the included papers. To begin with, related work to this thesis includes a similar systematic literature review to gather information regarding threat modeling, but for ICS [50]. There is also work reviewing different methods of how to perform risk or vulnerability assessments for SCADA [51], [52], but not for SAS as is done in this thesis. To help with assessing the cybersecurity of ICS, the knowledgebase the MITRE ATT&CK for ICS [53] was created, which is also used in the research of this thesis as described in Chapter 3. Other works also make use of this knowledgebase by mapping OT-related cyber attacks to it [54] or using it to automatically generate attack sequences [55]. It is also used in the work of a modeling tool for cyber attacks on smart energy systems, SecuriDN, which uses an adaptation of MAL [56]. The tool can produce both attack graphs and dynamic Bayesian networks.

In researching related work, no other work that produces threat modeling languages to create threat models and attack graphs for SAS was found. Related work is a domain specific modeling language used for describing the standard IEC 62443 [57]. The domain specific modeling language is used for modeling the architecture of a system that is IEC 62443 compliant but cannot be used for threat modeling or attack graphs. Other related work is STRIDE threat modeling for CPS [58], the modeling of supply chain attacks in IEC 61850 substations [59] and hybrid attack graphs to model both the cyber and physical components of the smart grid [60]. This related work of threat modeling and attack graphs do not include the notion of a threat modeling

language, which is a central contribution in this thesis. In attack graphs used for security monitoring of substations, the authors, similar to the work in this thesis, use the information found in SCL files to create the attack graphs [61]. They also, in contrast to the work in this thesis, use dynamic information from, for example, log files and load on transmission lines.

3 Method

The details regarding the research methods can be found in the included papers of this thesis. In this section a summary to provide more background and context to the research methods used in those papers is given. First Design Science Research, DSR, is introduced which has been used as a guideline for the overall research of this thesis. Then the software tools that have been used during the development of the artifacts in Papers D, E and F are described. Papers B and C make use of databases or matrices with vulnerabilities, exploits and attacks and these are summarized at the end of this chapter.

3.1 Design Science Research

Design Science Research is a method of designing an artifact to conduct research [62]. This is the research approach that was followed when creating sasLang as a core contribution of this thesis and it can be applied, in parts, to all papers that this thesis includes. Artifacts were also produced in the research to estimate the TTC for ICS and when creating a parser for automatically generating threat models of substations. In this section, the method of the thesis is described by aligning it to the six steps that can be used as guidelines when following the DSR method, as seen in Figure 10. Overall, this thesis identifies the issues of cyber security for the substation, by for example finding attack scenarios against it. The thesis also aims to solve these issues by creating artifacts, such as a threat modeling language that can be used to create threat models and to generate attack graphs. Another artifact is the estimate of TTC for attacks against ICS. Lastly, the thesis evaluates threat modeling languages.

The first step of DSR is to identify the problem and motivate the solution of the problem. In Paper A, the problem of cybersecurity threats against the power system is identified as the paper aims to aid in the development of threat models for the domain. In Papers B and C, issues of cybersecurity in ICS are discussed that motivates developing a method of estimating the Time-To-Compromise of cyber attacks. The development of TTC is also motivated by the fact that this information can be included in threat modeling languages in the MAL framework to enhance cybersecurity assessments. The problem of cybersecurity of power systems is identified and motivated in Paper D where, for instance, a literature review found many different attack scenarios possible for the substation.

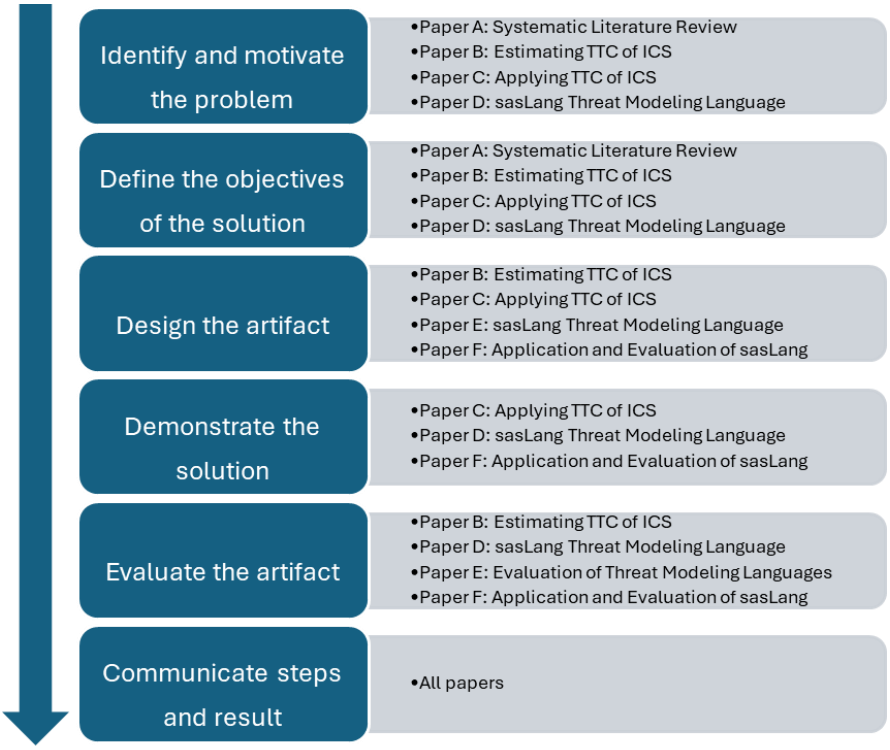


Figure 10: The six steps of Design Science Research (DSR) and which included paper aligns to them.

The second step is to, based on the problem statement, define the objectives of the solution. The overall objective of the solutions of this thesis is to help with the cybersecurity assessment of substations. This step is performed in Papers A, B, C and D. Paper A solves the problem of finding information

sources for creating threat models in the power systems domain by finding the information sources used in previous research with a systematic literature review. In a systematic literature review, the process of the literature review is described in detail so that it can be repeated, and any bias would be made clear. For Papers C and D, by creating a method to estimate the TTC specifically aligned to ICS and then applying it to the MITRE ATT&CK knowledge base the objective is to help in the assessment of cybersecurity of ICS. By finding the TTC of different attacks and comparing these, one can gain knowledge about how to assign resources and which attacks to prioritize defending against. Finally, in Paper D, the objective of the solution is to help in the creation of threat models by using a threat modeling language for the SAS domain. The threat models can, in turn, be used to help with assessing the cybersecurity of SAS.

The third step is designing the artifact and firstly in the case of sasLang the Meta Attack Framework (MAL) is used to reach the objective. The choice is also made to base sasLang on the previously defined languages coreLang [47] and icsLang [49]. coreLang and icsLang are also MAL based threat modeling languages and icsLang is an extension of coreLang. coreLang describes the general IT domain and icsLang describes the Industrial Control Systems (ICS). coreLang provides the logic of basic cybersecurity concepts, such as vulnerabilities, authentication and networking. icsLang includes the assets and attack techniques defined in MITRE ATT&CK for ICS [53], which served as an appropriate foundation for sasLang. In addition, sasLang is a second version of the threat modeling language SCL-Lang [46]. In Figure 11, the relationship between these languages, and other information sources used to create the language in Paper E, are described. As one of the guidelines for developing domain specific languages by Karsai et. al. using existing language definitions decreases the work when creating a new language and helps users to understand the new language if they can recognize pre-existing parts [63].

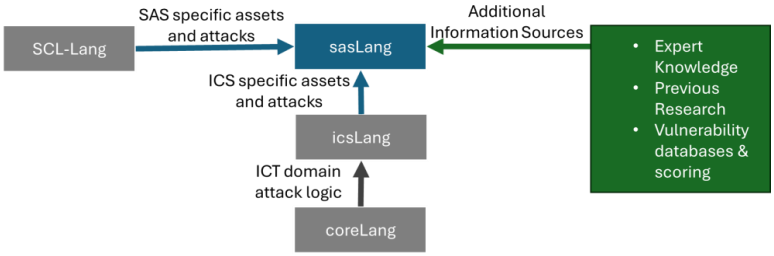


Figure 11: The different existing languages used when creating sasLang.

When creating sasLang, a data collection of SAS designs found in the industry was performed to find all important assets that should be included in the language. This data collection was done by first identifying the SAS market leaders and then finding information regarding their designs of SAS. The choice was made to include assets that were mentioned by at least two vendor designs. Then a review of attack scenarios against SAS was performed. There are existing collections of attacks for the ICS and OT domain, such as MITRE ATT&CK for ICS [53], as described in Section 2.7. To model how different attack steps relate, examples of entire attack scenarios for SAS being described were found. There were also specific inclusion criteria for the attack scenarios, such as, they must be related to an IEC 61850 substation and have sufficient detail of the attack so that the scenario can be modeled. This made it necessary to perform a literature review to find the attack scenarios. Google Scholar[3] was chosen for the literature review as it finds not only scientific research papers but also documents from the industry. After finding 76 non-duplicate papers, six inclusion criteria were applied, and this resulted in 14 papers describing attack scenarios for IEC 61850 based SAS.

Secondly, in Paper B an artifact was also designed, which is the equation for estimating the TTC of cyber attacks in the ICS domain in combination with an Excel sheet with which the TTC_{ICS}[4] is estimated. The Excel sheet includes the method of how to estimate the Time-To-Compromise for the MITRE ATT&CK Techniques in the ICS domain. The choice was made to create an adaptation of the original TTC specifically aligned to ICS. The original TTC was created in 2006 and uses some fixed values based on the research available at that time. The equation was created by both researching related works that also update the original TTC, as well as by finding new research and information. The concept of TTC estimated by dividing the equation up into three different processes is kept for TTC_{ICS}. What has been changed are several fixed values and methods of gathering data for variables both to update it to more recent research and to make it specific to the ICS domain. Parameters of the total number of vulnerabilities a specific component and the total number of vulnerabilities found in the database have been updated to be ICS specific. The number of available exploits has been updated since there are more exploits

[3] Google Scholar, https://scholar.google.com/, Accessed 27 March 2025
[4] ttc-ics, https://github.com/EngLi/ttc-ics, Accessed 27 March 2025

and new information available since the original TTC was developed. The notion of the severity of the different vulnerabilities has also been added to the estimation of TTC_{ICS}. The time taken to develop a new exploit is updated according to new research. Lastly, updated values are provided for the fraction of vulnerabilities that are exploitable and the mean time between vulnerabilities.

Lastly, the artifact SCL Parser that can automatically generate a threat model for SAS based on an SCL description file is presented in Paper F. The SCL Parser was created by using the information of the IEC 61850 standard and three different configuration files. This information was useful in deciding which information from the configuration files that should be extracted and translated to assets and associations when creating the threat model. For instance, there are assets in SCL to describe functions outside of the main functions of the substation, but this was not defined in any of the test files or clearly described in the standard. This was therefore not added as part of the SCL Parser. The test files were also used to test if the SCL Parser could extract the correct information and work as intended. The SCL configuration files are based on Extensible Markup Language (XML)[5]. XML structures the data with tags, which makes the information easier to parse for a computer. The SCL Parser uses the built-in Python module ElementTree[6] to be able to iterate the configuration file to extract the specific parts that is needed for creating the threat model.

The fourth step is to demonstrate the solution, and this is done in Papers C, D and F. In Paper C, TTC_{ICS} is demonstrated by estimating the TTC for MITRE ATT&CK techniques of ICS. In Paper D, two attack scenarios are used to demonstrate sasLang. The first scenario is a MITM attack that impacts a circuit breaker, and the second scenario is an SSL vulnerability exploit attack that allows the attacker to cause a transformer to overheat. For both scenarios the threat model and attack graph are illustrated. In Paper F, four attack scenarios based on threat models that were automatically created by the SCL Parser are described, and one of these scenario's threat model is illustrated.

The fifth step is to evaluate the artifact. The concept of evaluation is broad, and it is a term closely related to validation and verification. Evaluation is

[5] XML, https://www.w3.org/XML/, Accessed 27 March 2025
[6] ElementTree, https://docs.python.org/3/library/xml.etree.elementtree.html, Accessed 27 March 2025

defined as assessing something and in this thesis, the assessment is how well the threat modeling language, threat models or attack graphs perform. Validation and verification are more strict terminologies for assessing the correctness and establishing the truth. Using such a strong term is avoided since in this thesis the correctness can only be evaluated within the scope of the research conducted. Hevner et. al. summarizes five different typical evaluation methods in design science research [64]. These methods are observational, analytical, experimental, testing, and descriptive.

In Paper E, the threat modeling language is evaluated by using the falsification approach [65]. By this approach the paper strives to prove the correctness of the language by being unable to find any reasons why it would not be correct. In that evaluation there was also access to what is considered to be the truth of how difficult different attacks in the virtual environment were and compared this truth to industry expert assessment, simulations performed based on coreLang and random guessers. The evaluation was carried out by designing four experiments where 12 assessors had different time to make the assessments and access different amounts of information regarding the environment.

In Paper D, the evaluation of sasLang was made by using a different method than that in Paper E, since there was no access to what could be considered to be the true difficulty between attacks, or which actual attacks exist in the specific system. Instead, sasLang was evaluated by describing how the language can be used to model two different attack scenarios. Considering that the evaluation was limited and based on attack scenarios that were used to create the language, a more extensive evaluation was performed in Paper F. In Paper F, a parser was developed that can automatically create a threat model based on an IEC 61850 substation configuration file. Four attack scenarios were picked out to evaluate sasLang based on. These four attack scenarios were evaluated by asking four experts in the industry to assess their accuracy in illustrating real-world attack scenarios. TTC_{ICS} has been evaluated in Paper B by comparing the estimated TTC to the frequency of successful attacks [66] for six different attack scenarios. The assumption is made that an attack that is more frequently successful would have a lower TTC.

Finally, step six is to communicate the steps and results, and this has been done in all included papers. The research was communicated in the included papers and the resulting artifacts are available on GitHub. The conference papers have also been presented at conferences.

3.2 Software Tools

In Paper D the language was compiled with malcompiler[7] and created attack graphs with SecuriCAD [67]. SecuriCAD is a software program where one can import a MAL based language and create threat models. The software lets the user drag-and-drop the different assets that the language consists of and connect these to create a threat model. The threat models can be simulated to generate attack graphs, which according to the authors are similar to Bayesian networks. The simulation can show the shortest path based on the information included in the language. SecuriCAD was used to run the simulations for Paper E when evaluating coreLang. The evaluation of coreLang included not only the simulation but also a virtual environment that the experts had access to for making their assessments. This is the same virtual environment that was used when gathering the real-world data and what is considered to be the truth in the evaluation. This virtual environment was hosted on Google Cloud[8] and ran 79 virtual machines that were managed by Ansible[9].

In Paper F, sasLang was updated and used newly available tools for compilation and working with MAL based languages. For this paper MAL Compiler[10] was used for language compilation and MAL Toolbox[11] as well as mal-traverser[12] for developing threat models and attack graphs. The SCL parser[13] that was created in Paper F was written in Python and with Visual Studio Code. GitHub has been used for version management of code and to allow external access to all the artifacts created in this thesis.

3.3 Datasets and Metrics

An ICS specific TTC, TTC_{ICS}, was created in Paper B, by using information found in a vulnerability dataset specific to ICS, called RITICS Learning from Vulnerabilities dataset[14]. The dataset and how it was created is explained in more detail in their research paper [68]. The dataset by Thomas and Chothia

[7] Malcompiler, https://github.com/mal-lang/malcompiler Accessed 27 March 2025
[8] Google Cloud, https://cloud.google.com/, Accessed 27 March 2025
[9] Ansible, https://www.redhat.com/en/ansible-collaborative, Accessed 27 March 2025
[10] malc, https://github.com/mal-lang/malc, Accessed 27 March 2025
[11] mal-toolbox, https://pypi.org/project/mal-toolbox, Accessed 27 March 2025
[12] mal-traverser, https://github.com/mal-lang/mal-traverser, Accessed 27 March 2025
[13] SCL Parser, https://github.com/EngLi/scl-parser, Accessed 27 March 2025
[14] RITICS learning from vulnerabilities dataset, https://uob-ritics.github.io/learning-from-vulnerabilities/, Accessed 27 March 2025

uses the Common Vulnerabilities and Exposures, CVE, which is an enumeration system for vulnerabilities intended to help identify and cataloguing them[15]. Each CVE has an assigned Common Vulnerability Scoring System (CVSS) [69]. The CVSS is a numerical value indicating how severe a vulnerability is. The dataset includes CVSS version 2 and 3 and the latest version of CVSS is version 4. To create TTC_{ICS} the number of exploits available in Metasploit and their ranking in terms of its potential impact is also used. Metasploit is a penetration testing framework, which includes many available exploits[16].

In Paper C, the MITRE ATT&CK matric for ICS [53] attack techniques are used to estimate the Time-To-Compromise (TTC). MITRE ATT&CK for ICS was created as a framework to include all tactics and techniques possible for attacking an ICS. The version that is used in Paper C is version 12.1 and the latest one is version 16.1. The difference between the versions is that some additions have been made in terms of, for instance, techniques. The reason that these two datasets of MITRE ATT&CK matric for ICS and the RITICS Learning from Vulnerabilities dataset are used is because they focus on the ICS domain specifically. It made it possible to create an ICS specific estimation of TTC where it is also possible to make the estimation per asset and type of attack. The assets and type of attacks are not exactly a match to those in sasLang and it would require adaptation to add the TTC values to the language.

[15] CVE, https://www.cve.org/, Accessed 27 March 2025
[16] Metasploit, https://www.metasploit.com/, Accessed 27 March 2025

4 Contributions

The three research questions are answered with four distinct contributions as seen in Figure 12. The first contribution is a systematic literature review where previously used information sources for threat modeling in the power systems domain were found. The second contribution is an estimation of TTC for the Industrial Control Systems, TTC_{ICS}. The third contribution is the SAS domain specific threat modeling language sasLang. These three contributions answers research question 1. The fourth contribution is work with evaluation of threat modeling languages. The third contribution of sasLang combined with the fourth contribution of evaluation answers research question 2. Finally, the fourth contribution of evaluation answers research question 3.

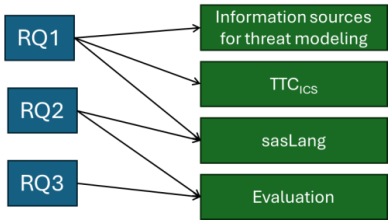


Figure 12: The relation between research questions and contributions.

4.1 Information Sources for Threat Modeling

It is important that the information used to create a threat model is accurate so that the threat model and conclusions drawn from it can be trusted. In the process of threat modeling, one must gather information about the system and the threats against it. In Paper A, the contribution is a systematic literature review that found the different information sources used when creating threat

models in the power systems domain and a discussion regarding them. Six information sources were found, and categorized as expert knowledge, logs & alerts, previous research, system's state, vulnerability scoring & databases, and vulnerability scanners, as seen in Figure 13. This goes back to answering research question 1 as different information sources are found and discussed. The most commonly used information sources found were expert knowledge, previous research, and vulnerability scoring & databases. These are also information sources that have been used for research in this thesis. The system's state is also used as an information source since the SCL Parser created in Paper F uses the configuration file of a substation as input.

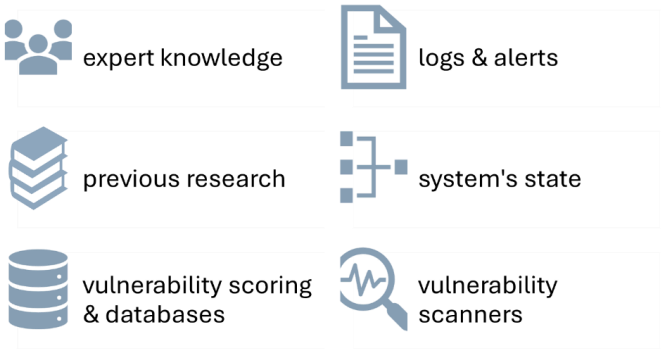


Figure 13: Information sources found in power systems threat modelling.

4.2 Time-To-Compromise for ICS, TTC_{ICS}

When assessing the cybersecurity of a system, it helps to prioritize your resources by knowing which attack would be the fastest for an attacker to succeed with. One of the measures of how to estimate this is the Time-To-Compromise (TTC). The attack steps in an attack graph can be assigned TTC values, which helps answer research question 1. Based on the original work on TTC [70] an updated and ICS domain specific TTC estimation, TTC_{ICS}, is created in Paper B. TTC is estimated based on the probability that an attacker is in three different processes and the time taken to complete these processes. In process 1, P_1, the asset that is target has at least one known vulnerability and at least one available exploit. In process 2, P_2, there are no known available exploits, but there is at least one known vulnerability. The last process, P_3, is the continuously ongoing process of finding new vulnerabilities and developing new exploits. This process is considered to run at the same time as the other two. According to the original definition, a more skilled attacker would be able

to use a higher number of exploits and therefore the estimation also takes into consideration the attacker's skill level. In this section the final equation introduced in Paper B of how to estimate the TTC_{ICS} is described, and more details can be found in the included paper.

$$T = t_1 * P_1 + t_2 * (1 - P_1) * (1 - u) + t_3 * u(1 - P_1) \quad (1)$$

where T is the expected TTC estimated in days, t_1 is the time taken to complete process 1, t_2 is the time taken to complete process 2, t_3 is the time taken to complete process 3, $u = (1 - f)v$, which is the probability that P_2 is unsuccessful where v is the number of vulnerabilities and f is the fraction of vulnerabilities that are exploitable for a specific skill level. Also, $u = 1$ if $v = 0$. P_1 is the probability that an attacker is in process 1 and therefore have an exploit readily available.

In Paper C, a method to assign the TTC to every technique of the MITRE ATT&CK knowledge base for the ICS domain [53] is created. This contribution improves the assessment of ICS cybersecurity since one can anticipate the time that different attacks would take. In this way, one can prioritize where to place defenses. To be able to assign the TTC per technique, a mapping of each technique to both assets and category of vulnerability is also presented. In the article an example is presented and the TTC of a MITM attack on HMI is estimated to be 2501 days for a novice and 6 days for an expert hacker.

4.3 Threat Modeling Language for SAS, sasLang

The central contribution of this thesis is the threat modeling language sasLang, which is described in Paper D. The entire MAL specification is hosted on a GitHub repository[17]. In this summary the latest version of sasLang, version 2, is described. sasLang was updated from the original version 1 described in Paper D when applying and evaluating the language in Paper F. sasLang was updated because the languages that it extends, icsLang version 0.0.1 and coreLang version 0.4.0 were updated to versions icsLang 0.0.2 and coreLang 1.0.0. The assets of sasLang and the associations between the assets are illustrated in Figure 14. The figure shows the inheritance of the assets between the languages. The assets shown are all the assets of sasLang and the new assets created for sasLang have been colored blue. If the asset is an extension

[17] sasLang MAL specification, https://github.com/mal-lang/sasLang, Accessed 27 March 2025.

from icsLang, the extended asset is added in green and if it is from coreLang, it is added in orange. Where the associations of assets in sasLang have been defined in icsLang or coreLang, assets and associations have been added to show how they are associated in a SAS. The color of the association indicates in which language the specific association has been defined. The figure does not show all the associations and assets of icsLang and coreLang, but those that help explain how sasLang assets are associated.

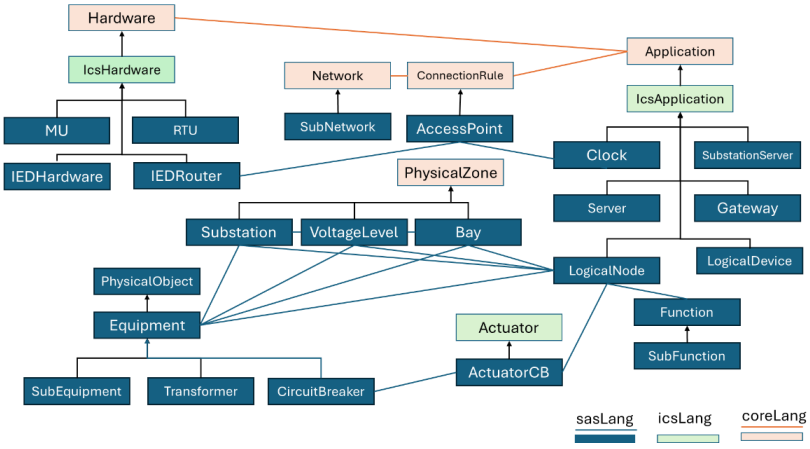


Figure 14: A class diagram showing the assets and associations of sasLang and inheritance from icsLang and coreLang.

When creating sasLang different cyber attacks that are possible per each of the components or protocols found in a SAS were gathered. Most of the cyber attacks could be modeled by using icsLang or coreLang attack steps and details regarding these cyber attacks are included Paper D.

Another contribution related to sasLang is the SCL parser that was developed in Paper F to evaluate sasLang. An SCD file and sasLang are used as input to the parser, which in turn automatically creates a threat model to be used for cybersecurity assessment. sasLang answers research questions 1 and 2 since it not only includes possible cyber attacks on digital substations and uses it for cybersecurity assessment of digital substations, but it also enables automatically creating threat models based on existing configuration files.

4.4 Evaluation of Threat Modelling Languages

It is important that the threat modeling languages that are used in this thesis are accurate according to the real-world and consequently, also the threat models created with them and the attack graphs that are generated. The

evaluation of the threat modeling languages answers research question 3. In Paper D, sasLang is evaluated by considering if attack scenarios found in the literature can be modelled with sasLang. Four attack scenarios are modeled and two of these are presented in the paper. The attack scenarios used to evaluate were also used as input when creating sasLang. Therefore, sasLang was further evaluated in Paper F. In Paper F four different attack scenarios were evaluated by asking industry experts several questions. These attack scenarios were not taken from previous research, as in Paper D. Instead, threat models were automatically generated from substation configuration files according to IEC 61850 by using sasLang and generated attack graphs from these were used. Four attack scenarios were then chosen that, according to the threat model and sasLang, would be possible in the specific substation. In Paper E, before the evaluation of sasLang, an evaluation was conducted of coreLang, but this did not include the icsLang or sasLang aspects. In the evaluation of coreLang, there was access to real-world data since students as part of a university course had hacked the system that was also simulated by using coreLang. In that evaluation the simulation made by coreLang, a random guesser and industry expert opinion with the real-world data were compared. coreLang includes default TTC values, added by the developers of the language, on some attack steps. These TTC values were inherently evaluated in Paper E as the TTC of the attack paths were compared to measure their relative difficulty.

5 Conclusion and Future Work

Our society is clearly dependent on electricity and since modern substations are digital, we must protect them from cybersecurity attacks. Stable, safe and secure electric distributions via substations are important for sustainability. Without electricity it is difficult to provide good healthcare and support critical infrastructures, such as sanitation. Albeit that work with assessing the cybersecurity of substation can help in protection against malicious attacks and, on a larger scale, cyber warfare, there is also an ethical aspect. The work in this thesis can be used by malicious actors to gain knowledge about which attacks they should perform. This thesis assumes that security does not lie in obscurity, but rather that it is important to gain as much knowledge about cybersecurity as possible even if it means sharing this information with a malicious actor. In this thesis research has been conducted towards finding the different cybersecurity attacks that substations may be vulnerable to, and which ones could be the most important to prioritize protecting against by using threat modeling. The results presented in this thesis help stakeholders with assessing the cybersecurity of their substations to keep them secure from cyber attacks. The stakeholders can create threat models of their substation and by using the sasLang threat modeling language generate attack graphs. By analyzing the attack graph, the stakeholder can assign their security resources to protect against these attacks. The thesis also helps by providing an estimate of the TTC of attacks against ICS, which can further aid in the assessment of the cybersecurity. Some of the constraints and requirements of correct cybersecurity assessments made from the results of this thesis are described in the following description of future work.

The research in this thesis to assess the cybersecurity of SAS with threat modeling can continue in many directions. Here two directions are discussed according to the different domain that this thesis combines. First, in terms of cybersecurity, as the attacker continuously tries to find new vulnerabilities and create new exploits of these, the defender's work to protect the system will continue. Future work includes continued efforts to find the different vulnerabilities and exploits so that a defender of a system knows what to protect against. By further researching the TTC of the different attacks, the attack graphs can be improved by more accurately finding the more crucial attacks to prioritize defending against. The method of estimating TTC can also be evaluated and other methods of how to estimate the TTC can be researched. The current version of sasLang includes TTC values that have been inherited from coreLang, but the language does not include ICS specific TTC values. Future work is to add TTC values for the ICS attack techniques in icsLang that will be inherited by sasLang. Future work could also be studies on TTC for SAS.

Continuing the research of sasLang is also part of the future work of this thesis as part of the threat modeling domain. Further research could be to add support to model different types of communication protocols. The threat model of a substation that is automatically generated could be extended, as based on the results on the evaluation, to include assets beyond the scope of SCL and therefore enable a cybersecurity assessment of an entire substation. To do this, one could add information from firewall rules or the IED software. Considering that sasLang includes coreLang and icsLang, future work could be threat modeling of not only the SAS but also including the business IT network that may connect to the OT part. There are efforts to communicate the possible attacks against ICS as with the increasingly popular MITRE ATT&CK knowledge base, but there may still be a need for a graphical visualization of attack graphs to help stakeholders make decisions [71]. Another research direction is towards the graphical representation of the attack graph and focusing on the usability and ability to understand and draw conclusions from the analysis. Graphical representation is not part of this thesis as already available tools as described in Section 3.2 have been used instead.

References

[1] Y.-C. Liao, "Quantitative Information Security Vulnerability Assessment for Norwegian Critical Infrastructure," in *International Conference on Critical Information Infrastructures Security, Lecture Notes in Computer Science (LNSC)*, 2020.

[2] S. K. Venkatachary, J. Prasad and R. Samikannu, "Cybersecurity and cyber terrorism - in energy sector – a review," *Journal of Cyber Security Technology,* pp. 111-130, 2018.

[3] Dragos, "Crashoverride Analysis of the Threat to Electric Grid Operations," 2017. [Online]. Available: https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf. [Accessed 27 March 2025].

[4] Dragonfly Intelligence, "Europe | Evolving cyber threats to energy sector," 2024. [Online]. Available: https://dragonflyintelligence.com/news/europe-evolving-cyber-threats-to-energy-sector/. [Accessed 27 March 2025].

[5] E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid," 2016. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf. [Accessed 27 March 2025].

[6] EnergiCert, "Cyber attacks against European energy & utility companies," 2022. [Online]. Available: https://sektorcert.dk/wp-content/uploads/2022/09/Attacks-against-European-energy-and-utility-companies-2020-09-05-v3.pdf. [Accessed 27 March 2025].

[7] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadegh, M. Maniatakos and R. Karri, "The Cybersecurity Landscape in Industrial Control Systems," in *Proceedings of the IEEE,* 2016.

[8] Dragos, "OT/ICS Cybersecurity Report," 2025. [Online]. Available: https://hub.dragos.com/hubfs/312-Year-in-Review/2025/Dragos-2025-OT-Cybersecurity-Report-A-Year-in-Review.pdf. [Accessed 27 March 2025].

[9] O. Andreeva, S. Gordeychik, G. Gritsai, O. Kochetova, E. Potseluevskaya, S. I. Sidorov and A. A. Timorin, "Industrial Control Systems Vulnerability Statistics," 2017.

[10] M. Alanazi, A. Mahmood, J. Morshed and M. Chowdhury, "ICS-LTU2022: A dataset for ICS vulnerabilities," *Computers & Security,* vol. 148, 2025.

[11] M. M. Aslam, A. Tufail, R. A. A. H. M. Apong, L. C. D. Silva and M. T. Raza, "Scrutinizing Security in Industrial Control Systems: An Architectural Vulnerabilities and Communication Network Perspective," *IEEE Access,* vol. 12, pp. 67537-67573, 2024.

[12] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule and M. Thompson, "NIST Special Publication, NIST SP 800-82r3, Guide to Operational Technology (OT) Security," 2023.

[13] K. Yskout, T. Heyman, D. V. Landuyt, L. Sion, K. Wuyts and W. Joosen, "Threat modeling: from infancy to maturity," in *ACM/IEEE 42nd International Conference on Software Engineering: New Ideas and Emerging Results*, 2020.

[14] P. Johnson, R. Lagerström and M. Ekstedt, "A Meta Language for Threat Modeling and Attack Simulations," in *ARES '18: Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018.

[15] J. Burke and A.-M. Sahazizian, "How a Substation Happens," in *Electric Power Substations Engineering*, 3rd ed., J. D. McDonald, Ed., 2021, pp. 1-8.

[16] J. W. Evans, "Interface between Automatin and Substation," in *Electrical Power Substations Engineering*, 3rd ed., J. D. McDonalds, Ed., 2021, pp. 1-29.

[17] IEC, "IEC 61850 Series," 2025. [Online]. Available: https://webstore.iec.ch/en/publication/6028. [Accessed 27 March 2025].

[18] IEC, "IEC News and Blogs," 26 February 2021. [Online]. Available: https://www.iec.ch/blog/understanding-iec-62443. [Accessed 27 March 2025].

[19] D. Dolezilek, D. Gammel and W. Fernandes, "Cybersecurity Based on IEC 62351 and IEC 62443 for IEC 61850 Systems," in *15th International Conference on Developments in Power System Protection*, 2020.

[20] IEC, February 2025. [Online]. Available: https://webstore.iec.ch/en/publication/6912. [Accessed 27 March 2025].

[21] N. Moreira, E. Molina, J. Lázaro, E. Jacob and A. Astarloa, "Cyber-security in substation automation systems," *Renewable and Sustainable Energy Reviews,* vol. 54, pp. 1552-1562, 2016.

[22] M. F. Elrawy, L. Hadjidemetriou, C. Laoudias and M. K. Michael, "Modelling and Analysing Security Threats Targeting Protective Relay Operations in Digital Substations," in *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2023.

[23] T. A. Youssef, M. E. Hariri, N. Bugay and O. A. Mohammed, "IEC 61850: Technology standards and cyber-threats," in *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*, Florence, 2016.

[24] A. Akbarzadeh, L. Erdodi, S. H. Houmb and T. G. Soltvedt, "Two-stage advanced persistent threat (APT) attack on an IEC 61850 power grid

substation," *International Journal of Information Security,* vol. 23, p. 2739–2758, 2024.

[25] G. Dondossola, J. Szanto, M. Masera and I. N. Fovino, "Effects of intentional threats to power substation control systems," *International Journal of Critical Infrastructures,* vol. 4, pp. 129-143, 2008.

[26] S. Hussain, J. H. Fernandez, A. K. Al-Ali and A. Shikfa, "Vulnerabilities and countermeasures in electrical substations," *International Journal of Critical Infrastructure Protection,* vol. 33, 2021.

[27] W. Xiong and R. Lagerström, "Threat modeling – A systematic literature review," *Computers & Security,* pp. 53-69, 2019.

[28] Microsoft, "The STRIDE Threat Model," 2009. [Online]. Available: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20). [Accessed 27 March 2025].

[29] A. Shostack, Threat Modeling: Designing for Security, Wiley, 2014.

[30] VerSprite, "Risk-Based Security Threat Modeling: 7-Step Process for Risk Analysis," 27 March 2025. [Online]. Available: https://versprite.com/security-resources/risk-based-threat-modeling/.

[31] T. UcedaVelez and M. M. Morana, Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis, Hoboken, NJ: Wiley, 2015.

[32] L. Sion, K. Yskout, D. Van Landuyt, A. van den Berghe and W. Joosen, "Security Threat Modeling: Are Data Flow Diagrams Enough?," in *ICSEW'20: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, 2020.

[33] K. Fakhroutdinov, "UML Diagrams," 2025. [Online]. Available: https://www.uml-diagrams.org/class-diagrams-overview.html. [Accessed 27 March 2025].

[34] C. Phillips and L. Painton Swiler, "A graph-based system for network-vulnerability analysis," in *NSPW '98: Proceedings of the 1998 workshop on New security paradigms*, 1998.

[35] B. Schneier, "Attack Trees, Dr. Dobb's Journal," December 1999. [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html. [Accessed 27 March 2025].

[36] B. Kordy, S. Mauw, S. Radomirović and P. Schweitzer, "Foundations of Attack–Defense Trees," in *Formal Aspects of Security and Trust - 7th International Workshop, FAST 2010*, Pisa, 2010.

[37] K. Zenitani, "Attack graph analysis: An explanatory guide," *Computers & Security,* vol. 126, 2023.

[38] K. Milousi, P. Kiriakidis, N. Mengidis, G. Rizos, M. S. Mazi, A. Voulgaridis, K. Votis and D. Tzovaras, "Evaluating Cybersecurity Risk: A Comprehensive Comparison of Vulnerability Scoring Methodologies," in *ARES '24: Proceedings of the 19th International Conference on Availability, Reliability and Security*, 2024.

[39] S. Elder, M. R. Rahman, G. Fringer, K. Kapoor and L. Williams, "A Survey on Software Vulnerability Exploitability Assessment," *ACM Computing Surveys,* vol. 56, pp. 1-41, 2024.

[40] K. Ingols, M. Chu, R. Lippmann, S. Webster and S. Boyer, "Modeling Modern Network Attacks and Countermeasures Using Attack Graphs," in *2009 Annual Computer Security Applications Conference*, Honolulu, 2009.

[41] S. Jha, O. Sheyner and J. Wing, "Two Formal Analyses of Attack Graphs," in *Computer Security Foundations Workshop, 2002*, 2002.

[42] J. Homer, S. Zhang, X. Ou, D. Schmidt, Y. Du, S. Rajagopalan and A. Singhal, "Aggregating Vulnerability Metrics in Enterprise Networks using Attack Graphs," *Journal of Computer Security,* vol. 21, pp. 561-597, 2013.

[43] T. Sommestad, M. Ekstedt and H. Holm, "The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures," *IEEE Systems Journal,* vol. 7, p. 363–373, 2013.

[44] W. Wideł, S. Hacks, M. Ekstedt, P. Johnson and R. Lagerström, "The meta attack language - a formal description," *Computers & Security,* vol. 130, 2023.

[45] S. Katsikeas, P. Johnsson, S. Hacks and R. Lagerström, "VehicleLang: A probabilistic modeling and simulation language for modern vehicle IT infrastructures," *Computers & Security,* vol. 117, 2022.

[46] E. Rencelj Ling and M. Ekstedt, "Generating Threat Models and Attack Graphs based on the IEC 61850 System Configuration description Language," in *SAT-CPS 2021 - Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*, 2021.

[47] S. Katsikeas, S. Hacks, P. Johnson, M. Ekstedt, R. Lagerström, J. Jacobsson, M. Wällstedt and P. Eliasson, "An Attack Simulation Language for the IT Domain," in *Graphical Models for Security. GraMSec 2020. Lecture Notes in Computer Science()*, 2020.

[48] S. Hacks, S. Katsikeas, E. Ling, R. Lagerström and M. Ekstedt, "powerLang: a probabilistic attack simulation language for the power domain," *Energy Informatics,* 2020.

[49] S. Hacks and S. Katsikeas, "Towards an Ecosystem of Domain Specific Languages for Threat Modeling," in *Advanced Information Systems Engineering. CAiSE 2021. Lecture Notes in Computer Science()*, 2021.

[50] S. M. Khalil, H. Bahsi and T. Korõtko, "Threat modeling of industrial control systems: A systematic literature review," *Computers & Security,* vol. 136, 2024.

[51] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," *Computers & Security,* vol. 56, pp. 1-27, 2016.

[52] S. Nazir, S. Patel and D. Patel, "Assessing and augmenting SCADA cyber security: A survey of techniques," *Computers & Security,* pp. 436-454, 2017.

[53] MITRE ATT&CK, 2022. [Online]. Available: https://attack.mitre.org/versions/v12/. [Accessed 27 March 2025].

[54] S. Kempinski, "OTCAD - Operational Technology Cyber Attack Database," 2021. [Online]. Available: https://www.secura.com/uploads/whitepapers/Secura-White-Paper-OTCAD.pdf. [Accessed 27 March 2025].

[55] S. Choi, J.-H. Yun and B.-G. Min, "Probabilistic Attack Sequence Generation and Execution Based on MITRE ATT&CK for ICS Datasets," in *Proceedings of the 14th Cyber Security Experimentation and Test Workshop*, 2021.

[56] D. Cerotti, D. Codetta Raiteri, G. Dondossola, L. Egidi, G. Franceschinis, L. Portinale, D. Savarro and R. Terruggia, "SecuriDN: A Modeling Tool Supporting the Early Detection of Cyberattacks to Smart Energy Systems," *Energies,* vol. 17, 2024.

[57] J. Vaudey, S. Mocanu, G. Delaval and E. Rutten, "An IEC 62443-security oriented domain specific modelling language," in *ARES '24: Proceedings of the 19th International Conference on Availability, Reliability and Security*, 2024.

[58] S. M. Khalil, H. Bahsi, H. O. Dola, T. Korõtko, K. McLaughlin and V. Kotkas, "Threat Modeling of Cyber-Physical Systems - A Case Study of a Microgrid System," *Computers & Security,* vol. 123, 2023.

[59] O. Duman, M. Ghafouri, M. Kassouf, R. Atallah, L. Wang and M. Debbabi, "Modeling supply chain attacks in IEC 61850 substations," in *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2019.

[60] P. J. Hawrylak, M. Haney, M. Papa and J. Hale, "Using hybrid attack graphs to model cyber-physical attacks in the Smart Grid," in *2012 5th International Symposium on Resilient Control Systems*, 2012.

[61] O. Duman, M. Zhang, L. Wang and M. Debbabi, "SecMonS: A Security Monitoring Framework for IEC 61850 Substations Based on Configuration

Files and Logs," in *Detection of Intrusions and Malware, and Vulnerability Assessment: 21st International Conference, DIMVA*, 2024.

[62] K. Peffers, T. Tuunanen, M. A. Rothenberger and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems,* pp. 45-77, 2007.

[63] G. Karsai, H. Krahn, C. Pinkernell, B. Rumpe, M. Schindler and S. Völkel, "Design Guidelines for Domain Specific Languages," in *9th OOPSLA Workshop on Domain-Specific Modeling (DSM' 09)*, 2009.

[64] A. R. Hevner, S. T. March, J. Park and S. Ram, "Design science in information systems research," *MIS Quarterly,* vol. 28, pp. 75-105, Mars 2004.

[65] K. Popper, The Logic of Scientific Discovery, New York, NY: Basic Books, 2002.

[66] Y. Zhang, Y. Xiang and L. Wang, "Reliability analysis of power grids with cyber vulnerability in SCADA system," in *2014 IEEE PES General Meeting | Conference & Exposition*, 2014.

[67] M. Ekstedt, P. Johnson, R. Lagerström, D. Gorton, J. Nydrén and K. Shahzad, "Securi CAD by Foreseeti: A CAD Tool for Enterprise Cyber Security Management," in *2015 IEEE 19th International Enterprise Distributed Object Computing Workshop*, Adelaide, 2015.

[68] R. J. Thomas and T. Chothia, "Learning from Vulnerabilities - Categorising, Understanding and Detecting Weaknesses in Industrial Control Systems," in *Computer Security - ESORICS 2020 International Workshops, CyberICPS, SECPRE, and ADIoT, 2020, Revised Selected Papers*, 2020.

[69] FIRST, "CVSS," 2025. [Online]. Available: https://www.first.org/cvss/. [Accessed 27 March 2025].

[70] M. A. McQueen, W. F. Boyer, M. A. Flynn and G. A. Beitel, "Time-to-Compromise Model for Cyber Risk Reduction Estimation," in *Quality of Protection, Advances in Information Security*, Boston, MA, 2006.

[71] A. M. Pirca and H. S. Lallie, "An empirical evaluation of the effectiveness of attack graphs and MITRE ATT&CK matrices in aiding cyber attack perception amongst decision-makers," *Computers & Security,* vol. 130, 2023.