Smart Grid challenges - Device Trustworthiness*

André Waltoft-Olsen[1,2][0000−0003−3016−7824], Lasse Øverlier[2][0000−0002−7640−8446], Geir Olav Dyrkolbotn[2][], and Arvind Sharma[2][0000−0003−3467−9560]

[1] Statnett SF, Oslo, Norway
[2] Norwegian University of Science and Technology, Gjøvik, Norway

Abstract. The Power Grid development brings about technological design changes, resulting in increased connectivity and dependency on IoT devices. The changes offer opportunities to manipulate the IoT hardware as the root of trust. Although terrifying, hardware attacks are considered resource-demanding and rare. Nonetheless, Power Grids are attractive targets for resourceful attackers. As such, the Ukraine attacks boosted Power Grid cybersecurity focus. However, physical assurance and hardware device trustworthiness received less attention.
Overhead Line Sensors are utilized in Dynamic Line Rating doctrines for Power Grids. They are potentially essential in the future to optimize conductor ampacity. Conductor optimization is crucial for Power Grids because future throughput volatility demands a high level of grid flexibility. However, there may be challenges to the integrity and availability of the data collected using Overhead Line sensors. We believe that in securing the future Smart Grid, stakeholders need to raise attention to device trustworthiness entailing the hardware layer. That said, integrated into cloud-enhanced digital ecosystems, Overhead Line Sensors can also be manipulated through the network, software, and supply chain to impact their trustworthiness.

Keywords: Overhead Line Sensor · Hardware attacks · Smart Grid · Dynamic Line Rating

1 Introduction

Securing a digital system is a multilevel approach. Generally, the user interacts with a software-based Human Machine Interface (HMI). Then, the HMI sends its instructions to the hardware for digital circuit processing. From the user to the digital circuits there are inherent vulnerabilities that can be exploited as illustrated in Figure 1 from the 1979 Rand Report R609 [5]. Information leakage through radiation, crosstalk, and human factors are some of the inherent vulnerabilities. Attacks on a digital system may encompass a broad spectrum of attack vectors. We attempt to raise awareness of hardware security for several

* This work is made possible by the support of the Norwegian Research Council, Statnett SF, and The Norwegian University of Science and Technology

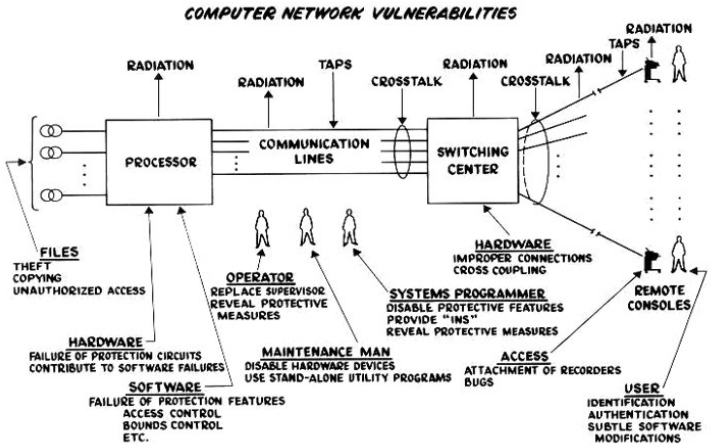

Fig. 1. Computer network vulnerabilities. Permission for reprint by Rand Corp. [5]

reasons. The hardware is a vital security foundation for any digital system. It is often considered the root of trust and an essential part of the trusted computing base. A generic software and hardware stack model is depicted in Figure 2 and illustrates how hardware may serve as the root of trust. Thus, hardware attacks can enhance software attacks by providing backdoor access. Hardware backdoor access may become even more attractive as digital systems are increasingly connected. In addition, connected cloud technology expands digital systems to achieve operational efficiency and business revenue. This hyper-connected situation offers increased possibilities to pivot from system to system. Pivoting is a well-known technique to compromise the weakest link and exploit the established trust between systems. Software attacks may exploit unpatched software or inject software trojans. However, software attacks can be remediated in-field through software support, while hardware manipulations may need hardware replacements for remediation [8]. We present some key terms that help discuss

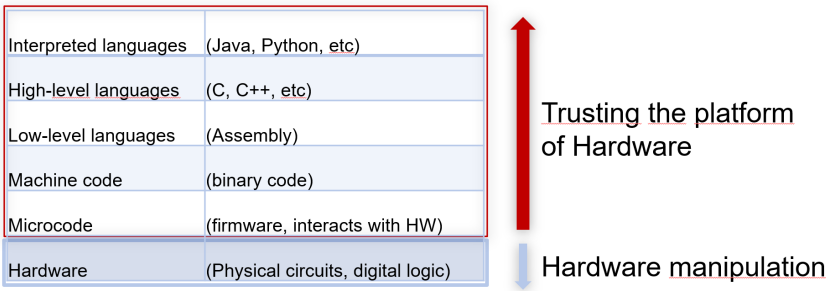

Fig. 2. Model of Software and Hardware Layers

cybersecurity challenges for our Overhead Line (OHL) sensor study. The *Power System* is a collective description of all the parts that produce power and transport it to the end consumer and entails the Power Grid. The *Power Grid*, or the Electrical Grid or Grid, has its primary function in interconnecting networks to deliver electricity from producers to consumers. Power Grids are complex networks in which power balance is essential. The Cleantech Group defines *Grid Flexibility* as "The capability of a Power System to maintain the balance between generation and load during uncertainty, resulting in increased Grid efficiency, resiliency, and the integration of variable renewables into the Grid." [18]. Grid flexibility is desirable because it helps the process of balancing the Grid. Opposite, The Green shift[22] and growing power-demand ramp-up Power Systems throughput volatility and complicates the Grid balance process. Volatility in power generation and consumption requires situational awareness and forecasting to maintain power balance. Therefore, Power Systems will evolve into connected Smart Grids, a concept aiming to enhance reliability, availability, and efficiency. OHL sensors used in Dynamic Line Rating (DLR) help Smart Grids to achieve their goal by providing data to optimize transmission line[3] use. Future Smart Grids will thus integrate and connect legacy systems, cloud services, and numerous sensor devices in a system of systems architecture. A concern is that Grid legacy systems are often designed as isolated systems and do not feature adequate cybersecurity defenses for Internet connectivity. Opposite, cloud services are designed to be accessible through the Internet. Furthermore, sensors like OHL Sensors are often bundled with cloud services to increase their value beyond local measurements. For example, sensor data can be sent to a vendor cloud storage, where customers are offered access and analytics to enrich sensor data for business revenue.

1.1 Problem formulation

Smart Grid development will bring about technological design changes in which attack possibilities increase. Malicious hardware manipulation in OHL sensor devices can cause untrustworthy DLR calculations and potentially impact Power Grid balance. An optimal situation for risk owners is to ensure trustworthy hardware by physical inspection. However, physical inspection requires access to specialized knowledge and costly test facilities. In addition, testing methods such as invasive structural reverse engineering[4] may damage expensive equipment. The complexity and cost of testing and the potential equipment damage appear unattractive. Nevertheless, from the perspective of cybersecurity teams and risk owners, the challenge is a lack of attention, discussion, and knowledge about how untrustworthy devices can impact business risk.

1.2 Contribution

The study explore challenges for untrustworthy devices related to OHL sensors and DLR in the Norwegian Power System. An OHL sensor serves as a study

[3] The word *Conductor* is also commonly used for the physical transmission line

case to describe potential security challenges and explore different hardware-related attacks. To the best of our knowledge, this is the first time Overhead Line sensor trustworthiness is discussed as a risk to DLR calculations impacting Grid balance. The main contribution of this paper is as follows:

- We provide a high-level perspective on the importance of DLR doctrines entailing Overhead Line sensors to balance the future Grid.
- We provide perspectives on how untrustworthy Overhead Line sensor devices used in DLR doctrines can impact Grid balance.
- We discuss cybersecurity challenges that can degrade trustworthiness in an Overhead Line sensor use case.

1.3 Organization

The following paper layout is as follows. In Section 2, we describe the motivation for Statnett SF (Statnett) as the Norwegian Transmission System Operator (TSO) to deploy OHL sensors as part of their DLR doctrine. In addition, we review some of the related work for Grid security. Section 3 describes our method and study approach. The findings and discussion of results are provided in Section 4. Lastly, in Section 5 is our conclusion.

2 Background

2.1 A Transmission System Operator perspective

Statnett, the Norwegian Transmission System Operator, manages the Norwegian Power Grid as a Critical Infrastructure (CI). Statnett works continuously to ensure that the Norwegian Power Grid operates within the laws of physics to avoid damage and critical service disruption of the power supply. Power generation and consumption are the basis for balance in any Power System. Therefore, balancing the Power System requires high accuracy to maintain Grid frequency at an optimal level. In addition, harsh weather, defective equipment, and other unwanted situations have unforeseen effects that need instantaneous actions to balance the Grid. For example, Statnett experienced numerous service outages due to unexpected ice loads on transmission lines. Breakdowns lead to costly and hazardous operations for restoration and contribute to Grid imbalance. Timely and relevant Grid data help mitigate safety hazards and Grid imbalance. Therefore, a DLR doctrine enhanced with sensor technology is desired to aid decision support for optimal Grid operation.

In Europe, the industry group European Network of Transmission System Operators for Electricity (ENTSO-E) considers the DLR methods and technology mature [23]. In addition, transmission utilities in Asia, Europe, North America, and South America have already included the deployment of DLR in their grid development roadmaps. DLR doctrines may deploy sensors mounted on the power lines or power masts for real-time data gathering. Two-way communication is established for data extraction and command and control. However,

our interpretation is that commercial-grade sensor devices may have security challenges due to limited space and a production philosophy to accommodate affordable prices. In addition, there is often a complex component and manufacturing supply chain [24], [9] where components are usually produced in multiple countries. Device parts are then shipped for assembly without a proper investigation for malicious or counterfeit content.

2.2 Power Grid Cybersecurity challenges

Modern digital systems are in a continuous state of change. They are expanded, altered, and integrated with other systems for the sake of optimization. Thus, the initial security posture is rapidly challenged when put into operation. As such, an essential activity is offensive security testing to assess the state of the system's security. Testing real-world security can map the delta between documented security and actual security. Even so, the Grid is a complex network entailing several interconnected devices supplied by different vendors. Furthermore, the networked devices communicate through various protocols and pose a challenge to measure/evaluate network security. Current tools to security test Grid networks are generally designed for smaller and more homogeneous networks [10]. In addition, offensive testing in operational Grid networks may cause critical failures as they are sensitive to disruptions. An alternative for live testing is simulations in virtual environments. Virtual environments offer flexibility, such as rapid environment resetting and no risk of disruptions. However, it requires extensive knowledge to program a virtual environment to simulate every effect during attacks. Emulating Grid substations using Hardware-in-the-Loop (HiL) offers some of the same flexibility and low risk as simulated setups. In addition, test results in a fit-for-purpose HiL provide high internal validity. Furthermore, real-world responses can be recorded and analyzed for knowledge purposes [1]. An important note is that establishing a HiL may require a broad spectrum of domain expertise and access to costly equipment to achieve high fidelity and desired validity.

The Grid has a tradition of isolating Operational Technology (OT) from other networks, such as the Internet. Thus, Power Grids and OT systems have experienced relatively few cyberattacks. However, Grid innovation and new technologies push Internet connectivity for OT systems. As a result, Internet connectivity offers added opportunities for cyberattacks. Acknowledging adversary tactics and techniques is essential to model network threats for mitigation. In 2013, Hoque et al.[3] provided a taxonomy for network-attack launching tools and information-gathering tools to help understand attack-tool purpose and behavior. Since then, the MITRE ATT&CK framework[19] has grown into a reputable tool for cybersecurity practitioners. The framework objective is to disseminate knowledge of past attacks to help assess cybersecurity risk and attack classification. For hardware, the framework details the attack technique *Hardware additions* where rogue devices are used to gain network-level access. Furthermore, *Compromise of Hardware Supply Chain* is added as an attack technique to obtain initial access propagated through hardware-backdoors. There are few

documented attacks where the physical hardware has been exploited. Thus, the framework does not cover the full spectrum of potential physical hardware attack techniques.

Today, the software is often an embedded part of modern digital devices. Software development is a multi-billionaire industry and poses an attractive target for attackers. Software development techniques have evolved from Waterfall to Agile to DevOps and continue to evolve. Likewise, advanced coding languages continuously evolve. It is important to acknowledge how attacks on software development can impact device trustworthiness. The software supply chain is a high-value target as it offers the attacker coverage and range in an attack. Ladisa et al. [20] propose a general taxonomy for attacks on open-source software supply chains. The taxonomy is independent of specific programming languages or ecosystems, covering all supply chain stages from code contributions to package distribution. Furthermore, the taxonomy is presented in an attack tree where the attacker's objective is to insert attack code in open-source projects. As a result, downstream users may execute malicious code or unwillingly include it as a library

In [11], Hutle and Kammerstetter investigate resilience against Physical Attacks related to Smart Grid hardware security. A description of various physical attacks is provided with relevant practical examples. In addition, they classify the attacker's purpose into two goals: a) Information gathering and b) Manipulating the device under attack. In a) an example is provided where an attacker compromises a smart meter and obtains firmware level code. Code can be reverse-engineered and used to shut down neighboring smart meters or for under-reporting power consumption for economic gain. For reverse engineering purposes, Konstantinou et al. [12] add that physical access or possession is needed to perform hardware layered information gathering attacks. The attacker can dismantle the device for reverse engineering purposes to deduce security features or steal intellectual property. In b) an IED is compromised. This could be a device entailing a circuit breaker. With this foothold, the attacker can attack other devices connected to the same field bus, such as actuators and sensors. Furthermore, the uplink to the Energy Management System (EMS), or Supervisory Control and Data Acquisition (SCADA), often use communication protocols that do not have or deploy built-in authentication, integrity, or confidentiality checks. Thus, the attacker can perform attacks on EMS/SCADA, leading to a loss of view and control for EMS/SCADA operators. Other hardware attacks can be for sabotage purposes, such as accelerated device aging or malfunctioning as a denial of service attack.

Kimani et al. [13] review cybersecurity challenges for IoT-based Smart Grid networks. The authors further provide a classification of smart grid attacks divided into devices, data, privacy, and networks related to the IoT domain. The paper discusses physical security to mitigate device tampering attacks. For example, countermeasures are remote wiping, device locking, and denial of physical access to the device to prevent unauthorized device tampering. Xie et al. [14] also discuss the denial of physical access as a security measure. They further investi-

gate how sabotage of substation equipment in coordinated physical attacks can cause outages for the US Power Grid. An interesting aspect is that Power Grid equipment is often installed at unmanned sites and perhaps in rural areas. Thus, the time for law enforcement to be on-site may exceed 20 minutes. The time it takes for the system operators to assess and understand that their equipment is under attack must be added to the time it takes for a proper response. Also, not all equipment is monitored, so instantaneous verification of physical attacks may not be possible. If the attacker carefully chooses her target, the time to perform attacks requiring physical proximity should be ample. However, the two articles do not discuss in-depth physical hardware attacks and how they may impact the Power Grid.

Rakas et al. [15] discuss cybersecurity challenges related to Dynamic Line Rating. A conclusion is that the sensor's GPRS Internet connection is its weakest link. Therefore, it is attractive for the attacker to breach the DLR sensors as a staging point for further attacks. Compromising the GPRS link can leverage attacks that can cause severe harm to the EMS/SCADA. VPN and SSL are some of the measures mentioned to counter GPRS attacks.

3 Method and study approach

For our study, an assumption is that the stakeholder has little to no guarantee for device trustworthiness. We discuss the attacker's possibilities to compromise device trustworthiness. We evaluate a limited subset of the Power Grid related to DLR and the OHL sensor, addressing potential attacks to degrade device trustworthiness.

To provide high-level perspectives on the importance of DLR doctrines and challenges related to untrustworthy OHL sensors, we performed an unstructured interview with two subject matter experts (SME) from Statnett SF and its ICEBOX project. One expert for DLR technologies and the other as a system architect expert for IT/OT. The ICEBOX project evaluates the optimal use of OHL sensors in Statnett's DLR doctrine. We also interviewed the Chief Executive Officer for Laki Power, a state-of-the-art manufacturer of OHL sensors for monitoring Transmission Systems. Statnett and Laki Power represent expertise given the challenges of malfunctioning OHL sensors in DLR calculations. In addition, the OHL challenges were discussed with the lead, and senior analyst, for RnD from the Norwegian Energy Cert, KraftCert. KraftCERT is part of the Norwegian sector response community and a member of the Forum of Incident Response and Security Teams (FIRST). KraftCert is the primary incident response body for the Norwegian energy sector. Their evaluation of the potential Grid impact provides value to the OHL sensor cybersecurity perspectives.

We interviewed the Hardware RnD manager for the ICEBOX internal logic to pursue an understanding of the design and functionality. A common situation is that multiple subcontractors are involved in designing and developing the product. Responsibility for built-in security can be spread among many stakeholders. Therefore, we pursued several subcontractors to gather as much information as

possible. Second, we searched open sources for additional information on the device. For example, we visited the web page for the System in Package (SiP) vendor, Nordic Semiconductor, and downloaded the available open documentation. A documentation study provided details and a model illustrating potential areas of interest for hardware attacks.

We performed a systematic physical investigation in a Hardware Reverse Engineering (HRE) workshop to better understand the ICEBOX device hardware architecture. We dismantled the sensor and identified components and areas of interest. In addition, we discussed and modeled potential attacks impacting device trustworthiness, referencing documentation and physical observations.

To discuss attacks on the ICEBOX sensor, we assume potential adversaries in:

a) The supply chain during assembly and shipment for hardware and code development for firmware and software
b) Third-party maintenance and upgrade actors
c) Adversaries that gain physical proximity, possession, or copy of the device and can launch physical hardware-related attacks
d) Cyberattacks that work in combination with hardware manipulation attacks

4 Results and Discussion

4.1 Motivation for Overhead Line Sensors

Laki Power defines three problem spaces for transmission lines that OHL sensors can contribute to counter. One relates to line sag, where sensors can verify actual sag based on local metrics. The second is the pollution on insulators which can result in flashovers. Methods such as resistance sensors and camera monitoring help measure and verify salinity and dust on the insulators. Lastly, wildfires pose severe threats to CI owners and local settlements.

OHL sensors contribute with real-time data, while historical data provide baselines for transmission corridors. Typically, data harvested from OHL sensors are complimented with weather forecasting before sending it to the Energy Management System (EMS), as illustrated in Figure 3. However, OHL sensors are not mandatory for DLR calculations. Grids in Finland and Denmark utilize static values to calculate transmission line limitations. A drawback is that the fixed limits cannot consider all the local conditions, such as unforeseen weather changes. Indirect methods, or non-contact technologies, calculate limits based on weather data from meteorological models, forecasting and line load. However, contact technologies such as sensors provide real-time data to help continuously optimize transmission line utilization and maximize lifetime. Sensors can provide important measurement data such as conductor temperature, conductor sag through tension, vibration frequency, and angle of the transmission line at the span points[4]. Laki Power and Statnett suggest that drawing upon both indirect

[4] Span point is the support where the conductor is attached

and direct calculation methods gives the best DLR optimization. A primary concern for data used in DLR calculations is sensor and weather forecasting data integrity. Denied availability of sensor- data, systems and infrastructures may reduce optimization drastically.

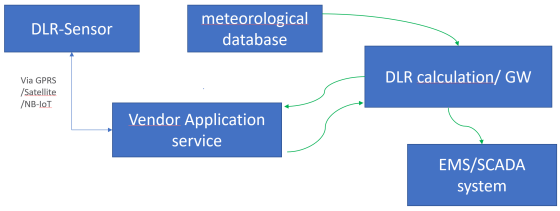

Fig. 3. Illustration of OHL sensor providing data to the Energy Management System

Laki Power further explains that adding renewable energy sources to the Power Grid presents challenges that sensors in DLR doctrines can help solve. A motivation for renewable energy is to replace carbonized energy. However, renewables such as solar and wind have fixed geographical placements dictated by optimal harvesting conditions. Typically, this is in rural areas, while most consumers are in cities. Moreover, solar and wind are instantaneous and add volatility to the Grid. A result is that renewables, combined with growth in power demand, increase power transportation. In sum, it requires the strengthening and expansion of Grids. Grid infrastructure build-ups are expensive and take time. Thus, it makes sense to enhance DLR doctrines with sensors to optimize Grid infrastructure for power transportation.

OHL sensors are expected to have a significant role in Smart Grids. Moreover, increased Machine-to-Machine (M2M) communications enable ubiquitous connectivity and often communicate autonomously without human intervention. M2M communication contributes to swift decisions in automation processes and is helpful when time constraints are essential. Despite the positive effects, Laki Power and Statnett underline that OHL sensor data integrity is critical for accurate DLR calculations. And depending on how DLR is implemented, the consequences for corrupt data may vary. For example, corrupt data related to a specific transmission corridor may break down that single transmission line. However, a worst-case scenario is multiple breakdowns potentially causing cascading failures in the Grid.

Looking at Figure 3, we assume potential attacks entailing compromise of the DLR-sensor (OHL), Vendor Application Services, meteorological data, or even the DLR calculation/GW. Manipulating data input to the DLR calculation/GW could lead to erroneous DLR calculation and interpretation of transmission line limits leading to possible breakdowns. The same result could be achieved by manipulating the DLR calculation/GW output to the EMS.

4.2 Analysis of The ICEBOX load sensor

The physical location of OHL sensors is either at the power masts or on the conductor. Sensors mounted on conductors can harvest power using methods such as Laki Power's PowerGrab. While PowerGrab harvests power from the conductor, the ICEBOX sensor is mounted at the power mast and has its own power source. A strain gauge is fitted in the middle-lower part of the sensor body 4. Load on the conductor results in a stretch of the sensor body. The strain gauge registers this movement and sends a voltage signal to the internal digital logic. Apart from the antenna, the ICEBOX sensor internals is encased in a metal/alloy housing. The power source is 2 LSH 20 batteries providing 3,6V each and 13000mAh total. The batteries are expected to last ten years of operational service.

Fig. 4. The ICEBOX Line Sensor strain gauge.

A block diagram in Figure 6 depicts the internal nRf9160 PCB[5]. The board hosts an LTE-M/NB-IoT modem with an integrated Radio Frequency Front-End (RFFE) for communication. The application processor is a 64 MHz Arm Cortex-M33 CPU with Arm TrustZone for trusted execution. An Arm CryptoCell 310 is provided for accelerated cryptography. The microcontroller interface entails several general-purpose input-output (GPIOs) signals routed through analog switches for utilizing the onboard functionality of the electronics board. These interfaces include switches for Universal Asynchronous Receiver-Transmitter (UART), external memory card, SIM card, RF control, etc. A regulated power supply circuit provides stable power to different board components. External sensors can be connected through analog switches to the microcontroller for measuring and monitoring various parameters. The board houses two antenna interfaces mounted, represented as LTE and GPS. To support global navigation, a dedicated GPS port is used. The GPS signal is amplified and filtered in the LNA that has integrated pre-filter and post-filter before it is fed to the microcontroller. The LTE antenna is optimized for global operation, supporting all LTE frequency bands in the region of 698–960 MHz and 1710– 2200 Mhz. The designed circuit of the line sensor supports both regular and embedded SIM (eSIM). The standard SIM has a pluggable SIM card socket that can fit a nano-sized SIM (4FF); however, a non-populated footprint is given for an eSIM purpose. External memory can be connected to the microcontroller using the Serial Peripheral Interface (SPI) interface. An external debugger can access the device via the debug input port connected to the main board for microcontroller programming.

4.3 Network and Software attacks

Network and software attacks can compromise the device's trustworthiness by manipulating data confidentiality, integrity, and availability. OHL sensors are of-

[5] The nRf9160 IoT System-In-Package is manufactured at Nordic Semiconductor

ten designed to communicate out of band. For example, Lindsey Systems' next generation DLR system named SMARTLINE-TCF entail the TLM monitors (sensor device) fitted with a satellite radio with all data being passed directly to the Lindsey SMARTLINE Cloud server. The benefit is that the TLM monitors can be located in the most remote locations. Since a connection externally to the cloud is already established, cloud computing can correlate and analyze the bulk of sensor and weather data. In addition, other data sources can be added to enhance the DLR calculations to improve situational awareness. However, external data in storage or transit must be trustworthy. As such, data integrity, availability, and confidentiality for external cloud services are challenging to assure compared to locked-down on-premises solutions. For example, an attack on the meteorological database can compromise the integrity of the DLR calculation and degrade DLR trustworthiness [2]. On the other hand, in-house systems to correlate and analyze numerous data sources and large amounts of data require costly infrastructure, expertise, maintenance, and operational costs. Thus, cloud computing may provide economic gain and enhanced business for the CI stakeholder. Lastly, an important note is the Smart Grid concept, whose essential ability is bi-directional data flow. The degree of network isolation one can maintain for Smart Grids is thus an open question. As such, Hoque et al. presented a list of network attack tools [3]. We extract three objectives for network attacks on OHL sensors:

- Recon: active and passive discovery to enumerate the network, devices, and their responses to deduce weaknesses. The results can be used to exploit vulnerabilities and gain a foothold as a staging point for further attacks.
- Access: compromise and pivot the network to gain access to data and infrastructure/system communicating with the sensor device.
- Denial of Service: deny access to sensor data or systems.

We extract from Ladisa et al. [20] potential attacks on software and its supply chain. Attacks may have the goal of gaining a foothold in the sensor by:

- Attacking software: Missed updates and patching, third-party libraries.
- Injecting malicious code to trusted (signed) parties such as vendor and developer: build and update infrastructures, stolen developer certificates.
- Injecting specialized hardware-near software such as Firmware: Preinstalled malware on devices.

4.4 Supply Chain attacks

Hutle and Kammerstetter[11] investigated resilience against Physical Attacks related to Smart Grid hardware security. Our understanding is that the attacker needs physical proximity for physical hardware attacks. Physical access enables the attacker to interact directly with the device. For example, it is not unusual for devices to provide a physical maintenance interface that offers direct access to the security configuration. However, in the smart meter case, physical access is easier obtained than for an OHL sensor. In addition, due to safety reasons,

physical security is high for Power Grid infrastructure. As such, physical security strengthens overall cybersecurity and helps prevent physical proximity for the attacker. However, detection and timely response to physical attacks at remote locations remains a challenge.

Despite strong Grid physical security, devices such as OHL sensors are still subject to supply chain attacks. For example, semiconductor Hardware trojans (HT) are pre-silicon malicious hardware manipulations inserted during design and manufacturing. Consequently, the HT becomes an integral part of the device. HTs are hard to detect for the CI owner due to their stealthy nature. An HT typically contains two parts: trigger and payload [6] that are hidden in the semiconductor. Debugging and careful inspection of the code may detect software trojans for software. However, to reveal dormant HTs pose challenges as their footprint is hard to discover under normal operation and functional testing [8]. Pre-silicon insertion of HTs requires a capable and motivated attacker to compromise the design or manufacturing process. However, HTs may also be inserted during assembly, shipment, maintenance, or by a malicious insider as a post-assembly attack. An example is to manipulate the Bill of Materials (BOM) for assembly. In a BOM swap, the attacker can insert malicious components into the assembly before the product is shipped to the customer. Xiao et al.[16] provided us with a model to visualize the semiconductor supply chain flow from designing the Specification to the Market. We enhanced the model with two additions 1) The Stage the attacker chooses to launch the attack divided into the Pre-Assembly or Post-Assembly stage. 2) The parts of the supply chain the Trojan implementation strategy entail. We divided this into a Seeding and Interdiction strategy. Seeding is the act of embedding the HT as part of the device before it is sent to the Market or the customer. Interdiction is the targeted strategy to interdict shipments for malicious manipulation before it reaches the customer.

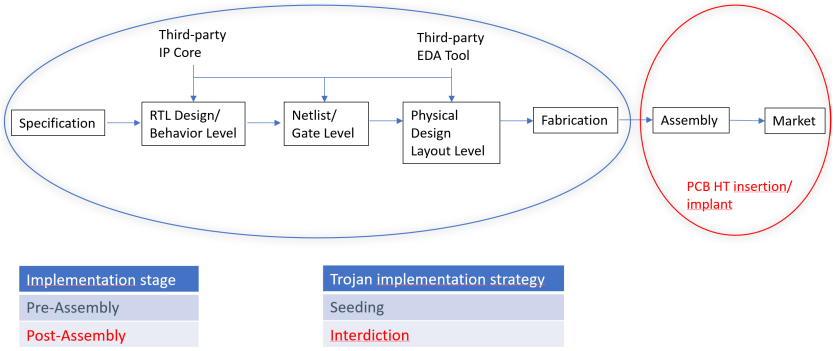

Fig. 5. Semiconductor supply chain by Xiao et al.[16] enhanced with two additions

Software supply chain attacks are not illustrated in the augmented block diagram in Figure 6. However, such attacks can insert malicious backdoor access into the device firmware or software. For example, the ICEBOX firmware can be updated remotely. Thus, an attacker can load the ICEBOX with backdoor-enabled firmware. Consequently, the OHL sensor is untrustworthy and a tool to manipulate the DLR calculations to impact Grid balance. In addition, compromising any other third-party software supply chain, such as cloud services, are viable for degrading the ICEBOX's trustworthiness. Subsequently, the vendor application service and DLR calculation gateway in Figure 3 provide opportunities to inject malicious software and firmware. As a result, both integrity and availability of the sensor's upstream data can be manipulated, resulting in erroneous DLR calculations, potential conductor breakdown, and Grid imbalance.

4.5 Physical hardware attacks

According to Skorobogatov [17], physical hardware attacks are classified into three levels depending upon the physical interaction with the device. 1) Invasive: Micro-probing, Reverse Engineering. 2) Semi-invasive: UV-light exposure, Optical fault injection, Advanced Imaging, Optical Side-Channel. 3) Non-invasive: Side Channel attacks, Fault injection. To launch physical hardware attacks, the attacker must possess the device or be in proximity, bypass any tamper security measures and mount the attack. The goal can be device secret information leakage, denial of service, or even age acceleration. In the previous section, different components of the ICEBOX sensor are described in terms of functionality and application. Thus, we enhanced the block diagram in Figure 6 to also illustrate potential hardware attacks:

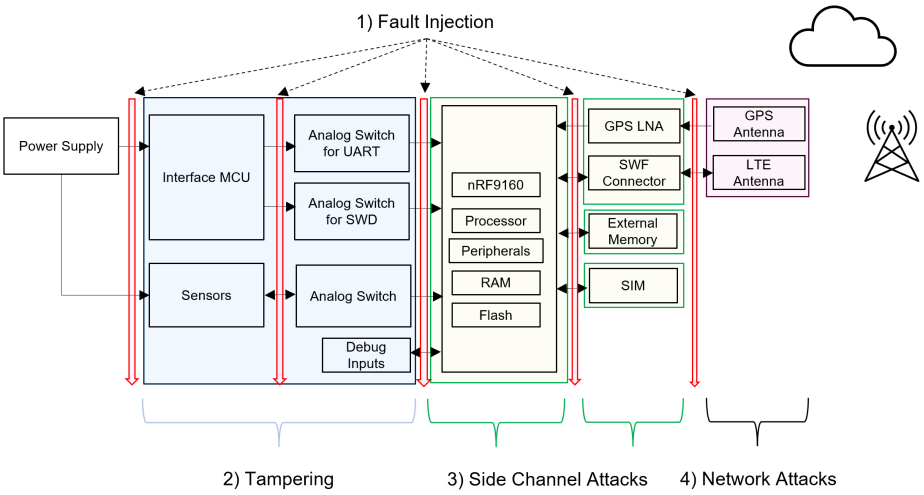

Fig. 6. Potential hardware attacks

1) Fault injection attacks: Fault injections tamper with the device to induce faulty behavior, cryptanalysis, and bypass security features. Timed power glitch attacks can make the device skip specific instructions, bypassing security features. As we can see from the augmented block diagram 6, voltage glitching can be inserted between the power supply and the sensors to induce malfunctioning. Voltage glitching can also target the processor for cryptanalysis. Furthermore, voltage glitching targeting the modem and RFFE can potentially cause a sensor denial of service situation.

2) Tampering: Here we discuss some potential tamper attacks that replace or add malicious hardware. As such, reverse engineering helps the attacker to understand device functionalities and vulnerabilities. The Gerber file is an open ASCII vector format for PCB designs. The Gerber file for the ICEBOX sensor is openly available, which helps deduce areas of interest for further hardware attacks or counterfeiting. Counterfeit products with embedded malicious manipulation can be used in the interdiction of product shipment or targeted attacks on the maintenance supplier. Furthermore, tampering with the voltage signal for the ICEBOX strain gauge might corrupt the integrity of tension measurements of the line sag. Since the ICEBOX sensor carries its power source, tampering with the device's power usage can accelerate power depletion and incur maintenance costs for the CI owner.

3) Side Channel Attacks: Side Channel Attacks harvest the information gained from the hardware implementation. The electronic circuits carry sensitive data stored in one of the memory locations in the microcontroller. This information includes sensor measurements communicated to the local server through the LTE network during real-time operation. If an attacker has physical access to the device, it is vulnerable to physical attacks in the form of side-channel leakage. A side-channel leakage can be observed in several ways, such as by measuring the physical characteristics (e.g., power dissipation, electromagnetic radiation, signal delays, transient current leakage, noise, etc.) to deduce secret encryption keys.

4) Network attacks: The nRF9160 PCB board has three antenna interfaces mounted representing LTE, GPS, and the 2.4 GHz radio. Although not a hardware attack, attacks such as jamming could deny the availability of the device. By blocking radio signals, the CI owner would need to deploy service teams to investigate. For the EMS/SCADA operators to comprehend the situation, deploying service teams and deducing that they suffer a jamming attack would take considerable time. Jamming a single transmission corridor may not be devastating for the Grid. However, enduring jamming of multiple transmission corridors to connect regions may pose severe implications for the Grid. Furthermore, but not related to the ICEBOX sensor, GPS signals are sometimes used to measure line sag. An attacker can jam or spoof GPS signals to corrupt line sag measurement data.

5 Conclusion and Future Work

This study described some of the Power Grid's challenges in integrating renewables and meeting growing power demand. We provide expert perspectives on the outlook for OHL sensors and their importance for DLR doctrines. Sensors will significantly contribute to real-time data for DLR calculations in future Smart Grids. Thus, sensor-data integrity and availability are essential for the doctrine. In an analysis of the ICEBOX load sensor, we investigated potential attacks that can manipulate data confidentiality, integrity, and availability. Consequently, physical hardware attacks require physical proximity. However, physical security for Grid infrastructure is high due to strict safety requirements. Regardless, supply chain attacks appear as a threat challenging to counter for the risk owner. It is challenging because the physical assurance of device trustworthiness requires access to highly specialized knowledge and testing infrastructures.

We acknowledge that executing our described attacks would raise the value of our work. In future work, we aim to investigate hardware attacks on OHL sensors and hope to experiment using a capable hardware reverse engineering lab. Although unable to perform attacks, we hope our work has contributed to a better understanding of the attackers' arsenal for attacking future Smart Grids.

References

1. Jørgensen, P., Waltoft-Olsen, A., Houmb, S. H., Toppe, A. L., Soltvedt, T. G., Muggerud, H. K.: Building a Hardware-in-the-Loop (HiL) Digital Energy Station Infrastructure for Cyber Operation Resiliency Testing. 2022 IEEE/ACM 3rd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS), 9–16 (2022)
2. Ahmadi, A., Mojtaba, N., Behnam, M., Vahid, V.: Ensemble learning-based dynamic line rating forecasting under cyberattacks. In: IEEE Transactions on Power Delivery 37, **no. 1**, 230-238 (2021).
3. Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., Kalita, J. K.: Network attacks: Taxonomy, tools and systems. Journal of Network and Computer Applications **40**, 307–324 (2014)
4. Asadizanjani, N., Rahman, M. T., Tehranipoor, M.: Physical Assurance: For Electronic Devices and Systems. Springer International Publishing, Cham (2021)
5. Ware, W.: Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security. RAND Corporation (1979)
6. Vosatka, J.: Introduction to hardware trojans. In: The Hardware Trojan War, pp. 15-51. Springer, Cham, 2018. https://doi.org/10.1007/978-3-319-68511-3_2
7. Becker, G. T., Regazzoni, F., Paar, C., Burleson, W. P.: Stealthy dopant-level hardware trojans. In: International Conference on Cryptographic Hardware and Embedded Systems, pp. 197-214. Springer, Berlin, Heidelberg, (2013). https://doi.org/10.1007/978-3-642-40349-1_12
8. Bhunia, S., Hsiao, M. S., Banga, M., Narasimhan, S.: Hardware Trojan Attacks: Threat Analysis and Countermeasures. In Proceedings of the IEEE, vol. 102, no. 8, pp. 1229-1247. Aug. (2014). https://doi.org/10.1109/JPROC.2014.2334493

9. Gurunath, R., Agarwal, M., Nandi, A., Samanta, D.: Security Issue in IoT Network. In: 2018 2nd International Conference on 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), pp. 104–107. IEEE (2018). https://doi.org/10.1109/I-SMAC.2018.8653728
10. Atalay, M., Angin, P.: A digital twins approach to smart grid security testing and standardization. In 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT, pp. 435–440. IEEE (2020).
11. Hutle, M., Kammerstetter, M.: Resilience Against Physical Attacks. In: Smart Grid Security, pp. 79–112, Syngress (2015). https://doi.org/10.1016/B978-0-12-802122-4.00004-3
12. Konstantinou, C., Maniatakos, M.: Hardware-layer intelligence collection for smart grid embedded systems. In: Journal of Hardware and Systems Security 3, no. 2 (2019), pp. 132–146.
13. Kimani, K., Oduol, V., Langat, K.: Cyber security challenges for IoT-based smart grid networks. In: International Journal of Critical Infrastructure Protection 25 (2019), pp. 36–49. https://doi.org/10.1016/j.ijcip.2019.01.001
14. Xie, J., Stefanov, A., Liu, C.: Physical and Cybersecurity in a Smart Grid Environment. In: Advances in Energy Systems: The Large-scale Renewable Energy Integration Challenge (2019), pp. 85-109. https://doi.org/10.1002/wene.202
15. Rakas, S. B., Timcenko, V., Kabovic, M., Kabovic, A.: Cyber security issues in conductor temperature and meteorological measurement based DLR system. In: Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion (MedPower 2016), pp. 1–7. IET, 2016. https://doi.org/10.1049/cp.2016.1107
16. Xiao, K., Domenic F., Jin, Y., Ramesh, K., Swarup, B., Tehranipoor, M.: Hardware trojans: Lessons learned after one decade of research. In: ACM Transactions on Design Automation of Electronic Systems (TODAES) 22, no. 1. ACM (2016): 1–23. https://doi.org/10.1145/2906147
17. Skorobogatov, S.: Physical attacks and tamper resistance. In: Introduction to Hardware Security and Trust, Tehranipoor, M. and Wang, C., pp. 143–173. Springer, New York, NY, (2012). https://doi.org/10.1007/978-1-4419-8080-9_7
18. Cleantech Group, https://www.cleantech.com/smart-grid-flexibility-markets-entering-an-era-of-localization/. Last accessed Oct 2022
19. MITRE ATT&CK®, https://attack.mitre.org/. Last accessed 9 Oct 2022
20. arXiv:2204.04008 [cs], http://arxiv.org/abs/2204.04008. Last accessed Apr 2022
21. Qualcomm, https://developer.qualcomm.com/blog/hardware-software-convergence-developer-s-viewpoint. Last accessed Apr 2022
22. European Commission, https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal/energy-and-green-deal_en. Last accessed Apr 2022
23. ENTSO-E. https://www.entsoe.eu/Technopedia/techsheets/dynamic-line-rating-dlr. Last accessed Apr 2022
24. Automation World. https://www.automationworld.com/products/data/article/13320007/battle-for-cybersecurity-spreads-to-sensors. Last accessed Jul 2022