Physical Impact Analysis of Cyberattacks on Inverter-based Consumer Energy Resources

Sarah Maria Engel
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
sarah.engel@kit.edu

Kaibin Bao
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
kaibin.bao@kit.edu

Arman A. Attar
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
arman.attar@kit.edu

Richard Rudolph
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
richard.rudolph@kit.edu

Veit Hagenmeyer
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
veit.hagenmeyer@kit.edu

Abstract

The increasing adoption of Consumer Energy Resources shifts security concerns toward the edge of the grid. Traditional security models, which focus on protecting a small number of large infrastructure components, do not fully apply to this new paradigm. Despite extensive research on attack types and mitigation strategies, there is less research into the *feasible* impact of such attacks on distributed energy systems and their components.

In this work, we begin at the end of a typical attack by exploring reasonable physical impacts an adversary may seek to cause in an inverter-based Consumer Energy Resource or the distribution grid. To achieve this, simulation models capable of portraying the edge cases caused by an attack are required. Thus, we identify various cyberattacks and their impacts on smart inverters from the literature. A selection of these attacks are then chosen for simulation.

Our simulation results demonstrate that the expected impacts of these attacks manifest as intended. The methodology introduced in the present paper can be used as a template for implementing and evaluating the physical impacts of other cyberattacks on power systems. The simulation models are available as open source.

CCS Concepts

• **Computer systems organization** → **Embedded systems**; *Real-time system architecture*; • **Hardware** → Renewable energy; **Smart grid**; **Power networks**; • **Security and privacy** → **Distributed systems security**.

Keywords

Smart Grid, Cybersecurity, Simulation Models, Physical Impact, Inverter, PLL, PWM, FDI, Protection, Grid Support, Supply Chain

E-ENERGY '25, Rotterdam, Netherlands
© 2025 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1125-1/25/06
https://doi.org/10.1145/3679240.3734651

ACM Reference Format:
Sarah Maria Engel, Kaibin Bao, Arman A. Attar, Richard Rudolph, and Veit Hagenmeyer. 2025. Physical Impact Analysis of Cyberattacks on Inverter-based Consumer Energy Resources. In *The 16th ACM International Conference on Future and Sustainable Energy Systems (E-ENERGY '25), June 17–20, 2025, Rotterdam, Netherlands.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3679240.3734651

1 Introduction

Unlike conventional cyberattacks focused on data theft or breaches, modern attacks can inflict physical damage, disrupt operations, and even trigger large-scale power outages. This threat underscores the urgent need to understand the interplay between cyber-physical systems and cyberattacks to develop effective countermeasures.

Several high-profile incidents highlight the importance of safeguarding critical infrastructure. For example, the AcidRain malware in 2022 disrupted control communications for 5,800 Enercon wind turbines in Germany, potentially putting 11 GW of generation power at risk [20]. Other notable examples include RedEcho's infiltration of the Indian power grid [12], the 2015 attack on the Ukrainian power grid [10] and the emergence of INDUSTROYER.V2 in the ongoing conflict in Ukraine [16].

As power grids transition to inverter-dominated, low-inertia systems, the attack surface is evolving, necessitating a fresh perspective on the physical impact of cyberattacks. While existing research heavily focuses on IT-based threats the operational technology (OT) domain, especially the physical impacts of cyberattacks, remains underexplored. Thus, the present paper addresses this gap by modeling expected physical impacts of cyberattacks on electrical grid components, with a focus on Consumer Energy Resources (CER). Five attacks are modeled and simulated to evaluate their potential to induce edge cases and damage scenarios.

As attacks with physical impact ultimately involve physical damage, repeated experiments with physical destruction would lead to high costs. Therefore, we chose to simulate inverters and attacks on inverters. This enables repeatability for our experiments as well as scaling of our virtual testbeds for a fraction of the cost compared to physical testbeds. Another added benefit is the possible repeatability of our experiments by other scientists. The goal of our research efforts is to emulate complete cyberattacks end-to-end, beginning on the IT surface and ending at physical impact. This paper is one building block for our goal and addresses the following key research questions:

1. Which cyberattacks on inverters are feasible?
2. What is the impact of such cyberattacks?
3. How can the physical impact of a cyberattack be modeled?

The present paper summarizes the Master's thesis of Engel [9] and provides the following major contributions:

1. A review of cyberattacks misusing inverters,
2. An analysis of the physical impact of these attacks, by
3. Development of simulation models for selected attacks, and
4. Publishing these simulation models as open source.

In the remainder of the present paper, we describe fundamental knowledge about inverters and related work with a comparable motivation. In Section 2, we collect references to cyberattacks on inverters or using inverters. We describe the two Simulink base simulation models in Section 3. This is followed by Section 4 where our five attacks are described the implementation is outlined. We then describe the results in Section 5 and finally conclude in Section 6.

1.1 Fundamentals

To effectively analyze cyberattacks on inverters, it is essential to understand their operational principles. An inverter converts direct current (DC) into alternating current (AC), allowing compatibility between DC-based distributed energy resources (DERs), such as solar panels or batteries, and AC loads or the power grid [25].

Inverters operate by using power transistors, such as Metal-Oxide-Semiconductor Field-Effect Transistors (MOSFETs) or Insulated Gate Bipolar Transistors (IGBTs). These transistors switch rapidly and are controlled using Pulse Width Modulation (PWM) to approximate a sinusoidal waveform in the inverter's output voltage. The smoothness in the waveform is achieved by filters. [3, 14]

A pair of power transistors is a half-bridge configuration and it controls the polarity of the voltage applied to the load, alternating the current flow to create the desired AC waveform. In three-phase inverters, three half-bridges are used, with each phase offset by 120 degrees. In addition to the switching unit, inverters integrate control systems such as the Maximum Power Point Tracker (MPPT), which maximizes power extraction from variable DC sources by adjusting operating conditions dynamically. Voltage and current controllers synchronize the output with the grid, ensuring power control and compliance with grid codes. [4, 26]

Inverters can be categorized into two main operational modes: *Grid-following* inverters synchronize their output with an existing grid by matching its voltage and frequency. These are commonly used in residential and commercial solar applications [8]. In contrast, *grid-forming* inverters actively regulate both voltage and frequency, making them essential for microgrids and isolated systems where stability is maintained independently of the main grid [8].

Modern smart inverters extend basic functionality by supporting grid services such as reactive power compensation, voltage regulation, and frequency stabilization. These functions may be used in enhancing grid resilience and enabling smart grid operations [17].

Figure 1 illustrates the schematic of the DC/AC conversion process in a three-phase half-bridge inverter.

1.2 Related Work

Recent literature has increasingly addressed the simulation of cyber-physical attacks on electric power systems, including inverter-based resources. Yohanandhan et al. [32] review strategies for modeling and simulating cyber-physical power systems but do not validate their concepts through experiments or simulated cyberattacks. Similarly, Li and Yan [17] provide an overview of cyberattacks on smart inverters. They describe cyberattacks and their impacts, but they do not provide any simulation models. However, they reference some work that includes simulation models. Examples of such work, including cyberattacks on inverters and simulation models, are provided by Ustun [28], Johnson et al. [15], Olowu et al. [22], and Yadav et al. [31]. Nonetheless, they show the attacks in a narrow context and do not explore the impacts in detail. Another example of work that looks at attacks and its impacts is from Siaterlis et al. [24]. They looked at attacks on boiling water power plants and their effect on the pressure in those plants.

Other publications, like Carter et al. [5], often assume impacts of attacks but do not provide an insight into the impacts themselves.

Rajkumar et al. [23] review cascading failures in power grids and present a case study simulating a cyberattack on the IEEE 39-bus system, including OT infrastructure and IEC 61850 communication. Their setup uses DIgSILENT PowerFactory with RTDS real-time simulators and models generic generators and protections in a transmission grid.

In contrast, our work focuses on simulating detailed physical effects of cyberattacks on inverters within a distribution grid, using MathWorks Simulink. While their study emphasizes OT-layer interaction, our attacks are abstracted, and OT modeling is part of ongoing research.

2 Review of Cyberattacks using Inverters

Li and Yan [17] categorize cyberattacks on inverters as device-level, targeting individual units, and grid-level, affecting the broader system. We adopt this structure in the following two subsections, but we use terminology from the MITRE ATT&CK Framework [2] to express the physical consequences.

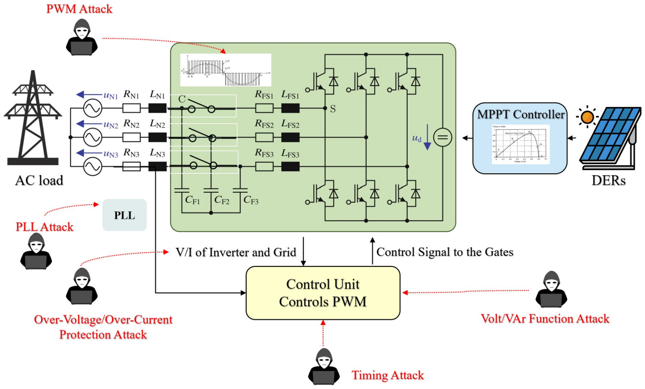

Figure 1: Schematic of a Three-phase Inverter with Selected Attacks (Figure based on [3, 18, 33]).

While attack taxonomies can be organized by techniques, vulnerabilities, or goals, we focus solely on the physical impact. Attack vectors and impact exhibit a many-to-many relationship.

2.1 Impact on Electrical Devices

Firmware Manipulation. The device firmware can be replaced, modified, or targeted via a supply-chain attack, allowing an attacker to compromise the entire device with high privileges. This is referred by Li and Yan [17] as a "firmware attack". The level of access required depends on how firmware updates are handled by the specific inverter model. Some require physical access, others allow remote updates.

Carter et al. [5] attempted remote firmware updates on two devices using modified vendor-provided firmware. The updates were rejected, likely due to checksum validation. Even unsuccessful updates had side effects: For one device, a failed update caused a disconnection until it was manually reconfigured.

We simulate the impact of firmware manipulation with a *Timing Attack* (Section 4.1) representing a low-privilege case, and a *PWM Attack* (Section 4.2) representing a high-privilege scenario which the attacker may gain by rewriting the real-time controller code.

Tripping the Protection. Protection functions ensure inverter safety and compliance to grid codes. According to Li and Yan [17], typical systems include: (a) DC short-circuit/over-current detection, (b) ground fault detection, (c) transistor over-temperature detection, and (d) AC-side over/under voltage and frequency detection.

Attacks on these functions can involve false data injection (FDI) into measurement inputs or modification via firmware replacement. These attacks may falsely trigger shutdowns or mask real faults, potentially leading to premature wear or damage. Islanding detection can also be exploited for disconnects [15], or its deactivation can pose safety risks such as electric shock [17]. The immediate effects of tripping protection functions are simulated in Section 4.3.

Loss of Grid Synchronization. Albunashee et al. [1] describe an attack that disrupts the Phase-Locked Loop (PLL) in inverters by injecting high-voltage signals near the target device. This causes effects such as overcurrent, overvoltage, rapid frequency changes, reverse power flow, and unintended protection activation.

We model this scenario as the *Phase-Locked Loop Attack* (Section 5.4). Note that not all inverters rely on PLLs—alternatives like Resonant Controllers and Direct Power Control (DPC) are also used for grid synchronization.

2.2 Impact on the Power Grid

Load Altering. Zhang et al. [34] demonstrate a FDI attack on the maximum power point tracker (MPPT) controller, leading to a reduced power production. Controllers can be attacked in general by manipulating their input values or control parameters.

A load altering effect, as described by Li and Yan [17], is simulated by our experiment for the *Timing Attack* (Section 4.1) and indirectly by tripping the *Over-Voltage/Over-Current Protection* (Section 4.3).

Voltage Stability. Voltage stability can be impaired by manipulating the inverter's grid support function, which controls the ratio of reactive to active current to meet power demands. Reactive power, is expected to play an important role in future smart grids. Similar to controller attacks, false data injection (FDI) can be used to alter grid support parameters [17]. A straightforward method is modifying the active (P) and reactive (Q) power set-points. Hossen et al. [13] show that setting harmful P/Q values can push the inverter beyond its operational limits. Likewise, Teymouri et al. [27] demonstrate that inappropriate setpoints can force the inverter to absorb reactive power, resulting in real power loss. Naderi et al. [21] propose an attack where an under-voltage is induced in one distribution grid segment and an over-voltage simultaneously in another. In this case, the situation cannot be resolved by adjusting the taps of an on-load tap-changing transformer.

We demonstrate such a harmful reduction in voltage stability in the *Volt-VAr Function Attack* (Section 4.5).

Frequency Stability. Attacks on frequency stability were recently discussed by Goerke et al. [11], who describe load-altering attacks that synchronize large numbers of controllable loads, such as EVs or inverter-based PV and battery systems. We do not consider frequency stability in the present paper as the number of inverters needed to significantly influence the grid frequency exceed the number of inverters usually available in only one distribution grid. In order to reach the limits of the frequency containment reserve of the European grid, an accumulated load of at least 3.000 MW is needed [11].

Resonance Attacks. Hossen et al. [13] note that an over-modulated inverter can inject low-order current harmonics. This could lead to distorted voltage at the point of common coupling (PCC), especially if the state of the grid is that of a weak grid. Similarly, Mohan et al. [19] suggest that altering the power load or tie-line signal can induce harmonic resonance into the grid.

Escalation to Other Devices. A compromised inverter could be used to attack other devices in the grid. Examples of target devices are smart meters or on-load tap changers [17]. An example is shown by Teymouri et al. [27]. They caused unwanted tap changes through FDI on voltage measurements.

3 Base Simulation Models

To evaluate the impacts of cyberattacks on inverters, simulation models were investigated to serve as a foundation for further development. These models should focus on low-voltage grids, where inverters are typically deployed in distributed energy systems. The simulations should aim to represent actual operating conditions and provide insights into the interactions between inverters, grid components, and attack-induced disruptions.

We chose the electromagnetic transient (EMT) model of a low-voltage grid by De Paola et al. [6] depicted in Figure 2 as this model contains typical grid components with relatively high level of detail. Although this model does not represent the topology of a real distribution grid, it is well suited to study the interaction between different grid components. It includes essential components such as transformers, dynamic and static loads, and connections to medium-voltage grids. These elements enable the study of cascading effects within the network, providing a comprehensive perspective on how cyberattacks propagate through interconnected systems. Additionally, the inclusion of diverse grid components ensures that the models can account for various operating conditions [6].

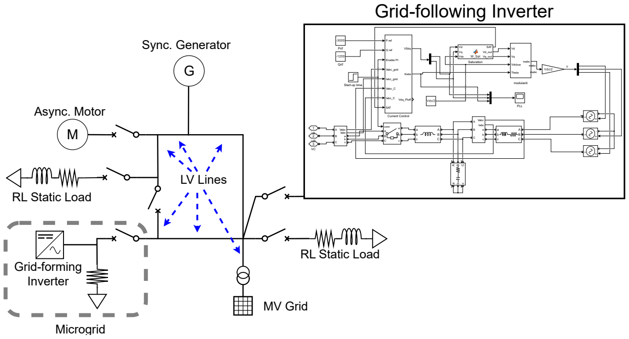

Figure 2: Simplified Grid Model as Single Line Diagram Based on the Model by De Paola et al. [6] and the Detailed Simulink Inverter Model by the same authors [7].

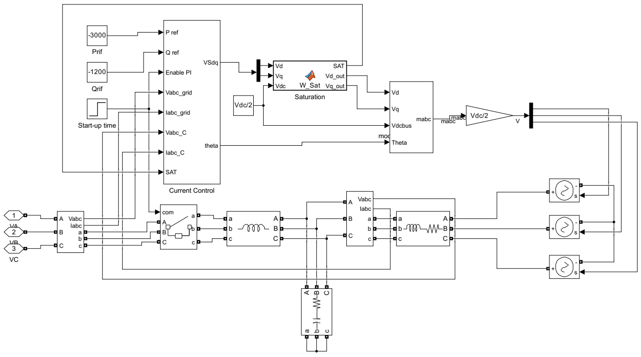

Figure 3: Simulink Implementation of a High Abstraction Model of an Inverter, both by De Paola et al. [6, 7].

For one of the simulated attacks, we need a first principle model of the PWM control inside the inverter. The inverter of the low-voltage grid model, as shown in Figure 3, is on a higher abstraction level that does not allow modeling the manipulation of the PWM control easily. This is why for this scenario, we use the simulation model by Vijay [30] (see upper part of Figure 7 in the Appendix).

Electromagnetic transient (EMT) simulation techniques are chosen due to their capability to model high-resolution dynamics and fast transients, including voltage and frequency deviations, as well as protective function activations that may result from cyberattacks or conversely, prevent a real impact. EMT simulations also highlight interactions between inverters and the grid, emphasizing potential risks to stability and performance [28].

The development of these models is guided by accessibility and reproducibility. Open source simulation models are selected, enabling collaboration and validation within the research community. Existing benchmark models for low-voltage grids are adapted to meet the study's requirements. Specific modifications are implemented to incorporate attack parameters and behaviors, enhancing the models' relevance [6, 17].

Furthermore, EMT models are compatible with hardware-in-the-loop (HIL) setups, which extend their applicability for experimental validation. This adaptability bridges the gap between simulation and real-world testing, allowing for more accurate evaluation of defense strategies against cyberattacks. While the current work focuses on simulation results, the flexibility of these models provides a foundation for future experimental research.

4 Cyberattacks and Implementation

Our selected attacks on photovoltaic inverters are implemented in Simulink to portray the attacks' effects on the inverters. There are different approaches to implementing these attacks depending on the abstraction level of the base model. When the model is built on first principles, attacks can be simulated by directly modifying the fundamental components and their interactions. If the base model operates at a higher abstraction level, equivalent effects must be modeled at appropriate points in the system to replicate the behavior of the attack. The following sections describe the implementation of specific attacks using these guidelines.

Figure 1 represents the schematic of the selected attacks on the device level. The selected attacks are described in details in the following. All simulation models are published as open source on Zenodo[1] and maintained on Github[2] .

4.1 Timing Attack

The *Timing Attack* is designed to simulate a synchronized disconnection of an inverter from the grid at a predefined time. This attack showcases the effect of a vulnerability in the remote control of the inverter or a supply-chain attack planted inside the inverter's firmware.

The attack time is set to 0.2 seconds after the start of the simulation. The simulated grid has reached a quasi steady state by that time. This attack signal is then connected to the control input of a circuit breaker block, which opens the circuit and disconnects the inverter from the grid. The Simulink model of the attack is depicted in the Appendix Figure 6.

The key parameters in this implementation include the attack time, which determines when the inverter disconnection occurs, and the circuit breaker delay, which is minimized to reflect realistic switching behavior.

4.2 Pulse Width Modulation Attack

The *Pulse Width Modulation (PWM) Attack* is designed to disrupt the normal operation of the inverter by manipulating the controller responsible for pulse width modulation. The attack is implemented to cause a short circuit on one or more phases of the inverter by forcing specific transistors of the half-bridge to remain in the on-state.

Once the predefined time is reached, the timer triggers a switch that overrides the PWM control signals. The manipulated signal forces both transistors of a half-bridge to be active simultaneously, leading to a short circuit on the affected phase.

In the Simulink model (Figure 7 in the Appendix), custom pseudo-fuses are added to the model to simulate the physical effects of the short circuit, including current surges and ultimately line breakage caused by trace evaporation. The timer block initiates the attack

[1] https://doi.org/10.5281/zenodo.14737206
[2] https://github.com/drbaka-de/simulation_models_of_cyberattacks_on_inverters

by modifying the input of the targeted transistor from the PWM signal so that the transistor remains permanently on.

A pseudo-fuse model (Figure 11 in the Appendix) simulates the line breakage. This component measures the current flowing through the line and compares it to a predefined threshold. When the threshold is exceeded, the fuse model triggers a disconnection to simulate permanent damage.

The key components of the *PWM Attack* implementation include the timer block, the modified PWM signal logic, and the pseudo-fuse model.

4.3 Over-Voltage/Over-Current Protection

This attack manipulates the measurement values taken by the over-voltage or over-current protection unit of the inverter. False high-voltage or high-current values are injected into the measurement system, causing the protection mechanism to disconnect the inverter from the grid.

In Simulink, the attack is implemented by introducing a function block that changes the measurements starting at 0.2 seconds into the simulation. This block intercepts the measurement signals and replaces them with artificially elevated values that exceed the protection threshold. When the over-voltage or over-current protection system detects these values, it triggers a disconnection.

The modified inverter model, including the over-voltage manipulation block, is shown in the Appendix, Figure 12. This attack demonstrates how false data injection (FDI) can exploit vulnerabilities in the protection logic of photovoltaic inverters.

4.4 Phase-Locked Loop Attack

The Phase-Locked Loop (PLL) Attack targets the synchronization mechanism of the inverter by injecting short pulse signals into the point of common coupling (PCC) over the grid from another inverter. These goal of the pulses is to disrupt the PLL, leading to instability in the inverter's operation.

In Simulink (see Figure 9 in the Appendix), the attack is implemented by adding a custom pulse generator in the attackers inverter. This block generates high-frequency pulses that interfere with the PLL's ability to lock onto the grid's phase. The parameters of the pulse generator, such as frequency and amplitude, can be adjusted to analyze the extent of disruption caused by the attack.

This attack highlights the vulnerabilities in synchronization mechanisms and emphasizes the importance of robust grid synchronization.

4.5 Volt-VAr Function Attack

The Volt-VAr function manages the inverter's reactive power response to voltage fluctuations in the grid, stabilizing voltage by absorbing or supplying reactive power as needed. The Volt-VAr function attack manipulates its parameters or setpoints to reverse this behavior, exacerbating grid instability. Specifically, the function's slope is flipped, causing the inverter to supply reactive power during over-voltage conditions and absorb reactive power during under-voltage conditions.

In the simulation, this is achieved by first implementing the Volt-VAr grid support function (Figure 13 in the Appendix) which did not exist in the base model. The attack is realized by altering the control logic, reversing the Volt-VAr curve (Figure 17 in the Appendix).

4.6 Model Soundness

For the inverter, we used the simulation model developed and evaluated by De Paola et al. [6, 7]. This model was validated by the authors, therefore we assumed the correctness of the model for regular operation modes without cyberattacks.

The PWM model by Vijay [30] was compared against power systems and electrical engineering textbooks ([3, 18, 33]) to infer the correctness of the model.

For each attack, the inverter simulation model was extended by components necessary for the attack. Then an expected behavior was formulated. To evaluate an attack, the expected behaviour was compared against the behavior and results from the simulation.

5 Results

This section presents the evaluation results for the five implemented attacks on photovoltaic inverters. For each attack, the expected outcomes are discussed and how the simulation results validate these expectations.

5.1 Timing Attack

The expected outcome of the *Timing Attack* is a disconnection of the inverter from the grid at the predefined time.

Figure 14 in the Appendix illustrates the simulation results, showing the inverter's current measured at the point of common coupling (PCC) over time. After acquiring the synchronization in the first 0.05 seconds, the inverter connects to the mains. The attack is triggered at 0.2 seconds. The circuit breaker disconnects each phase at the nearest zero crossing. This rather trivial experiment confirms the basic functions of the simulation model with the expected synchronization delay before grid connection, the transients shortly after the connection and the disconnection delay of the circuit breakers.

5.2 Pulse Width Modulation Attack

The expected outcome of the *Pulse Width Modulation Attack* is the occurrence of a short circuit on one phase of the inverter due to the forced permanent activation of one transistor in a half-bridge. This should lead to abnormal current spikes and eventual line breakage, simulated via pseudo-fuses.

The Simulink model used in this experiment only consists of an grid-forming inverter with its half-bridges and PWM control in detail. This kind of simulation is hardly possible using the inverter model of the grid model by De Paola et al. [6], because in these models, the half-bridges and PWM control are abstracted.

Figure 15 in the Appendix depicts the inverter's current measured at the point of common coupling (PCC) during the PWM Attack. The observed current waveform changes after 0.2 seconds with a certain delay. Current spikes happen inside the device and are not observed at the PCC. The pseudo-fuse model successfully disconnects the third phase.

The other two phases continue to operate, but the three phase system is imbalanced. A real inverter would have a mains connection protection that monitor the imbalance and disconnect the

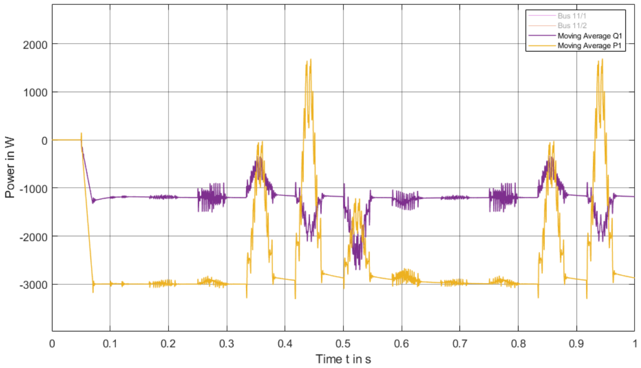

Figure 4: Active and Reactive Power of the Attacked Inverter.

whole device. This demonstrates the incompleteness of simulation models when cyberattacks are to be modeled holistically.

5.3 Over-Voltage/Over-Current Protection

The expected outcome of the *Over-Voltage/Over-Current Protection Attack* is the triggering of the protection mechanism due to artificially elevated voltage or current measurements. As protection devices have characteristic curves describing the sensitivity of the protection, disconnection does not happen immediately but after a variable delay which depends on the severeness of the voltage or current violation. Eventually, the disconnection of the inverter from the grid should be observed.

The detailed current of the inverter is depicted in the Appendix, Figure 16: High current transients at the connection to mains are visible around 0.05 seconds. The current value manipulation is starting at 0.2 seconds. The disconnection happens shortly after at the next zero crossings of each phase individually. For this, we can qualitatively confirm the effectiveness of the attack.

5.4 Phase-Locked Loop Attack

We expect the intermediate outcome of the *Phase-Locked Loop (PLL) Attack* to be an disturbance of frequency and phase detection in the targeted inverter. This should lead to desynchronization with the real frequency and phase of the grid. Desynchronization should lead to fluctuations in the active and reactive power flows.

The simulation result is depicted in Figure 4 with the power flow measured at the grid connection point of the inverter in import-positive metering. After an initial grid synchronization phase of 0.05 seconds, the inverter is ramping up active power generation to 3.000 W and reactive power to 1.250 W. Without attack, active and reactive power is expected to stay constant. Under the influence of the *PLL Attack*, we see a repeating pattern of disturbances especially in the active power flow, which is even inverted sometimes. In an auxiliary frequency over time plot (Appendix Figure 18), the acquisition of the grid frequency is clearly perturbed.

The results validate the capability of the attack to destabilize the PLL which in turn disturbs the stability of the active and reactive power flows.

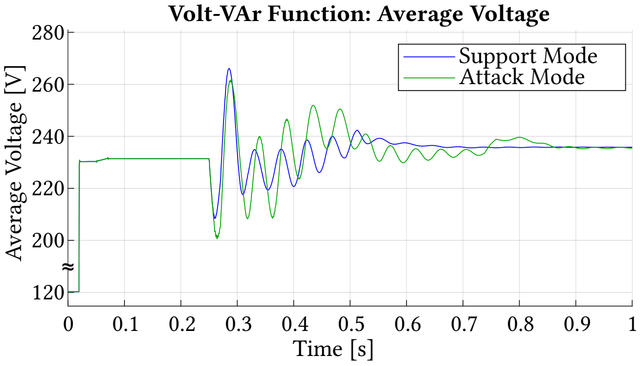

Figure 5: Simulation Results of the Volt-VAr Function Attack.

5.5 Volt-VAr Function Attack

The expected outcome of this attack is only visible during grid disturbances. In the simulation, a grid disturbance is triggered at 0.25 seconds. We compare the influence of the inverter on the grid voltage in grid support mode and in grid attack mode. In support mode, the Volt-VAr function stabilizes the grid by absorbing reactive power during over-voltage conditions and supplying reactive power during under-voltage conditions. In attack mode, these behaviors are reversed, causing the inverter to amplify voltage deviations instead of mitigating them. The simulation results confirm these expectations. Figure 5 illustrates the impact of this manipulation, where the inverter's reactive power responses exacerbate grid's voltage instability. The results validate that the expected destabilizing effects of the attack are successfully realized.

6 Conclusion

In this paper, we present insight into component-based cyberattacks on inverter systems by providing a review of cyberattacks that target inverters and protection systems, as well as an analysis of the physical impacts of those attacks. Furthermore, we implemented selected attacks in Simulink based on the grid model by De Paola et al. [6]. The benefits of simulating cyberattacks include better scalability for large systems while keeping low costs for large-scale testbeds as well as reproducibility, as physical impact ultimately involves physical damage and therefore cost. The simulation models are provided open source to benefit the scientific community and accelerate science on cybersecurity for energy systems. Our work highlights the importance of an electrical engineering perspective in assessing the physical impacts of cyberattacks on inverter-based consumer energy resources. By simulating selected attacks, we demonstrated how vulnerabilities in inverters can disrupt grid stability and cause physical damage. Our findings show that in existing energy system models, effects of cyberattacks are not necessarily modeled. This is making re-modeling of physical impact and real-world validation essential for research on cybersecurity.

Future work will include the implementation and validation of the presented attacks using a real-world low-voltage grid environment, as well as validations of the presented attack models with a hardware testbed. Also, we plan to extend the inverter model to represent real-world inverters more accurately. Practical experiments are crucial to identify unforeseen factors, improve model accuracy, and bridge the gap between simulation and real-world applications. These efforts will enhance our understanding of cyber-physical threats and strengthen mitigation strategies.

Acknowledgements

This work was supported by the Helmholtz Association under the programs "Energy System Design (ESD)" (topic number 37.12.01) and "Engineering Digital Futures (EDF)" as part of the KASTEL Security Research Labs, Karlsruhe (topic number 46.23.02).

References

[1] Hamdi M. Albunashee, Chris Farnell, Andrew Suchanek, Kelby Haulmark, Roy A. McCann, Jia Di, and Alan Mantooth. 2022. A Test Bed for Detecting False Data Injection Attacks in Systems With Distributed Energy Resources. *IEEE Journal of Emerging and Selected Topics in Power Electronics* 10, 1 (Feb. 2022), 1303–1315. doi:10.1109/JESTPE.2019.2948216

[2] Otis Alexander, Misha Belisle, and Jacob Steele. 2020. *MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy.* Technical Report. https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf

[3] Issa Batarseh and Ahmad Harb. 2018. *Power Electronics.* Springer International Publishing, Cham. doi:10.1007/978-3-319-68366-9

[4] Andrew J. Butterfield and John Szymanski (Eds.). 2018. *A Dictionary of Electronics and Electrical Engineering.* Vol. 1. Oxford University Press. doi:10.1093/acref/9780198725725.001.0001

[5] Cedric Carter, Ifeoma Onunkwo, Patricia Cordeiro, and Jay Johnson. 2017. Cyber Security Assessment of Distributed Energy Resources. In *2017 IEEE 44th Photovoltaic Specialist Conference (PVSC).* IEEE, Washington, DC, 2135–2140. doi:10.1109/PVSC.2017.8366503

[6] Antonio De Paola, Dimitrios Thomas, Evangelos Kotsakis, Antonios Marinopoulos, Marcelo Masera, Alexandros Paspatis, Alkistis Kontou, Panos Kotsampopoulos, and Nikos Hatziargyriou. 2022. Benchmark Models for Low-Voltage Networks: a Novel Open-Source Approach. In *2022 Open Source Modelling and Simulation of Energy Systems (OSMSES).* IEEE, Aachen, Germany, 1–6. doi:10.1109/OSMSES54027.2022.9769097

[7] Antonio DePaola. 2021. *ERIGrid2/benchmark-model-electrical-network: v1.1.* doi:10.5281/zenodo.5707769

[8] Mohamed E. Elkhatib, Wei Du, and Robert H. Lasseter. 2018. Evaluation of Inverter-based Grid Frequency Support using Frequency-Watt and Grid-Forming PV Inverters. In *2018 IEEE Power & Energy Society General Meeting (PESGM).* IEEE, Portland, OR, 1–5. doi:10.1109/PESGM.2018.8585958

[9] Sarah Maria Engel. 2024. *Simulation Models for Cyber Attacks on Electrical Grid Components.* Master's thesis. Karlsruhe Institute of Technology (KIT), Karlsruhe.

[10] Marcus Geiger, Jochen Bauer, Michael Masuch, and Jorg Franke. 2020. An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems. In *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA).* IEEE, Vienna, Austria, 1537–1543. doi:10.1109/ETFA46521.2020.9212128

[11] Niklas Goerke, Alexandra Märtz, and Ingmar Baumgart. 2024. Who Controls Your Power Grid? On the Impact of Misdirected Distributed Energy Resources on Grid Stability. In *The 15th ACM International Conference on Future and Sustainable Energy Systems.* ACM, Singapore Singapore, 46–54. doi:10.1145/3632775.3661943

[12] Insikt Group. 2022. *Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group.* Technical Report. https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf

[13] Tareq Hossen, Mehmetcan Gursoy, and Behrooz Mirafzal. 2022. Self-Protective Inverters Against Malicious Setpoints Using Analytical Reference Models. *IEEE Journal of Emerging and Selected Topics in Industrial Electronics* 3, 4 (Oct. 2022), 871–877. doi:10.1109/JESTIE.2022.3199672

[14] Dong Jiang, Zewei Shen, Qiao Li, Jianan Chen, and Zicheng Liu. 2021. *Advanced Pulse-Width-Modulation: With Freedom to Optimize Power Electronics Converters.* Springer Singapore, Singapore. doi:10.1007/978-981-33-4385-6

[15] Jay Johnson, Jimmy Quiroz, Ricky Concepcion, Felipe Wilches-Bernal, and Matthew J. Reno. 2019. Power system effects and mitigation recommendations for DER cyberattacks. *IET Cyber-Physical Systems: Theory & Applications* 4, 3 (Sept. 2019), 240–249. doi:10.1049/iet-cps.2018.5014

[16] Pavel Kozak, Ivo Klaban, and Tomáš Šlajs. 2023. Industroyer cyber-attacks on Ukraine's critical infrastructure. In *2023 International Conference on Military Technologies (ICMT).* IEEE, Brno, Czech Republic, 1–6. doi:10.1109/ICMT58149.2023.10171308

[17] Yuanliang Li and Jun Yan. 2023. Cybersecurity of Smart Inverters in the Smart Grid: A Survey. *IEEE Transactions on Power Electronics* 38, 2 (Feb. 2023), 2364–2383. doi:10.1109/TPEL.2022.3206239 Conference Name: IEEE Transactions on Power Electronics.

[18] Florian Mahr, Stefan Henninger, Martin Biller, and Johann Jäger. 2021. *Elektrische Energiesysteme: Wissensvernetzung von Stromrichter, Netzbetrieb und Netzschutz.* Springer Fachmedien Wiesbaden, Wiesbaden. doi:10.1007/978-3-658-34908-0

[19] Athira M. Mohan, Nader Meskin, and Hasan Mehrjerdi. 2020. A Comprehensive Review of the Cyber-Attacks and Cyber-Security on Load Frequency Control of Power Systems. *Energies* 13, 15 (July 2020), 3860. doi:10.3390/en13153860

[20] Alessandro Mura. 2024. *From technical details to the overall relevance for cybersecurity of critical infrastructures.* Technical Report. https://centri.unibo.it/computational-social-science/it/cosa-facciamo/our-students-papers/mura_cs-cw2024_final.pdf/@@download/file/Mura_CS&CW2024_FINAL.pdf

[21] Ehsan Naderi, Samaneh Pazouki, and Arash Asrari. 2023. A coordinated cyberattack targeting load centers and renewable distributed energy resources for undervoltage/overvoltage in the most vulnerable regions of a modern distribution system. *Sustainable Cities and Society* 88 (2023), 104276. doi:10.1016/j.scs.2022.104276

[22] Temitayo O. Olowu, Shamini Dharmasena, Hassan Jafari, and Arif. Sarwat. 2020. Investigation of False Data Injection Attacks on Smart Inverter Settings. In *2020 IEEE CyberPELS (CyberPELS).* IEEE, Miami, FL, USA, 1–6. doi:10.1109/CyberPELS49534.2020.9311541

[23] Vetrivel Subramaniam Rajkumar, Alexandru Ştefanov, Alfan Presekal, Peter Palensky, and José Luis Rueda Torres. 2023. Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures. *IEEE Access* 11 (2023), 103154–103176. doi:10.1109/ACCESS.2023.3317695 Conference Name: IEEE Access.

[24] Christos Siaterlis, Bela Genge, and Marc Hohenadel. 2013. EPIC: A Testbed for Scientifically Rigorous Cyber-Physical Security Experimentation. *IEEE Transactions on Emerging Topics in Computing* 1, 2 (Dec. 2013), 319–330. doi:10.1109/TETC.2013.2287188

[25] Arno Hendrikus Marie Smets, Klaus Jäger, Olindo Isabella, René van Swaaij, and Miro Zeman. 2016. *Solar energy: the physics and engineering of photovoltaic conversion, technologies and systems.* UIT Cambridge, Cambridge, England.

[26] Ryszard Michal Strzelecki and Grzegorz Benysek (Eds.). 2008. *Power Electronics in Smart Electrical Energy Networks.* Springer London, London. doi:10.1007/978-1-84800-318-7

[27] Armin Teymouri, Ali Mehrizi-Sani, and Chen-Ching Liu. 2018. Cyber Security Risk Assessment of Solar PV Units with Reactive Power Capability. In *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society.* IEEE, Washington, DC, 2872–2877. doi:10.1109/IECON.2018.8591583

[28] Taha Selim Ustun. 2019. Cybersecurity Vulnerabilities of Smart Inverters and Their Impacts on Power System Operation. In *2019 International Conference on Power Electronics, Control and Automation (ICPECA).* IEEE, New Delhi, India, 1–4. doi:10.1109/ICPECA47973.2019.8975537

[29] VDE-AR-N 4105. 2018. VDE-AR-N 4105 Anwendungsregel: 2018-11 Erzeugungsanlagen am Niederspannungsnetz - Technische Mindestanforderungen für Anschluss und Parallelbetrieb von Erzeugungsanlagen am Niederspannungsnetz.

[30] Vijay. 2024. Sinusoidal PWM based 3-phase Inverter using MATLAB - File Exchange - MATLAB Central. https://de.mathworks.com/matlabcentral/fileexchange/72334-sinusoidal-pwm-based-3-phase-inverter-using-matlab (Accessed 04-03-2024).

[31] Seema Yadav, Nand Kishor, Shubhi Purwar, and Saikat Chakrabarti. 2023. Indirect Cyber-Physical Attack with Combined Circuit Breaker and Excitation System. In *IEEE EUROCON 2023 - 20th International Conference on Smart Technologies.* IEEE, Torino, Italy, 204–209. doi:10.1109/EUROCON56442.2023.10199068

[32] Rajaa Vikhram Yohanandhan, Rajvikram Madurai Elavarasan, Premkumar Manoharan, and Lucian Mihet-Popa. 2020. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. *IEEE Access* 8 (2020), 151019–151064. doi:10.1109/ACCESS.2020.3016826 Conference Name: IEEE Access.

[33] Richard Zahoransky, Hans-Josef Allelein, Elmar Bollin, Helmut Oehler, Udo Schelling, and Harald Schwarz. 2013. *Energietechnik: Systeme zur Energieumwandlung. Kompaktwissen für Studium und Beruf.* Springer Fachmedien Wiesbaden, Wiesbaden. doi:10.1007/978-3-8348-2279-6

[34] Jinan Zhang, Qi Li, Jin Ye, and Lulu Guo. 2020. Cyber-physical security framework for Photovoltaic Farms. In *2020 IEEE CyberPELS (CyberPELS).* IEEE, Miami, FL, USA, 1–7. doi:10.1109/CyberPELS49534.2020.9311533

A Additional Figures

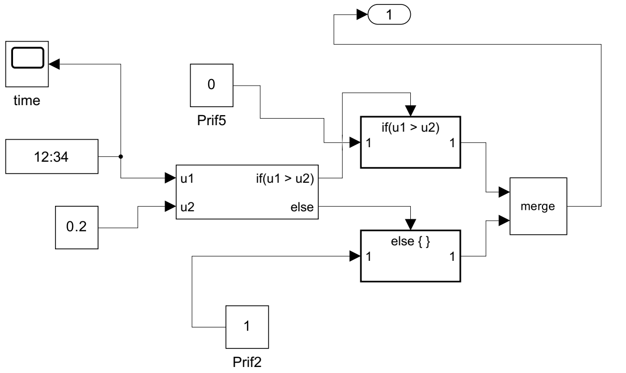

Figure 6: Simulink Component Implementing the Timing Attack.

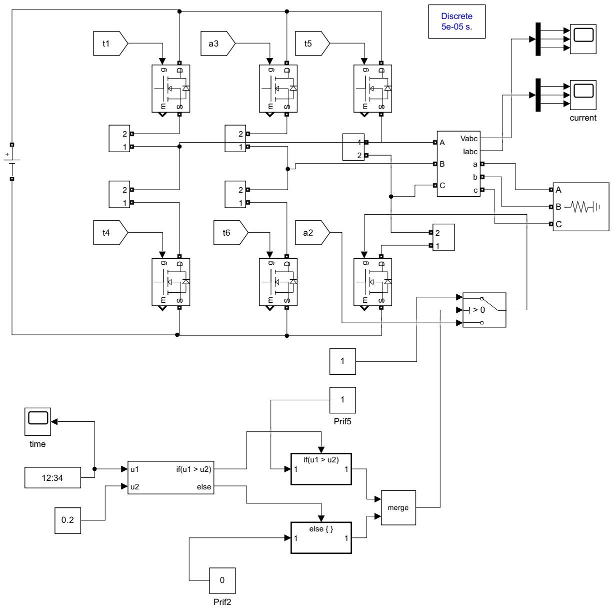

Figure 7: Simulink Implementation of the PWM Attack Integrated into the Inverter Model by Vijay [30].

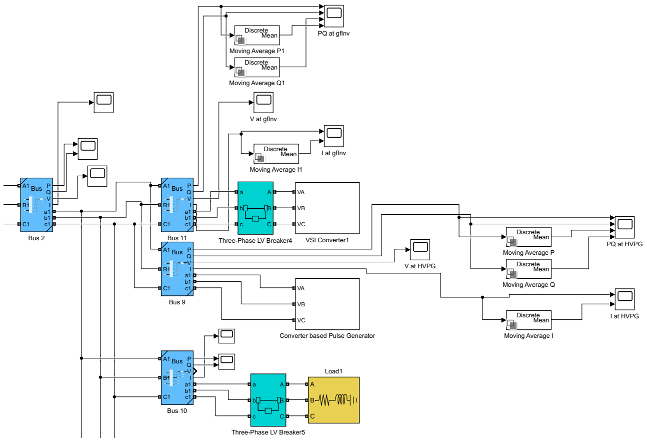

Figure 8: Simulink Diagram of the Grid Interconnection between Attacker Inverter (below) and Target Inverter (above) for the Phase-Locked Loop Attack Implementation.

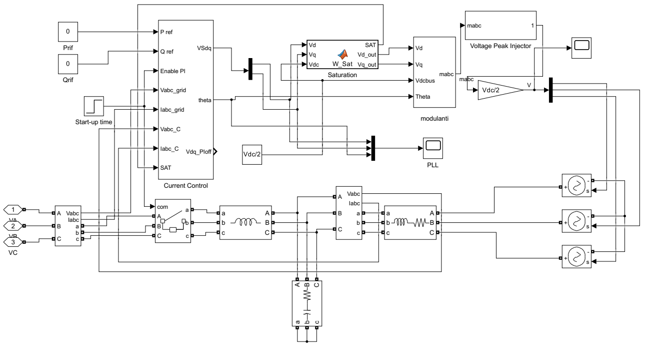

Figure 9: Simulink Diagram of the Attacking Inverter to Implement the Phase-Locked Loop Attack.

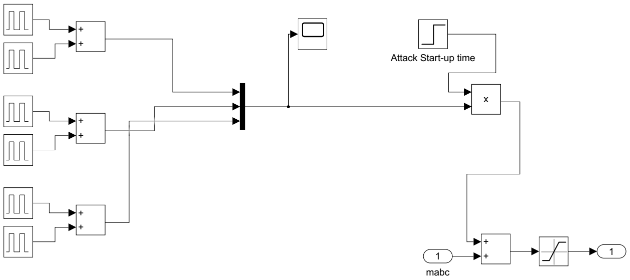

Figure 10: Simulink Diagram of the Voltage Peak Signal Generator.

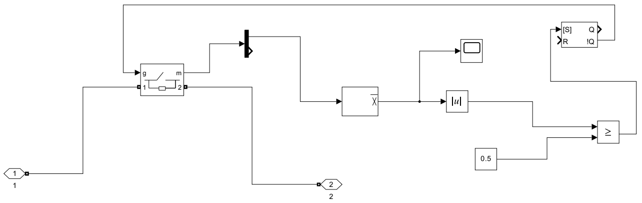

Figure 11: Pseudo-Fuse Model for Line Breakage Simulation.

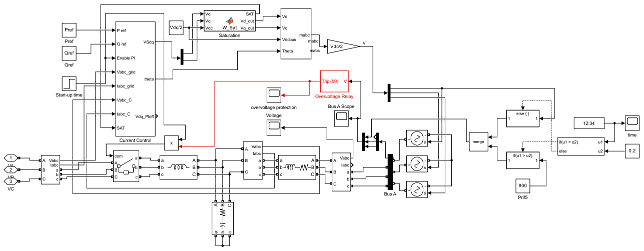

Figure 12: Simulink Diagram of the Over-Voltage Protection Attack Implementation.

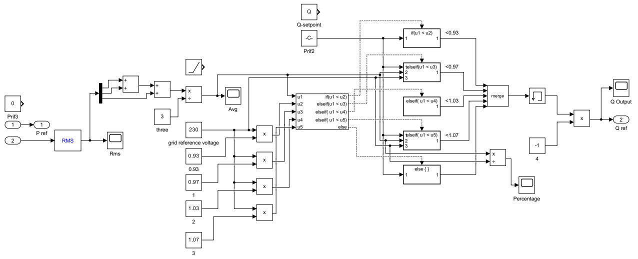

Figure 13: Implementation of the Volt-VAr Grid Support Function.

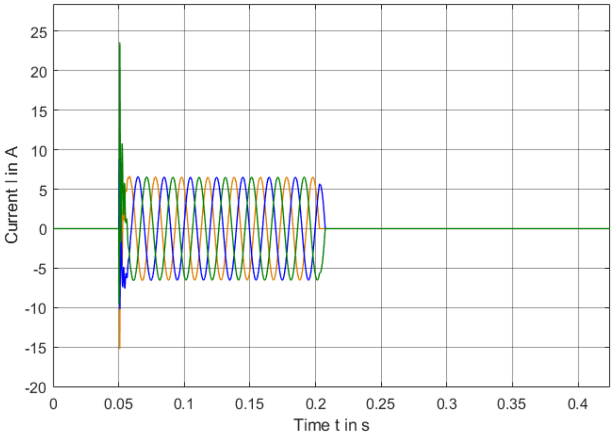

Figure 14: Current Profile of the Timing Attack Simulation.

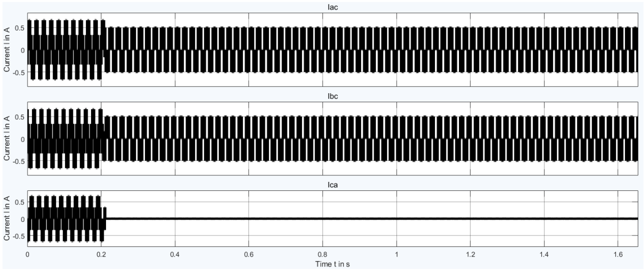

Figure 15: Current Profile During the PWM Attack Simulation.

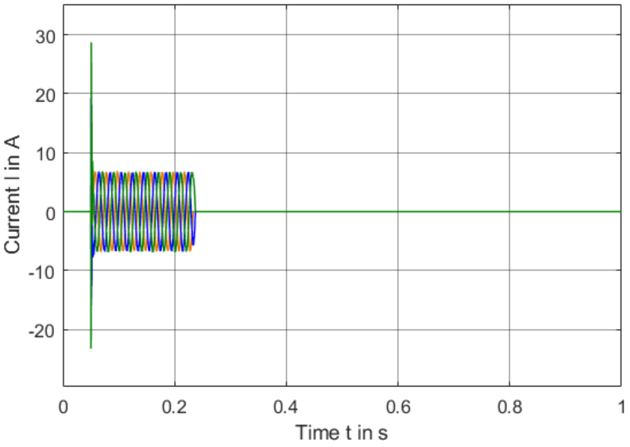

Figure 16: Current Profile During the Over-Current Protection Attack Simulation.

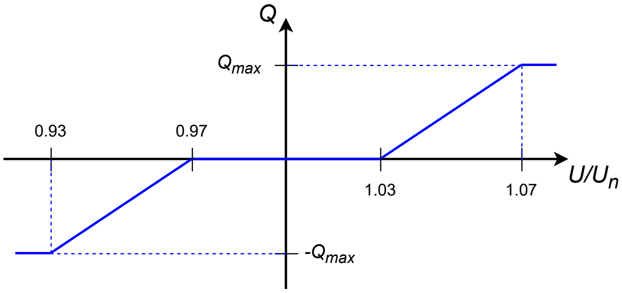

Figure 17: Volt-VAr Function in Attack Mode (Signs in Generator Convention). Figure based on [29].

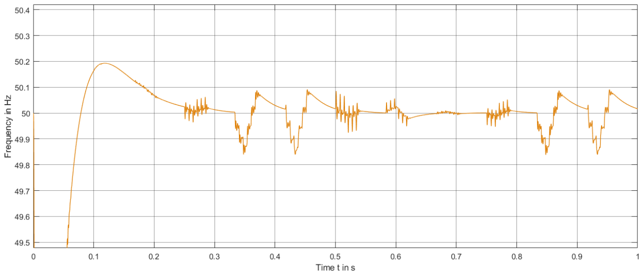

Figure 18: Detected Grid Frequency by the Phase-Locked Loop (PLL).

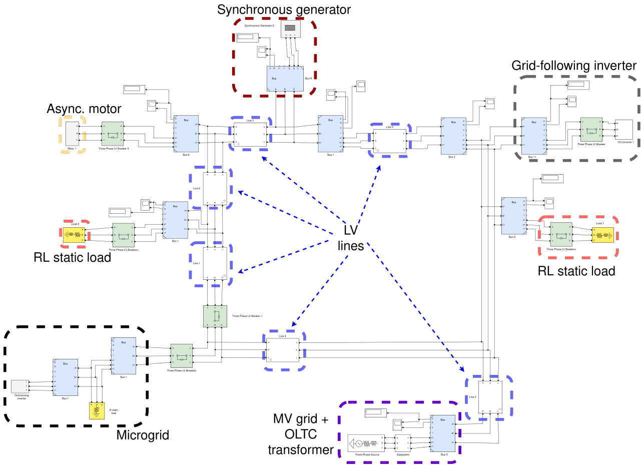

Figure 19: Low Voltage Grid Model based on De Paola et al. [6].