Scaling Up, Staying Secure

Assessing the Cyber Risks of Distributed Energy Resources in the Smart Grid

J.M. (Mike) van der Boon

Delft University of Technology

TU Delft

Scaling Up, Staying Secure

Assessing the Cyber Risks of Distributed Energy Resources in the Smart Grid

by

J.M. (Mike) van der Boon

to obtain the degree of Master of Science

at the Delft University of Technology,

to be defended publicly on Friday January 13, 2023 at 15:00.

Project duration: June 10, 2022 – January 13, 2023
Thesis committee: Prof. dr. G. Smaragdakis, TU Delft, supervisor
Dr. K Liang, TU Delft
Dr. G. Iosifidis, TU Delft

An electronic version of this thesis is available at `http://repository.tudelft.nl/`.

TU Delft

Preface

”Op jacht naar de titel van ingenieur”
”Mooie dingen zijn mooi”

It feels pretty unreal writing this preface; it is the culmination of what has most definitely been an amazing period. However, some significant hurdles were thrown my way, and I would not have been able to get this far on my own.

First, I would express my deepest gratitude to my supervisor Prof. dr. G. Smaragdakis. George, thank you for your flexibility and amazing attitude during this whole process. It really went far to get me here. I hope ever to return the favour.

Furthermore, I would like to thank all my friends and family. There is a phrase, ”It takes a village”. Perhaps we are not that numerous, but without your support, I am certain I would not have been at this point.

This report, however, came to be a result of many experiences. In it are pieces of my TPM bachelor, Cyber Security master, and professional experience as a cybersecurity consultant.

I truly wish you all the best, and please try not to be too disparaged by the conclusions,

J.M. (Mike) van der Boon
Delft, January 2023

Summary

Distributed Energy Resources (DER), like solar panels, are projected to take over power generation responsibilities. This will happen during the transition of the current power grid to the Smart Grid. Due to the importance of this power to society, it is crucial that the grid stays stable.

DER devices are similar to IoT devices in scale, low user interaction and the use of firmware. IoT cyberattacks have been shown to have the ability to scale horizontally quickly. A vulnerability in DER devices could lead to such a scalable attack if the market for DER is oligopolistic. Due to the same underlying economic drivers such as economy-of-scale, market-for-lemons, first-mover-advantage and tragedy-of-the-commons, DER devices will likely have the same issues as IoT devices had if nothing is changed.

This research focuses on the role of the grid's transition state and the DER market's state in introducing this risk. Eight thousand one hundred (8100) scenarios were created based on a combination of parameters describing these states. An agent-based model created for this research simulated the grid and obtained the required data.

Results indicate that the grid and market parameters can introduce a cyber risk into the Smart Grid. The results show that if 5% of the households are infected, an attacker could abuse them to manipulate the grid, perhaps a blackout.

Furthermore, related work did not show any references to this particular risk and some proposed grid monitoring solutions include the usage of neighbouring DER to monitor. An attack of this nature would be able to manipulate such a monitoring solution. If the risk of an oligopolistic DER market is not considered, the Smart Grid may not have any ways of effective monitoring or mitigation.

Recommendations for policymakers and regulators were made as part of this research. The first recommendation is to allow the collection of real-time information on the grid-connected DER by grid operators. Furthermore, consideration has to be made to the usage of forced patching on DER. A delay in patching could impact the grid too much. Finally, the recommendation is to develop a policy on the local diversity of DER. Devices with the same firmware should not be allowed to obtain a critical mass in a region.

Contents

1 Introduction

Power is essential for our society. It is even so crucial that civilisations are assigned a level based on the amount of power they use [1]. To prove this, one only has to imagine what would happen with daily life if there is no power for an hour, a day, or even a week. The impact would be enormous [2], and a state of emergency would be almost guaranteed. Ensuring a reliable power grid that keeps functioning is thus paramount even when the grid changes.

Smart Grid

The power grid is transforming into the Smart Grid, a power grid where the dichotomy of user and provider is no longer present. Everyone connected can now use or provide the grid's power [3]. Among others, a driver for this process is the push towards more renewable energy sources [4].

Distributed Energy Resources (DERs) such as solar panels, wind turbines, and energy storage systems can bring many benefits to the electric grid, including increased efficiency, resiliency, and sustainability. Furthermore, the energy created by DER is cheaper in the long term, providing an economic driver to the transition [5]. This transition is not a future perspective; it is already happening and can not be stopped [6]. Action must be taken to prevent the grid from transitioning into a state more vulnerable to cyberattacks, making it unreliable.

Coordination and stability

As energy cannot be destroyed or created, the production of electricity has to be equal to the current demand. If there is a big enough mismatch, the grid could fail [7, 8]. This onerous coordination responsibility falls on the grid operator [9]; to ensure that energy generation matches energy consumption.

Communication between all actors is needed to ensure reliable power delivery to deal with this complexity, scale, and lack of reliability [7]. The coordination is even more challenging due to the rise in the absolute number of power generation devices connected to the grid [10]. Furthermore, the production capacity of DER is more erratic and less reliable, making the role of the grid operator more difficult as the need for coordination increases [5].

Currently, the coordination uses multiple assumptions to ensure the grid's stability. Firstly, it assumes that every device connected to the grid acts in good faith and follows the instructions provided by the Grid Operator. Secondly, the assumption is that the data provided to the Grid Operator is correct and reliable. The required coordination does not work if these assumptions are not correct.

Oligopolistic market

An oligopolistic market is a market that is dominated by a small number of suppliers [11]. Distributed Energy Resources will likely be such a market, as these devices have a long lifetime and are often purchased in bulk [12]. Innovation on the control part within the device is limited; if changes are needed, they can be done by updating the firmware.

The amount of DER built will be extensive, as they will be placed everywhere at every node of the Smart Grid. Production on this scale brings the economy of scale, an economic principle that drives down the cost of production per device if the total amount of produced devices is increased. When all other things are equal, a consumer will buy the cheaper product; this leads to an increase in market concentration. The result is an oligopolistic market for Distributed Energy Resources.

Cybersecurity

As with any connected technology, there are also potential cyber risks associated with integrating DERs into the Smart Grid. The assumptions used in grid coordination introduce a significant cybersecurity risk. If the Grid Operator blindly trusts DER, it will likely leave the grid vulnerable to cyberattacks. The confidentiality, integrity, and availability of the information used in grid coordination require verification.

IoT devices provide a simile in the context of cybersecurity. They are also stand-alone devices with limited end-user interaction produced in high quantities. Attacks on IoT devices have been recorded and are usually impactful due to the sheer number of devices and firmware sharing, including vulnerabilities. These aspects allowed an IoT botnet named Mirai to be responsible for the biggest-ever DDOS attack [13]. A botnet consisting of Smart Grid devices would have a massive impact; one botnet could be enough to create blackouts or cause permanent damage to the grid [14].

From a threat perspective, the Smart Grid would be an attractive target [15]. Both for nation-state actors and organised crime because of societal disruption or monetary gain, respectively. Power is vital for society; if one's goal is to disrupt it, an attack on the grid would have a huge impact. Organised crime can leverage the power market by injecting false information and exploiting this to obtain monetary gain [16].

Society

The transition towards the Smart Grid is not solely technical; institutions must also adapt to the new situation. Currently, regulators acknowledge that they do not have enough expertise and insight to effectively regulate the cybersecurity risks of the Smart Grid [17, 18]. This research topic's importance is shown by the reaction to a vulnerability found in the firmware of SolarMan. Due to this vulnerability, it was possible to simultaneously change the settings of more than 42,000 systems. The reaction involved heavy media coverage [19] and parliamentary enquiries [20].

The European Union is already taking significant steps in regulating cybersecurity risks. The NIS directive and its successor, NIS2, require operators that provide essential services, such as power, to control their cybersecurity risks. Manufacturers will be required to provide security updates for all their produced devices for the entire lifetime [21] However, these (proposed) pieces of legislation may not prove adequate for the risk that is the topic of the research. More means may be needed for proper mitigation.

Mitigation

Research has shown that it is possible to reduce cybersecurity risks to the Smart Grid [22]. It is essential for DERs to be designed with security in mind and to use secure communication protocols to mitigate these risks. However, the risk introduced by an oligopolistic market for DER brings specific hurdles. A vulnerability in the firmware of a specific model would impact a significant portion of the Smart Grid.

Difficulty arises from the fact that owners of DER are not responsible for ensuring a stable power grid. Therefore they have little to no motivation to address the cybersecurity issues or mitigate the risk. A patch for a vulnerability in a DER model will not be installed if this is not forced [23]. Currently, there are no possibilities for grid operators to force patching. Cybersecurity regulation only covers larger installations, and the terms for connecting to the grid do not include cybersecurity controls.

Goal

This research aims to highlight the cybersecurity risk of an oligopolistic Distributed Energy Recourses market for the Smart Grid. To the author's best knowledge, this is the first research into this combination of fields. Another aim is to provide insight and practical guidance to policymakers and regulators, allowing them to make informed decisions.

To obtain this research's goals, first must determine if the oligopolistic market indeed introduces a cybersecurity risk. If a risk is found, the focus shifts to when does this risk appear. The formal research question and its subquestions, therefore, are formulated as follows:

RQ *Does an oligopolistic Distributed Energy Recourses market introduce a cybersecurity risk to the Smart Grid?*

- RSQ1 *When would the risk appear due to market and grid parameters?*
- RSQ2 *What would be the impact of a successful attack due to market parameters?*
- RSQ3 *Is it possible to mitigate this risk?*

Structure of thesis

The remainder of this thesis is constructed as follows: In chapter 2, background information relevant to the topics is provided. Chapter 3 places the research in context with relevant academic work. Next, chapter 4 describes the methods used for obtaining the data needed. It also contains the experiment design. Results are given in chapter 5. In chapter 6, the limitations of this research are described, and future research recommendations are made. Lastly, the answer to the research question will be given in chapter 7 alongside recommendations for policymakers and regulators.

2

Background

The transition to a Smart Grid is currently underway. However, the current grid's principles will also apply to the new grid. Knowledge of these fundamentals will give better context to the system and provide background information for the system boundaries. Only the fundamentals that have a relationship with this research will be explained.

First, the concepts of the grid are introduced, including the definition of the Smart Grid. Next, the cybersecurity aspects of the Smart Grid are described. The third section covers an analysis of the actors related to this research. Economic and regulation concepts regarding the Smart Grid and Cybersecurity follow in the next sections. As last, modelling is introduced, including the reasoning behind the chosen modelling method.

2.1. Grid

This section will explain multiple aspects that are related to the grid. It provides the required background information that is referred to later in this research.

2.1.1. Electricity

As energy cannot be created nor destroyed, as stated by the First Law of Thermodynamics [24], the power provided to the grid needs to match the power used by the grid users. When seen in the complex domain, electrical power can be separated into four parts:

1. **Apparant power (S)** is the vector of power in the complex domain. It is measured in Volt-Ampere (VA).
2. **Active power (P)**, also known as real power, is the part of power consumed by the grid's reactive load. It is measured in Wattage (W).
3. **Reactive power (Q)** is introduced by inductive loads on the grid. Also called imaginary power, it is measured in Volt-Ampere-reactive.
4. **Phase (ϕ)** is the phase of the voltage relative to the current.

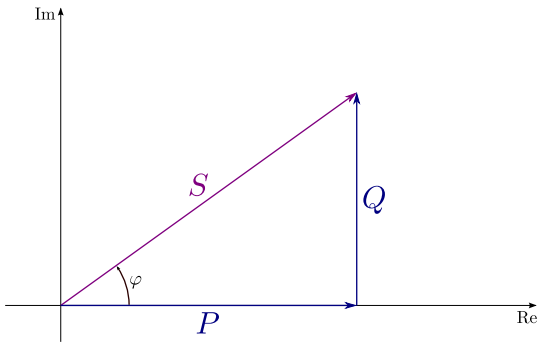

Figure 2.1: Different types of power[1]

[1] By Eli Osherovich - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=15308452

2.1.2. Layout

In figure 2.2, a simplified mockup of the grid can be seen; this is the same setup of the grid used in the created model. This layout is based on open data provided by the grid operators of the Netherlands [25] and by enthousiasts [26]. The model created in this research also uses this layout.

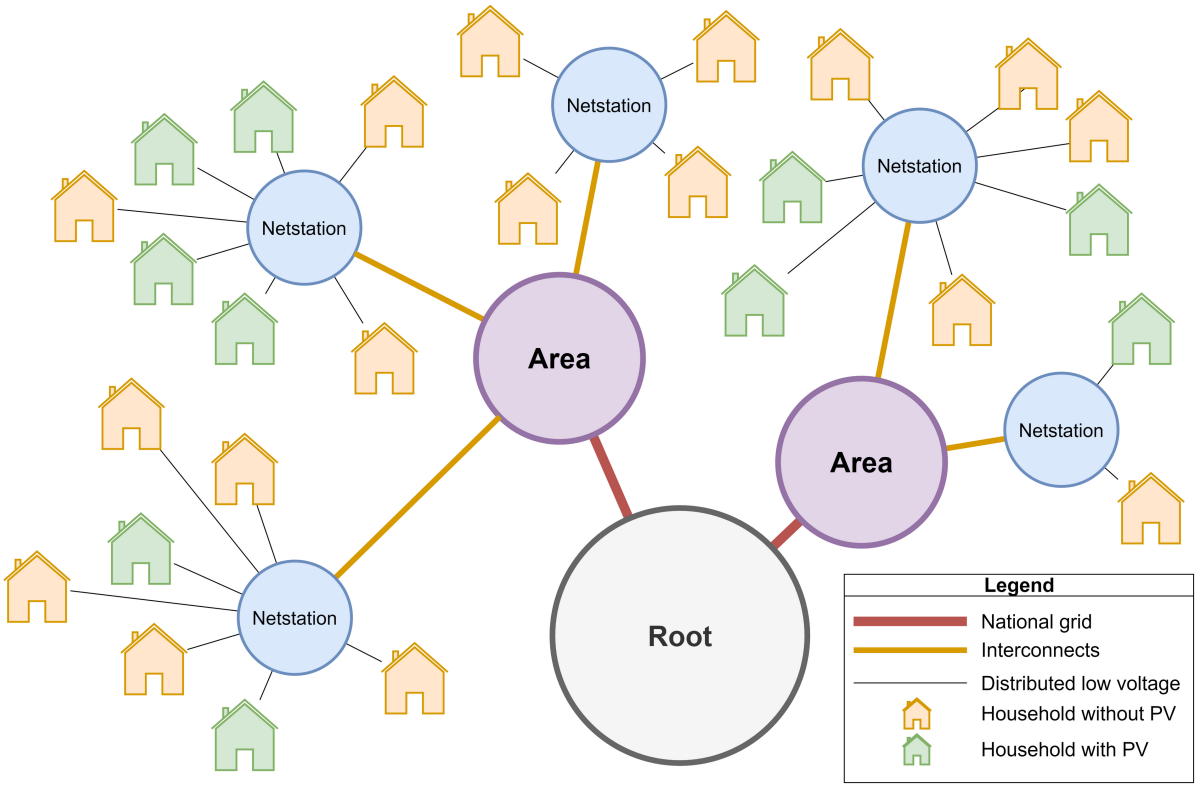

Figure 2.2: Mockup layout of the grid

A distinction is between grid layers:

1. **HV - High Voltage > 100 kV**
   Part of the grid connecting different regions and also connects across borders.
2. **MV - Medium Voltage > 3 kV & < 100 kV**
   Power connections to distribution houses and high consumption companies.
3. **LV - Low Voltage < 3 kV**
   Connections between distribution houses and households.

2.1.3. Roles

Different elements in the grid play an important role. The ones shown above in figure 2.2 are the ones that are included in the model used in this research. A small summary of these roles is given in table 2.1. This overview is incomplete; other elements are also present in the grid. As they are assumed not to impact the research experiments' results, they were left out of scope.

2.1.4. Smart Grid

The foundational blocks for the Smart Grid are currently being developed, and many directions are possible. What is clear is that the power grid will change fundamentally [3, 5, 6, 7]. No longer will there be central points that generate power with many consumers connected to it by the power grid, where the generators are grid-forming [30]. In the future, households will generate their energy using grid-following Distributed Energy Resources (DER) [29] in the form of photovoltaic (PV) panels.

Table 2.1: Roles in the grid used in this research

Role	Description
National grid	The national grid is the grid operator's domain that balances supply and demand. In the Netherlands, the operator is TenneT [27]. On this level, they also connect with other grids across the border [28].
Area	Regional areas distribute the power within a region. It positions itself on the border between HV and MV, delivering power to netstations and bigger factories 'with' high power requirements.
Netstation	Netstations are the distribution houses seen within cities and neighbourhoods. They step down the voltage from MV to LV to enable them to be used by households.
Household	A household is a house or small office building connected to a netstation. It is occupied and may or may not have a DER. Households adopt DER.
DER	Distributed Energy Resources are systems placed inside households and create power locally [29, figure 2]. These devices may house the risks that this research is looking into.

During this thesis, the definition of Smart Grid used is the one proposed by James Momoh [5, p.11]:

"The Smart Grid is an advanced digital two-way power flow power system capable of self-healing, adaptive, resilient, and sustainable, with foresight for prediction under different uncertainties. It is equipped for interoperability with present and future standards of components, devices, and systems that are cyber-secured against malicious attack."

Coordination and communication

Difficulties arise from the coordination needed to keep the grid stable [7, 31, 32]. To coordinate all DER devices in the grid, new paradigms of control are needed [32, 33, 34, 35]. All these paradigms have in common that there will be a massive increase in communication. Similarities are found in SCADA systems, as seen in manufacturing environments, due to considerable geographic distances, cyber-physical systems, and the high number of connected devices [36, 37, 38]. The Smart Grid introduces new concepts to add to the power grid, such as Virtual PowerPlants (VPP) [31, 39], Microgrids [7, 39], and Advanced Metering Infrastructure (AMI) [4, 40]. The concepts are used to reduce the span-of-control of the grid operator and reduce the amount of communication by trying to match on a local level first.

Effects of Distributed Energy Resources on the grid

The power grid is affected by the inclusion of DER. It causes the power quality to decrease [41]. DER devices impact the grid by virtue of being asynchronous power generators [42, 43]. Conventional synchronous generators stabilise the grid's frequency by coupling it to the rotation of their rotor. This damping is not present in the asynchronous variants; thus, more coordination is required [30, 44]. The same issue also impacts the quality of the voltage levels in the grid [45].

2.1.5. Quality indicators

Keeping the grid operational and stable is the main objective. This is what is ultimately required to keep society functioning. Multiple indicators are available to determine the stability and quality of the grid. Below are explained the indicators chosen for the model. Other indicators, such as frequency harmonics, are also present. However, due to the scope of the research, they were not included.

Frequency

50 Hertz is the agreed-upon frequency of the grid in the Netherlands and Europe [46]. If the power consumption increases, all things other being equal, the result is a decrease in the frequency of the entire network [8, p.190]. The change in frequency is proportional to the size of the power imbalance and the total amount of power in the grid [8]. This effect is represented in equation (2.1). The size of the power generation capacity on the grid, therefore, impacts the grid's stability. Measuring the grid's frequency allows the grid operator to adjust supply to the grid's demand.

$$\lambda = \frac{\Delta P}{\Delta f} \tag{2.1}$$

λ = *The network power frequency characteristic* [MW/Hz]
P = *The amount of power imbalance* [MW]
f = *The difference in frequency* [Hz]

Equation taken from [8, Eq 5.18].

Regulation on the grid frequency is found in the Network Code of the European Union [46]. The relevant values for the frequency from this directive are seen in table 2.2. It shows the values the frequency of the grid may have and how long these values may be present.

Table 2.2: Permissible frequency range in Continental Europe - [46, Article 13 - Table 2]

Frequency range	Time period for operation
47,5 Hz - 48,5 Hz	Maximum of 30 minutes
48,5 Hz - 49,0 Hz	Maximum of 30 minutes
49,0 Hz - 51,0 Hz	Unlimited
51,0 Hz - 51,5 Hz	Maximum of 30 minutes

Voltage

Voltage indicators are more suited for local imbalances. The magnitude of the voltage is impacted mainly by the reactive part of the power; this is represented by equation (2.2) and equation (2.3). Tap-changing transformers address the changing voltage levels at local points.

$$\Delta\delta = -[B']^{-1}\frac{\Delta Q_i}{V_i} \tag{2.2}$$

$$\Delta\delta = -[B']^{-1}\frac{\Delta P_i}{V_i} \tag{2.3}$$

$B'B''$ = *Susceptance matrices*
Q = *Real power*
P = *Reactive power*
V = *Voltage*

Equations taken from [47, p9].

Regulation on the grid's voltage is found in the Network Code of the European Union [46]. The relevant values for the voltage from this directive are seen in table 2.3. It shows the values the voltage of the grid may have and how long these values may be present.

Table 2.3: Permissible voltage range in Continental Europe - [46, Article 16 - Table 6.1]

Voltage range	Time period for operation
0,850 pu - 0,900 pu	Maximum of 60 minutes
0,900 pu - 1,118 pu	Unlimited
1,118 pu - 1,150 pu	Maximum of 60 minutes

Area Control Error

The Area Control Error (**ACE**) is an indicator that is calculated [8, Eq.5.26] to determine where an imbalance takes place on the grid. It is a product of measurements of the power flows going into and out of the area, as shown in equation (2.4). Grid operators use this indicator to monitor imbalance [9].

$$ACE_i = \Delta P_i + \lambda_i \tag{2.4}$$

2.1.6. State calculation

Finding the state of the power grid is done by using load flow calculations [8, 47]. The model uses these equations as relationships between the different elements and calculates the next state based on them. This is the mathematical foundation of our model.

Load flow

Load flow calculations provide gain insight into the steady-state behaviour of the network. The analysis that approaches reality the most is the AC load flow variant [8]. It includes the different types of power seen in reality and the different types of loads. The disadvantage is that it is a non-linear problem that needs to be solved numerically.

A DC load flow variant addresses the issue of expensive calculations [8]. Using assumptions to simplify reality decreases the cost significantly. Without this reduction in computational power, generating the data needed would not be feasible. These assumptions include the ”neglecting of the resistance of the transmission lines” and ”The differences between the voltage angles are small” [8, section 6.2].

Fast decoupled load flow method

By decoupling, the computational costs of the state estimation decrease even more. By using the fact that the change in active power primarily shows in the changes to the voltage angles [47] Moreover, the changes in reactive power are influenced mainly by the voltage magnitudes, which allows the decoupling of these different forms of power.

2.1.7. Cascading failures

The power grid is an unstable system that is kept functioning by an enormous amount of coordination. This instability is most prevalently shown in the phenomenon of a cascading failure of the power grid.

Generators connected to the grid have safety systems built in that trip when certain conditions are met, for example, when it overheats [48]. Another trigger is the too-slow rotation of the rotor, the rotation that is coupled to the frequency of the grid. When these safety systems trigger, they disconnect the generator from the grid.

When there is too much load and the power grid is overloaded, the frequency of the grid drops. When a generator is disconnected due to its safety system triggering, the power that was generated by that generator then has to be produced by the remaining generators on the grid. Adding extra stress to an already overloaded grid can result in even more generators being disconnected.

2.1.8. DER adoption in the Netherlands

According to Diffusion of Innovations, the adoption of new technology follows an S-curve [49, 50]. Data from CBS [51], shown in figure 2.3, shows a possible beginning of an s-curve. Currently, almost 20% of households in the Netherlands have PV panels, an increase of 2.5x since 2017 [52] Furthermore, 36% of people in the Netherlands in 2022 report owning solar panels, almost double than in 2019 [53, 54]. This may show that the adoption of DER in the Netherlands is fast on its way.

2.2. Cybersecurity

This section will highlight relevant aspects of the cybersecurity of the Smart Grid. It will do this by taking two approaches. First, it takes a risk-based view by looking at the threats, vulnerabilities and impact. The second aspect is by looking via the CIA triangle [55].

2.2.1. Threat actors

The threat actors to the Smart Grid are described in table 2.4. They are a selection of commonly mentioned threat actors in Cybersecurity, selected on relevance for the Smart Grid. The main threats are Nation-State actors and Organized Crime.

2.2.2. Potential vulnerabilities

As shown in the taxonomy provided by Li et al., multiple types of attacks are possible on the Smart Grid [57, Table 2]. These categories are related to the CIA triangle [55, 56] impacting different aspects of confidentiality, integrity, and availability.

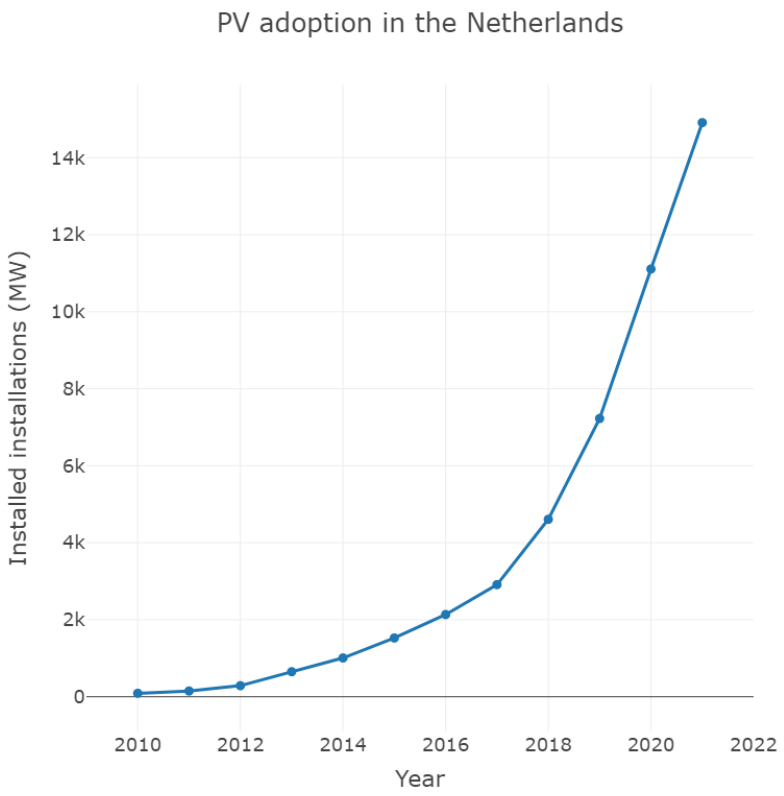

Figure 2.3: Adoption of solar power in the Netherlands

Table 2.4: Threat actors to the Smart Grid, based on NIST [56]

Threat	Motive	Capability
Nation-State	Disrupt the society of a hostile nation. Perhaps as part of a bigger military goal.	Very capable, almost impossible to defend against.
Organised Crime	Monetary gain. By manipulating the market, monetary gains can be made [16].	Reasonably capable, uses advanced techniques.
Individuals	Activism or no real motive, such as a script kiddie.	Low to medium capacity. Will likely use tools made by others.

Table 2.5: Targets that can be attacked in the Smart Grid

Attack target	Description
Device	DER devices are on the edge of the grid allowing physical access. As this type of device is used in many more places, a found vulnerability could be scaled quite easily.
Data	The target is the data sent between the actors on the Smart Grid. Its goal is to destabilise the grid by tricking it into making wrong decisions.
Privacy	These are attacks that threaten the privacy of the end-users. Among others, occupancy can be detectable using this data.
Network	The goal of this attack is to impact the availability of the Smart Grid. This makes it difficult for actors on the Smart Grid to communicate and keep the grid stable.

False Data Injection (FDI)

This research focuses on False Data Injection attacks. In these attacks, the communication between the devices is altered, resulting in a mismatch between the actual and communicated states. This causes instability to occur [58]. As our focus is on the firmware of DER devices, the scenario's attack combines a device attack and a data attack.

The attack can be performed stealthily, bypassing the current detection methods for finding the instability on the grid. It can impact the state estimation of the grid in such a way that it does not trigger any alarms [58]. One aspect that makes this attack more interesting is that financial gain is possible [16]. This introduces an extra reason to attack the Smart Grid.

2.2.3. Detection

For detecting attacks on the grid, many solutions are explored. Traditionally a state estimator is used to see if the measurements align with the state expectations. If the difference between the state estimator and measurement is higher than a threshold, it is flagged [58, Eq. 3]. However, this detection method can be fooled as the state estimator uses previous data as its reference. It can change what the state estimator considers normal by slowly changing it, staying under the threshold [59].

Other solutions proposed include, among others, a Bilevel Attack Model based on pre and post-dispatch [60], using machine learning-based classification [59], and a graph-theory-based solution [61].

2.3. Actor analysis

For this research, an actor analysis has been performed to identify all relevant actors and determine their roles. "An actor is a social entity, a person or an organisation, able to act on or exert influence on a decision." [62, p.79] Actor analysis gives insight into the interaction in the system and provides context. This analysis is documented in appendix A.

The relevant actors are:

1. Grid operator (TenneT)
2. Smart Grid user (Household)
3. Energy producers (Legacy)
4. Agentschap Telecom (Regulator)
5. Local Grid operators

2.4. Economics

Cybersecurity does not only include the technical aspects of security. It involves humans and, with it, economics. Economic principles give insight into the behaviour of humans and companies and allow the prediction of possible outcomes. This section will first cover the topic of economics in cybersecurity, followed by the drivers behind market consolidation, and as topics are introduced that explain the interaction of users with the topic.

2.4.1. Cybersecurity

The economics of cybersecurity has proven to be an exciting topic [63, 64]. Economics can help explain human behaviour making it an excellent combination with cybersecurity. Different economic principles are of interest to this research topic; they are described below.

Return on investment

From a business perspective alone, investing in cybersecurity is tricky. Regular business decisions are based on the return on investment (ROI). As cybersecurity is difficult to quantify, measuring return on investment is impossible with any certainty. This is because one can not say if it would have suffered an attack if the investment was not made. The lack of hard metrics such as ROI produces misaligned incentives within companies regarding security investments [64, 65].

Tragedy of the commons

Cybersecurity can be a *tragedy-of-the-commons* situation because the risk of a security issue is commonplace. In this context, the risk of the grid collapsing by a cyber-incident is not felt by the DER manufacturers. This decoupling of a negative consequence and economic activity is called an externality [66].

First mover advantage

At the same time, manufacturers have the incentive to skip security to be first in the market, the so-called first-mover advantage [67]. First to market is crucial to have the most significant market share [67]. Security is not relevant for release; as such, it is forgotten, creating an externality [63]. This results in a *race-to-the-bottom* regarding security if not addressed with regulation.

2.4.2. Market consolidation

General economics also has relevant aspects regarding DER and the Smart Grid. Relevant to this is the role that market consolidation plays [68]. A study commissioned by the EU shows that these kinds of products, like DER, in the EU's single market, are highly suited to create a highly consolidated market [12].

Economy of scale

Market consolidation is relevant in the scope of this research because it reduces the number of different DER devices produced. As IoT devices have shown, this allows a detected vulnerability to scale enormously [13].

The mobile phone market is an example of market consolidation in the technical field. A study by Cerre found that most countries have only three or four different manufacturers [69]. In 2022 in the United States of America, the top two manufacturers had 85.67% of the market [70]. A vulnerability in one of them would have an enormous impact because of the economy of scale.

2.4.3. Users

The interaction between users and DER devices concerning security also has interesting aspects. They are the owners of the device that produces the electricity, which can pose a risk to the grid.

Market for lemons

Cybersecurity is generally not considered when purchasing a DER device, such as a PV system. This is because the consumers face information-asymmetry [65]. The vast majority of users will not have the expertise to determine the level of security of a device. Furthermore, they probably do not care because they, as an individual, do not own the negative consequence of the risk. A *race-to-the-bottom* situation for consumers. This information asymmetry leads to less secure products because the added value of the security is not known by the consumer [63]. A situation that is called a *market-for-lemons*.

Rejection of Security Advice

Even if all potential risks are known by the consumers, likely, they will not act accordingly [71]. People are bad at assessing risks, especially in complex situations like the Smart Grid. As a result, the risks of DER devices will not be addressed by the combination of the market and consumers.

2.5. Regulation

Regulation gives governments the means to address the unwanted economic behaviours addressed in the previous section. It can also create means that can be acted on to address cybersecurity issues.

2.5.1. Grid regulation

For the power grid, relevant regulation includes the Network code directive [46] implemented in the Netherlands as the NetCode [72]. The requirements for participating in the power grid are defined in this.

Requirements for generators

Relevant regulations for power generators can be found in the NetCode [72, Chapter 3]. Including asynchronous generators requires updating the power grid legislation [42] as they differ vastly from regular synchronous generators.

The NetCode also provides the means for network operators to use a contract to require power generators to adhere to their agreements. However, this does not cover cyber-security-related aspects.

2.5.2. Economic regulation

The European Union has taken the lead in defining new legislation to define responsibilities by avoiding the tragedy of the commons by not assigning the cost of externalities [64]. Regarding cybersecurity, critical legislative pieces are the NIS directive and its successor, NIS2. They require providers of essential services, such as those involved with the power grid, to control their cyber risks.

Furthermore, manufacturers must implement security and privacy by design principles when creating new products [21]. The same regulation also makes manufacturers responsible for providing security updates for the entire lifetime of the devices they create [21].

2.5.3. Privacy

The GDPR is also relevant as the users' privacy needs to be protected, most notably at the level of the Smart Meter [73, 74]. When consumers are confident in the protection of their privacy, they will adopt measures or innovations faster [75].

2.5.4. Institutional change

With this power grid change towards the Smart Grid, institutions that accompany it must also change [76]. Their roles are being redefined at this moment, and everyone is trying to find their new role, including the regulator [17]. This brings a lot of friction and uncertainty about who is responsible for what [77] impacting the cybersecurity aspects. If not done correctly, certain crucial aspects can be overlooked in this hectic time.

2.6. Modelling

The goal of the model is to simulate the behaviour of the grid in specific scenarios. As the focus of this research is the future risks of the Smart Grid, this entails that the current grid is not suitable for obtaining relevant data. The enormous change in the power grid brings with it many unknowns. Reducing this uncertainty is done by simulating different aspects of the Smart Grid. A model, therefore, is needed.

System Dynamics

Different models could be used, for example, System Dynamics [78]. This method relies on mathematical equations for dynamic modelling. The most appropriate diagram, in this case, would be a Causal Loop Diagram (CLD). It connects all high-level concepts mathematically; it would be an expanded version of figure 4.1. Due to the high interdependencies of the grid and the communication and reduced flexibility of the grid layout in this way of modelling, this method is not chosen.

IEEE Bus System

From a grid simulation perspective, the use of the IEEE 13 bus system would be logical [79]. It is battle-tested and comes with predefined mathematical-correct behaviour. However, as the grid is changing towards Microgrids and other new concepts introduced in section 2.1.4, this system is not guaranteed to be correct.

Agent-Based modelling

The method chosen is Agent-based modelling (ABM). The concept behind ABM is that ”many phenomena, even very complex ones, can best be understood as systems of autonomous agents that are relatively simple and follow relatively simple rules for interaction” [80]. The agents in the grid are relatively simple to create and are well-described. The interactions between them as well [8].

Current Smart Grid Models

There are currently already simulations of the Smart Grid. The GridLAB-D [81] and Panda Power [82] frameworks are efforts that aim to speed up the creation of models of the Smart Grid, which also are ABM. Digital twins [83] simulate the grid as a whole; this provides the most accurate image of a future system. However, they are the most time-consuming to implement and are very time-consuming to run. Other systems focus on the stability and quality of the grid [44].

Employing a graph-based architecture that focuses on the connections of the grid allows the accurate modelling of energy flows [84]. When communication and coordination is the goal of the model, a data-centric approach is taken [40, 85].

Literature also finds efforts to simulate the Smart Grid’s security. A framework to simulate cyberattacks on the Smart Grid [86] builds on GridLAB-D, adding cyber attacks to it. Testbeds are simulations created to see how the Smart Grid will react to being attacked [87, 88]. Evaluating the security of control systems is done using a co-simulation platform [37]. An explanation of why these are not used can be found in section 2.6.

3

Related Work

This chapter presents an overview of the academic publications relevant to this research. As mentioned in the introduction, to the author's best knowledge, this is the first research into this combination of fields. As of writing, only a footnote in a report of October 2022 mentions this risk in passing [89].

Therefore, works will be discussed from the interactions of three identified fields that provide insight. This method is shown in figure 3.1. The Cybersecurity field and the Smart Grid field are chosen as they are foundational blocks for this research. The IoT field is chosen as it is a simile for Distributed Energy Resources and is much more developed.

The first section focuses on cybersecurity in combination with the Smart Grid. Secondly, research on IoT technologies in the Smart Grid is presented. The cybersecurity aspects of IoT technologies follow afterwards. Closing this chapter is a discussion of the research gap identified that this research aims to address.

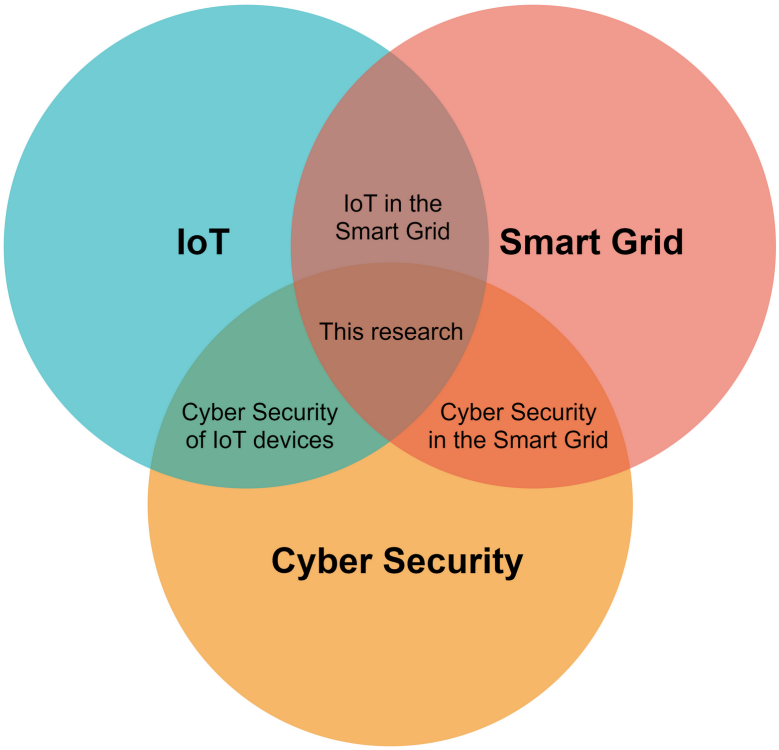

Figure 3.1: Positioning of this research

3.1. Cybersecurity in the Smart Grid

Publications on a broad front cover the cybersecurity aspects of the Smart Grid. Academic research extensively defines the threats to and possible attacks on the Smart Grid and their prevention and detection [90, 91, 92]. Attention is even given to the practicalities of assessing the Smart Grid's resilience to cyber-attacks [93, 94, 95, 96] and with specifics on AMI testing [97].

The immense impact of a successful attack makes this attention well deserved [98, 99]. Among the effects are most notably, voltages sags [30], frequency drops [14], and cascade failures [100] that all can lead to blackouts [96, 101].

Threats and attacks

Potential targeted attackers of the Smart Grid include nation-states in the form of Advanced Persistent Threats (APT) [100]. The disruption of power delivery is their goal in itself [96, 102]. However, a monetary gain could also be a reason to perform a cyberattack [16]. By utilising the electricity price market, an attack can leverage an attacker to obtain profits [103], expanding the scope of threats Untargeted attacks are also an issue for connected devices, as seen in the example of the NHS and Wannacry [104].

Different kinds of attacks on the Smart Grid are possible; most commonly, they are differentiated by the aspects they target [100]. Options include attacking the device, invading users' privacy, focusing on the data sent, and attacking the network. The quickly gained physical access to DER on the Smart Grid allows hardware attacks [105], such as key-extraction [106, 107].

User privacy is essential for adoption and legislation [73, 74]. False Data Injection (FDI) is the topic regarding Smart Grid attacks that has gained the most attention. This type of attack focuses on creating a difference between the expected and actual behaviour of a device [16, 60]. The network itself is vulnerable to topology attacks [108, 109] including line disconnection [110, 111].

Further specificity is also found in attacks that focus on creating the most amount of damage by coordination [112], attacking the Advanced Metering Infrastructure [113] or the use of Electric Vehicles [14].

Protection and detections

That the Smart Grid needs protection is clear. Multiple architectures have been proposed to achieve this protection. Current research only includes possible approaches, as the architecture and underlying technologies of the Smart Grid are still unclear.

A centralised approach using a Security Information and Event Management (SIEM) [22, 114] is possible, as is the implementation of an Intrusion Detection System [115]. These options most closely resemble the grid monitoring of the present day. False Data Injection attacks or Dynamic Load Altering attacks can, for example, be discovered with this architecture using AC State Estimation [116], Robust sliding mode observer [117], and Graph Theory [61, 118]. A specific subset of this approach is detecting attacks on the Advanced Metering Infrastructure of the grid [99].

Most architectures use an agent-based approach [40, 119, 120], using DER to monitor their neighbours in the Microgrid [112, 121]. One of the reasons to choose this architecture is because it removes the single point of failure in the grid supervision [121].

Machine learning methods that are used to detect attacks are Semi-Supervised Deep Learning for FDI attack [59], Ensemble Learning for anomaly-based intrusion detection systems [122], Extremely Randomized Tree-based schemes [123], and Reinforcement Learning [124].

3.2. IoT technologies in the Smart Grid

The link between the Smart Grid and IoT has been made multiple times [101, 125]. Often this is because of the high number of devices, the massive scale of communication, and the cyber-physical aspects [125]. Furthermore, the agent-based structure of proposed concepts in the grid, mainly in the coordination used to balance the grid [126], are very similar to IoT systems. Coordination structures will likely rely on the autonomous actions of the DER systems [32].

The topic of cybersecurity regarding IoT and the Smart Grid is also found in literature [92, 100]. It includes topics focusing on the communication protocols that resemble IoT protocols [127]. Furthermore, standardisation and certification are also proposed in this combination of IoT and the Smart Grid [128].

3.3. Cybersecurity of IoT devices

IoT devices are a relatively new concept as a class of devices when compared to servers and personal use laptops. They are devices that are usually stand-alone, are often used as a cyber-physical system, and require no interaction from the user besides their functionality. As mentioned by the reasons in section 2.4, a lack of regulation has led to cybersecurity issues. This is why the European Union, in the form of ENISA, published multiple guides to implement security for IoT devices [129].

The scale of an attack when a vulnerability in an IoT device is found can be enormous. The most prominent example of an attack is the Mirai botnet [13], which caused the largest DDOS attack ever recorded. The high amount of physical devices created in combination with the use of identical firmware are to blame.

Compared to other cyber-physical systems, such as OT systems found in manufacturing, the difference is that IoT devices are more likely to be attacked. This results from the fact that IoT devices have a much bigger attack surface [97, 113]. Most of them are connected to the internet and not behind network segmentation or NAT. This issue may become even more pressing when IPv6 is the default connection used [130].

Attacks that use a physical component are more prevalent on IoT devices. Key extraction from hardware is possible [92, 107], and if the key infrastructure of the device ecosystem is not well thought out, this could allow the attacker to scale horizontally. Another threat derived from physical access is the possibility of firmware dumping. When the firmware is dumped, it could be analysed to find vulnerabilities or exploits much faster [92].

3.4. Research gap

This research focuses on the intersection of all three topics: Cybersecurity, IoT, and Smart Grid. This is not the only research found in this intersection. Testing the IoT Smart Grid using a proposed security framework is found [131]; it does not address the causes of potential vulnerabilities, in contrast to this research. An IoT attack was already made Distributed Energy Resources in the Smart Grid [132]. This research focussed on a vulnerability in implementing a TCP/IP stack shared across many devices. This vulnerability is used to attack different devices connected to the grid, presenting a proof-of-concept. The difference between it and this research is the development over time and the effect on the Smart Grid. It also does not address the underlying factors that cause vulnerabilities.

The identified gap focuses on the IoT risk of attacks scaling horizontally and the underlying causes that increase grid instability. Because of the market concentration, shown in section 2.4, and the necessity for coordination, attacks can likely quickly spread. The homogeneity of the DER in the Smart Grid also might prevent the agent-based detection methods as the neighbouring devices could also be impacted. It is easily imagined that a real-estate developer might select a single DER manufacturer when building a new neighbourhood.

As little research is done on this topic, there are currently no means for regulators to mitigate this specific risk; as discussed in section 2.5. This risk and its mitigation could not be found in current research and is therefore chosen to be the topic of this research.

4

Methodology

This chapter focuses on the method used to obtain the information used to answer the research question. An explanation of why the method is used is found in section 2.6. First, a description of the model that is built is given. Secondly, the assumptions made in the model's making are highlighted. Then the input parameters are described to make different scenarios, followed by the collected data that acts as output.

4.1. Model

An Agent-based model is built to answer the research question. As the model focuses on the cybersecurity issues of the grid, already-built grid simulation efforts did not provide enough flexibility to simulate an attack. Because these models aim to be as accurate as possible regarding the power calculations, they are also much more expensive to run regarding computational costs.

Cybersecurity testbeds that were found did not focus on the horizontal escalation of a cybersecurity attack when looking at the kind of risk this research is focussed on. As a result, the scale of the model did not accurately reflect the grid size on a national scale. The choice is made to program a simulation model from the ground up that fulfilled the requirements in table 4.1.

4.1.1. System boundary

A border needs to be drawn when building a model, the system boundary. It decides what is included in the model and what is left out. The goal is to make the model as small as possible, including only what is needed.

The model created for this research has chosen to limit the scale of the grid to a national level. This is done as data for the national level of the Netherlands is available, allowing validation of the model. The downside is that an interconnected grid is more resilient to power swings. However, countries with a connected grid also are part of the EU single market. As such, they have the same market consolidation in DER.

Furthermore, power generation plants are not included as agents in the model. They are not part of the IoT risk identified in this research and are represented at the root level as bulk generation. In the same idea, big power consumers like factories are not included and are represented at the root level as bulk consumption.

4.1.2. System diagram

A system diagram is used to give insight into the behaviour of a system in general by showing how relevant factors interact with each other [62, 133]. The goal of this diagram is to give insight into the system that is being modelled. This information is needed to verify later that the model is generating the expected behaviour.

Table 4.1: Model requirements

Requirement	Reasoning
Flexible grid design	Due to the uncertainty of how the Smart Grid will look, flexibility in the grid setup is needed. This research also focuses on the emergence of the identified risk; as such, every step towards the new grid needs to be able to be produced.
National scale	As the desire is to simulate an attack that will scale out horizontally, it is important to get the scale of the grid correct.
Accurate frequency and voltage values	The focus of the research is the grid's stability when it is under attack. The quality indicators frequency and voltage give the grid stability. Therefore these values need to be accurate.
Short runtime	Identifying when the identified risk is of impact to the Smart Grid is one of the goals of this research. Therefore multiple stages of DER adoption are needed to simulate. To be able to perform all these different experiments, a short runtime is required.
Adjustable step size	The industry standard in the grid is for data to be collected at a 15-minute interval; this is the base value for the step size of the model. However, for future-proofing and looking at smaller timeframes, this value needs to be an input of the model.
Predictable output	To obtain reliable data that can be used to compare results, the model's output needs to be predictable. This can be achieved by using seeded PRNG instead of true RNG.
Answer research question	The model needs to provide the data needed to answer the research questions of this research or provide insight to answer the research question.

In figure 4.1, the adoption of DER into the Smart Grid is modelled, focusing on the cybersecurity risks accompanying it. Interesting aspects are the loop seen in orange and the multipliers in blue. The loop shows a positive feedback loop within the system that drives the IoT-DER penetration in the market while reducing the variety of devices. This increases the risks this research is focussing on. The multipliers are relevant because they indicate that adopting DER into the Smart Grid does not lead to a linear increase in risk. It increases the risk significantly more than that.

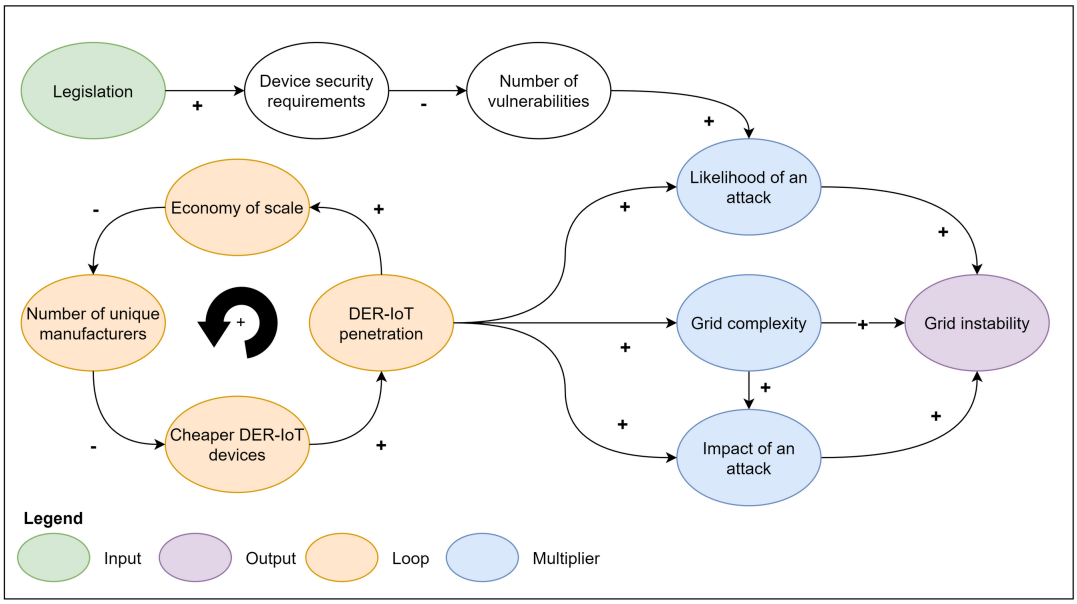

Figure 4.1: System Diagram

4.1.3. Coding

To fulfil the requirements of the model, it is built in Rust using a graph layout. Rust is ideal as it is very fast to run when compiled. Fulfilling the requirement that an experiment has to be completed in a relatively short time. Furthermore, its type system and borrow checker help verification of the model. The input for the model is three parameter files: the grid, attack and model parameters. They are explained further in section 4.3.

The model's output is given as a log file per run that logs any errors or warnings from the grid. Also, it can save the state of the grid per step it takes. When developing, attention was given to the possible further development of the model, preventing choices that would limit expansion where possible. This is also described in more detail in section 4.4.

Every decision in the model that uses RNG is made using a PRNG seeded with a seed in the model parameters file. This allows the model to obtain the same results whenever nothing has changed. Giving it a predictable nature that is suited to run experiments.

4.1.4. Agents

Agents are the decision-making units in the model. They are the Root, Areas, Netstation and Households roles as mentioned in section 2.1.3 and the regulation capacity of the grid.

Average power

All households have an average power consumption target determined when the agent is created in the code. It obtains this value using the seeded PRNG and a Uniform distribution, both given in the parameters files. This value is not changed during the run of the model.

Generation and consumption

Generation and consumption of power follow the distributions given by MFFBAS [134], a collaboration between grid parties. It changes during the course of a day. For variety between households, there is also a noise component. The parameters of these are also able to be set via the parameter files.

Regulation capacity

The regulation capacity of the grid is modelled as a bandwidth of power regulation capacity available when running the model. The values from these were derived from TenneT, based on historical data [135].

The model starts with the used capacity at zero and then tries to compensate for the power error using the capacity it has. Limits to the possible compensation are the bandwidth limits and the amount of compensation it can do per single step. These parameters are also given in the parameter files.

4.1.5. Powerstate

The powerstate of an agent is the summary of the power flows that are related to the agent and is the foundational data structure used for grid state calculations. In this state, certain aspects are included; they are described in table 4.2. The powerstate forms the foundational data structure used to calculate the grid's state.

Table 4.2: Powerstate description

Aspect	Description
Power generated	Power generated by the DER in case of a household or summed from the agent's children.
Power consumed	Power consumed by the agent in case of a household or summed from the agent's children.
Power used	Power consumed - power generated.
Power reported	Power used communicated to the grid by the DER in case of a household or summed from the agent's children.
Power error	Power reported - power used.

4.1.6. Actions per step

Below is described the list of steps the model takes during each step/tick of the model.

1. *Update the current step value in all agents.*
2. *Generate new powerstates for the households.*
3. *Try to infect vulnerable households.*
4. *Try to patch infected or vulnerable households.*
5. *Change the powerstate of the infected devices.*
6. *Calculate the powerstate for netstation, area and root agents.*
7. *Try to compensate power mismatch on a grid level.*
8. *Calculate the impact of the power mismatch.*
9. *Report if the voltage and/or frequency boundaries are crossed.*
10. *Output grid state, if desired.*

4.2. Assumptions

Simplifications and assumptions were made to make the creation of the model feasible. In table 4.3, they are made explicit and given a reason for doing it. The main reason for making these assumptions is for simplicity, reducing the complexity of the model.

Table 4.3: Assumptions

Assumption	Reasoning
Linear relation voltage and power mismatch	An power mismatch causes the voltage to change using a more complicated method than is done with frequency. However, this relationship is partially linear, as shown in equation (2.2). A simplification was made to replace this relationship with a fixed parameter given to the model.
Only active power	Due to the previous assumption and the fact that frequency only changes on the total amount of power delta, there is no need to simulate a complex power system.
DER only as PV	Only PV panels are simulated as DER in this model. This is because, currently, they are the only type of DER adopted on a bigger scale by society.
Grid simplification	No capacitance or resistance is modelled in the grid. This research focuses on the cybersecurity risks, not the actual power grid simulation.
No storage at houses	No local energy storage is modelled at the households. Storage could impact the behaviour of the grid; however, currently, there is no significant adoption.
Static regulation capacity	The regulation capacity of the grid operator is static. It does not change over time, even though this would be likely as the grid operator would see that it reaches its limit.
Distributions	Distributions used are uniform or normally distributed. This is not completely truthful to reality. However, it does not impact the validity of the model's results.

4.3. Input

Giving the model input is done using different parameter files. There are three different files split into the usage of their contents; model, grid, and attack. The model file only discusses options related to the general settings of running the model. It will not be described below; however, more information can be found in the documentation of the model in the repository.

Grid parameters

The grid parameters describe the construction of the grid and the power characteristics of the grid. Further details are given in table 4.4 and can also be found in the documentation of the code.

Table 4.4: Grid input parameters for the model

Parameter	Description
n areas	The number of areas included in the model; they are the children of the root agent.
ns per a	The number of netstations per area. A uniform distribution's lower and upper bounds are given that are used when creating the grid.
hs per ns	The number of households per netstation. Also given as a lower and upper bound of a uniform distribution.
num noise functions	Number of noise functions that are used to create a variance in household power consumption and generation.
percentage noise on power	The percentage of noise to the average power used.
percentage generation of usage	The percentage of power generated by the DER to the average power used.
pv adoption	The percentage of households with a PV installation. A random number is generated when generating the grid; if it is smaller than this value, the household has a PV installation.
max gen inc tick	Amount of compensation possible from the regulation capacity of the grid per tick.
energy storage	Upper and lower bounds of regulation capacity.
power consumption bounds	The average power consumption of a household is determined by creating a uniform distribution using the upper and lower bound given in this parameter.
bulk consumption	The amount of bulk consumption present in the grid. More bulk consumption produces a more stable grid as change is relative.

Attack

All available options for the attack are described in table 4.5. Further details are given in table 4.5 and can also be found in the documentation of the code.

Table 4.5: Attack input parameters for the model

Parameter	Description
percentage vuln devices	The percentage of vulnerable PV installations.
infection rate per step	The likelihood of a vulnerable PV installation to be infected.
patch rate per step	The likelihood of a vulnerable or infected PV installation to be patched.
infection start	The step on which the infection starts.
patch start	The step on which the patching process starts.
attack behaviour	A list of behaviours that infected devices perform. Per behaviour, the start, end, and modifiers are given.
patch stop	The step on which the patching process stops.
infection stop	The step on which infection stops.

4.4. Output

The output of the model is used for answering the research question. To obtain the answers, the model outputs data in two different ways. It can log the state of the model at each step. However, the primary way of obtaining answers is using the log file created by the model. The log file contains the warnings and errors generated by the model.

The grid warnings and errors are produced when the boundaries show in table 2.2 and table 2.3 are crossed. Warnings are produced when the grid deviates from routine behaviour. Errors are generated when the deviation is present longer than allowed.

Frequency output

Frequency is checked at the root node as this is universal across the grid. A single check reduces the computational cost of running the model. The regulation capacity of the grid mitigates the impact of the power mismatch for frequency.

Voltage output

At the level of netstations is where voltage levels are calculated and checked. This is because this is the level on the grid where the power mismatch is generated and not separated by a transformer. Each netstation has a tapped transformer to reduce the voltage for the households. This transformer can change its reduction factor. Due to this effect and the fact that mitigation is not done on this level, each step is independent and not impacted by the previous steps.

4.5. Validation and Verification

When a model is made, it needs to be validated and verified to check the validity of the result. Verification is checking if the model behaves as it is designed. Validation is comparing if the behaviour of the model conforms to reality.

4.5.1. Verification

Verification of the model is partially done by using the characteristics of the Rust programming language. Using the type system, all values are modelled with the correct unit. This ensures that no values can be used where they are not intended. Furthermore, the borrow checker in Rust prevents unwanted changes in the values during simulation. Tests were also written for the key parts to ensure proper behaviour.

4.5.2. Validation

Two options can be used to validate the model. It can be validated by experts who deeply understand the modelled system. The other option is to validate the model by using data. Simulating the current grid and comparing the output data with current data shows that the model generates correct information, at least for the current grid. The assumption is that the same underlying principles will produce relevant results. The data available for this research are the open data provided by TenneT, MFFBAS and data given by Enexis for this research.

Examples of the validation performed are provided in figure 4.2 and figure 4.3. In these figures, a reference line is shown that is created from the open-source data provided by MFFBAS. To compare this with the values produced by the model, it created distributions for 100 different households. The minimum, maximum and mean are derived and plotted in the figures from this information. As is shown, the distributions are similar.

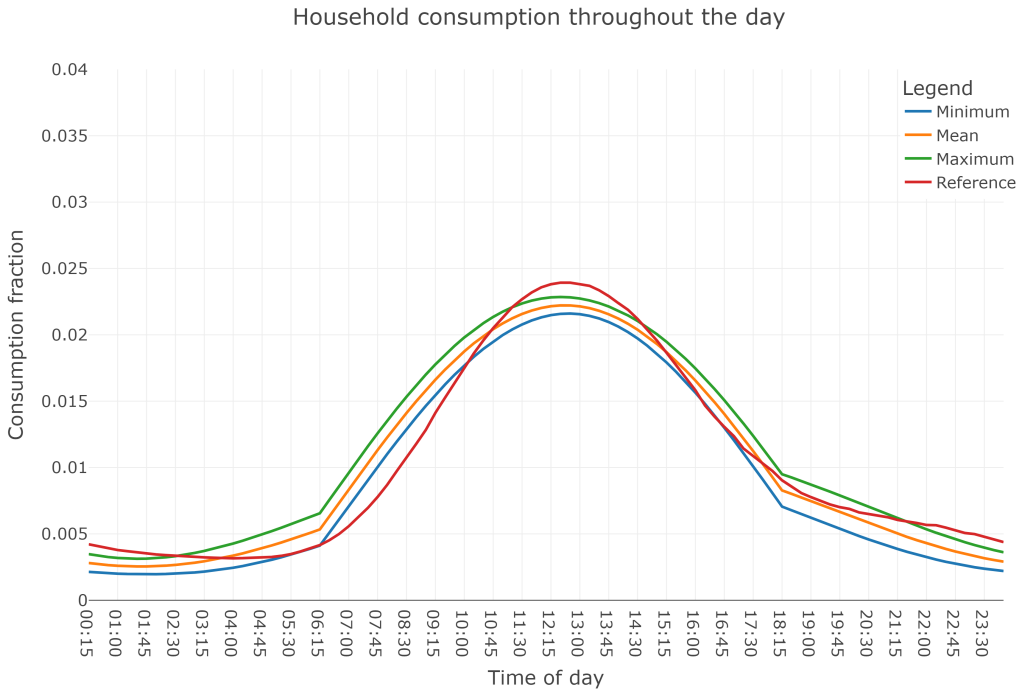

Figure 4.2: Validation of power consumption distribution

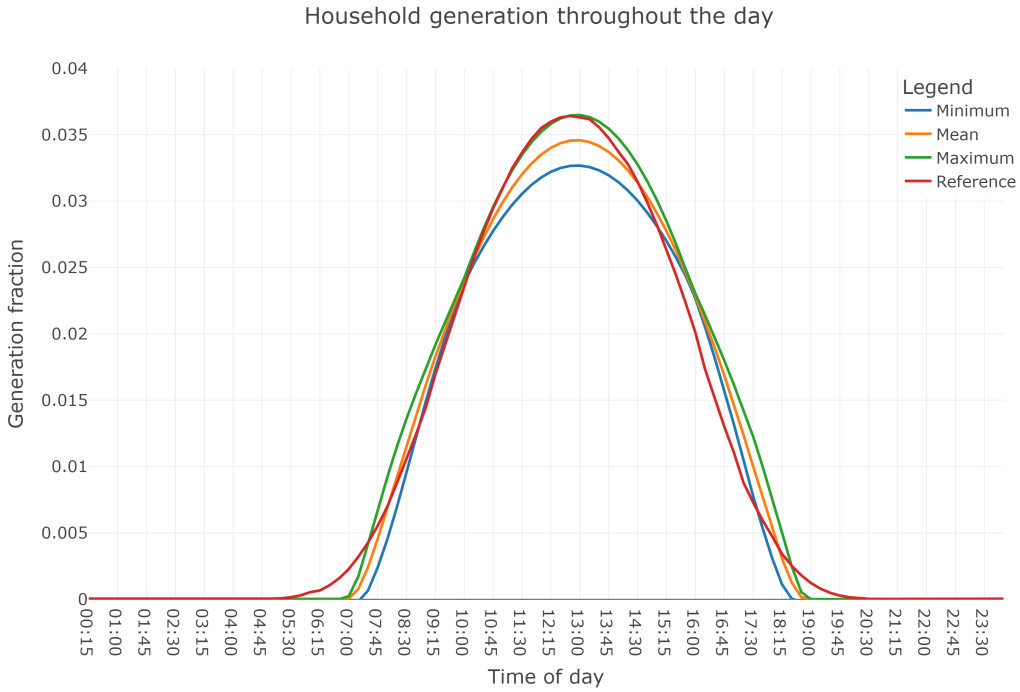

Figure 4.3: Validation of power generation distribution

4.6. Experiment design

The model created in this chapter uses the model to translate the input parameters to output data. Answering the research question is done by looking at what combination of input parameters produces specific behaviour.

Not all parameters described in the input are used to create scenarios. Each scenario is a separate run of the model. The parameters used for creating scenarios are selected as they are the most relevant to answering the research question. The chosen parameters are described in table 4.6. Values for the parameters are derived from real-world data. TenneT provided open data, and Enexis was willing to share real-world data. The values to create the grid were derived from this provided data and are shown in table 4.7.

The creation of the experiments is done using an orthogonal experiment design. This entails that all possible combinations of all values per parameter are generated. As a result, 8100 different scenarios were created and run. These scenarios cover the changes in DER adoption, grid layout, and market consolidation. The scenarios for the model only include one type of attack. This is done to limit the scope of the research because it is not likely to impact the research goal.

Computing cost

Each scenario takes around 40 seconds when run on a Microsoft Azure Standard_F8s_v2 VM (8 cores, 16 threads, 3.4GHz, 16GB Memory, AVX-512). In these 40 seconds, the grid is created and populated with around 8 million agents. All these agents take 250 steps, each representing a 15-minute interval. During each step, statistics are calculated and outputted to the log file.

Table 4.6: Different values used to create the scenarios

Parameter	# values	Values used
seed	2	117, 2010
Percentage of vulnerable devices	6	0.0, 0.2, 0.4, 0.6, 0.8, 1.0
Adoption of DER systems	5	0.0, 0.25, 0.5, 0.75, 1.0
Percentage of power generated	5	0.0, 0.25, 0.5, 0.75, 1.0
Amount of regulation capacity	3	42000000, 31500000, 52500000
Amount of regulation capacity	3	850000000, 637500000, 1062500000
Amount of bulk consumption	3	10000000000, 7500000000, 12500000000

Table 4.7: Values used to create the grid

Parameter	Values used
number of areas in the grid	20
number of netstations per area	(200, 300)
number of households per netstation	(120, 200)
percentage of noise on power	0.15
attack behaviour	”(24,250,1,0)”

5

Results

This chapter will describe how the data generated by the methodology from the previous chapter will be parsed into information that can be used to answer the research question. At first, the parsing will describe how the data obtained from the model is made usable for analysis. Then tests will be undertaken to determine the emergence of the risk, followed by its materialisation.

5.1. Parsing data

The log files of each scenario are parsed and turned into a collection of metrics. These metrics were devised to reflect the grid's stability during its run and are shown in table 5.1. Combined with its input parameters, each scenario becomes a row in the data frame created from this experiment. The values in the factors *Amount of bulk consumption*, *Amount of regulation capacity*, and *Amount of regulation capacity* have their values changed by effect encoding as only their effect is essential.

Table 5.1: Parsed experiment parameters

Parameter	Voltage (V) or Frequency (F)	
Lowest value during the run.	V & F	Ratio
Highest value during the run.	V & F	Ratio
Had any warnings or errors during the run.	V & F	Categorical
Amount of warnings during the run.	V & F	Ratio
Amount of errors during the run.	V & F	Ratio
Time to the first warning in the number of steps since the start.	V & F	Ratio
Time to the first error in the number of steps since the start.	V & F	Ratio
Amount of steps between the first warning and the first error.	V & F	Ratio
Amount of unique netstations that produced a warning.	V	Ratio
Amount of unique netstations that produced an error.	V	Ratio

5.1.1. Insight

After creating the data set, the first step of the data analysis is getting insight into general trends. With this insight, the direction of the analysis can be determined and used to explain the observed behaviour. Two methods are used to find the input parameters' influence on the grid's stability. These are simple descriptives and the ANOVA method.

Descriptives

The first step is to check if the input parameters, table 4.6, led to a difference in the number of errors and warnings. The data set is first separated into a subset of scenarios with errors and warnings and a subset without them. The results are shown in table 5.2 and the boxplot of figure 5.1.

Interesting to see is that the mean of *Amount of bulk consumption*, *Amount of regulation capacity*, *Amount of regulation capacity*, and *Percentage of power generated* are identical, indicating no impact on the grid's stability. The *Percentage of vulnerable devices* and *Adoption of DER systems* factors have different means, indicating an impact. This is an indication that this research is looking in the right direction. What is notable is that *Adoption of DER systems* seems to impact the results more than the *Percentage of vulnerable devices*, as indicated by the considerable difference in the mean.

Further indication that both factors impact the grid stability is the minimum values found in the group with errors. Both need to be present to impact the grid. The values listed here are the lowest options that were not zero used in creating the scenarios.

Table 5.2: Data descriptives split on having errors or warnings

With errors or warnings, n=5397				
Factor	**Mean**	**Std.**	**Min**	**Max**
Amount of bulk consumption	0.000	0.816	-1.000	1.000
Regulation capacity increase step	0.000	0.816	-1.000	1.000
Amount of regulation capacity	0.000	0.816	-1.000	1.000
Adoption of DER systems	**0.625**	0.279	**0.250**	1.000
Percentage of power generated	0.500	0.353	0.000	1.000
Percentage of vulnerable devices	**0.600**	0.282	**0.200**	1.000
Without errors or warnings, n=2703				
Factor	**Mean**	**Std.**	**Min**	**Max**
Amount of bulk consumption	-0.000	0.816	-1.000	1.000
Regulation capacity increase step	-0.001	0.816	-1.000	1.000
Amount of regulation capacity	-0.000	0.816	-1.000	1.000
Adoption of DER systems	**0.250**	0.353	0.000	1.000
Percentage of power generated	0.500	0.353	0.000	1.000
Percentage of vulnerable devices	**0.300**	0.360	0.000	1.000

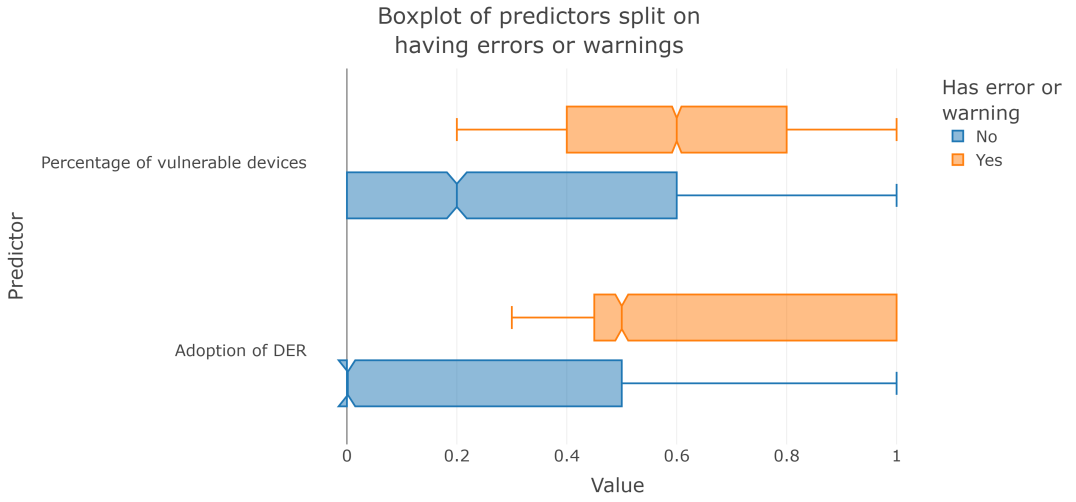

Figure 5.1

ANOVA

The next step is to check if the differences are statistically significant by using the analysis of variance (ANOVA) method. ANOVA hypothesises that the means are derived from the same population and that the grouping factor is not of impact. It computes an F-score and the accompanying probability of the validity of that hypothesis. The hypothesis is rejected if this probability (p-value) is lower than a chosen alpha; in this research, 0.05. The prerequisites checks for ANOVA are that the distributions of all groups are homogenous and the remaining variance is distributed normally.

Table 5.3: Anova results for identifying relevant factors - $\alpha < 0.05$

Dependent	Predicting factor	p-value	F score	Homogeneity / Normal distributed
Has frequency warnings				
	Adoption of DER systems	0.000	2205.396	T / T
	Percentage of vulnerable devices	0.000	1336.206	T / T
	Amount of bulk consumption	0.008	6.942	T / F
Has frequency errors				
	Adoption of DER systems	0.000	2691.353	T / F
	Percentage of vulnerable devices	0.000	1670.963	T / T
Has voltage warnings				
	Adoption of DER systems	0.000	3591.412	T / T
	Percentage of vulnerable devices	0.000	3276.509	T / T
	Percentage of power generated	0.000	134.640	T / T
Has voltage errors				
	Adoption of DER systems	0.000	3364.383	T / T
	Percentage of vulnerable devices	0.000	3237.748	T / T
	Percentage of power generated	0.000	141.052	T / F

The results of the ANOVA test shown in table 5.3 show that the *Adoption of DER systems* and the *Percentage of vulnerable devices* influence all error and warning groups. Interestingly, the percentage of generation is only found with voltage errors; the suspicion is that it is due to the modelled behaviour of the tapped transformer that can change its step-down characteristics. Furthermore, the *Amount of bulk consumption* factor, which is a stand-in for the size of the grid, shows that it only contributes to the frequency warnings, not the errors. This indicates that it probably has a weaker impact on the grid's stability in the model, also indicated by the lower F score.

5.1.2. Factor creation

While gaining insight, the data appeared to have high multicollinearity between the *Adoption of DER systems* and *Percentage of vulnerable devices* factors. This may cause higher confidence intervals when determining the influence of each variable on the dependent. One solution for this is to create a new factor that counteracts this.

Vulnerable households

The factor *Percentage of vulnerable households* was created as a product of *Percentage of vulnerable devices* and *Adoption of DER systems*. In table 5.4, the F scores of the calculated factor and the factors it is derived from. From these numbers, an indication can be seen that the *Percentage of vulnerable households* is a better predictor due to its score being higher than *Percentage of vulnerable devices* and *Adoption of DER systems*. The considerable increase in the voltage groups is notable, especially compared to the frequency groups.

Table 5.4: F score of ANOVA test on the grouping factor on the presence of warnings and errors

Grouping factor	Frequency warnings	Frequency errors	Voltage warnings	Voltage errors
Adoption of DER systems	2205.3968	2691.3530	3591.4127	3364.3837
Percentage vulnerable devices	1336.2061	1670.9634	3276.5091	3237.7481
Percentage vulnerable households	4021.4087	5762.3178	**18353.1240**	**19277.9014**

5.2. Emergence of the risk

This section focuses on determining if and when a cybersecurity risk is present in the Smart Grid due to grid and market parameters. The answers of this section will allow answering research sub-question: RSQ1.

Setup

Linear regression analysis is performed to determine what are relevant factors and find the amount of impact that they have. The chosen attack only lowers the values; therefore, the highest value is irrelevant. The lowest value found during the run will be the dependent variable for both frequency and voltage; they are a stand-in for the instability of the grid.

The data from the experiment includes values that are impossible in real life due to excluding the safety systems of the generators from the model. These systems disconnect generators from the grid when the quality is too low, producing a blackout. However, this is beneficial for the regression analysis as it keeps the dependent continuous.

5.2.1. Frequency

Frequency is a quality indicator that is shared across the grid. Results found in a single place are valid for the entirety of the grid. Values are given for the test run, including the calculated factor *Percentage of vulnerable households*. The regression model is run multiple times, eliminating the lowest predictor if its effect is insignificant ($p < 0.05$).

Regression

Looking at the results, shown in table 5.5, the results expected from the literature appeared. The predictors *Adoption of DER systems*, *Percentage of vulnerable devices*, and *Percentage of vulnerable households* decrease the quality of the grid when increased. They allow a cyberattacker to impact the grid.

The *Percentage of power generated* shows that the total amount of power involved with an attack is essential. *Amount of bulk consumption* is the only predictor with a positive impact on the dependent; this is expected as this amount acts as a buffer to reduce the attack's impact.

R^2 is the variance the model can predict, indicating how well the model fits. A value of 0.864 entails that this is an excellent fit. It is also an indication that some other factors are not yet included. The other model results, in table 5.5, also indicate an excellent fit.

Plots

As an example, the effect of the *Percentage of vulnerable households* is plotted in figure 5.2. It shows a clear downward trend; however, the fitted line is less than perfect. The data would suggest a diminishing impact, not a linear relation.

Another defect is that the prediction value is lower than 50Hz when no vulnerable device is present, likely the result of the leverage effect due to all values being lower than 50Hz. The outliers at 0.6 *Percent of vulnerable households* are interesting; they may indicate an error in data collection during the experiment.

Table 5.5: Linear regression on predicting the lowest frequency during the run.

Model results

R^2	Log-Likelihood	F score	p-value	AIC	BIC
0.864	-82850	1.031e+04	0.000	1.657e+05	1.658e+05

Factor results

Predicting factor	β	Coef	Std. error	T-test	p-value
Percentage of power generated	-0.1252	-6437.0852	210.547	-30.573	0.000
Amount of bulk consumption	0.0902	8.038e-07	3.65e-08	22.040	0.000
Adoption of DER systems	-0.2296	-1.18e+04	373.260	-31.624	0.000
Percentage of vulnerable devices	-0.2115	-1.126e+04	377.478	-29.819	0.000
Percentage of vulnerable households	-0.6263	-4.158e+04	616.418	-67.451	0.000

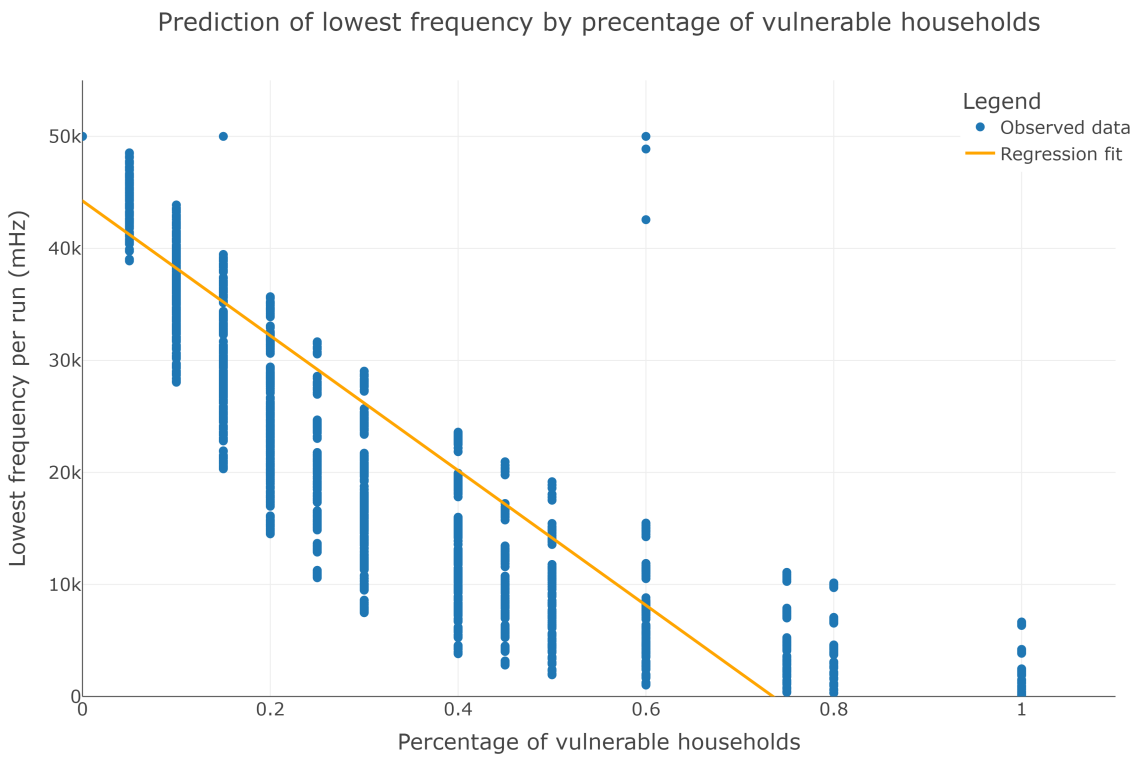

Figure 5.2: Prediction of lowest frequency value by *Percentage of vulnerable households*

5.2.2. Voltage

Voltage levels are measured at every netstation, at the edge. This is done because of the transformer in the netstation that steps it down to 230V. Values are given for the test run, including the calculated factor *Percentage of vulnerable households*. The regression model is run multiple times, eliminating the lowest predictor if its effect is insignificant ($p < 0.05$).

Regression

The results, shown in table 5.6, are different than what was found for the frequency test. The counterintuitive behaviour shown by *Adoption of DER systems* indicates that this model suffers from multicollinearity. Therefore, a run was done where the *Adoption of DER systems* and *Percentage of vulnerable devices* factors are removed.

As seen in table 5.7, *Percentage of vulnerable households* is the only relevant factor found and can predict almost 83% of the variance only 3& less than the original model. Furthermore, the AIC, BIC, Log-Likelihood, and F score indicate that the latter model would be preferred.

Voltage levels are impacted harder by market factors than frequency levels. This difference is likely due to the inability of the grid operator to compensate at the local level. It requires local intervention; this is also seen by the absence of the *Amount of bulk consumption* factor in both runs.

Table 5.6: Linear regression on predicting the lowest voltage.

Model results

R^2	Log-Likelihood	F score	p-value	AIC	BIC
0.860	1.652e+04	-3543.1	0.000	7094	7122

Factor results

Predicting factor	β	Coef	Std. error	T-test	p-value
Percentage of power generated	-0.1806	-9386.2375	216.468	-43.361	0.000
Adoption of DER systems	0.0130	677.3257	283.424	2.390	0.017
Percentage of vulnerable households	-0.9177	-6.158e+04	365.898	-168.285	0.000

Table 5.7: Linear regression on predicting the lowest voltage with only the predictor *Percentage of vulnerable households*.

Model results

R^2	Log-Likelihood	F score	p-value	AIC	BIC
0.827	-83923	3.867e+04	0.000	1.679e+05	1.679e+05

Factor results

Predicting factor	β	Coef	Std. error	T-test	p-value
Percentage of vulnerable households	-0.9093	-6.101e+04	310.267	-196.639	0.000

Plots

The plot produced is similar to figure 5.2, as this is the only relevant predictor present. The effect of the *Percentage of vulnerable households* on the *Lowest voltage* is plotted in figure 5.3.

The fitted line shows a more linear fit than the line for frequency. It shows a clear downward trend and a linear relationship; one remark must be placed on this observation. One of the model's assumptions is modelling the relationship between power mismatch and voltage behaviour as linear. Likely, this has at least some impact on the fit of the line.

An error during modelling was the lack of voltage levels logging at netstations when no warnings or errors were generated. These null values were to be filled with the default 230V value. The outliers here may also indicate an error in data collection during the experiment.

5.2.3. Answer

As mentioned in the introduction, this section focuses on determining if and when a cybersecurity risk is present for the Smart Grid. The clear and present relationship between the market parameters and the quality indicators would undoubtedly indicate this. What also is shown in this section is that the grid parameters are of relatively little influence in this model. The data collected from the model allowed the creation of a model that could predict more than 80% of the variance for both quality indicators.

The combination of observing behaviour, as expected from the literature, and the lack of unexplainable effects boost the confidence in the model.

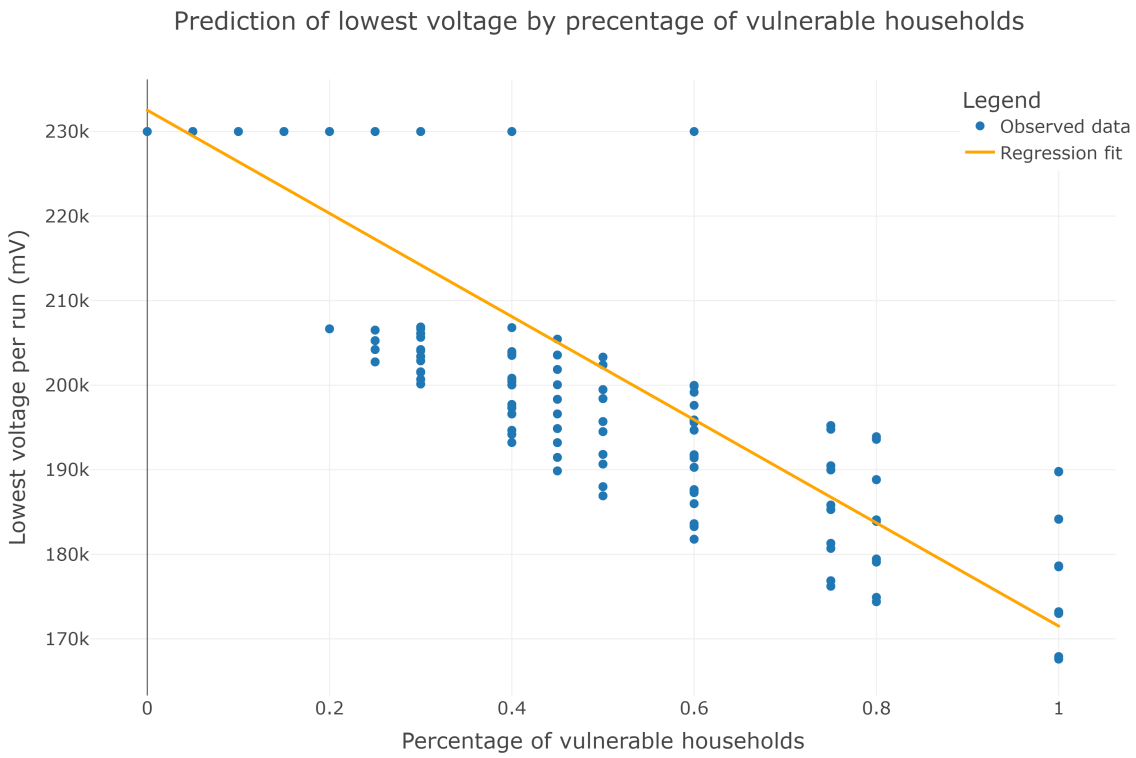

Figure 5.3: Prediction of lowest voltage value by *Percentage of vulnerable households*

5.3. Materialisation of the risk

After concluding that the risk is present, the next step is to determine the size of its impact. The goal is to determine how large of a risk an oligopolistic Distributed Energy Recourses market is for the Smart Grid. The results of this section should allow research sub-question RSQ2 to be answered.

Setup

The predictors used are the input parameters used in scenario creation, as seen in table 4.6. In the results of the following sections, only the significant factors are given.

The attack in this model started at step 24. The *Time to the first warning* and *Time to the first error* factors in combination with *Time between warning and error* to determine the impact's size. These factors also contain null values if no warning or error is found in the run; this is encoded in a dummy variable.

5.3.1. Time for mitigation

This subsection focuses on the time between the first presence of a warning and an error. The time that separates them is when an operator has to intervene and mitigate the attack's impact. As in the previous subsection, only frequency is used for analysis.

In figure 5.4, a heatmap shows the effect that *Percentage of vulnerable devices* and *Adoption of DER systems* have on the emergence of the risk. It demonstrates that both predictors must also be present and that the impact appears rapidly. The appearance is shown by the *Time to the first warning* after an attack starts.

The heatmap in figure 5.5 shows that the *Time between warning and error* is always zero steps if an error is present. An error during the experiment is the likely culprit. All values logged per experiment for the first warning and the first error are equal per scenario. The time that is available to mitigate an attack cannot be analysed.

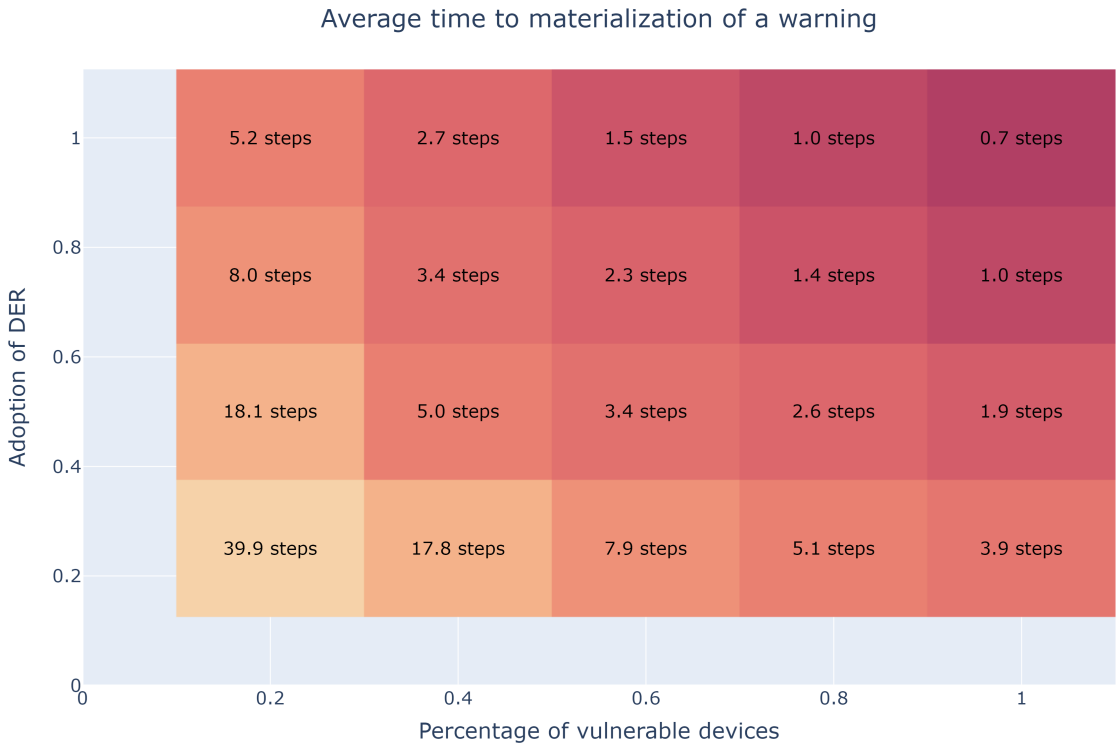

Figure 5.4

Figure 5.5: Heatmap of the significant predictors on the maximum *Time between warning and error*

5.3.2. Size of impact

This subsection will only discuss the analysis of an indicator for the voltage quality indicator. The relevant analysis is already shown in table 5.5 for frequency.

Unique netstations

For the voltage quality indicator, the impact of an attack is by the netstations producing a voltage warning. There are 5.032 netstations present in the model. A regression analysis is performed to find relevant predictors and the size of their impact.

The results, shown in table 5.8, show the same behaviour as the analysis shown in table 5.7. Therefore the same conclusions are drawn about the predictors present. However, it is interesting that the amount of variance that can be explained is lower for this analysis than for the *Lowest voltage*. The suspicion is that this is due to local differences from the PRNG-selected households per netstation.

To demonstrate the behaviour of the *Percentage of vulnerable households* factor on the impacted netstations, a plot is shown in figure 5.6. When combined, *Percentage of vulnerable devices* and *Adoption of DER systems* produce a much more significant impact than on their own. This effect is shown by the higher increase of impacted netstations by *Percentage of vulnerable households*.

Table 5.8: Linear regression on predicting the number of unique netstations producing a voltage warning.

Model results

R^2	Log-Likelihood	F score	p-value	AIC	BIC
0.749	-5901.9	2.411e+04	0.000	1.181e+04	1.182e+04

Factor results

Predicting factor	β	Coef	Std. error	T-test	p-value
Percentage of vulnerable households	0.8652	6402.7012	41.238	155.263	0.000

5.3.3. Answer

The impact that an oligopolistic market for Distributed Energy Recourses combined with a cyberattack is substantial. The goal is to determine how large of a risk an oligopolistic Distributed Energy Recourses market is for the Smart Grid. Figure 5.4 shows that the maximum amount of time that it takes an attack to is less than 40 steps, about 10 hours. Most results are less than an hour before a grid warning is produced.

5.4. Notes

The information gained from the data analysis gave insight into grid behaviour previously not realised by the author. The diagram of figure 4.1 was missing the damping effect of the synchronous generators in the grid. The updated diagram is now shown in figure 5.7.

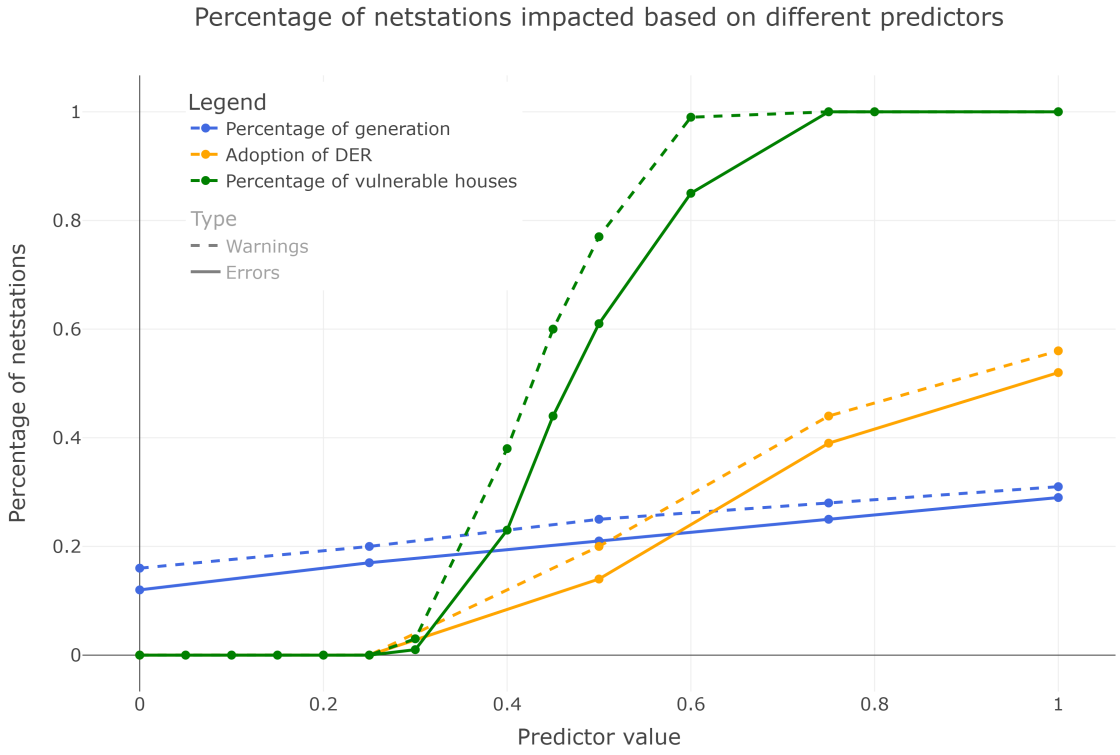

Figure 5.6: Percentage of netstations impacted based on predictor value

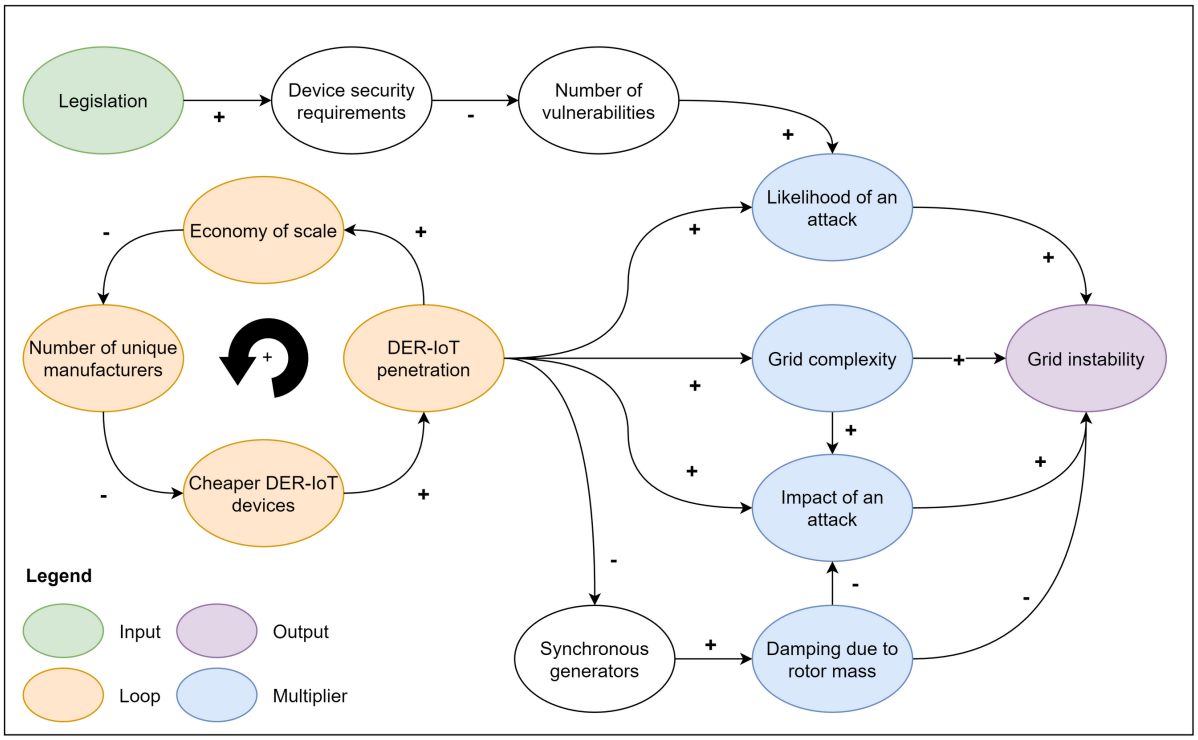

Figure 5.7: Updated System diagram

6

Discussion

The results of the experiment show that concentration in the market for Distributed Energy Resources is impacting the Smart Grid and its stability. The obtained results are not without limitations and context. This chapter starts with the research limitations and proceeds to recommendations for research topics to explore the found risks further

6.1. Limitations

Limitations may impact the validity of the research, which would prevent answering the research question with any scientific value. The extent and impact of the limitations that face this research have been considered and are described based on their potential impact.

Interpretation of the results

The used model is created using the assumptions listed in table 4.3. No indications are found that the assumptions made make the results invalid; however, they reduce their accuracy. Therefore, only statements about the results' direction and order of magnitude can be made. The research question can be answered with those kinds of statements.

Generalisation

The model's grid is modelled after and validated on the power grid of the Netherlands without any interconnects to other grids. As a bigger and more connected grid is inherently more stable, this could significantly impact the results. However, the interconnected grid that the Netherlands is part of falls under the EU's single market, except for the UK. Therefore, the obtained results can be generalised to at least the level of the interconnected grid.

Scope of model

Certain aspects left out of scope for this research influence the results obtained. The most important one is other grid elements, such as local energy storage or electric vehicles. Other aspects include using a different type of attack, load shedding, and the heterogeneity of netstations. As this research aims to highlight and give context to the identified issue, including these elements would not have added value to the results. All aspects that were purposefully left out of scope attributed to the reduction in complexity and computational costs, allowing more scenarios to be created and explored.

6.2. Further research

In the process of performing this research, many improvements that could be made came to light. These will be discussed below as recommendations.

Besides improvements to this research, another risk worthy of serious attention is found. This topic is described first, followed by mitigation aspects of the identified risk. Improvements and varieties that can be made to the model follow after.

Harmonics

The connection of DER to the grid includes an inverter to generate the 50Hz 230V signal used on the grid. These inverters are known to introduce harmonics into the grid; these are higher frequencies that are integer multiples of the fundamental frequency. Harmonics can lead to distorted voltage waveforms, blown capacitor fuses, and transformer overheating [136]. Also, due to the skin effect, they can significantly increase a conductor's resistance.

Harmonic attacks can, therefore, impact the grid much more significantly than the load switching used in this research. They also increase effectiveness when many devices combine to produce a cumulative harmonic attack. Furthermore, the grid operator cannot reduce the harmonics on the grid except by eliminating the source. These reasons make harmonic attacks a threat worthy of research.

Mitigation

This identified risk has shown to be of a considerable proportion. A logical follow-up question that can be used in further research would be: how can it be mitigated? Exploring the impact of an oligopolistic market on proposed mitigation strategies by academics can also be of interest.

Improve simulation

The model created during this research can be changed to answer other questions. The dilemma between computational costs and the validity of the results is always present. A digital twin approach would bring high-fidelity answers as it creates a total copy of the grid. Steps that can be taken as an intermediary are:

- Use of real power generation data for the DER.
- Reduction of assumptions mentioned in table 4.3.
- Performing more validation to reduce uncertainty.
- Adding relevant grid elements, such as EVs with the ability to act as energy storage.

Diversify attack

Only a single attack type is used during the creation of the scenarios run as part of this research. However, the created model currently already can perform multiple types of attacks. It would be interesting to see if different attacks would impact the results in other aspects. Possibilties for attacks are:

- Dynamic attacks that vary over time.
- Attacks that are designed to be undetectable.
- Usage of game theory as the base of interaction between attacker and grid operator.

7

Conclusion

This chapter will answer the research question and its subquestions first. They are followed by a list of recommendations for policymakers and regulators to help mitigate the risk identified by this research.

7.1. Answer to research question

The Smart Grid is at risk for a cybersecurity attack due to an oligopolistic market for Distributed Energy resources. Eight thousand one hundred different scenarios were created that simulate different levels of market concentration and the adoption of DER. These scenarios were then used by a purposefully built agent-based model that simulates the grid and determines the impact of a cyberattack. Data analysis on the model's output shows that this risk is indeed present and should be accounted for.

Influence of market and grid parameters

Market parameters such as the Adoption of DER systems and the market share of the vulnerable device are shown to impact the grid's quality indicators. A derived parameter percentage of vulnerable households, the product of the aforementioned market parameters, can predict most of the impact. This variable is representative of the oligopolistic nature of the market. The risk appears from a 25% of DER adoption and a market share of 20% for the vulnerable DER, entailing only 5% of households. This value should not be taken as an exact answer; however, it does indicate that this risk might appear sooner rather than later.

Impact of an attack

A cascading failure of the grid that leads to a blackout can be obtained due to the horizontal escalation possibilities of a cyberattack. An attacker only needs to abuse the devices under its control to trigger the safety systems of other generators, disconnecting them, which adds to the overload on the grid. One option to achieve this is by dropping the grid frequency below 48.5Hz for more than 30 minutes or below 47.5Hz for a single moment. As the capacity of synchronous power generators decreases in the transition to more renewable resources, the ability of an attack to manipulate the grid grows.

Mitigation options

Mitigating this risk appears to be quite challenging, as both communication signals and power travel at the speed of light. Current methods to identify power mismatch rely on the electrical characteristics off the grid; they are not fit for the Smart Grid with its need for more communication and coordination. Most methods proposed by academia suitable for the Smart Grid identified by this research use a solution where a DER is checked by their neighbouring DER in the local grid. However, this assumes that the information given by the neighbours can be trusted, which cannot be made in an oligopolistic market.

7.2. Recommendations

One of the goals of this research is to provide insight and practical guidance to policymakers and regulators, allowing them to make informed decisions. The following recommendations are made based on the insights gained during this research.

Collection of information

Owners of a power-generating device connected to the grid are already required to provide the grid operator with information on the device. The inclusion of cybersecurity-related information such as make, model, and firmware version will likely prove very beneficial to cause identification of an issue on the grid. As this data changes over time because of firmware updates, the recommendation is to perform the data collection automatically.

Forced patching

When a vulnerability is identified, there is usually a period between the publication of its patch and its exploitation. The issue facing patching, in general, is that the roll-out is problematic. Many owners of devices do not know that their device is vulnerable; even if they do, it is not top-of-mind for many. This results in a situation where patching may take an enormous amount of time to obtain a suitable patching rate.

Waiting for patches to roll out naturally is not acceptable in the context of the Smart Grid and the opportunity to scale an attack horizontally due to an oligopolistic market. DER are the property of their owners; they are the only ones allowed to install a patch on it if no other provisions have been made. To mitigate the risk in a period suitable for the grid, the recommendation is to make a provision that updates can be forced onto DER.

Increasing diversity in DER market

In real estate development, bulk purchasing is often used to reduce costs. DER, as solar panels, are no exception to this practice. Therefore there are many new neighbourhoods that all have an identical model. To give room to possible mitigation and detection methods, the recommendation is to demand a minimum level of diversity in DER at each grid level.

References

[1] N. S. Kardashev, 'Transmission of Information by Extraterrestrial Civilizations.', *Soviet Astronomy*, vol. 8, p. 217, 1st Oct. 1964, ISSN: 0038-5301. [Online]. Available: https://ui.adsabs.harvard.edu/abs/1964SvA.....8..217K (visited on 24/05/2022).

[2] M. v. J. en Veiligheid, 'Geïntegreerde Risicoanalyse Nationale Veiligheid - Publicatie - Nationaal Coördinator Terrorismebestrijding en Veiligheid', Ministerie van Justitie en Veiligheid, publicatie, 7th Jun. 2019. [Online]. Available: https://www.nctv.nl/documenten/publicaties/2019/6/07/geintegreerde-risicoanalyse-nationale-veiligheid (visited on 25/05/2022).

[3] A. Ipakchi and F. Albuyeh, 'Grid of the future', *IEEE Power and Energy Magazine*, vol. 7, no. 2, pp. 52–62, Mar. 2009, ISSN: 1558-4216. DOI: 10.1109/MPE.2008.931384.

[4] H. Farhangi, 'The path of the smart grid', *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, Jan. 2010, ISSN: 1558-4216. DOI: 10.1109/MPE.2009.934876.

[5] J. A. Momoh, *Smart Grid: Fundamentals of Design and Analysis*. John Wiley & Sons, 7th Mar. 2012, 234 pp., ISBN: 978-1-118-15610-0. Google Books: tHmmCUrQP2gC.

[6] International Smart Grid Action Network (ISGAN), 'Power Transmission & Distribution Systems', Annex 6, 3rd May 2021, p. 5. [Online]. Available: https://www.iea-isgan.org/annex6_key_messages/ (visited on 03/05/2021).

[7] A. Bari, J. Jiang, W. Saad and A. Jaekel, 'Challenges in the Smart Grid Applications', *International Journal of Distributed Sensor Networks*, vol. 10, no. 2, p. 974 682, 2 1st Feb. 2014, ISSN: 1550-1477. DOI: 10.1155/2014/974682. [Online]. Available: https://doi.org/10.1155/2014/974682 (visited on 03/05/2021).

[8] P. Schavemaker, L. van der Sluis and L. van der Sluis, *Electrical Power System Essentials*. New York, UNITED KINGDOM: John Wiley & Sons, Incorporated, 2017, ISBN: 978-1-118-80345-5. [Online]. Available: http://ebookcentral.proquest.com/lib/delft/detail.action?docID=4857452 (visited on 23/05/2022).

[9] T. NI, 'Imbalance Management TenneT Analysis report', p. 39,

[10] IEA. 'Digital Demand-Driven Electricity Networks Initiative – Programmes', IEA. (28th Jan. 2021), [Online]. Available: https://www.iea.org/areas-of-work/promoting-digital-demand-driven-electricity-networks (visited on 03/05/2021).

[11] OECD. 'Oligopoly markets'. (), [Online]. Available: https://www.oecd.org/daf/competition/oligopoly-markets.htm (visited on 01/08/2022).

[12] European Commission, DG II – Economic, Financial Affairs, DG XV – Internal Market and Financial Services, *The Single Market Review : Impact on Competition and Scale Effects : Economies of Scale. Volume IV* (Single Market Review V). Publications Office, 1997, vol. IV.

[13] M. Antonakakis *et al.*, 'Understanding the Mirai Botnet', presented at the 26th {USENIX} Security Symposium ({USENIX} Security 17), 2017, pp. 1093–1110, ISBN: 978-1-931971-40-9. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis (visited on 21/06/2021).

[14] M. A. Sayed, R. Atallah, C. Assi and M. Debbabi, 'Electric vehicle attack impact on power grid operation', *International Journal of Electrical Power & Energy Systems*, vol. 137, p. 107 784, 1st May 2022, ISSN: 0142-0615. DOI: 10.1016/j.ijepes.2021.107784. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061521010048 (visited on 15/08/2022).

[15] Algemene Inlichtingen- en Veiligheidsdienst, 'Jaarverslag AIVD 2021', Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag, Jaarverslag 2021, Apr. 2022, p. 35.

[16] L. Xie, Y. Mo and B. Sinopoli, 'False Data Injection Attacks in Electricity Markets', in *2010 First IEEE International Conference on Smart Grid Communications*, Oct. 2010, pp. 226–231. DOI: 10.1109/SMARTGRID.2010.5622048.

[17] Ministerie van Economische Zaken en Klimaat and Agentschap Telecom, 'Rapport Verkenning rollen Agentschap Telecom in de energietransitie - Rapport - Agentschap Telecom', Ministerie van Economische Zaken en Klimaat, rapport, 12th Jul. 2021. [Online]. Available: https://www.agentschaptelecom.nl/documenten/rapporten/2021/07/12/verkenning-rollen-agentschap-telecom-energietransitie (visited on 15/08/2022).

[18] Agentschap Telecom and Ministerie van Economische Zaken en Klimaat, 'Samenhangend inspectiebeeld cybersecurity vitale processen', Ministerie van Economische Zaken en Klimaat, publicatie, 29th Jun. 2021. [Online]. Available: https://www.agentschaptelecom.nl/documenten/rapporten/2021/06/29/rapport-samenhangend-inspectiebeeld-cybersecurity-vitale-processen-2020-2021 (visited on 25/05/2022).

[19] Stan Hulsen, 'Hacker kon tienduizenden zonnepanelen saboteren door rondslingerend wachtwoord', *RTL Nieuws*, 24th Jul. 2022. [Online]. Available: https://www.rtlnieuws.nl/tech/artikel/5322854/hacker-kon-tienduizenden-zonnepanelen-saboteren-door-rondslingerend-wachtwoord (visited on 08/08/2022).

[20] F. Breedijk. 'DIVD-2022-00009 - SolarMan backend administrator account/password', DIVD CSIRT. (12th Aug. 2022), [Online]. Available: https://csirt.divd.nl/cases/DIVD-2022-00009/ (visited on 15/08/2022).

[21] European Commission. *Cyber Resilience Act (Proposed)*. (2023), [Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en.

[22] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, 'Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems', *IEEE Access*, vol. 7, pp. 46 595–46 620, 2019, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2909807.

[23] T. Duebendorfer and S. Frei, 'Why Silent Updates Boost Security', p. 9, 2009. [Online]. Available: http://www.techzoom.net/publications/silent-updates/.

[24] K. S. Schmitz, 'Chapter 2 - Five Important Equations in Thermodynamics', in *Physical Chemistry*, K. S. Schmitz, Ed., Boston: Elsevier, 1st Jan. 2017, pp. 41–98, ISBN: 978-0-12-800514-9. DOI: 10.1016/B978-0-12-800514-9.00002-X. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B978012800514900002X (visited on 15/08/2022).

[25] TenneT. 'Maps of our onshore and offshore high voltage grid', TenneT. (), [Online]. Available: https://www.tennet.eu/grid/grid-maps (visited on 25/08/2022).

[26] 'Netschema van Nederland', HoogspanningsNet. (), [Online]. Available: https://www.hoogspanningsnet.com/netschema/ (visited on 15/08/2022).

[27] TenneT. 'About TenneT', TenneT. (Dec. 2022), [Online]. Available: https://www.tennet.eu/about-tennet (visited on 20/12/2022).

[28] TenneT. 'International connections', TenneT. (), [Online]. Available: https://www.tennet.eu/our-projects/international-connections (visited on 25/11/2022).

[29] M. F. Akorede, H. Hizam and E. Pouresmaeil, 'Distributed energy resources and benefits to the environment', *Renewable and Sustainable Energy Reviews*, vol. 14, no. 2, pp. 724–734, 1st Feb. 2010, ISSN: 1364-0321. DOI: 10.1016/j.rser.2009.10.025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1364032109002561 (visited on 15/08/2022).

[30] F. Gonzalez-Longatt, J. L. Rueda, P. Palensky, H. R. Chamorro and V. Sood, 'Frequency Support provided by Inverted Based-Generation using Grid-Forming Controllers: A Comparison during Islanded Operation', in *2021 IEEE Electrical Power and Energy Conference (EPEC)*, Toronto, ON, Canada: IEEE, 22nd Oct. 2021, pp. 113–118, ISBN: 978-1-66542-928-3. DOI: 10.1109/EPEC52095.2021.9621418. [Online]. Available: https://ieeexplore.ieee.org/document/9621418/ (visited on 21/06/2022).

[31] L. F. M. van Summeren, A. J. Wieczorek, G. J. T. Bombaerts and G. P. J. Verbong, 'Community energy meets smart grids: Reviewing goals, structure, and roles in Virtual Power Plants in Ireland, Belgium and the Netherlands', *Energy Research & Social Science*, vol. 63, p. 101 415, 1st May 2020, ISSN: 2214-6296. DOI: 10.1016/j.erss.2019.101415. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214629619304335 (visited on 18/05/2021).

[32] B. Li, Y. Wang, J. Li and S. Cao, 'A Fully Distributed Approach for Economic Dispatch Problem of Smart Grid', *Energies*, vol. 11, no. 8, p. 1993, 8 Aug. 2018, ISSN: 1996-1073. DOI: 10.3390/en11081993. [Online]. Available: https://www.mdpi.com/1996-1073/11/8/1993 (visited on 18/05/2022).

[33] J. Gao, Y. Xiao, J. Liu, W. Liang and C. L. P. Chen, 'A survey of communication/networking in Smart Grids', *Future Generation Computer Systems*, vol. 28, no. 2, pp. 391–404, 2 1st Feb. 2012, ISSN: 0167-739X. DOI: 10.1016/j.future.2011.04.014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X11000653 (visited on 18/05/2021).

[34] H. Lund, A. N. Andersen, P. A. Østergaard, B. V. Mathiesen and D. Connolly, 'From electricity smart grids to smart energy systems – A market operation based approach and understanding', *Energy*, 8th World Energy System Conference, WESC 2010, vol. 42, no. 1, pp. 96–102, 1 1st Jun. 2012, ISSN: 0360-5442. DOI: 10.1016/j.energy.2012.04.003. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0360544212002836 (visited on 18/05/2021).

[35] X. Liu, B. Chen, C. Chen and D. Jin, 'Electric power grid resilience with interdependencies between power and communication networks – a review', *IET Smart Grid*, vol. 3, no. 2, pp. 182–193, 2020, ISSN: 2515-2947. DOI: 10.1049/iet-stg.2019.0202. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1049/iet-stg.2019.0202 (visited on 18/05/2022).

[36] S. Sridhar, A. Hahn and M. Govindarasu, 'Cyber–Physical System Security for the Electric Power Grid', *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 1 Jan. 2012, ISSN: 1558-2256. DOI: 10.1109/JPROC.2011.2165269.

[37] E. de Souza, O. Ardakanian and I. Nikolaidis, 'A Co-simulation Platform for Evaluating Cyber Security and Control Applications in the Smart Grid', in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, Jun. 2020, pp. 1–7. DOI: 10.1109/ICC40277.2020.9149212.

[38] P. Radoglou-Grammatikis *et al.*, 'SPEAR SIEM: A Security Information and Event Management system for the Smart Grid', *Computer Networks*, vol. 193, p. 108 008, 5th Jul. 2021, ISSN: 1389-1286. DOI: 10.1016/j.comnet.2021.108008. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128621001237 (visited on 23/05/2022).

[39] N. Campagna, M. Caruso, V. Castiglia, R. Miceli and F. Viola, 'Energy Management Concepts for the Evolution of Smart Grids', in *2020 8th International Conference on Smart Grid (icSmartGrid)*, Jun. 2020, pp. 208–213. DOI: 10.1109/icSmartGrid49881.2020.9144909.

[40] A. A. Saad, S. Faddel and O. Mohammed, 'A secured distributed control system for future interconnected smart grids', *Applied Energy*, vol. 243, pp. 57–70, 1st Jun. 2019, ISSN: 0306-2619. DOI: 10.1016/j.apenergy.2019.03.185. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261919306014 (visited on 18/05/2022).

[41] N. Hatziargyriou *et al.*, 'Definition and Classification of Power System Stability – Revisited & Extended', *IEEE Transactions on Power Systems*, vol. 36, no. 4, pp. 3271–3281, Jul. 2021, ISSN: 0885-8950, 1558-0679. DOI: 10.1109/TPWRS.2020.3041774. [Online]. Available: https://ieeexplore.ieee.org/document/9286772/ (visited on 19/05/2022).

[42] J. McDowell *et al.*, 'Reactive power interconnection requirements for PV and wind plants : Recommendations to NERC.', SAND2012-1098, 1039006, 1st Feb. 2012, SAND2012–1098, 1 039 006. DOI: 10.2172/1039006. [Online]. Available: https://www.osti.gov/servlets/purl/1039006/ (visited on 19/12/2022).

[43] G. M. Tina and G. Celsa, 'Active and reactive power regulation in grid-connected PV systems', in *2015 50th International Universities Power Engineering Conference (UPEC)*, Stoke On Trent, United Kingdom: IEEE, Sep. 2015, pp. 1–6, ISBN: 978-1-4673-9682-0. DOI: 10.1109/UPEC.2015.7339821. [Online]. Available: http://ieeexplore.ieee.org/document/7339821/ (visited on 28/09/2022).

[44] A. W. Korai, M. E. Adabi, E. Rakhshani, J. L. Rueda Torres and M. A. M. M. van der Meijden, 'A Benchmark Test System for the Power System Stability Assessment Considering Very High Penetration of Converter-Based Generation Units Including Grid Forming Converters', in *Modelling and Simulation of Power Electronic Converter Dominated Power Systems in PowerFactory*, ser. Power Systems, F. M. Gonzalez-Longatt and J. L. Rueda Torres, Eds., Cham: Springer International Publishing, 2021, pp. 201–216, ISBN: 978-3-030-54124-8. DOI: 10.1007/978-3-030-54124-8_8. [Online]. Available: https://doi.org/10.1007/978-3-030-54124-8_8 (visited on 21/06/2022).

[45] N. B. G. Brinkel *et al.*, 'Impact of rapid PV fluctuations on power quality in the low-voltage grid and mitigation strategies using electric vehicles', *International Journal of Electrical Power & Energy Systems*, vol. 118, p. 105 741, 1st Jun. 2020, ISSN: 0142-0615. DOI: 10.1016/j.ijepes.2019.105741. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061519319994 (visited on 03/05/2021).

[46] *Commission Regulation (EU) 2016/631 of 14 April 2016 establishing a network code on requirements for grid connection of generators (Text with EEA relevance)*. (14th Apr. 2016), [Online]. Available: http://data.europa.eu/eli/reg/2016/631/oj/eng (visited on 28/09/2022).

[47] D. I. Sharieff, 'Fast Decoupled Load Flow (FDLF)', p. 281,

[48] V. Trovato, I. M. Sanz, B. Chaudhuri and G. Strbac, 'Preventing cascading tripping of distributed generators during non-islanding conditions using thermostatic loads', *International Journal of Electrical Power & Energy Systems*, vol. 106, pp. 183–191, 1st Mar. 2019, ISSN: 0142-0615. DOI: 10.1016/j.ijepes.2018.09.045. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061518308196 (visited on 20/12/2022).

[49] B. H. Hall and B. Khan, *Adoption of New Technology*, Working Paper, May 2003. DOI: 10.3386/w9730. [Online]. Available: https://www.nber.org/papers/w9730 (visited on 23/12/2022).

[50] E. M. Rogers, A. Singhal and M. M. Quinlan, *Diffusion of Innovations*. Routledge, 1962.

[51] CBS. 'Renewable electricity; production and capacity', StatLine. (), [Online]. Available: https://opendata.cbs.nl/statline/#/CBS/en/dataset/82610ENG/table?ts=1672258830551 (visited on 23/12/2022).

[52] K. van Groesen. 'Bijna 1 op de 5 woningen heeft zonnepanelen', Independer.nl. (12th May 2022), [Online]. Available: https://weblog.independer.nl/persbericht/bijna-1-op-de-5-woningen-heeft-zonnepanelen/ (visited on 23/12/2022).

[53] Sophie van Gool, 'Duurzame keuzes', *FD.nl*, 30th Oct. 2022. [Online]. Available: https://fd.nl/opinie/1456457/duurzame-keuzes (visited on 23/12/2022).

[54] N. Theelen, P. Kanne, B. Wolf, J. van Beek and M. van Will, 'Duurzaam denken wordt (langzaamaan) duurzaam doen', I&O Research, Amsterdam, 2022/253, Oct. 2022. [Online]. Available: https://065.wpcdnnode.com/ioresearch.nl/wp-content/uploads/2022/10/rapport-duurzaamheid-2022-def.pdf (visited on 23/12/2022).

[55] M. Nieles, K. Dempsey and V. Pillitteri, 'An Introduction to Information Security', National Institute of Standards and Technology, NIST Special Publication (SP) 800-12 Rev. 1, 22nd Jun. 2017. DOI: 10.6028/NIST.SP.800-12r1. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final (visited on 25/05/2022).

[56] 'Executive Summary — NIST SP 1800-26 documentation'. (), [Online]. Available: https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html (visited on 25/05/2022).

[57] X. Li, X. Liang, R. Lu, X. Shen, X. Lin and H. Zhu, 'Securing smart grid: Cyber attacks, countermeasures, and challenges', *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38–45, 8 Aug. 2012, ISSN: 1558-1896. DOI: 10.1109/MCOM.2012.6257525.

[58] J. Sakhnini, H. Karimipour and A. Dehghantanha, 'Smart Grid Cyber Attacks Detection Using Supervised Learning and Heuristic Feature Selection', in *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*, Aug. 2019, pp. 108–112. DOI: 10.1109/SEGE.2019.8859946.

[59] Y. Zhang, J. Wang and B. Chen, 'Detecting False Data Injection Attacks in Smart Grids: A Semi-Supervised Deep Learning Approach', *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 623–634, 1 Jan. 2021, ISSN: 1949-3061. DOI: 10.1109/TSG.2020.3010510.

[60] S. Gao, J. Lei, X. Wei, Y. Liu and T. Wang, 'A Novel Bilevel False Data Injection Attack Model Based on Pre-and Post-Dispatch', *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 2487–2490, 2022, ISSN: 1949-3053. DOI: 10.1109/TSG.2022.3156445. [Online]. Available: http://www.scopus.com/inward/record.url?scp=85125755021&partnerID=8YFLogxK (visited on 21/06/2022).

[61] M. H. Ansari, V. T. Vakili, B. Bahrak and P. Tavassoli, 'Graph theoretical defense mechanisms against false data injection attacks in smart grids', *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 860–871, Sep. 2018, ISSN: 2196-5420. DOI: 10.1007/s40565-018-0432-2.

[62] B. Enserink, L. Hermans, J. Kwakkel, W. Thissen, J. Koppenjan and P. Bots, *Policy Analysis of Multi-Actor Systems*. Den Haag: Lemma, 2010, ISBN: 978-90-5931-538-9.

[63] R. Anderson and T. Moore, 'The Economics of Information Security', *Science*, vol. 314, no. 5799, pp. 610–613, 27th Oct. 2006, ISSN: 0036-8075, 1095-9203. DOI: 10.1126/science.1130992. [Online]. Available: https://www.science.org/doi/10.1126/science.1130992 (visited on 16/08/2022).

[64] T. Moore, 'The economics of cybersecurity: Principles and policy options', *International Journal of Critical Infrastructure Protection*, vol. 3, no. 3-4, pp. 103–117, Dec. 2010, ISSN: 18745482. DOI: 10.1016/j.ijcip.2010.10.002. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1874548210000429 (visited on 16/08/2022).

[65] H. Asghari, 'Economics of cybersecurity', in *Handbook on the Economics of the Internet*. Edward Elgar Publishing, 2016, pp. 262–287, ISBN: 978-0-85793-985-2. DOI: 10.4337/9780857939852.00021. [Online]. Available: http://www.elgaronline.com/view/9780857939845.00021.xml (visited on 16/08/2022).

[66] L. A. Gordon and M. P. Loeb, 'The Economics of Information Security Investment', *ACM Transactions on Information and System Security*, vol. 5, no. 4, p. 20, Nov. 2002.

[67] R. A. Kerin, P. R. Varadarajan and R. A. Peterson, 'First-Mover Advantage: A Synthesis, Conceptual Framework, and Research Propositions', *Journal of Marketing*, vol. 56, no. 4, p. 33, Oct. 1992, ISSN: 00222429. [Online]. Available: https://www.proquest.com/docview/227823405/abstract/7142E290AAC342DAPQ/1 (visited on 16/08/2022).

[68] Thomas Philippon, 'The Economics and Politics of Market Concentration', *NBER*, The Reporter, 4th Dec. 2019. [Online]. Available: http://www.nber.org/reporter/2019number4/economics-and-politics-market-concentration (visited on 16/08/2022).

[69] C. Genakos, T. Valletti and F. Verboven, 'Evaluating Market Consolidation in Mobile Communications', Centre on Regulation in Europe, Brussels, 15th Sep. 2015, p. 50. [Online]. Available: https://cerre.eu/wp-content/uploads/2020/07/150915_CERRE_Mobile_Consolidation_Report_Final.pdf.

[70] Statcounter. 'Mobile Vendor Market Share United States Of America', StatCounter Global Stats. (2022), [Online]. Available: https://gs.statcounter.com/vendor-market-share/mobile/united-states-of-america/ (visited on 20/12/2022).

[71] C. Herley, 'So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users', 20th Apr. 2009. [Online]. Available: https://www.microsoft.com/en-us/research/publication/so-long-and-no-thanks-for-the-externalities-the-rational-rejection-of-security-advice-by-users/ (visited on 19/12/2022).

[72] *Netcode elektriciteit*. in collab. with M. v. B. Z. en Koninkrijksrelaties. (2022), [Online]. Available: https://wetten.overheid.nl/BWBR0037940/#Hoofdstuk10 (visited on 28/09/2022).

[73] D. Lee and D. J. Hess, 'Data privacy and residential smart meters: Comparative analysis and harmonization potential', *Utilities Policy*, vol. 70, p. 101 188, 1st Jun. 2021, ISSN: 0957-1787. DOI: 10.1016/j.jup.2021.101188. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957178721000229 (visited on 15/08/2022).

[74] E. Haber and A. Tamò-Larrieux, 'Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security', *Computer Law & Security Review*, vol. 37, p. 105 409, 1st Jul. 2020, ISSN: 0267-3649. DOI: 10.1016/j.clsr.2020.105409. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364920300145 (visited on 15/08/2022).

[75] V. L. Johnson, R. W. Woolridge, W. Wang and J. R. Bell, 'The Impact of Perceived Privacy, Accuracy and Security on the Adoption of Mobile Self-Checkout Systems', *Journal of Innovation Economics & Management*, vol. 31, no. 1, pp. 221–247, 2020, ISSN: 2032-5355. DOI: 10.3917/jie.pr1.0065. [Online]. Available: https://www.cairn.info/revue-journal-of-innovation-economics-2020-1-page-221.htm (visited on 20/12/2022).

[76] M. Galeano Galvan, E. Cuppen and M. Taanman, 'Exploring incumbents' agency: Institutional work by grid operators in decentralized energy innovations', *Environmental Innovation and Societal Transitions*, vol. 37, pp. 79–92, 1st Dec. 2020, ISSN: 2210-4224. DOI: 10.1016/j.eist.2020.07.008. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2210422420300952 (visited on 03/05/2021).

[77] F. Rohde and S. Hielscher, 'Smart grids and institutional change: Emerging contestations between organisations over smart energy transitions', *Energy Research & Social Science*, vol. 74, p. 101 974, 1st Apr. 2021, ISSN: 2214-6296. DOI: 10.1016/j.erss.2021.101974. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214629621000670 (visited on 03/05/2021).

[78] E. Pruyt, 'Small system dynamics models for big issues: Triple jump towards real-world complexity', 2013.

[79] Illinois Center for a Smarter Electric Grid, *IEEE 14-Bus System*, Grainger College of Engineering. [Online]. Available: https://icseg.iti.illinois.edu/ieee-14-bus-system/ (visited on 20/12/2022).

[80] D. A. Samuelson and C. M. Macal, 'Agent-based simulation comes of age:' *OR/MS Today*, vol. 33, no. 4, pp. 34–39, 1st Aug. 2006, ISSN: 10851038. DOI: 10.1287/orms.2006.04.13. [Online]. Available: https://go.gale.com/ps/i.do?p=AONE&sw=w&issn=10851038&v=2.1&it=r&id=GALE%7CA151387517&sid=googleScholar&linkaccess=abs (visited on 20/12/2022).

[81] U.S. Department of Energy. 'GridLAB-D Simulation Software'. (2022), [Online]. Available: https://www.gridlabd.org/ (visited on 31/05/2022).

[82] *e2nIEE/pandapower*, e2nIEE, 18th May 2022. [Online]. Available: https://github.com/e2nIEE/pandapower (visited on 19/05/2022).

[83] M. Atalay and P. Angin, 'A Digital Twins Approach to Smart Grid Security Testing and Standardization', in *2020 IEEE International Workshop on Metrology for Industry 4.0 IoT*, Jun. 2020, pp. 435–440. DOI: 10.1109/MetroInd4.0IoT48571.2020.9138264.

[84] B. Klaer, Ö. Sen, D. van der Velde, I. Hacker, M. Andres and M. Henze, 'Graph-based Model of Smart Grid Architectures', in *2020 International Conference on Smart Energy Systems and Technologies (SEST)*, Sep. 2020, pp. 1–6. DOI: 10.1109/SEST48500.2020.9203113.

[85] K. Jia, Z. Wang, S. Fan, S. Zhai and G. He, 'Data-Centric Approach: A Novel Systematic Approach for Cyber Physical System Heterogeneity in Smart Grid', *IEEJ Transactions on Electrical and Electronic Engineering*, vol. 14, no. 5, pp. 748–759, 2019, ISSN: 1931-4981. DOI: 10.1002/tee.22861. [Online]. Available: http://onlinelibrary.wiley.com/doi/abs/10.1002/tee.22861 (visited on 23/03/2022).

[86] T. D. Le, A. Anwar, S. W. Loke, R. Beuran and Y. Tan, 'GridAttackSim: A Cyber Attack Simulation Framework for Smart Grids', *Electronics*, vol. 9, no. 8, p. 1218, 8 Aug. 2020, ISSN: 2079-9292. DOI: 10.3390/electronics9081218. [Online]. Available: https://www.mdpi.com/2079-9292/9/8/1218 (visited on 23/03/2022).

[87] V. K. Singh, S. P. Callupe and M. Govindarasu, 'Testbed-based Evaluation of SIEM Tool for Cyber Kill Chain Model in Power Grid SCADA System', in *2019 North American Power Symposium (NAPS)*, Oct. 2019, pp. 1–6. DOI: 10.1109/NAPS46351.2019.9000344.

[88] M. Z. Gunduz and R. Das, 'A comparison of cyber-security oriented testbeds for IoT-based smart grids', in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Mar. 2018, pp. 1–6. DOI: 10.1109/ISDFS.2018.8355329.

[89] Office of Cybersecurity, Energy Security, and Emergency Response and Office of Energy Efficiency and Renewable Energy, 'Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid', U.S. Department of Energy, Oct. 2022. [Online]. Available: https://www.energy.gov/ceser/events/cybersecurity-considerations-distributed-energy-resources-us-electric-grid-briefing (visited on 21/12/2022).

[90] M. Z. Gunduz and R. Das, 'Cyber-security on smart grid: Threats and potential solutions', *Computer Networks*, vol. 169, p. 107 094, 14th Mar. 2020, ISSN: 1389-1286. DOI: 10.1016/j.comnet.2019.107094. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128619311235 (visited on 02/05/2021).

[91] Y. Yan, Y. Qian, H. Sharif and D. Tipper, 'A Survey on Cyber Security for Smart Grid Communications', *IEEE Communications Surveys Tutorials*, vol. 14, no. 4, pp. 998–1010, 4 Apr. 2012, ISSN: 1553-877X. DOI: 10.1109/SURV.2012.010912.00035.

[92] A. C. Panchal, V. M. Khadse and P. N. Mahalle, 'Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures', in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, Nov. 2018, pp. 124–130. DOI: 10.1109/GCWCN.2018.8668630.

[93] R. Leszczyna, 'Standards on cyber security assessment of smart grid', *International Journal of Critical Infrastructure Protection*, vol. 22, pp. 70–89, 1st Sep. 2018, ISSN: 1874-5482. DOI: 10.1016/j.ijcip.2018.05.006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548216301421 (visited on 23/03/2022).

[94] L. Das, S. Munikoti, B. Natarajan and B. Srinivasan, 'Measuring smart grid resilience: Methods, challenges and opportunities', *Renewable and Sustainable Energy Reviews*, vol. 130, p. 109 918, 1st Sep. 2020, ISSN: 1364-0321. DOI: 10.1016/j.rser.2020.109918. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1364032120302094 (visited on 23/03/2022).

[95] I. Semertzis, V. S. Rajkumar, A. Ştefanov, F. Fransen and P. Palensky, 'Quantitative Risk Assessment of Cyber Attacks on Cyber-Physical Systems using Attack Graphs', in *2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, May 2022, pp. 1–6. DOI: 10.1109/MSCPES55116.2022.9770140.

[96] Y. Wadhawan, A. AlMajali and C. Neuman, 'A Comprehensive Analysis of Smart Grid Systems against Cyber-Physical Attacks', *Electronics*, vol. 7, no. 10, p. 249, 10 Oct. 2018, ISSN: 2079-9292. DOI: 10.3390/electronics7100249. [Online]. Available: https://www.mdpi.com/2079-9292/7/10/249 (visited on 23/03/2022).

[97] A. Hahn and M. Govindarasu, 'Cyber Attack Exposure Evaluation Framework for the Smart Grid', *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 835–843, Dec. 2011, ISSN: 1949-3053. DOI: 10.1109/TSG.2011.2163829. [Online]. Available: http://ieeexplore.ieee.org/document/6025254/ (visited on 15/08/2022).

[98] Y. Yang, T. Littler, S. Sezer, K. McLaughlin and H. F. Wang, 'Impact of cyber-security issues on Smart Grid', in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, Dec. 2011, pp. 1–7. DOI: 10.1109/ISGTEurope.2011.6162722.

[99] L. Wei, L. P. Rondon, A. Moghadasi and A. I. Sarwat, 'Review of Cyber-Physical Attacks and Counter Defense Mechanisms for Advanced Metering Infrastructure in Smart Grid', in *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T D)*, Apr. 2018, pp. 1–9. DOI: 10.1109/TDC.2018.8440552.

[100] K. Kimani, V. Oduol and K. Langat, 'Cyber security challenges for IoT-based smart grid networks', *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36–49, 1st Jun. 2019, ISSN: 1874-5482. DOI: 10.1016/j.ijcip.2019.01.001. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548217301622 (visited on 23/03/2022).

[101] A. I. Kawoosa and D. Prashar, 'A Review of Cyber Securities in Smart Grid Technology', in *2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, Jan. 2021, pp. 151–156. DOI: 10.1109/ICCAKM50778.2021.9357698.

[102] G. Liang, S. R. Weller, J. Zhao, F. Luo and Z. Y. Dong, 'The 2015 Ukraine Blackout: Implications for False Data Injection Attacks', *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017, ISSN: 1558-0679. DOI: 10.1109/TPWRS.2016.2631891.

[103] R. Moslemi, A. Mesbahi and J. Mohammadpour Velni, 'Design of robust profitable false data injection attacks in multi-settlement electricity markets', *IET Generation, Transmission & Distribution*, vol. 12, no. 6, pp. 1263–1270, 2018, ISSN: 1751-8695. DOI: 10.1049/iet-gtd.2017.0294. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1049/iet-gtd.2017.0294 (visited on 23/12/2022).

[104] M. P. Jarrett, 'Cybersecurity—A Serious Patient Care Concern', *JAMA*, vol. 318, no. 14, pp. 1319–1320, 10th Oct. 2017, ISSN: 0098-7484. DOI: 10.1001/jama.2017.11986. [Online]. Available: https://doi.org/10.1001/jama.2017.11986 (visited on 23/12/2022).

[105] S. N. Islam, Z. Baig and S. Zeadally, 'Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures', *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6522–6530, Dec. 2019, ISSN: 1941-0050. DOI: 10.1109/TII.2019.2931436.

[106] L. Feiten and M. Sauer, 'Extracting the RC4 secret key of the Open Smart Grid Protocol', 21st Apr. 2016.

[107] D. Lim, J. Lee, B. Gassend, G. Suh, M. van Dijk and S. Devadas, 'Extracting secret keys from integrated circuits', *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200–1205, 10 Oct. 2005, ISSN: 1557-9999. DOI: 10.1109/TVLSI.2005.859470.

[108] Z. Wang, H. He, Z. Wan and Y. Sun, 'Coordinated Topology Attacks in Smart Grid Using Deep Reinforcement Learning', *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 1407–1415, Feb. 2021, ISSN: 1941-0050. DOI: 10.1109/TII.2020.2994977.

[109] H. Zhang, B. Liu and H. Wu, 'Smart Grid Cyber-Physical Attack and Defense: A Review', *IEEE Access*, vol. 9, pp. 29 641–29 659, 2021, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3058628.

[110] H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung, Y. Zhang and C.-K. Wen, 'Local Cyber-Physical Attack for Masking Line Outage and Topology Attack in Smart Grid', *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 4577–4588, Jul. 2019, ISSN: 1949-3061. DOI: 10.1109/TSG.2018.2865316.

[111] R. James Ranjith Kumar and B. Sikdar, 'Detection of Stealthy Cyber-Physical Line Disconnection Attacks in Smart Grid', *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4484–4493, Sep. 2021, ISSN: 1949-3061. DOI: 10.1109/TSG.2021.3082543.

[112] M. Tian, M. Cui, Z. Dong, X. Wang, S. Yin and L. Zhao, 'Multilevel Programming-Based Coordinated Cyber Physical Attacks and Countermeasures in Smart Grid', *IEEE Access*, vol. 7, pp. 9836–9847, 2019, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2018.2890604.

[113] J. Chris Foreman and D. Gurugubelli, 'Identifying the Cyber Attack Surface of the Advanced Metering Infrastructure', *The Electricity Journal*, vol. 28, no. 1, pp. 94–103, 1st Jan. 2015, ISSN: 1040-6190. DOI: 10.1016/j.tej.2014.12.007. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1040619014002899 (visited on 15/08/2022).

[114] P. R. Grammatikis *et al.*, 'Secure and Private Smart Grid: The SPEAR Architecture', in *2020 6th IEEE Conference on Network Softwarization (NetSoft)*, Jun. 2020, pp. 450–456. DOI: 10.1109/NetSoft48620.2020.9165420.

[115] Y. Zhang, L. Wang, W. Sun, R. C. Green II and M. Alam, 'Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids', *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 796–808, Dec. 2011, ISSN: 1949-3061. DOI: 10.1109/TSG.2011.2159818.

[116] G. Chaojun, P. Jirutitijaroen and M. Motani, 'Detecting False Data Injection Attacks in AC State Estimation', *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 5 Sep. 2015, ISSN: 1949-3061. DOI: 10.1109/TSG.2015.2388545.

[117] Q. Su, S. Li, Y. Gao, X. Huang and J. Li, 'Observer-based detection and reconstruction of dynamic load altering attack in smart grid', *Journal of the Franklin Institute*, vol. 358, no. 7, pp. 4013–4027, 1st May 2021, ISSN: 0016-0032. DOI: 10.1016/j.jfranklin.2021.02.008. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0016003221000946 (visited on 23/03/2022).

[118] N. K. Singh and V. Mahajan, 'Detection of cyber cascade failure in smart grid substation using advance grey wolf optimization', *Journal of Interdisciplinary Mathematics*, vol. 23, no. 1, pp. 69–79, 2nd Jan. 2020, ISSN: 0972-0502. DOI: 10.1080/09720502.2020.1721664. [Online]. Available: https://doi.org/10.1080/09720502.2020.1721664 (visited on 23/03/2022).

[119] M. S. Rahman and H. R. Pota, 'Agent-Based Smart Grid Protection and Security', in *Renewable Energy Integration: Challenges and Solutions*, ser. Green Energy and Technology, J. Hossain and A. Mahmud, Eds., Singapore: Springer, 2014, pp. 383–409, ISBN: 978-981-4585-27-9. DOI: 10.1007/978-981-4585-27-9_16. [Online]. Available: https://doi.org/10.1007/978-981-4585-27-9_16 (visited on 02/05/2021).

[120] M. S. Rahman, H. R. Pota and M. J. Hossain, 'Cyber vulnerabilities on agent-based smart grid protection system', in *2014 IEEE PES General Meeting | Conference Exposition*, Jul. 2014, pp. 1–5. DOI: 10.1109/PESGM.2014.6939298.

[121] P. Wang and M. Govindarasu, 'Multi-Agent Based Attack-Resilient System Integrity Protection for Smart Grid', *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3447–3456, 4 Jul. 2020, ISSN: 1949-3061. DOI: 10.1109/TSG.2020.2970755.

[122] T. T. Khoei, G. Aissou, W. C. Hu and N. Kaabouch, 'Ensemble Learning Methods for Anomaly Intrusion Detection System in Smart Grid', in *2021 IEEE International Conference on Electro Information Technology (EIT)*, May 2021, pp. 129–135. DOI: 10.1109/EIT51626.2021.9491891.

[123] M. R. Camana Acosta, S. Ahmed, C. E. Garcia and I. Koo, 'Extremely Randomized Trees-Based Scheme for Stealthy Cyber-Attack Detection in Smart Grid Networks', *IEEE Access*, vol. 8, pp. 19 921–19 933, 2020, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.2968934.

[124] M. N. Kurt, O. Ogundijo, C. Li and X. Wang, 'Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach', *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5174–5185, Sep. 2019, ISSN: 1949-3061. DOI: 10.1109/TSG.2018.2878570.

[125] A. R. Al-Ali and R. Aburukba, 'Role of Internet of Things in the Smart Grid Technology', *Journal of Computer and Communications*, vol. 3, no. 5, pp. 229–233, 5 25th May 2015. DOI: 10.4236/jcc.2015.35029. [Online]. Available: http://www.scirp.org/Journal/Paperabs.aspx?paperid=57559 (visited on 23/12/2022).

[126] J. A. Momoh, 'Smart grid design for efficient and flexible power networks operation and control', in *2009 IEEE/PES Power Systems Conference and Exposition*, Mar. 2009, pp. 1–8. DOI: 10.1109/PSCE.2009.4840074.

[127] L. Tightiz and H. Yang, 'A Comprehensive Review on IoT Protocols' Features in Smart Grid Communication', *Energies*, vol. 13, no. 11, p. 2762, 11 Jan. 2020, ISSN: 1996-1073. DOI: 10.3390/en13112762. [Online]. Available: https://www.mdpi.com/1996-1073/13/11/2762 (visited on 18/05/2022).

[128] E. Leverett, R. Clayton and R. Anderson, 'Standardisation and Certification of the 'Internet of Things'', p. 24,

[129] European Union Agency for Cybersecurity., *Guidelines for Securing the Internet of Things: Secure Supply Chain for IoT*. LU: Publications Office, 2020. [Online]. Available: https://data.europa.eu/doi/10.2824/314452 (visited on 15/08/2022).

[130] N. Kishore, 'Security in IPv6 enabled home networks: Are we ready yet?', 2021.

[131] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu and Z. Y. Dong, 'Cyber security framework for Internet of Things-based Energy Internet', *Future Generation Computer Systems*, vol. 93, pp. 849–859, 1st Apr. 2019, ISSN: 0167-739X. DOI: 10.1016/j.future.2018.01.029. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X1730660X (visited on 23/03/2022).

[132] V. Subramaniam Rajkumar, A. Stefanov, S. Musunuri and J. de Wit, 'Exploiting Ripple20 to Compromise Power Grid Cyber Security and Impact System Operations: 26th International Conference and Exhibition on Electricity Distribution', *CIRED 2021 Proceedings*, 2021.

[133] A. de Haan and P. de Heer, *Solving Complex Problems: Professional Group Decision-Making Support in Highly Complex Situations*. Eleven International, 2012, 178 pp., ISBN: 978-94-90947-71-2. Google Books: 5oF_MAEACAAJ.

[134] S. van Langen, P. van Tol, T. Quak, M. Sinke and M. van Bruggen, *Standardized profile Electricity 2023*, 2022.

[135] TenneT. 'TenneT - Offering of regulating and reserve capacity', Offering of regulating and reserve capacity. (), [Online]. Available: https://www.tennet.org/english/operational_management/system_data_preparation/offering_regulating_reserve_capacity/index.aspx (visited on 20/12/2022).

[136] M. Grady, *Understanding Power System Harmonics*. 2012.

List of Figures

List of Tables

A

Actor analysis

The identification of the actors was made using the imperative approach [62, p.85]. Furthermore, the formal relationships of the actors are defined. Finally, a summary is given in (table A.1).

Formal relations

The formal relations provide insight into the ways different actors are involved with each other. It shows the power dynamic that can be used to solve a problem.

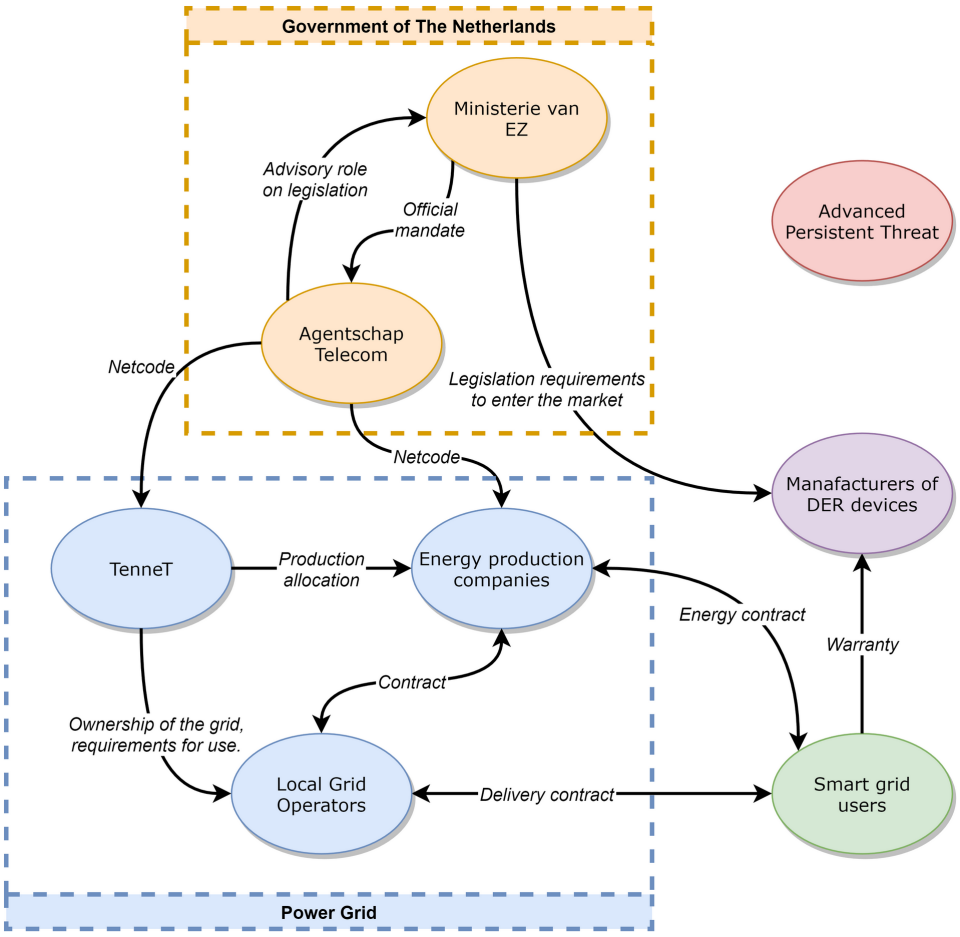

Figure A.1: Formal relationships between actors

Actor	Abbreviatio	Interests	Desired situation	Excisting or expected gap	Causes	Possible Solutions
Agentschap Telecom	AT	Protect the energy grid from cybersecurity risks.	A safe and reliable grid that society can you.	The expected introduction of cybersecurity-related risk.	Introduction of Distributed Energy Resources on a large scale.	Ensure that all devices connected to the grid are secure. Create legislation to this effect.
TenneT	TenneT	Ownership of the energy grid.	Have a safe and reliable grid.	Grid could become less reliable due to cybersecurity risks.	Introduction of Distributed Energy Resources on a large scale	Ensure that all devices connected to the grid are secure.
Smart Grid users	Users	A reliable source of power. Ownership of private DER.	Have the possibility to use solar panels at home, delivering power to the grid, and still have a reliable power source.	Possible uncertainty about the ability to deliver power to the grid.	Adoption of Distributed Energy Resources at home.	Mandated security by design on DER devices connected to the Smart Grid.
Energy production companies	Producers	Shift the business model towards one that can deal with the Smart Grid.	Have a profitable business model related to the energy production of the Smart Grid.	Change of current situation resulting in depreciation of capital. Less need for centrally produced energy.	The transition toward the Smart Grid.	Find a relevant part in the new situation that allows for a new business model.
Ministerie van Economische Zaken (Department of Economic Affairs)	EZ	Prevent climate change. Provide stability for the economy.	Have a net zero carbon economy. Ensure a reliable power situation for the economy.	The changing situation results in uncertainty.	The need to reduce climate change.	Legislation to ensure risk mitigation in the Smart Grid.
Energy storage providers	Storage	Turn profit. Usage of energy storage in the Smart Grid.	Use energy storage to mitigate peaks in demand of the grid.	Currently no presence in the grid.	Adoption of storage solution in the Smart Grid.	Promote storage solutions to other actors.
Advanced Persistent Threat	ATP	Destabilise the Netherlands.	Chaos and panic in the Netherlands and heavy economic damage caused by attacking the Smart Grid.	Currently, no attack vector for them to exploit.	No smart devices are present in the grid.	Wait for unsafe devices to be connected to the grid.

Table A.1: Identified actors