Final Scientific/Technical Report

GRIDTRUST: ELECTRICITY GRID ROOT-OF-TRUST DECENTRALIZED SUPPLY CHAIN CYBER-SECURITY

WORK PERFORMED UNDER AGREEMENT

DE-CR0000004

Georgia Tech Research Corporation

P.O. Box 100117

Atlanta, GA, 303840117

Award Period of Performance: 08/05/2020 **to** 08/04/2023

Submitted: 08/24/2023

PRINCIPAL INVESTIGATOR

Prof. Santiago Grijalva

Georgia Institute of Technology

404-894-2974, sgrijalva@ece.gtatech.edu

TEAM MEMBERS

Georgia Institute of Technology, Atlanta, GA

Sandia National Laboratory, Albuquerque, NM

Southern Company, Birmingham, AL

City of Marietta, Marietta, GA

Protect Our Power Institute, Chappaqua NY

SPONSORING PROGRAM OFFICE

U. S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Via the National Energy Technology Laboratory

Acknowledgment

This material is based upon work supported by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) under the Cybersecurity for Energy Delivery Systems (CEDS) Program and Agreement Number DE-CR0000004 to the Georgia Tech Research Corporation.

Disclaimer

TABLE OF CONTENTS

1.1 LIST OF TABLES

1.2 LIST OF FIGURES

1.3 LIST OF ACRONYMS AND ABBREVIATIONS

AES: Advanced Encryption Standard
APT: Advanced Persistent Threat
CA: Certificate Authority
CN: Communication Network
IED: Intelligent Electronic Device
NOS: Network Operations Center
OS: Operating System
OT: Operational Technology
PUF: Physical Unclonable Function
RoT: Root-of-Trust
RSA: Rivest Shamir Adelman
RTU: Remote Terminal Unit
SCADA: Supervisory Control And Data Acquisition
SHA: Secure Hash Algorithm
TLS: Transaction Layer Security

2 Executive Summary

GridTrust represents a departure from reliance on a single organization or a single person to multiple organizations and therefore multiple people across organizational structures. The motivating idea behind involving multiple organizations is the increase in security due to human factors. More specifically, the requirement that distinct people in different organizations sign off on a change or an update makes a cyberattack much less likely due to the inherent requirement that both organizations be penetrated and fooled.

GridTrust focuses on the software update process as the primary exemplar for the research and development work. A novel hardware-based technology referred to as a Physical Unclonable Function (PUF) provides a microchip Root-of-Trust (RoT), i.e., a starting point for verifying that the hardware being communicated with is the hardware the control center believes the hardware to be. As a result, staff at power grid control centers can ensure the accurate and reliable identification of hardware devices from the outset.

The GridTrust protocol introduces two key innovations, as detailed in this report. Firstly, the utilization of a PUF as a root-of-trust in the initial phase of a software or firmware update. Secondly, the application of multiple cryptographic signatures from two or more organizations to the update binary. These signatures are verified before implementing the update on a power grid device in the field.

In terms of GridTrust hardware design, this report outlines two main components. The first is the GridTrust Native Device, integrating PUF technology intrinsically into the hardware device itself. The second is the GridTrust Interfacing Device, which incorporates PUF technology and multiple cryptographic signatures. These signatures are cross-checked within a separate hardware positioned between the power grid control center and the legacy power grid device, functioning as an intermediary. While the GridTrust Interfacing Device offers the advantage of being applicable to existing power grid equipment, it may have reduced security if the intermediary component is targeted. On the other hand, the GridTrust Native Device boasts increased security due to protocol integration within a unified form factor.

The effectiveness of GridTrust technology has been extensively demonstrated, with multiple external red-team attackers unable to breach GridTrust's security measures. This was observed both in controlled laboratory settings during Phase 1 of the project and in real-world conditions within a City of Marietta substation during Phase 2 of the project.

3 Objectives

The overall aim of the project was to innovate the architecture and environment needed for the development of GridTrust Technology. The architectural work consists of (a) stakeholder identification, (b) specification of terminology, (c) development of use cases, (d) development of a decentralized framework, (e) power system supply chain cyber-attack surface, (f) GridTrust Box design, (g) PUF-based security protocols and (h) development of a power grid simulator. We describe these architectural elements below.

3.1 Stakeholders

The following stakeholders were identified as critical for the design and development of GridTrust technology. The stakeholder roles and relationships were established and documented:

- Electric Utility
  - Operations Division
  - IT/Cyber-Security Division
  - Supply-Chain/Procurement Division
- Control Device Provider
- Customers
- Regulators

3.2 Terminology

The architectural elements need to be defined formally. The following terms were utilized:

- Grid Device:
  - A device at the substation (e.g., an RTU, PMU or temperature sensor).
  - There are two types, which are control devices (e.g., RTUs) and power devices (e.g., sensors)
- Compute Device:
  - A device with computing capability
- GridTrust Native Device:
  - A grid device installed with GridTrust technology
- GridTrust Interfacing Device:
  - A compute device installed with GridTrust technology that interfaces with an existing grid device
- Software Update:
  - Either source code, binary, or both
  - Grid device firmware
  - Grid device's list of user credentials

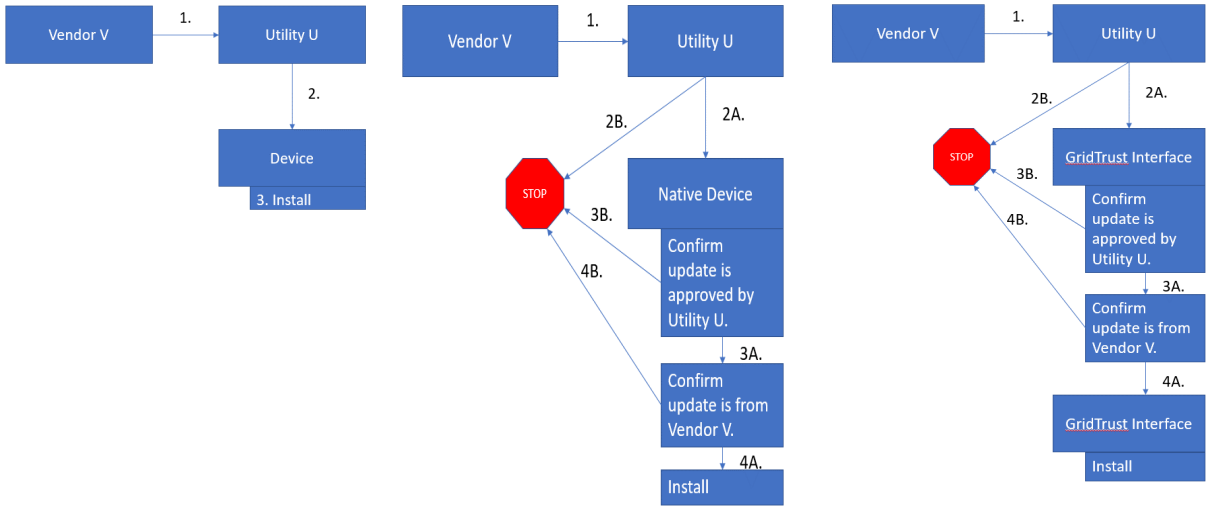
3.3 Use Cases

The main type of use case identified for grid supply chain cyber-security was software and hardware updates of control devices in the field.

There are three core use cases:

a) Business as Usual Software Update,
b) Software or Hardware Update to a Native GridTrust Device,
c) Software or Hardware Update to an Interfacing GridTrust Device.

These use cases are illustrated in
Figure 1.



a) Business as Usual b) Native Device c) Interfacing Device

Figure 1. GridTrust Base Use Cases for Field Software Update

The identified use cases have the following set of assumptions associated with their cyber module. The cyber-module relates to communication systems, security data management, and security key distribution.

- Key Distribution:
  - Upon power grid device installation, a database containing all necessary keys is generated.
  - The database is maintained by the utility **except** for vendor private asymmetric keys which are only maintained by the vendor.
- Database:
  - Option 1: A trusted third party can be introduced to host the database that the vendor and utility have access; however, private asymmetric keys should **only** be held by the utility or vendor.
  - Option 2: The database is maintained by the utility.
- Communication System
  - Loopback communication, which can be compatible with firewall and intrusion detection.
  - Vendors have access to the power system's closed-loop communication network.

- There may be security risks if network packets are not encrypted.

A graph representation of the use cases is conceptualized in Figure 2, which shows various grid supply chain cyber-security actors and the expected flow of information.

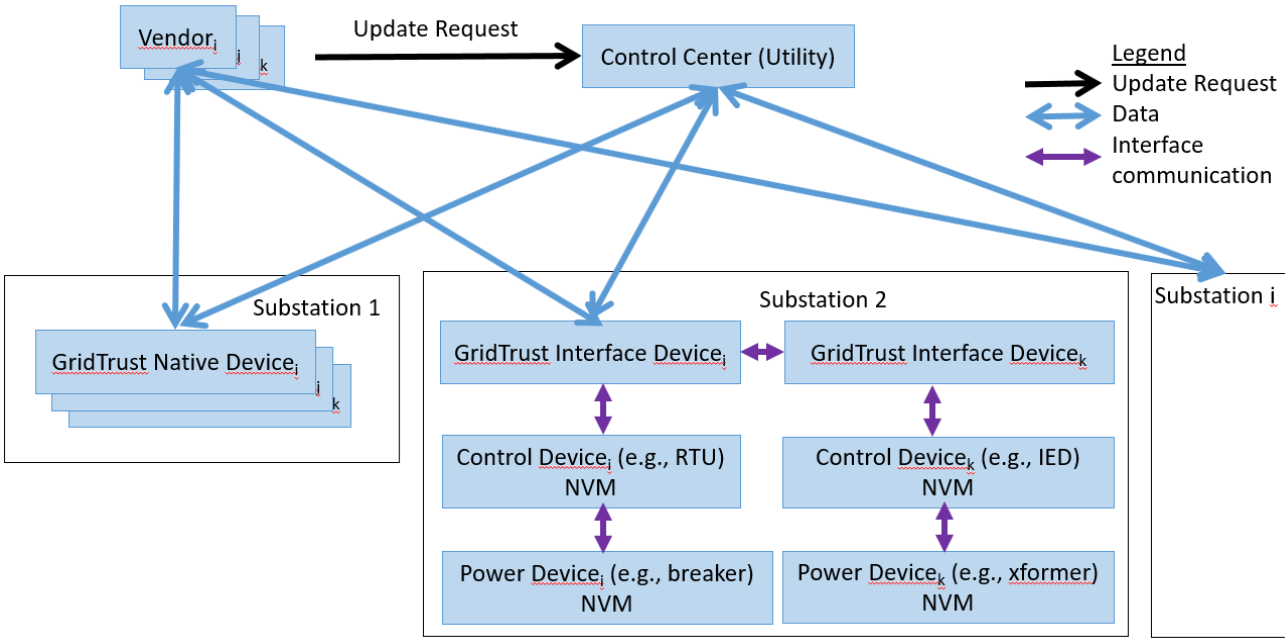


Figure 2. Flow of Information and Interaction for Use Cases

3.4 Decentralized Framework

Any framework for grid supply chain cyber-security must consider the decentralized nature of cyber-security decisions. We consider the actors such as the Utility, the Vendor, and Control Devices, and the decision-making processes associated with supply chain and their cyber security. Supply chain security traditionally requires secure custody throughout the chain, which may include multiple hops. Since this security is typically implemented through software, it is then exposed to all the potential attacks to software including all attack surfaces due to communication networks and the internet. The PUF technology proposed as part of GridTrust can drastically increase the security, since it can provide Root-of-Trust at the hardware level, locally, anywhere in the chain.

The team conducted a literature review at three levels: a) broad concerns of supply chain cyber-security, b) supply chain cyber-security of critical infrastructure, and c) supply chain cyber-security specific to the electric power grid. With inputs from Protect Our Power and Sandia National Laboratories, the team researched overall US policy regarding power system cyber-security focusing on the supply chain. We considered uses cases associated with software updates and a lone wolf insider. Table 1 below summarizes the attack surface for power system supply chain cyber-attack.

Table 1. Attack Surfaces

Attack Surfaces	Affected Area	Potential Outcomes
Network	• Equipment, controllers, software, and systems within OT and IT environments, • ICS Protocols	• Loss of access to target networks • Redirecting traffic on a network • Intercept and alter information during transmission
Communication	• Serial-based connections to communicate with a substation and/or remote devices • DNP3 communication protocols	• Loss of access to a utility's control system • Targeting a field device at a substation and loss of visibility • Attack against master control systems for a field device by sending a malicious frame, or message to the control system
Devices	• Automation components (such as PLCs function via micro-processors) • ICS related equipment	• Intercepting network traffic • Exposure of authentication credentials • Manipulation of larger and connection equipment (i.e., power station)
Remote access and mobile devices	• ICS networks or devices • Sensors, controllers, relays, meters, etc.	• Compromised public utility's control system network
Third party services and supply chains	• Maintenance of generation, transmission, and distribution • Maintenance SCADA systems • Supply chain integrity	• Giveaway of access to the backdoors of devices or software • Vendor validated malicious patches

3.5 Power System Supply Chain Cyber-Attack Surface

Protocols need to ensure decentralized security coordination by leveraging PUF functions. The central use case for protocol development is the update of control device software. Recent supply chain attacks such as SolarWinds point out the critical need to address security concerns regarding malicious software updates. In particular, a malicious software update in control system devices can have severe consequences for critical infrastructure such as the electric power grid. The protocols develop make use of multi-party decision-making as well as PUF-based device authentication. The GridTrust cryptographic protocols are focused on minimal cryptographic overhead, maintaining the security of the communication channel, and defense against modification, splicing, man-in-the-middle and forging of the information by use of approved encryption algorithm systems thus achieving authentication and confidentiality. Figure 2 illustrates the interactions between the various actors for use cases with and without GridTrust.

3.6 GridTrust Box Design

The GridTrust Box is designed to provide enhanced security for the Power Grid, focusing on securing the update process and software packages provided by a vendor. The GridTrust Box is conceived with flexibility of vendor/customer capabilities in mind. The attack model of GridTrust includes an attacker who impersonates the vendor (or is a lone-wolf insider threat) and provides malicious updates to control equipment intending to comprise the power grid. To provide enhanced trust, GridTrust leverage existing technologies and new and upcoming technologies – especially PUFs – into a combined package.

Figure 3 shows a high-level view of the GridTrust Native Device compatible with any power grid control network and control device for an element in the grid. A GridTrust Native Device has PUF technology included at the time of manufacture and which is fully designed to operate with the system as a whole with a high level of security.

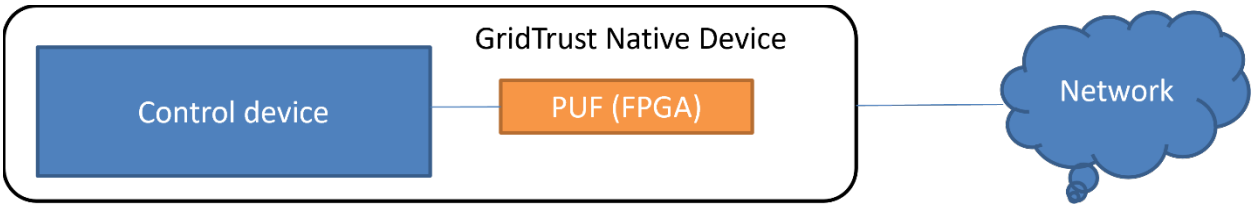


Figure 3. Conceptual Example of a GridTrust Native Device

We assume an update protocol which consists of three main entities: a vendor, a customer, and the customer's devices. When establishing trust for a new update package, the vendor provides credentials to the customer and provides the update package to the device. The customer wants to ensure the provided package is genuine and so requires authentication from the vendor. To enable authentication of the vendor and the customer, we include time-proven and trusted security components (RSA, AES, and SHA-256).

These security modules can be implemented in hardware or software, and we provide the ability in the GridTrust Box to utilize both methods. A computer implements the software-based encryption modules and a separate microchip implements the hardware versions.

In order to work with legacy control devices, Figure 4 shows a GridTrust Interface Device which is placed between a legacy control device in the power grid and the power grid network. A GridTrust Interface Device is a separate design that interfaces with legacy control devices as a bump-in-the-wire and adds security capabilities such as authentication enhanced over and beyond the original capabilities of the legacy device.

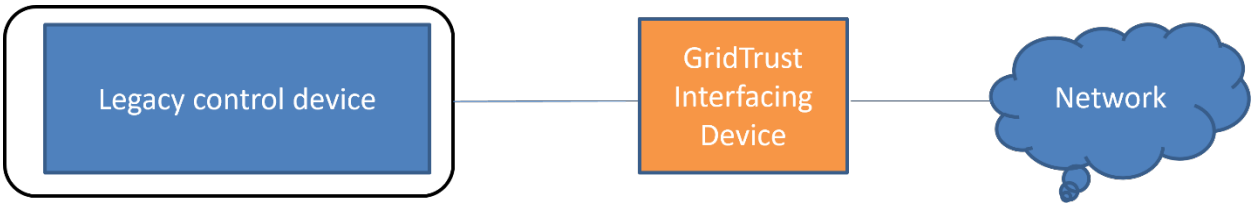


Figure 4. Conceptual Example of a GridTrust Interface Device

3.7 PUF-based Security Protocols

Additional security and authentication capability is provided in the GridTrust Box through the inclusion of a PUF. The PUF is implemented on a microchip. The inclusion of a PUF allows enrollment of PUF challenge response pairs (CRPs) between the vendor and the customer. PUF responses can require correction based on temperature and aging factors, so we have included a temperature sensor on the GridTrust Box.

In order to properly incorporate PUF technology into the system architecture, work must be carried out regarding how to utilize PUF-specific security. Figure 5 shows challenge-response protocols and associated database support necessary for use of PUF technology in the power grid.

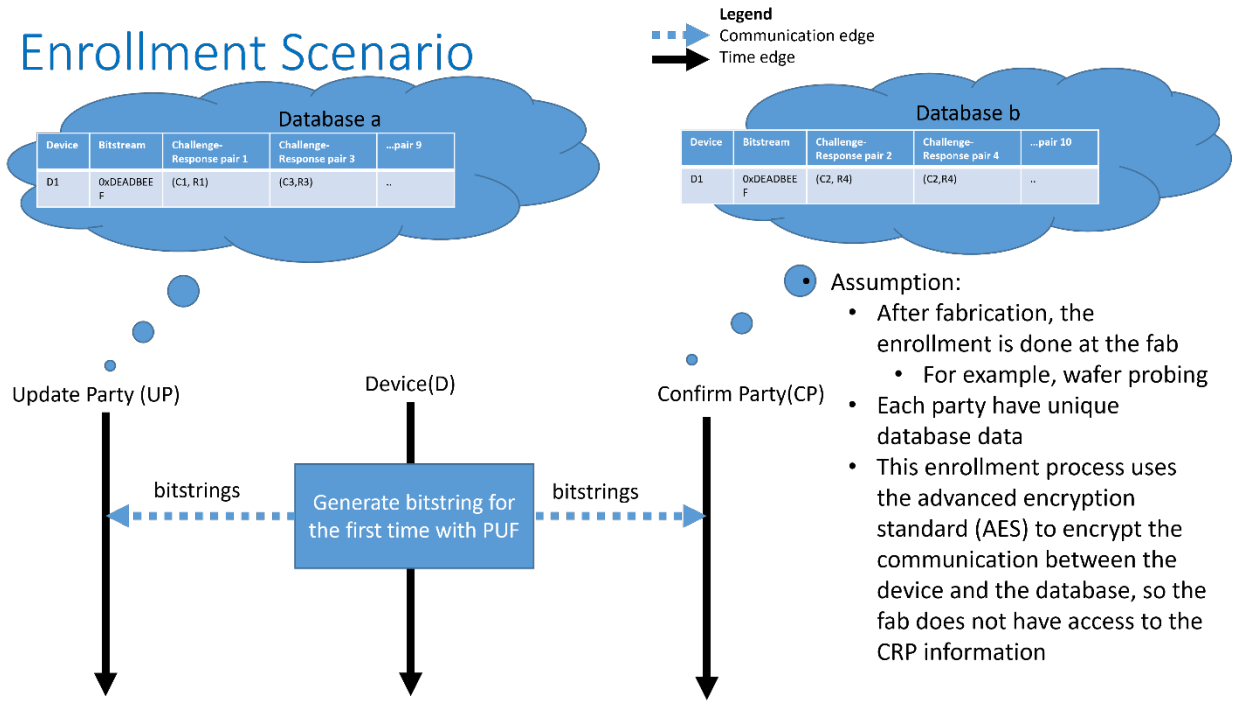


Figure 5. PUF Enrollment

By including traditional software encryption modules and hardware modules, as well as a PUF, we provide flexibility for a customer. The GridTrust Box can interact with a variety of vendors with various capabilities without needing custom GridTrust Boxes for each customer/vendor situation.

3.8 Power Grid Simulator

Power grid supply chain attack simulations can be divided into three fronts: a) developing simulation capability, b) integrating communication protocols for the control devices and c) implementing the GridTrust security protocol in commodity software.

In order to streamline and de-risk development of the GridTrust technology and to demonstrate its functionality in the laboratory benchtop setting, a GridTrust Simulator is developed. The GridTrust Simulator models and simulates the following key elements:

- Utility: An organization who is responsible for distributing electricity to the consumer via the electricity grid. The Utility owns and operate the power devices and the control devices.
- Vendor: One or more parties that manufacture the control devices.
- The power devices, such as synchronous generator, motor, transformer, substations, etc.
- The control devices: Control the power devices and enable power flow in the grid. Examples include relays, communication network switches, merging units, remote terminal units, etc.

In GridTrust, the identity of each of these components must be verified (authentication) for communication among these entities to have a high level of security. The GridTrust

security protocols ensure that each of the control devices can verify the unique identity of each device as a means of ensuring supply chain security (i.e., mitigating the risks of counterfeit software or firmware in control devices). Figure 6 illustrates the concept of GridTrust Root-of-Trust (RoT) cybersecurity. The arrows in the Figure represent the communications among entities. In order to update the control device software, vendors of the control devices communicate with the control center of the Utility and the IEDs in the substation. Similarly, the control center of the utility will communicate with the control devices at the substation and the vendor. These objects as well as their communication capabilities are modeled in software as part of the GridTrust Simulator. Figure 6 describes the workflow of multi-party software update process. This process is implemented in software the GridTrust Simulator.

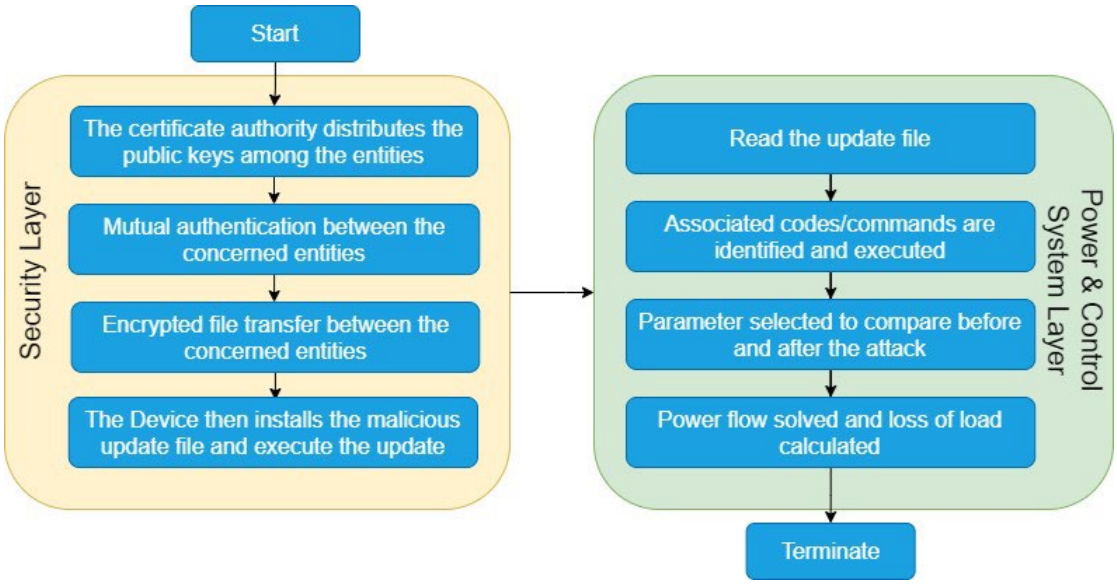


Figure 6. GridTrust Simulation Workflow

The process starts with the security mechanisms, which include authentication of the entities involved (i.e., utility, vendor and control device). Once the authentication process is complete, in the security layer, the workflow moves to the power and control system layers. In the control system layer, the update file is installed and executed. The device reads the update file, which contains the malicious commands (such as changes in the line status, generator setpoints, etc.). The changes are identified at the device's end and executed. This affects the power system quantities in the power layer. Then the simulator solves the power flow representing the physical power system. Specific simulated physical quantities, such as lines active power flows are selected and compared before and after the attack. Finally, the simulation is terminated by determining whether a blackout has occurred, by calculating the resulting loss of load. This metric is utilized to determine the effectiveness of the security scheme or the impact of the cyber-attack. Figure 7 shows the simulation environment.

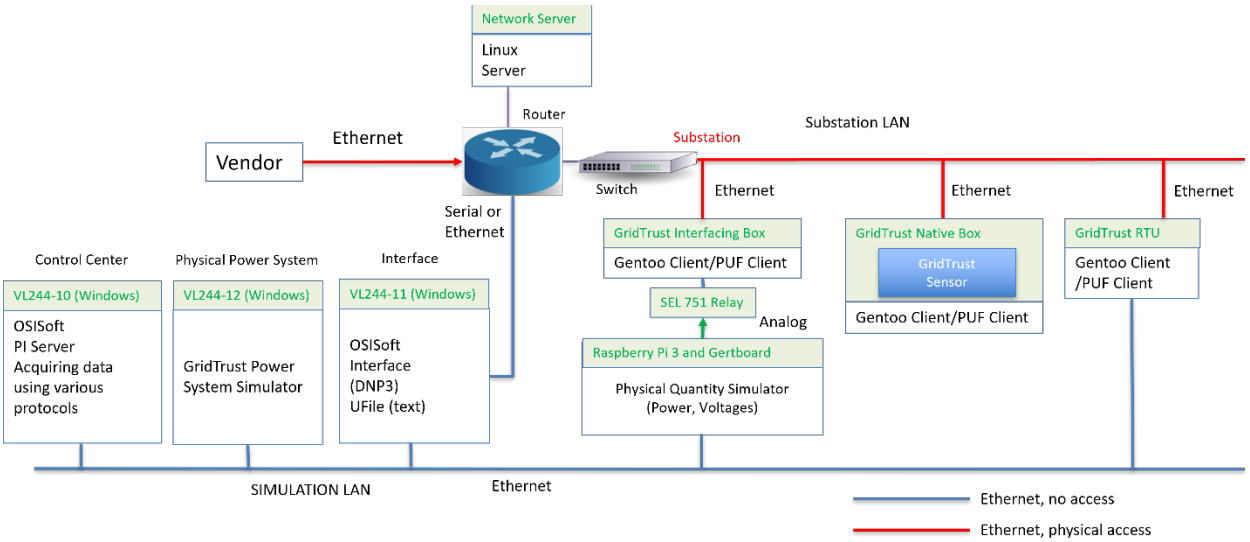


Figure 7. Simulation Environment

In order to provide fast analysis of the use cases and to de-risk research activities during the design and testing of the GridTrust technology, one objective is to develop simulation capability for GridTrust that includes power systems, communications, control devices, security devices, attack representations, and flows of information (messages/packets) [1].

The simulator implements a real-time discrete model simulation. It contains multiple classes, functions, I/O and supply chain attack components, and enables study of supply chain attack propagation and testing on how the GridTrust Technology can contribute to blocking attack attempts. Table 2 lists the major software classes of the Simulator.

Table 2. Major Classes of the GridTrust Simulator

Power System Module	Cyber Module	Security Module
Bus Branch Generator Load Energy Storage Substation	Control Device Intelligent Electronic Device Communication Link Communication Node Measurement Set Point	Key Attacker Security Database Attack Phase

Figure 8 illustrates the power and cyber modules for simulation of a power system example. The power module in this example consists of a 5-bus, 3 substation system. One can see the power topology of this system including the location of the generation sources and the load. The cyber module of the system contains remote terminal units (RTUs) at each substation and control center, as well as intelligent electronic devices (IEDs) connected to each RTU. One can see the topology of the communications network. Each IED contains corresponding measurements of power device quantities such as generation production or transmission line power flows, as well as control set points, such as line breaker opening or generation power regulations.

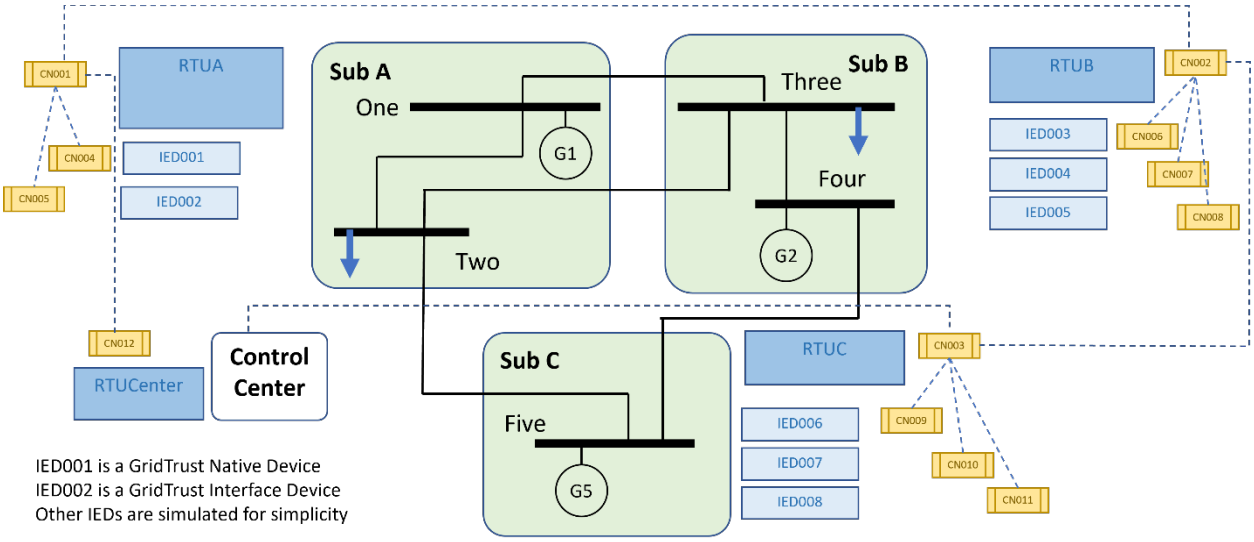


Figure 8. Example of System Simulation including Power and Cyber Layers

The Simulator provides the following functionality:

- Power System:
  - Power flow
  - Contingency analysis
  - Bad data detection
- Security
  - Authentication (enabled by PUF, GridTrust)
  - Encryption (enabled by PUF, GridTrust)
  - Remote update
  - Communication Network (CN) simulation as illustrated in Figure 8.
- Attack
  - Lone wolf attacker (at the vendor) applies malicious remote update
  - Lone wolf attacker (at the utility) is not considered, because the attacker could issue commands to cause blackouts
  - Lone wolf attacker injects bad data from a substation
- Security Interactions
  - Use hybrid attack model to estimate the probability of power loss due to a successful bad data injection attack
  - Power flow is used to determine the impact of successful bad data injection attack (i.e., one power flow calculation is done base on the data received by the Utility and another power flow calculation is done base on what is actually happening in the grid)

4 Technical Approach

4.1 GridTrust Protocol and Hardware Design

Figure 9 shows the overarching GridTrust protocol and hardware design. A Vendor prepares an update for a power grid device shown in the figure as a GridTrust Box. The device (GridTrust Box) functionality could be that of a relay, RTU, PMU, temperature sensor or anything else as appropriate.

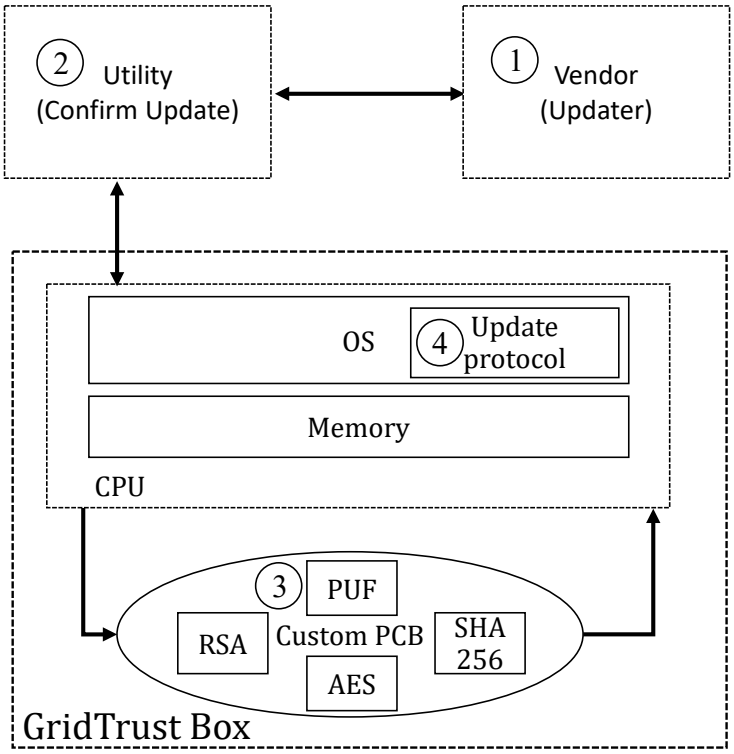


Figure 9. Overview of the Design of a GridTrust Box

Step 1 shown in the bubble at the top right of the figure shows the Vendor developing an update; for example, a vulnerability could have been discovered which needs to be patched. The Vendor cryptographically signs the update and sends the compiled binary to the Utility. To provide additional security, Step 1 may include source code which the Utility can inspect (alternatively, a third party can be hired, but this option is not shown). In Step 2 the Utility verifies/confirms the update and also cryptographically signs the update; as a result, the update binary to be installed now has two cryptographic signatures attached, one from the Vendor and a second from the Utility. In Step 3 the GridTrust Box to confirm its identity using its PUF. The PUF is akin to a digital fingerprint. After PUF-based authentication, the update cryptographically signed by both the Utility and the Vendor is sent to the GridTrust Box.

Step 4 in Figure 9 begins by checking the cryptographic signatures. For example, a standard approach utilizes asymmetric cryptography where the Vendor and Utility have each revealed a public key but have each kept the associated private key protected in

their internal company network. The Update Protocol uses the public asymmetric key of the Vendor and the public asymmetric key of the Utility to check the cryptographic signatures. Only if the binary code of the update is unchanged through the entire process will both cryptographic signatures pass. If both signatures pass, the update is installed; otherwise, the update is not installed and an error message is sent to the Utility indicating update failure [2, 3].

To implement this protocol the GridTrust Box contains a processor running an Operating System (OS) with memory and a suite of cryptographic functions including a PUF. In our prototype implementation we use RSA for asymmetric key cryptography and AES for symmetric key cryptography. We also use SHA-256 for hash generation.

4.2 GridTrust Native Device

A GridTrust Native Device provides all GridTrust and original legacy functionality in a single module, such as an IED or RTU. This is illustrated in Figure 10.

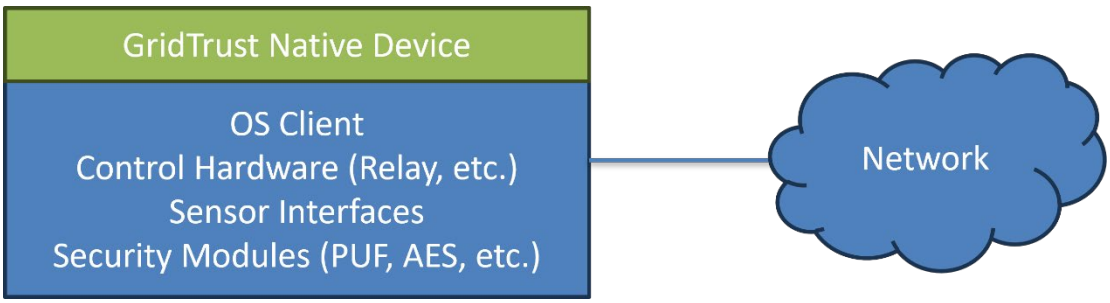


Figure 10. Illustration of GridTrust Native Device

The following steps occur to utilize a PUF and are shown below in Figure 11:

- Prior to usage, the PUF must be initialized and then enrolled
- Enrollment involves the Network Operations Center and the GridTrust Device containing the PUF
- Network Operations Center chooses an AES key and a counter value CTR
- The key and counter are passed via Transaction Layer Security (TLS) wrapped messages to the PUF hardware
- The PUF hardware securely stores the AES key and counter value in an encoded format
- The plaintext AES key and counter can be reconstructed via the PUF on the device without revealing the AES key to an observer

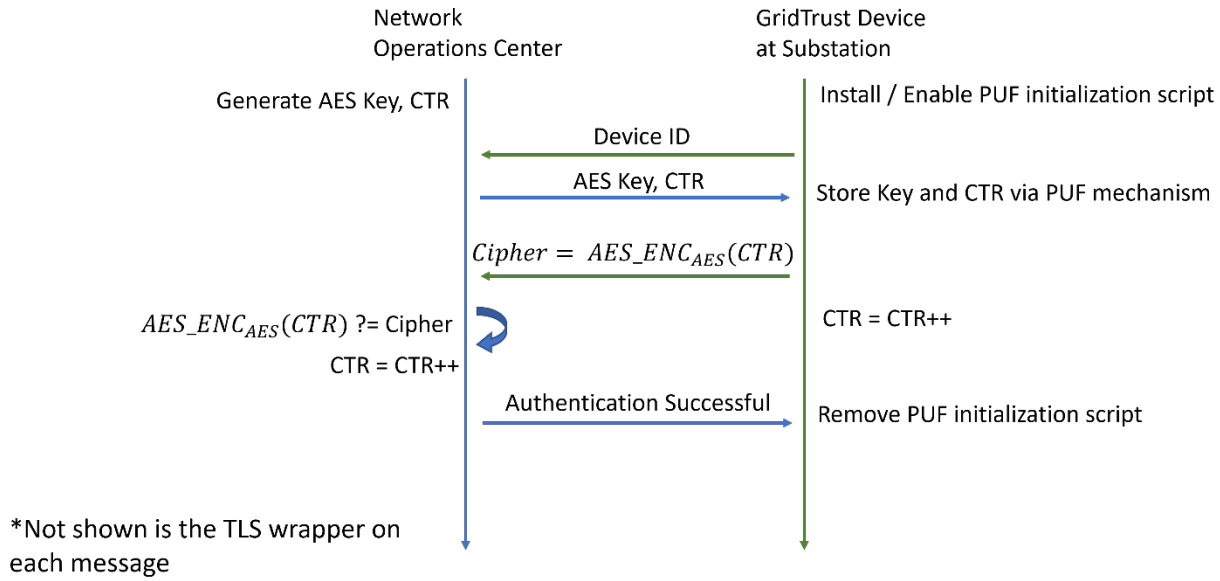


Figure 11. GridTrust Enrollment Process

In Figure 11, each GridTrust device has a unique Device Identification (ID) provided by the device manufacturer and stored in the power grid's Network Operations Center (NOC). Periodically, the NOC requests authentication, and the PUF provides an answer based on AES which is a standard cryptographic primitive. The AES key and counter (CTR) are stored by the PUF in an encrypted format based on the PUF and are not stored in plaintext in any nonvolatile memory location. Note that while the Device ID is a unique value for each GridTrust device, and is used for database management at the Network Operations Center, an attacker may be able to obtain a copy of the Device ID (e.g., by accessing nonvolatile memory). However, since the AES key and counter (CTR) are never stored in plaintext in long-term memory that can be read by an attacker, an attack that copies a device's nonvolatile memory storage – including disk drives and all flash memory locations even on-chip – will not provide the values of the AES key and CTR to the attacker. Furthermore, the AES key is also not stored in addressable volatile memory.

After the aforementioned enrollment process, the first steps of device update perform mutual authentication utilizing the PUF. The counter CTR is a large value, e.g., 128 or 256 bits, and so with a random starting point an attacker has no reasonable chance of guessing the value of CTR including after incrementing CTR to CTR + 1. This "counter mode" is standard in modern cryptography and has no known successful attacks; this mode has passed the so-called "test of time" where a cryptographic technique is used for decades with success and no attack method identified [3].

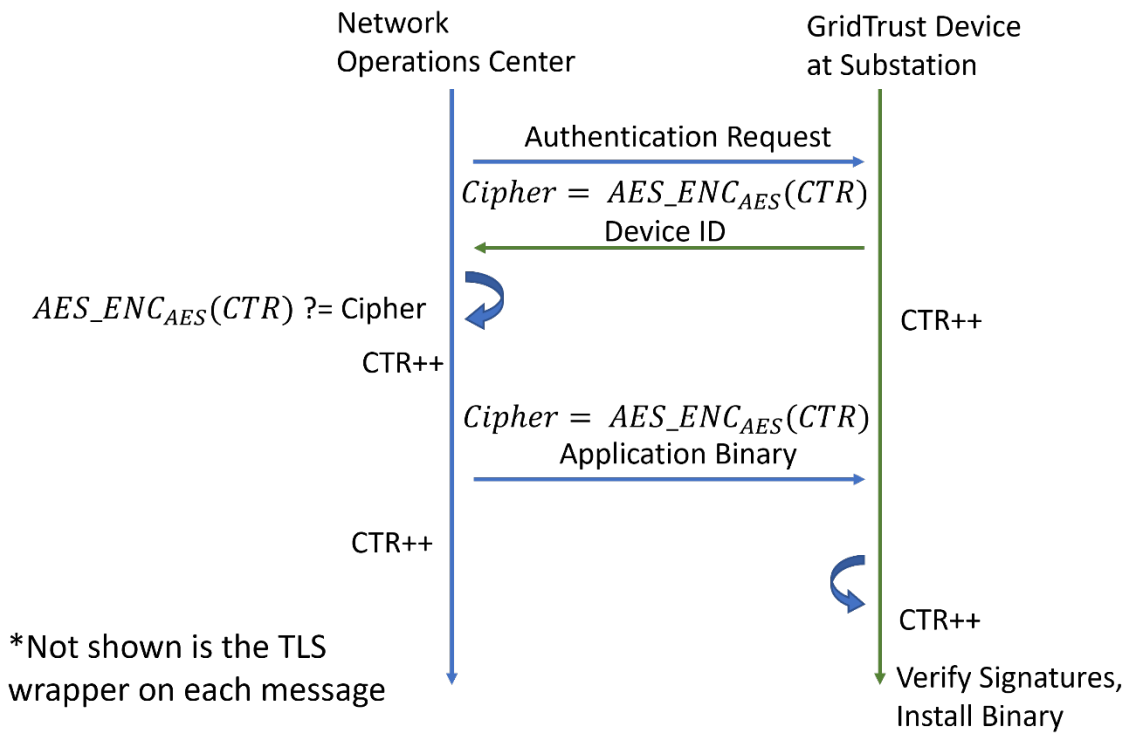


Figure 12. GridTrust Software Update Process with Updated Counter

In Figure 12, after PUF-based authentication, an application update binary is provided to the GridTrust device. Both Vendor and Utility signatures are cryptographically verified prior to installation of the update binary. Shown in Figure 12 are three critical checks: (i) PUF based device authentication, (ii) Vendor cryptographic signature verification, and (iii) Utility cryptographic signature verification.

4.3 GridTrust Interfacing Device

The design of the GridTrust Interfacing Device is identical to the GridTrust Native Device in terms of the protocol, however there is a connection between the legacy device and the GridTrust Interfacing Device that must be secured. If the connection is not secured, then an adversary may be able to access the legacy device directly. If the adversary can access the legacy device directly, then the GridTrust Interfacing Device will not be able to protect the legacy device from direct access including installation of a malicious update.

4.4 System Architecture

To create an architecture for both the GridTrust device as well as the power system, multiple devices were integrated. There were four groupings of computers: a control center where OSIsoft manages data between protocols and the power simulator values, a Network Operations Center (NOC) which contains network/web services, a substation where the relay and other equipment are held, and the Vendor's subnet. The control center focuses on creating simulation values to send to the relay as well as recording these values to observe the effects malicious updates have on the system. The other computer groups are more focused on cybersecurity, with the NOC and Vendor using

GridTrust for validation and the substation being protected by GridTrust. The architecture of the hardware devices is shown in Figure 13. For networking, the Control Center uses a Cisco router, the NOC uses an Ubiquiti Edge Router, and external connections from the NOC are handled through a Cisco router and switch. All software packages used are available through open source; for example, we use GitLab as a Git server, Rust/Cargo as the main programming language/dependency manager, and OSIsoft as the software platform for real-time data management. Please see [2] for a complete list of software packages and references.

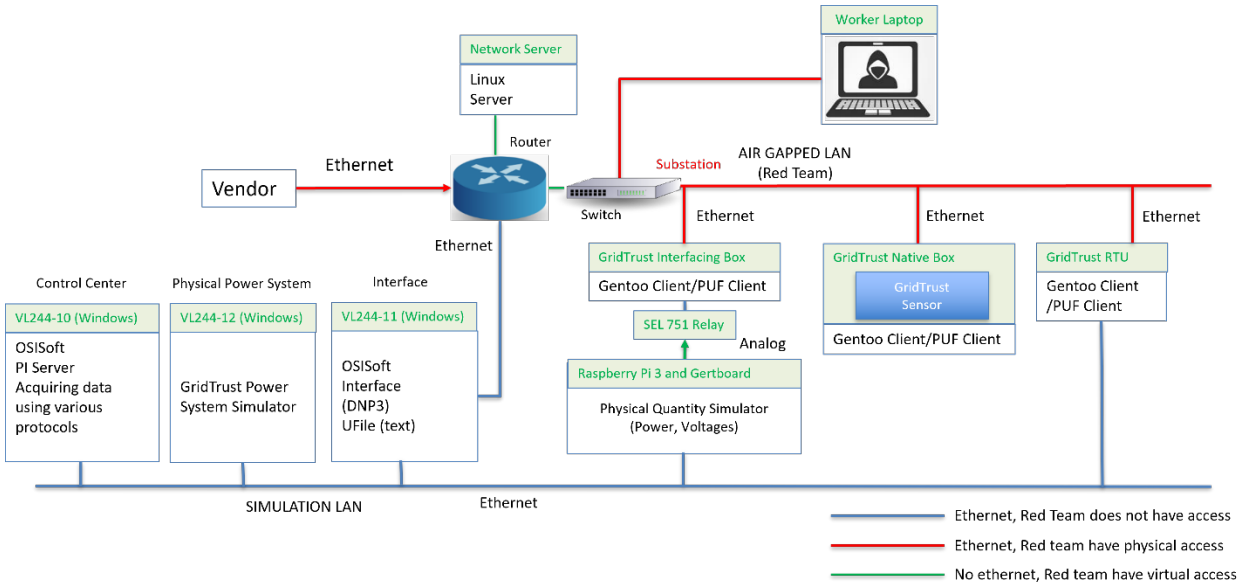


Figure 13. Networking Architecture

4.5 Hardware Design and Laboratory Testing

For the demonstration of GridTrust in the Laboratory setting, multiple computers were used to effectively demonstrate the update process. The first group includes the update components. These computers include a vendor computer which originally has the update files and a utility computer which will receive the file from the vendor before updating one of the devices (see Figure 14). The last group of computers involves the power system simulator. Of these computers, the first is the simulator computer itself, which performs the python code that reads the central model, opens lines, and calculates power flows. This computer communicates with the interface computer. The interface computer's role is to send the current magnitude to the signal generator which will then create a current to be sent to the SEL 751 relay. The interface computer also receives the trip response and the temperature from the relay and temperature sensor before reporting those values to the OSIsoft PI server computer. The PI server computer receives the trip response, temperature, and power system values from the interface computer before storing them as PI points. The power system simulator then reads the PI point for the temperature and trip response to change the central model if the temperature is too high or the relay is tripping. A summary of the power system simulator connections is shown on the next page in Figure 14.

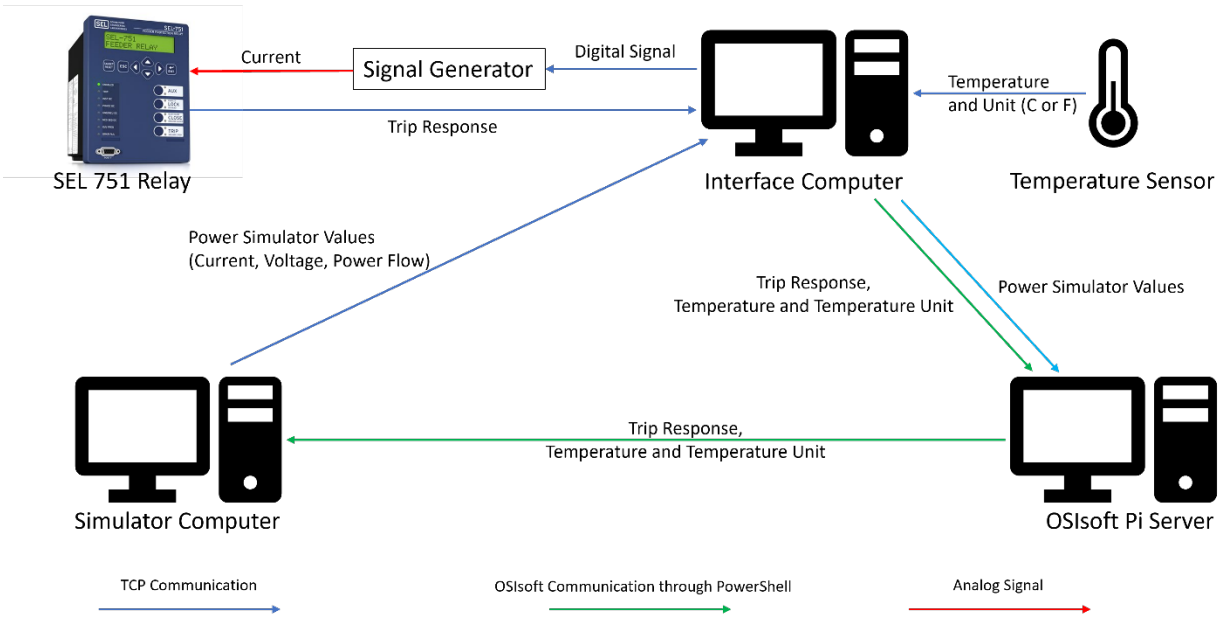


Figure 14. Power System Simulator Connections

The summary of the experiments is shown in Table 3. For clarity, the table shows the experiment setup and results independent of the device. For example, the difference between the GridTrust protocol for updating a temperature sensor and a relay is the update file itself. The main components of a GridTrust protocol consist of a utility signature, a vendor signature, and a Certificate Authority (CA). In Table 3, experiment 1 is the case where the device is successfully updated. Experiments 2 through 6 are the various attacks we have implemented with the results being that the incoming updates are rejected.

Table 3. Experiment Setup

TABLE 1: Experiment Setup and Results					
Experiment	Utility Signature	Vendor Signature	Certificate Authority	MITM	Result (at which point did it fail)
1st	Correct	Correct	Correct	Not tried	Update installed successfully
2nd	Missing	Correct	Correct	Not tried	Fails at hash check for source
3rd	Correct	Missing	Correct	Not tried	Fails at hash check for source
4th	Tampered by attacker	Tampered by attacker	Fake by attacker	Tried	Warning of unknown CA so nothing downloaded
5th	Tampered by attacker	Tampered by attacker	Removed	Tried	Fails since SSL connection cannot succeed
6th	Tampered by attacker	Tampered by attacker	Forged certificate using real CA's signing key	Tried	Fails at hash check for source

4.6 Phase 1 Simulation

4.6.1 Simulation Objectives

The objective of Phase 1 Simulation was to conduct studies that detail the expected behavior and outcomes of the eventual field demonstration experiments. The field demonstration consists of a number of experiments of the GridTrust technology for the two use cases: a) Native GridTrust Box and b) Interfacing GridTrust Box. The experiments are listed in Table 4 below, where the baseline is normal operation and no attack. The Native GridTrust Box corresponds to a temperature sensor located inside the substation shed. The Interfacing GridTrust Box corresponds is connected to a SEL relay that monitors, provides protections for and drives a power distribution feeder. The GridTrust Interfacing Box is located directly adjacent to the breaker controlled by the SEL relay, inside the breaker control panel in the substation yard.

Table 4. Plan for GridTrust Experiments

Native or Interfacing	Normal Operation or Attack	GridTrust Installed	Expected Outcome
Native	Normal	NO	Secure
Native	Normal	YES	Secure
Native	Attack	NO	Insecure
Native	Attack	YES	Secure
Interfacing	Normal	NO	Secure
Interfacing	Normal	YES	Secure
Interfacing	Attack	NO	Insecure
Interfacing	Attack	YES	Secure

4.6.2 GridTrust Simulator Summary

As new resources are added to the power grid, different supply chain vulnerabilities are also added. To assist with protecting these vulnerabilities. To properly evaluate the effectiveness of this framework, simulating different power grid supply chain entities (such as a Vendor and Utility) is required.

The first layer of the simulator is the power system layer. This layer includes the power system simulator, an interface computer, a signal generator, OSIsoft's PI System, and the protection devices. The power system simulator is a Python script that calculates power values (such as current, voltage, etc.) from a model. These values are then sent to the interface computer (see Figure 14) for distribution to other devices. One such device is the signal generator, which receives the current of one simulated power line before scaling it and applying it to our SEL 751 relay. The PI System is an OSIsoft real-time industry-level data acquisition and management platform. Its role in the power system simulator is to record the values generated from the power system simulator. Three protection and control devices are included in the simulation, these being an SEL 751 relay, a temperature sensor, and a computer functioning as an RTU.

The second layer of the simulation is the cybersecurity layer. This layer consists of GridTrust security devices (Native and Interfacing Boxes). Interaction with the security devices is managed by the centralized network operations server that performs key management while also acting as a repository for device updates and configuration files. The security devices (GridTrust Native and Interfacing Boxes) contain the hardware required for device and update validation.

The final layer of the simulation is the control layer. This layer involves the control operations associated with the devices and the power system simulator. The PI System from OSIsoft is the main control system for the simulation.

There are three computers dedicated to providing the control system and power system functionalities. The physical power system is simulated in the Power System computer (see Figure 14) and is connected to the Interface Computer (see Figure 14). The Interface Computer is responsible for pushing the data/measurements received from the power system to the PI System computer in Figure 14. The Interface Computer has multiple connections between the control and power system layers. The Interface Computer also connects to the SEL 751 relay via an Ethernet to USB cable and through the signal generator. A Python program is used to scale a line current received from the power system simulator and assign the magnitude to the signal generator. At the same time, another Python script waits to receive indication if the relay is tripping or not and sends the result to the power system simulator. The Interface Computer connects to the RTU for exchanging data such as measurements to the RTU and queries from the RTU.

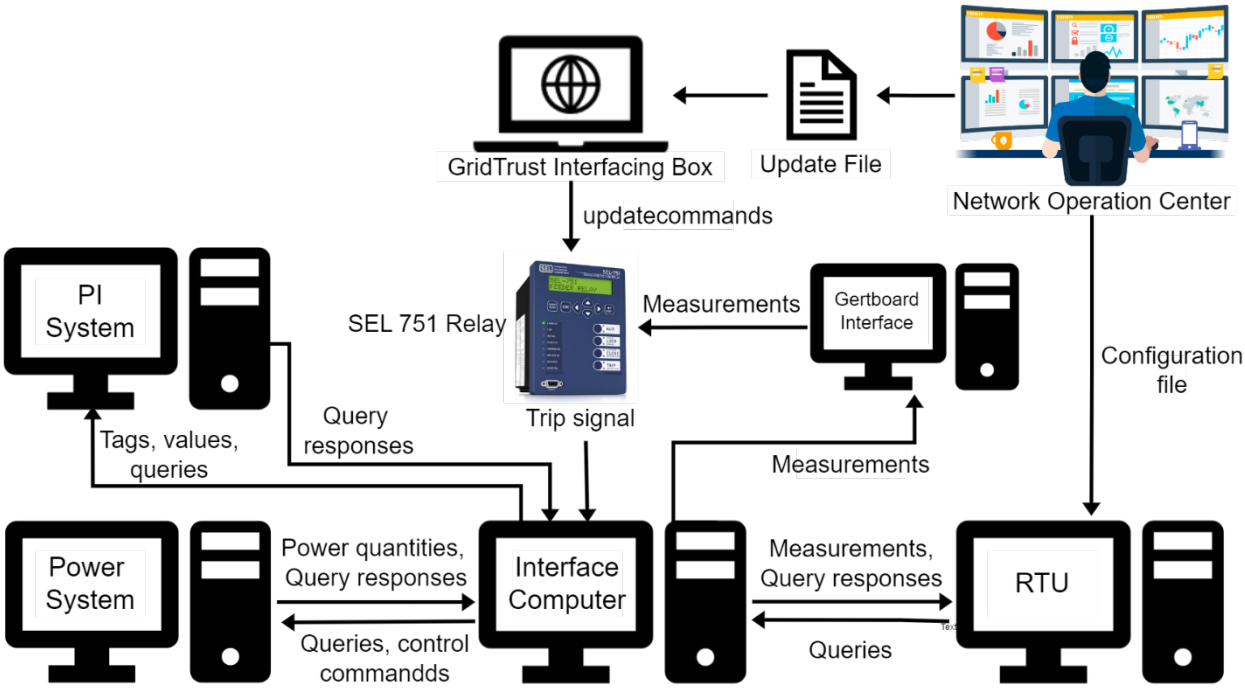


Figure 15. Overall Communication and Information Flow between OSIsoft PI Computers, RTU, SEL Relay and Network Operations Center

Lastly, the temperature sensor communicates its values to the interface, which will be sent to the power system simulator. If the temperature value is too high, the power system simulator turns off one of the generators, simulating an overheat.

The simulation process occurs as follows. The power system simulator generates values representative of realistic power system quantities and sends them to the Interface Computer. The power system simulator can also query for specific control commands from the PI System via the Interface Computer. The Interface Computer then sends the queries, values, and associated tags to the PI System. The PI System then stores the tags and their associated values from different assets in the PI server. The PI System also sends responses based on the queries made by the interface computer. Figure 15 summarizes the connections between computers and devices in the simulation infrastructure.

GridTrust utilizes an update protocol that implements security features that aim to prevent unauthorized software updates. The vendor computer is the original creator and provider of an update. After making an update, the vendor computer sends the update to the utility computer, signed with the vendor's RSA private key. The utility computer then signs the update with the utility's RSA private key. With the update signed by both the vendor and utility, a GridTrust device receives the update when required, as determined by the utility computer. The utility computer only sends the update after proving the identity of the GridTrust device by use of the unique PUF on the GridTrust device. The GridTrust device has the final authority in deciding whether to accept an update or not, and an update is only applied to the GridTrust device (e.g., an IED connected to a GridTrust Interfacing Box) when both signatures are verified.

The simulation techniques and models proposed represent software supply chain cyberattacks in the context of the electricity grid. Our model includes a generic transmission level power grid operation simulation, models for individual devices involved in electricity grid operation, and intercommunication between devices and the utility control center. With the simulation of multiple layers at various levels of abstraction, the effects of various cyberattacks on critical devices in the electrical grid can be simulated. The laboratory setup described showcased three devices (an RTU, a temperature sensor and a Relay) typical of real-world applications. Future work to develop the simulation capabilities can provide researchers with tools to accurately provide an estimation of the impacts of including various security features in an electric grid under an adversarial cyberattack.

4.6.3 System Simulation

The simulation takes place in the GridTrust Simulator developed on the project R&D Task. For the simulation, a portion of the power system is modeled including power lines, transformers and devices, such as breakers, as well as the corresponding communication network, network devices and control devices. Finally, the security protocols of GridTrust as well as the attacker, vendor and utility functions are simulated. Figure 16 below presents the portion of the power system being simulated. The substation under consideration is a double-fed system at 115kV. One transformer converts the voltage

from 115kV to 46kV to serve an industrial customer. The second transformer converts from 115kV to 12.47kV to service various distribution feeders.

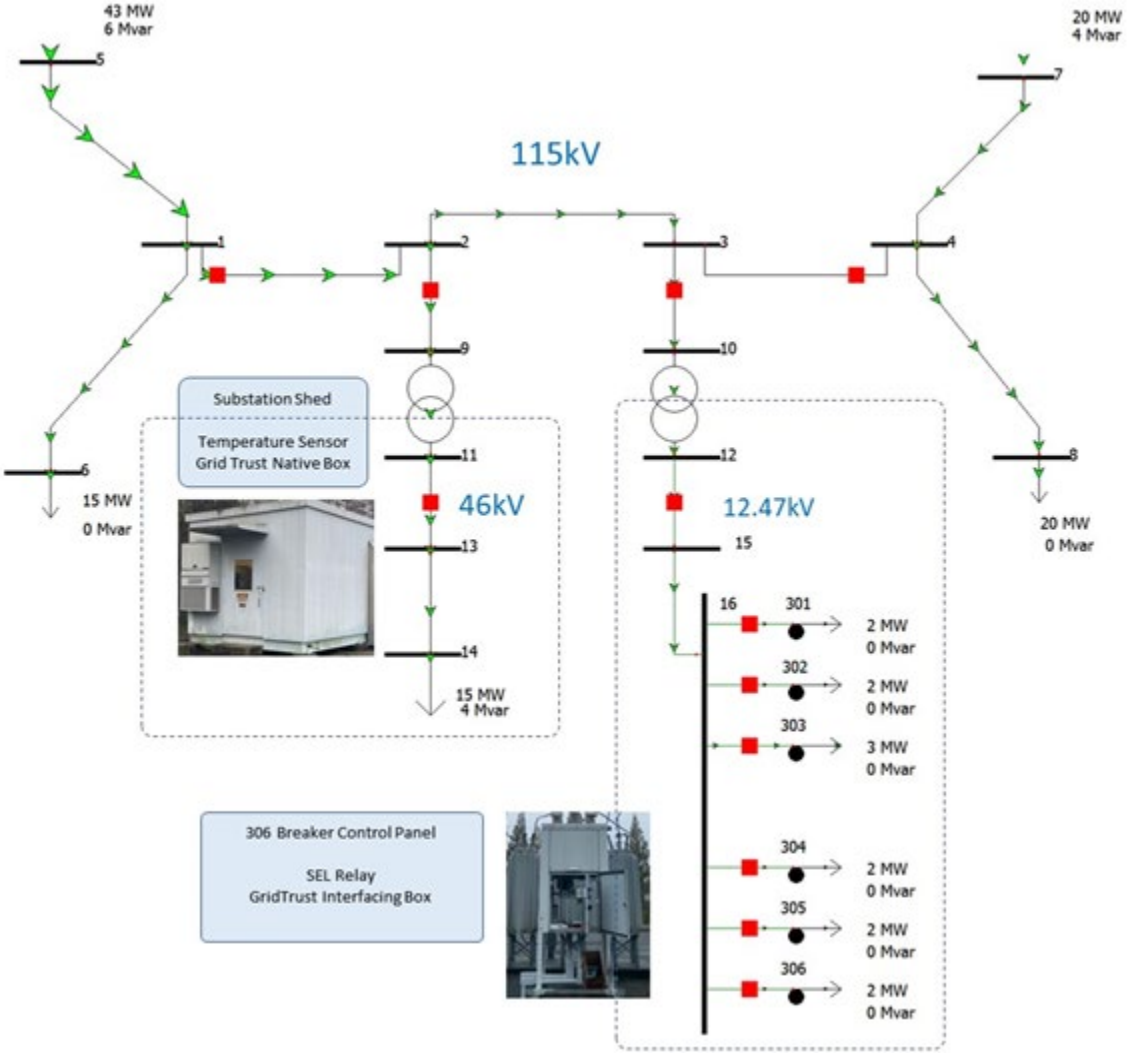


Figure 16. Substations Power Topology for GridTrust Demonstrations

The various use cases are simulated that involve deploying a software update to the control device. The vendor provides a software update to the utility, which reviews the update and instructs engineers to deploy the update at the substation. The update only takes place if the keys from the vendor and utility match, and if the PUF-verified keys match the authentication of the devices. Otherwise, the update is rejected by GridTrust.

4.6.4 Laboratory Red Team Testing (Phase 1)

Prior to execution of the vulnerability assessment, GridTrust researchers identified a key threat scenario representing real-world risk to energy utilities that formed the basis for their engineering design and the primary threat vector for this vulnerability assessment. The overarching threat scenario called for an Operational Technology (OT) engineer at a notional utility organization that has been compromised by a Nation-State Cyber Threat to install a malicious update on OT devices within a substation. The GridTrust prototype

system architecture, OT network architecture, and notional utility organization network were all designed in support of modeling this scenario. The system interfacing with the GridTrust technologies takes places in the Red Teaming Testing Environment shown in Figure 17.

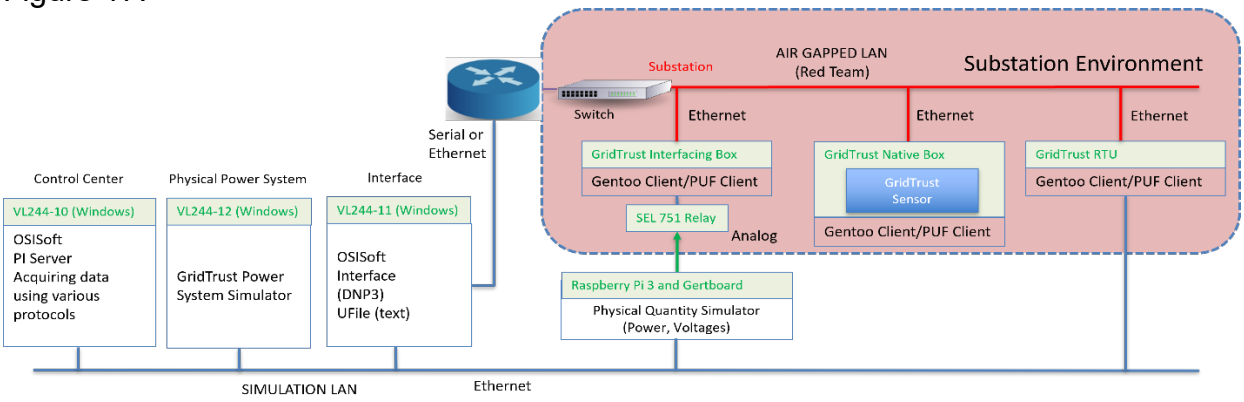


Figure 17: Laboratory Red Team Testing Environment

In April 2022, GTRI CIPHER Lab assessors performed an iterative vulnerability assessment against the GridTrust prototype system by modeling advanced persistent threat behaviors against GridTrust protected devices to identify if there were any weaknesses in the design or implementation of the GridTrust protections. The assessment team also assessed the state of vulnerabilities across supporting infrastructure to determine if the existence of vulnerabilities elsewhere in an architecture aids an attacker in compromising any component of the GridTrust protections. To identify the resilience of the GridTrust protections across the architecture, the assessment team performed a series of experiments against components in degraded security states.

4.6.5 Red Team Conclusions (Quote from Official Report)

At the conclusion of a 3-day long cooperative assessment, no critical vulnerabilities were identified in the GridTrust protections or workflow. Even under degraded conditions, with most protection mechanisms deliberately disabled, an attacker would need a high level of skill to effectively interfere with proper operation of the GridTrust network. Recommendations for improvement of the GridTrust process include 1) inclusion of a mechanism to ensure a device does not attempt to process an update for another device and 2) encryption of HTTP message bodies. The GridTrust system shows clear evidence of design and implementation with a concern for cybersecurity.

4.6.6 GridTrust Form Factor

In order to proceed to the field demonstration for Phase 2, the GridTrust design had to be reduced in size in order to fit in the substation power grid equipment planned for GridTrust protection. Two designs were implemented for the GridTrust substation demonstration form factor, one for each use case. The first represents a device with GridTrust incorporated into the device natively. This form factor contains both a temperature sensor, representing a critical device, and a PUF. The second design is for GridTrust interfacing with legacy devices. This form factor involves a PUF and a processor, an

OptiPlex 3000 Micro, being contained separately from a critical device, a relay for the substation demonstration. Figure 18 below shows the estimated size of the GridTrust enclosure. Beyond testing, a commercial enclosure will provide GridTrust protection from common physical concerns including extreme heat and cold, seismic activities, rain, snow, and other common weather aspects. Ballistic resistance may be considered for more exposed applications.

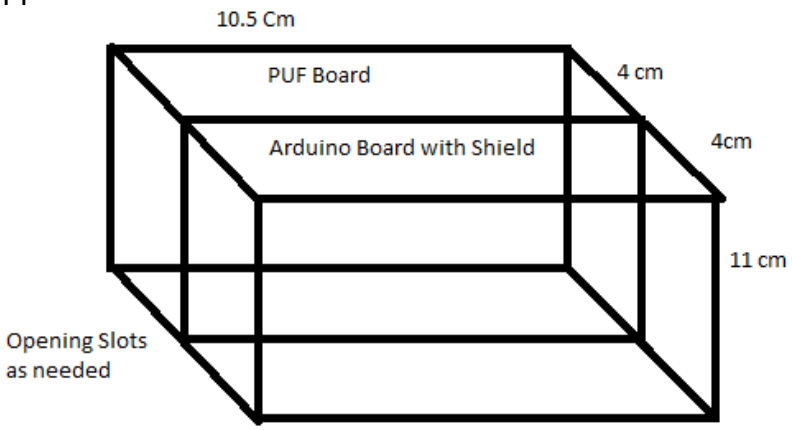


Figure 18: GridTrust Demonstration Form Factor Sizes

For creating GridTrust's form factor for the substation test, two options were considered, Front Panel Express and the Georgia Tech Makerspace. Front Panel Express offers software to design the enclosure, as well as creation capabilities in a variety of materials including aluminum, plastic, and non-ferrous metal. The Georgia Tech Makerspace has a variety of tools to produce the enclosure including two types of 3-D printers, a metalworking and woodworking room, and a plasma cutter. Front Panel Express offers a consistent and professional enclosure, but the Georgia Tech Makerspace gives the research team access to the final product without delays for delivery. The team chose to use the Georgia Tech Makerspace.

4.7 Field Demonstration

4.7.1 Objective

The goal of the GridTrust project demonstration task was to demonstrate PUF technology and multi-party authentication methods for electricity grid supply chain cyber-security at a power substation. Georgia Tech and the City of Marietta (Marietta, GA) developed a plan to test the GridTrust technology on a small portion of City of Marietta's power system. Marietta Power and Water is a large municipal utility in Marietta, Georgia. This demonstration allowed the team to gather insights regarding the GridTrust technology implementation as well as to advance GridTrust for eventual adoption by the industry.

4.7.2 Test Cases

Two target devices were developed for the field demonstration:

- Temperature Sensor, which represents the Native GridTrust Box
- Relay, which represent the Interfacing GridTrust Box

To facilitate testing, Marietta Power and Water allowed us to connect our equipment to their network interfaces in their SCADA operations center and in a substation control shed. We additionally connected equipment to a fully functional relay and circuit breaker in a substation yard which was not serving customer load, hence facilitating testing without risk. The demonstration extended the validation conducted in the lab to perform updates on equipment found in an operating environment at a real electric substation and network operations center.

We utilized the SCADA server network access points to connect our representative network operations center (NOC). Our server computer was connected to the Marietta network through an ethernet port. From the server room, connections to the various substations are realized via a utility fiber ring, which is converted back to ethernet at each substation.

In the substation there is a shed which houses control equipment interfacing with the substation equipment such as voltage regulators, circuits breakers, and transformers. The controlled equipment (i.e., circuit breakers and transformers) are located in the substation yard. The circuit breakers in the yard were interfaced through SEL 751 relays.

4.8 Field Demonstration Tasks and Schedule

The schedule described in Table 5 was followed for the demonstration tasks of the project from November 2022 to June 2023.

Table 5. Demonstration Schedule

Task	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun
1. Visit Sites to Discuss Specifics for Installation								
2. City of Marietta Prepares Network for GridTrust								
3. Test Communications for the Various Sites								
4. Install and Test GridTrust Temp. Sensor								
5. Install and Test GridTrust Operation of the Relay								
6. Red Team Test of the Temp. Sensor and Relay								
7. Demonstration for DOE								
8. Reporting and Available in Case of Delay								

4.8.1 Setup

The demonstration testing at the Marietta power substation comprised two separate target devices, as shown in Figure 19. First, a GridTrust Native Device was implemented targeting a temperature sensor placed inside the equipment shed found inside the electricity substation. The second target device was a GridTrust interfacing device used as the communication interface for a SEL 751 relay connected to a circuit breaker. The GridTrust interfacing device, relay, and circuit breaker were all located within the substation yard. The GridTrust server was located in Marietta's server room and utilized a VLAN to communicate with the GridTrust devices found in the substation. The two

GridTrust devices and the NOC server communicate with standard TCP/IP formatted packets containing the software updates and the software signatures.

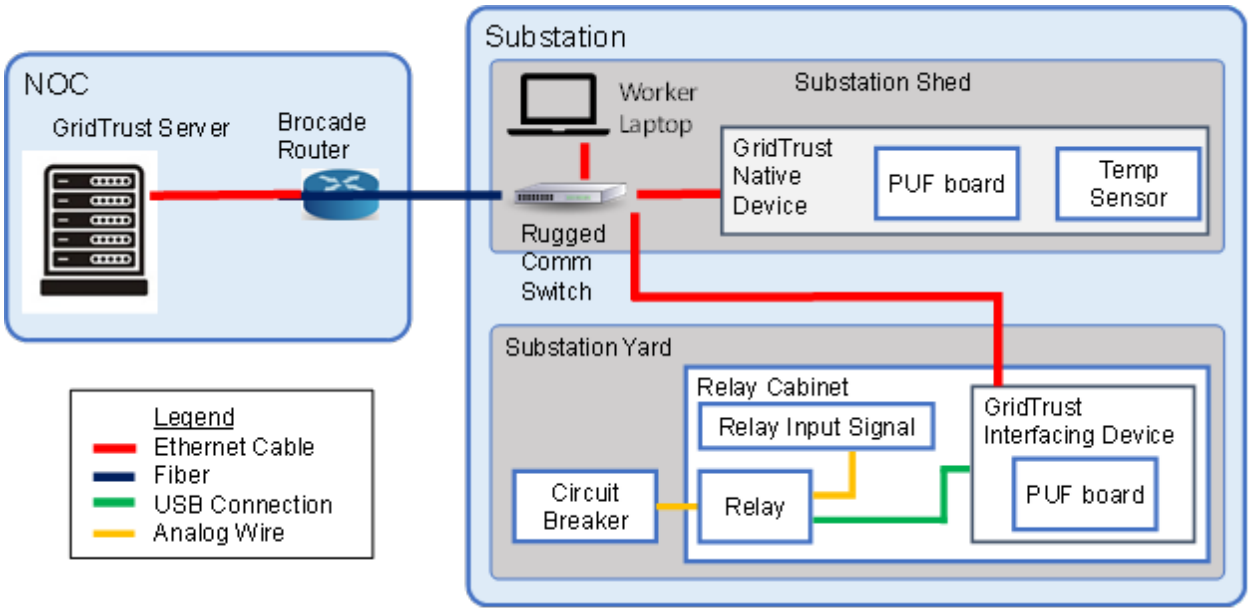


Figure 19. Demonstration Testing

Software updates representative of potential normal updates as well as malicious updates were developed for both the GridTrust native device and the GridTrust interfacing device. For the temperature sensor, these updates consisted of varying the temperature output format between Fahrenheit and Celsius for the legitimate updates, and outputting Fahrenheit values with a Celsius label for the malicious update. The updates for the relay consisted of altering the setpoint for the overcurrent trip setpoint. The legitimate update changed the setpoint to a value which is above the nominal operating condition of the connected bus and the malicious update changed the overcurrent setpoint to a value which was below the nominal operating condition.

To demonstrate the protections provided by GridTrust, several tests were conducted, shown in Table 6. Updates were successfully applied to both the GridTrust native device and the GridTrust interfacing device from both a local worker laptop and from the NOC server. All illegitimate updates as defined in Table 6 were stopped by the GridTrust protocol correctly. We further showed to ability to apply arbitrary software updates to both the temperature sensor and the relay when GridTrust protections were not enforced. This resulted in improper temperature measurements for the temperature sensor. For the relay this caused the attached circuit breaker to open on a spurious overcurrent condition.

Table 6. Attacks and Results

Attack Mechanism	With GridTrust?	Native Box		Interfacing Box	
		TLS On	TLS Off	TLS On	TLS Off
No Attack (Baseline)	NO	✓	✓	✓	✓
	YES	✓	✓	✓	✓
Missing/Tampered Signatures Utility Signature Vendor Signature	NO	X	X	X	X
	YES	✓	✓	✓	✓
Forged Certificate	NO	NA	NA	NA	NA
	YES	✓	NA	✓	NA
Man-in-the-middle (ARP*) GridTrust will not prevent ARP cache poisoning, but will still block the malicious update	NO	X	X	X	X
	YES	✓	✓	✓	✓
Man-in-the-middle (HTTP proxy)	NO	X	X	X	X
	YES	✓	✓	✓	✓

✓ means the update is secure
X means the update is insecure
NA: Not Applicable

test has been completed
test has yet to be completed
test completed w/o breaker operation

4.8.2 Field Red Team Testing

Context

Prior to execution of the red team engagement, GridTrust researchers performed a field demonstration of the GridTrust architecture within a City of Marietta/Marietta Power substation to identify the feasibility of the capabilities within a real-world environment. The final component to the field demonstration was the execution of a red team engagement on the GridTrust components within the Marietta substation. Execution of the red team engagement in a live substation environment served two purposes. First, the GridTrust architecture would be protecting real substation breakers and relays during the engagement to identify real-world effects of the attack techniques. Second, the Marietta substation network provided real-world networking characteristics that could be taken advantage of by an attacker. It should be noted that the City of Marietta/Marietta Power assigned unused substation breakers, relays, and feeders for the demonstration and red team engagement to ensure that the engagement would not be targeting the rest of the power network that serves customers. The engagement took place during a 3-day testing window in March 2023 and followed the same progression and scope as the lab-based vulnerability assessment that occurred in May 2022. This included testing the GridTrust architecture under the Optimal System Configuration (SSL/TLS turned on) and the Degraded System Configuration (SSL/TLS turned off).

Model

The primary purpose of this engagement was to assess the current GridTrust prototype system for vulnerabilities or weaknesses within the City of Marietta/Marietta Power

substation network. However, given that the prototype system is still nascent, the assessment needed to be focused on proving/disproving specific threat scenarios against core components/workflows of the GridTrust architecture. Prior to the engagement, the GridTrust team identified a key threat scenario that represents real-world risk to electric utilities. The overarching scenario called for an OT employee of the utility that had been compromised by an Advanced Persistent Threat (APT) group that is associated with a nation-state. These classes of threat groups often have access to significant resources, time and finances that support their larger operational goals. This scenario served as the basis for all of the specific threat techniques that would be executed during the engagement. In addition to these parameters for the assessment, the GridTrust team established strict scope/boundaries within the prototype system on which the assessment team should operate. These boundaries were set to ensure that assessment efforts focused on the core components implemented as part of the GridTrust research and nothing more within the City of Marietta/Marietta Power network. The scope and the core components under assessment were all devices located within the substation subnet either located in Marietta Power Substation #3 or the Marietta Power datacenter.

Result

At the conclusion of a 3-day long cooperative assessment, no critical vulnerabilities were identified in the GridTrust protections or workflows in the City of Marietta substation network. Even under degraded conditions, with most protection mechanisms deliberately disabled, an attacker would need a high level of skill to effectively interfere with proper operation of the GridTrust components. Recommendations for improvement of the GridTrust process include encryption of HTTP message bodies on top of TLS encryption to provide an additional layer of protection against Man-in-The-Middle attacks in the event that TLS is compromised within an environment or cannot be implemented. The GridTrust system shows clear evidence of design and implementation with a concern for cybersecurity. Table 6 illustrates the final state of the red team engagement showing all tested permutations and conclusions on which permutation of attack technique is prevented by GridTrust. For final conclusions on the red team engagement, GridTrust was able to prevent all permutations of the executed attack techniques illustrating the need for such a technology in utility networks.

4.9 Scalability Test Case

In addition to the power substation demonstration, the team extended the testing with an additional use case that involved two SEL relays and a distribution-level pole-switch. This was conducted in the Marietta's Operations and Maintenance (O&M) shop. This testing in the O&M shop utilized a single GridTrust Interfacing Device, as shown in Figure 20. The GridTrust device was connected to a SEL 751 relay connected to a pole switch. The GridTrust device was connected to the GridTrust server through a VLAN. Additionally connected to this network was an unprotected SEL 751 relay, with a simulated connection to a pole switch. Testing was performed with software updates which would change the overcurrent trip setpoint.

To certify the ability of the GridTrust device to protect pole switch relays, we sent the same update to both relays. The GridTrust protected relay successfully stopped all

malicious update attempts while the unprotected cabinet allowed the malicious update to be applied.

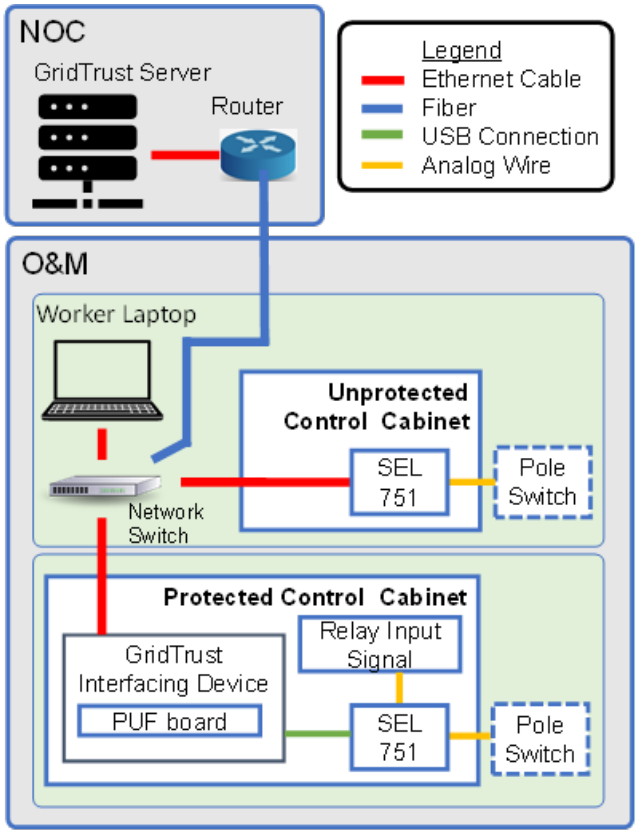


Figure 20. Pole Switch Relay Case

4.10 Post-Project Commercialization Plan

Efforts to bring GridTrust technology towards commercial use focused on four areas. The first area was continued interactions with a potential customer in the City of Marietta. The second area was writing up draft text for a possible patent disclosure on the core GridTrust protocol implementation. The third was interacting with Georgia Tech's VentureLab whose mission is to bring research results and prototypes to transition to industrial products. The fourth and final area of effort involves placing GridTrust in open-source form on the web to facilitate inclusion of GridTrust in future efforts and proposals in order to enhance the appeal of possible commercialization with a more comprehensive set of research and development results.

4.10.1 City of Marietta

The final demonstration and live red-team testing of GridTrust in an actual physical substation provided regular (approximately biweekly) meetings with the City of Marietta officials and staff responsible for the city's power grid. In this context, both potential attacks as well as the corresponding benefits of GridTrust technology became increasingly clear. Of particular interest was the protection against a possible line-wolf insider, e.g., a disgruntled or bribed low-level employee. Red-team testing in the Marietta

substation confirmed the success of GridTrust in preventing a wide range of lone-wolf actions (the best attacks we could think of or which the red team could conceive).

4.10.2 Patent Exploration

The text for a possible patent disclosure on GridTrust's software update protocol combining multi-party authentication and PUF technology was written up. The draft patent disclosure text was submitted to Georgia Tech's Office of Technology Licensing (OTL), and OTL staff met with the inventors (Co-PI Mooney, PI Grijalva and Ph.D. candidate Hutto, all from Georgia Tech) multiple times. However, after a multi-faceted review including comparison with prior existing patents and especially prior disclosed and published papers, a determination was reached that it is not clear that a person skilled in the state-of-the-art in possession of the prior disclosed publications could not reproduce the software update protocol. Therefore, a decision was reached to **not** file for a patent.

4.10.3 Georgia Tech VentureLab

Multiple meetings were held with GT's VentureLab to discuss a possible start-up company. One main question addressed in the wide-ranging discussions was the conservative nature of the power grid industry and the existing strength of the leading companies in the market. It was determined that a small company would face a very tall set of challenges to replace existing relay, RTU and other similar equipment currently in production.

A second main question addressed was the possibility of a startup based on open-source software. One of the most successful existing open-source software companies in the world is Red Hat with headquarters nearby in North Carolina. The discussions are still ongoing, although the small market size of the power grid industry appears to be a complicating issue for an open-source company. On the other hand, if the target market were to include operational technology (OT) more generally – e.g., including water treatment plans and other similar critical infrastructure – then the market size would be significantly increased.

4.10.4 Follow-on Research and Development

The determination that the core GridTrust PUF-based multi-party authentication protocol would not be patented catalyzed the decision to release GridTrust code via open-source software. The website https://mooney.gatech.edu/security/gridtrust was launched with plans to include this website in future press releases. PI Grijalva and Co-PI Mooney plan to leverage and advance GridTrust technology through possible additional research and development funding. Other universities, federal research laboratories and commercial companies may also use the open-source GridTrust code to learn from and enhance their own research, development and productization efforts. The goal is to enable ease of use of GridTrust software as well as the improvement of GridTrust by adding additional functionality in order to increase the appeal to commercialize GridTrust technology.

5 Accomplishments and Conclusions

GridTrust Development

The electric power grid stands as a cornerstone of modern society, a critical infrastructure that fuels and sustains our way of life. Its sprawling network of transmission and distribution circuits spans vast distances, linking power sources to substations and ultimately serving residential, commercial, and industrial customers. This intricate web has evolved into a sophisticated system, continually expanding to accommodate the demands of decarbonization, renewable energy integration, electric vehicles, and the surge in electricity consumption. Operating on the backbone of intricate cyber-control mechanisms, the grid plays an indispensable role in powering our world.

Central to the grid's integrity is the realm of cybersecurity, a vital safeguard against potential threats. Malicious actors with disruptive intentions could attempt to breach the cyber-system governing the grid, potentially causing widespread blackouts or equipment damage. Notably, the supply-chain of power control equipment emerges as a vulnerable juncture that demands robust defenses against cyber-attacks. Therefore, electric utilities must establish a robust cybersecurity posture, fortified by advanced technologies, to protect both their systems and the intricate supply chain that underpins their operations.

This project has developed GridTrust, an innovative advancement in Grid Supply Chain Cyber-Security. The majority of power grid control devices are located within power substations. These devices originate from various vendors, with their supply-chain journey spanning microprocessors, hardwired controls, software, and firmware. Given this landscape, malicious actors, including potential insiders, may endeavor to tamper with software at various stages—shipping, installation, maintenance, or setting adjustments. Our focus rests on the main use case: software updates.

During the project, the team leveraged two technological advancements. Firstly, physically unclonable functions (PUFs) which are fingerprints on microprocessors, offering unique identification and root-of-trust authentication for control devices. Secondly, a novel security protocol governs key exchange, involving vendors, third parties, utilities, and control device.

GridTrust introduces device-level authentication via PUF technology. A PUF-based fingerprint acts as an authorization prerequisite, rigorously verified before a firmware update proceeds. GridTrust integrates Vendor and Utility cryptographic signatures, adding an extra layer of assurance for updates. This strategic integration aims to render lone-wolf insider attacks, including those backed by external support, considerably less viable. The GridTrust prototypes, deployed in real-world scenarios, feature microprocessor chips paired with SRAM PUF technology. The SRAM bits, initially randomized through manufacturing variations, eventually evolve into deterministic behavior with the inclusion of error correction techniques. Our choice of an NXP board, armed with a PUF, supports the security strength of GridTrust. GridTrust uses asymmetric key technology, RSA, and cryptographic signatures from both Utility and

Vendor. The Utility examines Vendor source code, endorsing updates only when confident in their integrity. GridTrust Native and Interfacing devices carry a dual verification process: authenticating identity through PUF and scrutinizing Utility and Vendor signatures via RSA public keys. Solely upon successful completion of these checks does the firmware update proceed; otherwise, the system maintains status quo.

Demonstration

The field demonstration took place at a power substation of City of Marietta. Inside the substation shed, a temperature sensor demonstrated a comprehensive GridTrust solution for a new device—our so-called GridTrust Native device, which included form factor. During localized updates, engineers access the update on devices using the computer laptop. In the substation yard, an SEL 351 relay is protected using an GridTrust Interfacing Device. We utilized a signal generator to replicate applied currents and a commercial circuit breaker. The tests encompass malicious updates that, if successful, would trigger relay trips and circuit breaker activation.

A comprehensive set of tests with various permutations were developed on both the Native and Interfacing GridTrust Devices. In all cases, GridTrust was able to block the cyber-attack. The field red team further confirmed the security strength of the solution by replicating the attack permutations under various network and system configurations. Even with degraded security (TLS disabled), GridTrust was able to block all the attacks.

Red teaming studied in a live and authentic substation environment, scenarios wherein a compromised OT employee accesses cabinets containing network connectivity devices. In such a context, a potential attacker might exploit a network Man-in-the-Middle technique to implant malicious updates into the OT devices situated within the substation. Armed with a standardized suite of attack simulation tools, the red team established both a low-level Layer-2 MITM and a higher-level Layer-7 HTTP Man-in-The-Middle position. These positions enable the red team to intercept all network traffic flowing between the GridTrust-protected OT devices and the Network Operations Center, the source of updates. With these positions in place, the red team systematically explored permutations of experiments to gauge the resilience of GridTrust components against attacks within a live substation environment.

Upon the conclusion of the red team engagement, the GridTrust architecture emerged unscathed against all executed attack techniques directed at the Relay and temperature sensor housed behind the GridTrust interfacing box and native box, respectively. The cyber-security holds true across a spectrum of attack techniques, including digital signature tampering, forged TLS certificates, L2 Man-in-The-Middle via ARP poisoning, and L7 HTTP Man-in-The-Middle. This fortified protection stems from the installation of GridTrust components in front of devices, with each update double-secured through digital signatures from both vendors and utility sources. Devices without GridTrust components remain susceptible to tampering, granting attackers the ability to inject malicious updates.

Conclusion

The project and field test results underscore the strength of the GridTrust protocol and the technology's successful implementation within a genuine substation setting. GridTrust's has been effective in demonstrating effectiveness in countering direct supply-chain cyber-attacks on the power grid control system. Over the coming months, the team will be expanding and demonstrating GridTrust through diverse use cases in collaboration with the industry partners.

6 Appendix: Product or Technology Production

Table 7. Products and Technology Production

PRODUCTS AND TECHNOLOGY PRODUCTION		
Item Type	**Date**	**Title/Description**
Publications		
Journal Paper	June 2021	Y. Chen et al., “Grid Cyber-Security Strategy in an Attacker-Defender Model,” MDPI Journal of Cryptography, June 2021.
Conference Paper	February 2022	B. Newberg, V. Mooney and S. Grijalva, “Open-Source Architecture for Multi-Party Update Verification for Data Acquisition Devices”, PECI: Power and Energy Conference at Illinois, Champaign, IL, February 2022.
	February 2022	K. Hutto, V. Mooney and S. Grijalva, “Hardware-Based Randomized Encoding for Sensor Authentication in Power Grid SCADA Systems”, TPEC: Texas Power and Energy Conference, College Station, TX, February 28 - March 1, 2022.
	April 2022	S. Paul, Y. Chen, S. Grijalva and V. Mooney, “A Cryptographic Method for Defense Against MiTM Cyber Attack in the Electricity Grid Supply Chain”, IEEE Innovative Smart Grid Technologies Conference (ISGT), New Orleans, LA, April 2022.
	April 2022	K. Hutto, S. Paul, B. Newberg, V. Boyapati, Y. Vunnam, S. Grijalva and V. Mooney, "PUF-Based Two-Factor Authentication Protocol for Securing the Power Grid Against Insider Threat", KPEC: Kansas Power and Energy Conference, Manhattan, KS, April 2022.
	June 2022	K. Hutto, S. Grijalva and V. Mooney, “RanCompute: Computational Security in Embedded Devices via Random Input and Output Encodings”, 2022 11th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, June 2022. Best Paper Award
	October 2022	J. Keller, S. Paul, S. Grijalva and V. Mooney, “Experimental Setup for Grid Control Device Software Updates in Supply Chain Cyber-Security”, North American Power Symposium (NAPS), Salt Lake City, Utah, October 2022. Best Paper Award
	July 2023	K. Hutto and V. Mooney, “Late Breaking Results: COPPER: Computation Obfuscation by Producing Permutations for Encoding Randomly”, Design

		Automation Conference, San Francisco, CA, July 2023.
Presentations	October 2, 2020	"GridTrust: Electricity Grid Root-of-Trust Decentralized Supply Chain Cyber-Security," Southern Company, Atlanta, GA
	December 30, 2020	"GridTrust: Grid Root-of-Trust Supply Chain Cyber-Security," Beckwith Electric Corp., Largo, FL
	March 10, 2021	"GridTrust: Grid Root-of-Trust Supply Chain Cyber-Security," Southern Company and Power Secure, Atlanta, GA
	January 26, 2021	"GridTrust: Root-of-Trust Briefing," Meeting for General Electric, Atlanta, GA
	April 13, 2021	"GridTrust Microgrid Meeting," Southern Company and Power Secure
	June 2, 2021	SECURE Program Description Sandia National Laboratory
	June 16, 2021	GridTrust Architecture Meeting Sandia National Laboratory
	June 8, 2021	"GridTrust: GridTrust Root-of-Trust Supply Chain Cyber-Security", CISCO
	September 22, 2021	Protect Our Power: GridTrust Framework
	March, 2022	"GridTrust: Grid Root-of-Trust Supply Chain Cyber-Security," Beckwidth Electric, Atlanta, GA
	June, 2022	"GridTrust: Grid Root-of-Trust Supply Chain Cyber-Security," POP Organized Webinar NRECA, Edison Electric Institute, MITRE, New York Power Authority, EPRI, Dominion Energy, Southern California Edison, NATF, Salt-River Project, APPA, Duquesne, PSEG
	May, 2023	"GridTrust: Grid Root-of-Trust Supply Chain Cyber-Security," Siemens, Atlanta, GA
Books	N/A	
Website	July 2023	https://mooney.gatech.edu/security/gridtrust/ A website has been developed that contains a summary of the project and access to the open-source distribution of GridTrust software.
Technology Transfer		
Draft (Georgia Tech Office of Technology Licensing) Patent Disclosure	June 2023	GTRC 9296 - Multi-Party Software Update Authentication Scheme with Physical Uncloneable Function for Operational Technologies Inventors: Vincent J. Mooney III, Santiago Grijalva, and Kevin Hutto

Copyrighted Material	N/A	
Licenses	N/A	
Other Products		
Databases	N/A	
Audio or Video	June 2023	GridTrust Demonstration Video 17-minute video detailing the GridTrust Demonstration Activities. This was presented to DOE during the final project presentation on June 30, 2023.
Software	December 2022	GridTrust Simulator A real-time discrete model simulation. It contains multiple classes, functions, I/O and supply chain attack simulation, and enables study of supply chain attack propagation and testing on how the GridTrust Technology will contribute to blocking attack attempts.
Software	July 2023	Open-Source GridTrust Software Package https://mooney.gatech.edu/security/gridtrust/ Georgia Tech has released the code for two exemplary implementations of GridTrust, a GridTrust Native Device and a GridTrust Interfacing Device, implemented and tested.
Educational Material	N/A	
Instruments	12/31/2022	GridTrust Benchtop Testbed (100% Development) Is an air-gapped local area network that contains software and hardware infrastructure to test the GridTrust technology. It includes computer servers simulating SCADA systems, control devices, and the GridTrust Box.
Equipment	06/30/2022	GridTrust Digital Substation (100% Development) Is an equipment rack that contains various protection relays, controllers and actuators including intelligent electronic devices (IEDs) to emulate cyber-security use case in digital power substations.

7 References

[1] S. Paul, Y. Chen, S. Grijalva and V. Mooney, “A Cryptographic Method for Defense Against MiTM Cyber Attack in the Electricity Grid Supply Chain,” IEEE Innovative Smart Grid Technologies Conference (ISGT), New Orleans, LA, April, 2022.

[2] B. Newberg, V. Mooney and S. Grijalva, “Open-Source Architecture for Multi-Party Update Verification for Data Acquisition Devices”, PECI: Power and Energy Conference at Illinois, Champaign, IL, February 2022.

[3] K. Hutto, S. Paul, B. Newberg, V. Boyapati, Y. Vunnam, S. Grijalva and V. Mooney, "PUF-Based Two-Factor Authentication Protocol for Securing the Power Grid Against Insider Threat", KPEC: Kansas Power and Energy Conference, Manhattan, KS, April 25th-26th 2022.

[4] J. Keller, S. Paul, S. Grijalva and V. Mooney, “Experimental Setup for Grid Control Device Software Updates in Supply Chain Cyber-Security”, North American Power Symposium (NAPS), Salt Lake City, Utah, October 9-11, 2022.