energies

MDPI

Article

Cybersecurity Considerations for Grid-Connected Batteries with Hardware Demonstrations

Megan Culler [1,2,*] and Hannah Burroughs [3]

[1] Idaho National Laboratory, Idaho Falls, ID 83415, USA
[2] Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61820, USA
[3] Lawrence Livermore National Laboratory, Livermore, CA 94550, USA; burroughs5@llnl.gov
* Correspondence: megan.culler@inl.gov

Abstract: The share of renewable and distributed energy resources (DERs), like wind turbines, solar photovoltaics and grid-connected batteries, interconnected to the electric grid is rapidly increasing due to reduced costs, rising efficiency, and regulatory requirements aimed at incentivizing a lower-carbon electricity system. These distributed energy resources differ from traditional generation in many ways including the use of many smaller devices connected primarily (but not exclusively) to the distribution network, rather than few larger devices connected to the transmission network. DERs being installed today often include modern communication hardware like cellular modems and WiFi connectivity and, in addition, the inverters used to connect these resources to the grid are gaining increasingly complex capabilities, like providing voltage and frequency support or supporting microgrids. To perform these new functions safely, communications to the device and more complex controls are required. The distributed nature of DER devices combined with their network connectivity and complex controls interfaces present a larger potential attack surface for adversaries looking to create instability in power systems. To address this area of concern, the steps of a cyberattack on DERs have been studied, including the security of industrial protocols, the misuse of the DER interface, and the physical impacts. These different steps have not previously been tied together in practice and not specifically studied for grid-connected storage devices. In this work, we focus on grid-connected batteries. We explore the potential impacts of a cyberattack on a battery to power system stability, to the battery hardware, and on economics for various stakeholders. We then use real hardware to demonstrate end-to-end attack paths exist when security features are disabled or misconfigured. Our experimental focus is on control interface security and protocol security, with the initial assumption that an adversary has gained access to the network to which the device is connected. We provide real examples of the effectiveness of certain defenses. This work can be used to help utilities and other grid-connected battery owners and operators evaluate the severity of different threats and the effectiveness of defense strategies so they can effectively deploy and protect grid-connected storage devices.

Keywords: battery; cybersecurity; cyber-physical security; distributed energy resource

Citation: Culler, M.; Burroughs, H. Cybersecurity Considerations for Grid-Connected Batteries with Hardware Demonstrations. *Energies* **2021**, *14*, 3067. https://doi.org/10.3390/en14113067

Academic Editors: Taha Selim Ustun and Suhail S.M. Hussain

Received: 7 April 2021
Accepted: 10 May 2021
Published: 25 May 2021

1. Introduction

The safe, reliable, and resilient integration of Distributed Energy Resources (DER) remains an ongoing challenge for utilities that they will continue to face over the coming years. Lawmakers across the United States and the world have set aggressive renewable or carbon-free energy targets [1]. DER, including solar, wind, and storage technologies, will be an important part of meeting these goals. In addition to planning for clean energy standards, there is growing concern in the electric utility industry about cybersecurity threats. While the electric grid is designed to be resilient against a variety of natural hazards, the threat of a coordinated attack on power grids remains as a difficult risk to categorize. Utilities and other stakeholders are aware of the possibility of an attack, but

attack vectors are hard to classify, and it is impossible to enumerate all threats or all potential consequences. The combination of these two challenges, DER integration and cybersecurity, presents a unique challenge to overcome.

DER with advanced inverters have the capability to provide additional services to the grid including voltage support, frequency regulation, and emergency islanding functions. Storage devices are uniquely positioned to be able to absorb or inject both real and reactive power on demand with almost negligible start up time, make them ideal to support some of these ancillary services. It also makes batteries well suited to support various smart grid operations such as aiding with the efficiency of distribution system voltage management [2–4].

These are all valuable functions that contribute to a more resilient grid, but the additional capabilities require increased connectivity and communications, creating more opportunities for adversaries to misuse these functions to create or aggravate instability in the grid. This increase in communications is common across many smart grid applications, and the potential attack surfaces will only continue to grow. Grid-scale batteries can operate in a variety of grid-following and grid-forming modes, which requires more management of sensor data and more communications channels. Adversarial manipulation of these channels could cause negative effects on power stability, such as instructing the battery to absorb reactive power instead of inject reactive power when there is low voltage on a line, pushing the voltage even lower rather than driving it back towards nominal levels. In addition to impacting power quality and stability, adversarial misuse of batteries could cause hardware faults or permanent damage to the device itself. It could also result in equipment damage and in extreme cases pose safety hazards.

Even if adversarial manipulation of the battery does not impact the stability of a system there are other potential economic consequences. Causing resources to be used or not used at critical moments can lead to lost revenue or increased costs for the battery owner in a variety of use cases including, participation in regional markets (now permitted by the Federal Energy Regulatory Commission (FERC) rule 2222), time-of-use bill management, increased PV self-consumption, demand charge reduction [5].

There are three steps to a successful attack on operational technology (OT) systems. The adversary must gain network access, the adversary must be able to manipulate the controls interface, and there must be some actual physical outcome of the attack. Many examples of ways to gain network access to industrial control system (ICS) networks have been shown [6–8]. As the industry looks for guidance on how to safely and quickly integrate grid-scale batteries, researchers have quickly filled the gap to theorize about different ways that the common smart inverter functions could be misused to cause instability in power systems [9–12]. Other researchers have focused on the communication side to theorize about how an attacker might compromise DER [10,13,14]. No existing work has shown with actual devices that these three steps can be tied together for energy storage systems.

While academic research has not shown a full-scale demonstration of potential impacts for grid-scale batteries, it is important to note that research has shown that smart inverters in general can be adversarially manipulated, and real-life events have shown that the pathways for adversaries to gain access do exist. In research, simulations are used to show voltages and frequencies can be manipulated by manipulating the power output from the inverter [12,15]. Most academic research assumes that the adversary has already gained access to the network. This assumption is not unfounded, as multiple high profile attacks have demonstrated that it is possible to gain access to industrial networks to execute cyber-physical attacks. In December 2015, an attack on a Ukrainian distribution company disconnected seven substations after gaining network access, causing blackouts for over 200,000 customers [16]. Another attack on the power grid occurred in Ukraine in 2016, this time using more advanced malware, demonstrating that even after an attack it was difficult to totally protect the industrial networks [17]. Shortly following these attacks was another that raised concern, the Triton (or Trisis) malware targeted controllers used in safety system for oil and gas [18]. While not targeted towards a power grid, it raises concerns about

the ability of a motivated attacker to gain access to critical systems and deploy malicious payloads. The combination of demonstrated cyber-physical attacks on industrial control networks, along with research showing that smart inverters can be used to cause instability, motivates the case for studying cybersecurity for smart inverters in more detail. To properly understand the risks, we perform in-depth analysis on grid-scale batteries.

In this work, we discuss the potential impacts of a cyberattack on a grid-scale battery, and present experimental demonstrations that show the network access, communications, and smart inverter function misuse aspects of a successful adversarial campaign. We focus exclusively on energy storage systems as DER. Batteries by nature have the ability to inject and absorb power, which allows us to consider the widest range of smart inverter functions. We show that if proper defenses are not in place, a motivated adversary can send messages to a controller even when some protocol security features are in place. We show that controllers can be manipulated if the proper limitations are not in place and that this can cause adverse effects, like local voltage depression. We discuss the properties of security features that can block attacks at numerous points along the attack and emphasize that proper configuration and implementation of security, both at the network and device level, are critical to protecting batteries.

The remainder of this paper is organized as follows: Section 2 discusses related works. We analyze all potential impacts of an attack on storage devices as a starting point for a risk analysis in Section 3. Section 4 describes our approach to evaluating the security of real grid-scale batteries. Results from the experiments are presented in Section 5. Additional defenses to protect against the triggers for the most damaging effects are discussed in Section 6. Discussion and concluding remarks are in Section 7.

2. Related Works

This work is not the first to study cyberattacks on DER, but it is the only work to our knowledge that explores all three steps of a successful attack, demonstrates the risks with real hardware, and explains proper defenses. Critical infrastructure, and specifically electric infrastructure, has been called out as an emerging area in cybersecurity [19–21]. Specific challenges like the prevalence of proprietary solutions and old hardware, growing connections to the Internet, and unique interdependencies have been identified [22], and the potential for significant disruption to society has been presented [23].

Network security for DER has been studied, but not specifically for grid-scale storage. A lot of existing work focuses on home storage devices, which can be treated like home Internet-of-Things (IoT) devices. Marques et al. [24] discuss security features that can be added to a control area network (CAN) communication channel for home batteries. Standard network security issues, like distributed denial of service (DDoS) attacks, transport layer security (TLS) setup, and man-in-the-middle attacks are explored and found to be feasible in many home battery systems [25]. Other work studies DER networks in more detail, assessing the impacts of latency in various parts of the network and proposing network-based defenses against possible attacks [26]. At the device access level, there has been work studying the requirements and different outcomes of attacks that compromise individual hardware, local area networks, or cloud-based networks [9]. The device level attacks can also be studied from a network stack perspective. A detailed analysis of key vulnerabilities for solar and wind controllers at the protocol level guides discussion for best practices for improving DER cybersecurity [27]. These studies are useful as a reference but do not specifically analyze grid-scale batteries.

Attacks specific to battery interfaces have also been proposed, but most of them focus on batteries in electric vehicles (EVs). Attacks on the instrumentation to create harmful effects were proposed [28]. Effects on the grid from the manipulation of EV batteries were also surveyed in [29], and some of the same security concerns could apply to grid-connected batteries, while others are specific to the vehicle-charger interaction at public charging stations, which does not apply to grid-connected batteries. Even neural networks

have been proposed to attack EV state-of-charge [30]. More potential attack vectors for EVs are discussed in [31].

The physical outcomes of cyberattacks against grid-scale batteries have been studied, but mostly against DER generically, rather than batteries specifically. Batteries are unique since they have charging and discharging functions as part of the standard usage, so our work contributes to the field by focusing specifically on these applications. Generic smart inverter functions and the ways they could be taken advantage of has been extensively researched [9–12,14]. These works focus mostly on risk assessments and simulations, not demonstrations of the actual effects of adversarial manipulation. Some research considers both attack paths and attack impacts for DER, which is valuable for considering the entire cyber-physical threat model [10,32]. A hardware-in-the-loop architecture for protecting DER and protecting grid power quality is proposed for individual and heterogeneous mixes of DER [33,34]. Our work is unique in discussing threats and security measures for grid-scale batteries, rather than generic DER security, home IoT batteries, or electric vehicles.

Beyond adversarial manipulation of DER control functions, there has been research that studies other traditional cyberattacks that can be executed against DER and smart grid systems. In addition to compromising networks to send unauthorized commands to a DER, attacks may also compromise the data output from the battery device. False Data Injection (FDI) attacks have been proposed both to manipulate the data coming from the DER and used to make area-wide decisions and to manipulate the data used for the DER control functions to make their operation unstable [35–39]. In [40], authors assess the impact of FDI attacks on DER with communication networks built on IEC 61850 GOOSE messages. They use Hardware-in-the-Loop (HIL) and real-time simulations to demonstrate their attack. Replay attacks, a more specific type of FDI attacks, can also be used to fool the inverter control system and create instability [39,41,42]. Advanced methods for detecting anomalous data in DER systems have also been proposed [43]. Another class of attacks to consider is denial-of-service (DoS) attacks. These attacks have also been shown to create instability in smart grid systems [39,44,45]. Some attacks require physical proximity to the target and achieve DoS by a side channel attack [45], but targeting communication nodes is more common [44,46,47]. In this work, we focus primarily on attacks that aim to manipulate the controls of a grid-scale battery, as this kind of attack fits with the most impactful real-world attacks seen over the last 5 years.

Defenses to protect against cyberattacks against DER have been proposed. In [32], detection and mitigating measures at many levels are considered, including the cyber layer, physical layer, and utility layer. Detailed protocol and communications security for DER applications is discussed in [10]. DER and smart inverter functions can even be used to help detect broader attacks on the power system [48]. Advanced methods of cybersecurity traditionally applied to enterprise can also be adapted to DER environments [49,50]. These methods have been found to only minimally increase latency [51]. General best practices for securing DER networks are discussed in [10]. Our study builds on these works by discussing the security benefits of using protocols with security features like authentication, as well as showing in real implementations where bounds checking needs to occur.

3. Grid-Connected Battery Risk Assessment

In this section, we will discuss potential impacts of adversarial manipulation of a grid-scale battery. The purpose is not to raise undue alarm about the security of batteries, but rather to look at potential impacts from a risk perspective, so that we may mitigate the largest risk factors.

3.1. Power Grid Impacts

One concerning effect of the misuse of grid-scale storage resources is the impact on the stability or reliability of the connected power system, whether that is a microgrid, distribution system, or even transmission system using large batteries. All potential consequences will depend on the configuration the battery and the configuration of the

grid elements around the battery. The battery will have a much larger (positive and negative) potential for impact when there are few other sources that can quickly inject or stop injecting power. The impacts will also depend on the protective devices that are installed and the sensitivity of these relays and breakers. The following are the worst case scenarios of potential grid impacts and the actions that an attacker would need to cause them. Otherwise, stronger sources and devices will correct the attempted attacks before they cause an adverse impact, or protection devices will trip to isolate the affected portions of the grid before runaway instability occurs.

3.1.1. Grid Over-Voltage Event

Reactive power and voltage are tightly coupled in power systems. In many cases, it may be desirable to have the battery absorb reactive power or activate a lagging power factor when the voltage is high, as this will drive the voltage back to nominal levels. In fact, distribution systems with high solar penetration are known to sometimes have high voltage issues during high energy generation times of day [11,52]. Using battery inverters has been shown in practice to be effective for over-voltage events. [53,54].

A grid over-voltage event can occur if a storage device was expected to provide reactive power support, but fails to do so. If the battery is unable to correct the abnormally high voltage the battery will eventually disconnect [55], and the high voltage event may cause other equipment to trip as well.

Direct manipulation of the reactive power mode on the battery can be used to directly stop any reactive power from being absorbed, which means over-voltage events will not be corrected by the battery. On the extreme side, an adversary may set reactive power to max injection, driving up the local voltage. In the right scenario, lowering the power factor may be used to decrease the relative amount of reactive power that can be absorbed. With a power factor of 1, no reactive power would be injected or absorbed, and if acting in this mode, the battery would be unable to support an over-voltage scenario.

Another way to create this effect would be to deactivate Volt-VAR mode so the system does not respond dynamically to rising voltages, or to change the setpoints on a Volt-VAR curve, either by making the curve flat to prevent any response, or, more aggressively, by inverting the standard curve to make the battery inject reactive power during an over-voltage event.

3.1.2. Grid Under-Voltage Event

Like the previous case, reactive power support from a battery can be used to support the grid during an under-voltage event, namely by injecting reactive power [53,56]. If a grid operator expects the battery to provide this support, then the simple lack of support could cause the under-voltage event to reach tripping thresholds. Alternatively, a cyberattack could cause the battery to absorb reactive power, causing or aggravating a low voltage event.

Like the previous example, direct manipulation of the reactive power output can help create this scenario. The more obvious attack is to disable or modify the support provided by a Volt-VAR mode, where reactive power output is dynamically controlled in response to the local voltage.

3.1.3. Grid Over-Frequency Event

Active power and frequency are coupled in the power grid, which means that changes to active power output from the battery can affect the frequency in cases where the size of the battery is large compared to the overall size of the connected system. This property can be used for frequency regulation [57–59]. The value of using storage systems for frequency regulation has been demonstrated in practice in an isolated power system, in New York state, and in Puerto Rico [60–62].

If frequency is high, the battery can absorb real power to drive the frequency down to nominal levels. However, if this function is blocked, or if the battery responds by injecting

real power instead of absorbing it, the over-frequency correction does not occur properly and the over-frequency event can be exacerbated. This can cause local components to be out of sync with the local electric power system frequency, which could damage equipment or trip breakers.

An adversary that has access to a battery can manipulate real power output in a variety of ways. They can directly modify real power output commands to stop real power from being absorbed. They can set real power to maximum injection to drive up local frequency. They can set charge rates or real power ramp rates to very low values so the battery does not absorb power quickly if an over-frequency event occurs. They can directly disable frequency support modes, if available. They can modify frequency support bands so that frequency must rise even higher before corrective actions are taken. They can modify watt-frequency setpoints to flatten the curve and decrease the amount of real power that is absorbed in case of an over-frequency event. The extent of the effect of these actions would depend heavily on the inner mechanisms of the controller and the strength of the connected system.

3.1.4. Grid Under-Frequency Event

As in the previous case, real power can have an impact on global frequency. If frequency is low, the battery can inject real power to drive the frequency up to nominal levels. However, an adversary may try to block this function to create or exacerbate an under-frequency event. The same methods as described above could be used to trigger or amplify an under-frequency event.

While typically the bulk of a system contains sufficient inertia to keep frequency within a tight band, expanding penetration of distributed generation sources, including batteries, results in less physical inertia of the system and creates the possibility for local systems to operate in an islanded mode. In both of these scenarios, frequency regulation is a harder problem to solve [63]. If a large battery compared to system size does not provide the support required in an under-frequency scenario, loads may need to be shed to prevent the system from collapsing [64]. An adversary could potentially trigger a load-shedding event by forcing a battery to absorb enough real power to drive the frequency down, a scenario that is possible in a microgrid or other system where the battery represents a large enough portion of generation capacity.

3.1.5. Grid-Forming and Microgrids

When a battery system is in grid-forming mode, its control objective is to maintain system voltage and frequency and it adjusts its real and reactive power output to maintain stable voltage and frequency [65,66]. As the loads that it is serving change, feedback loops determine the amount of power output required to meet these setpoints.

If an attacker is able to modify the frequency setpoint, frequency droop parameters, voltage setpoint, or voltage droop parameters, they may be able to prevent the island from working as it should. Providing power at undesired voltages and frequencies could damage equipment or loads that are not designed to operate at these levels. Modification of grid-forming parameters can also effect power sharing and stability of islanded power systems with multiple sources. Alternatively, an attacker could modify the mode that the system is operating in, directly preventing it from supporting an islanded system.

From a risk perspective, it is currently uncommon to have a large islanded system powered only by grid-forming storage devices, therefore the consequences of compromising the grid-forming functions are low. However, if the grid-forming storage device is used in a microgrid that supports critical operations, the impact for those stakeholders could be meaningful.

3.2. Battery Hardware Impacts

Lithium-ion (Li-ion) batteries, the most commonly used technology for grid batteries, were developed in the 1980s, and the first commercial Li-ion battery was released in

1991. They have the advantages of the non-memory effect, high working cell voltage, low environmental pollution, low self-discharge rate, high power density by volume, and high specific energy and energy density [67]. These qualities make them well suited for deployment in electric grids. However, the voltage, current and temperature conditions for charging and discharging Li-ion batteries must be carefully controlled to prevent damage to cells. In the most extreme scenario, cell damage can lead to thermal runaway and fire.

3.2.1. Thermal Runaway

Thermal runaway occurs if cell temperature exceeds a critical temperature, above which the increase in temperature is irreversible. The cell may emit gases from the degradation reactions on the way to thermal runway, which can sometimes be seen as smoke. It is these gases that may cause cell ignition and combustion [68]. Heat generation inside the battery is mainly caused by charge transport and chemical reactions during normal charging and discharging. A fire study by the National Fire Protection Association (NFPA) on one type of commercial-scale Li-ion battery found that thermal runaway could be induced by high temperatures, but did not find evidence of explosions in their study [69]. No existing work points to grid-connected battery fires being triggered by cyberattacks, but it is good practice to identify all possible consequences, however unlikely, as part of a threat assessment.

3.2.2. Cell Degradation

There are two main processes that can cause cell degradation, which shortens the lifetime of the battery. The first is the growth of the solid-electrolyte interphase (SEI) layer at the graphite anode and the second is lithium plating [70]. An attack that aims to overcharge the battery causes an increase in the SEI growth rate and an increase in internal resistance. This increase translates to decreased capacity and shortens the lifetime of the battery. In [70], the authors find that an attack that lasts one hour after charging could shorten the lifetime of an EV battery to about 200 days at an overcharge voltage of about 0.4 V. If this type of attack were made more extreme and enough Li-plating occurs, the battery could experience thermal runaway. This attack has not been demonstrated for grid-storage batteries, but if another attack vector could cause overcharging, a similar process of degradation is likely. If an attacker can modify the upper cut-off voltage, then the pack can be charged at a higher voltage than normal charging voltage, which causes overcharging. This cannot typically be done through an externally-facing operator controls interface, but may be exploited though other hardware side-channels.

If the lower voltage cutoff is reduced, the battery pack can be overdischarged. During overdischarge, the anode potential increases abnormally and the SEI layer decomposes, which is followed by the dissolution of the copper ions from the current collectors, which creates the possibility of internal shorts [71–73]. The dissolution of copper can begin within hours, depending on the amount of power drawn during overdischarge, and eventually leads to the deposition of metallic copper. In addition, Li-ion batteries connected in series are more prone to be overdischarged [74].

The consequences of this attack could range from loss of energy to internal short to thermal and safety events. Researchers have showed that battery-draining cyberattacks on EVs are possible [74,75] by compromising other systems in the vehicle, but no similar attacks have been shown for grid-connceted batteries, and those same side-channel attack paths are not present in power systems. These attacks are significant because EV batteries and grid batteries have similar components. However, the attack paths would need to be modified for these attacks to have any effect on grid-scale storage devices.

3.3. Economic Impacts

Grid-connected batteries can provide a variety of economic benefits depending on where and how they are deployed. The Rocky Mountain Institute has identified 13 services that DER can provide that have an impact on three primary stakeholders: Independent

System Operators (ISOs)/Regional Transmission Organizations (RTOs), utilities/grid operators, and customers [76]. Their report details the values of these services. From an attacker's standpoint, this study and others like it can be used to help the attacker choose how to manipulate the grid-connected battery so that the stakeholders receive the least benefit or additional costs. From a defender's perspective, the same analysis should be conducted to determine when services are most critical and ensure that these services are well protected.

3.3.1. Utility-Scale Battery Assets (ISO/RTO and Utility Services)

ISOs and RTOs are responsible for the operation of the electricity transmission system and oversee both energy and ancillary services markets in their respective regions. Battery storage systems can participate in these markets.

- Frequency Regulation and Voltage Support: To prevent a utility or system operator from realizing the benefits of frequency regulation or voltage support provided by a battery the attacker can disable the feature used to provide this support or disable the battery entirely at specific times when these support features are needed.
- Spin/Non-spin Reserves: Taking advantage of stored energy in a battery at the right time, particularly in times of peak load, can prevent spinning reserves from having to be started. Instead, the battery is used as the reserve generation source. Unlike conventional spinning reserves, batteries require minimal start up time and do not require as much energy to keep them in a standby mode. An attacker could prevent batteries from being used as reserves by draining them and keeping them at minimal state-of-charge (SOC).
- Black Start: To prevent batteries from being used in black start an attacker can send a malicious command to keep the battery at a low SOC, or intercept the black start commands when they are sent.
- Distribution and Transmission Deferral: These services allow utilities to delay, reduce the size of, or completely avoid investments in upgrades to the distribution and transmission systems respectively, which would otherwise be required to meet projected load growth in certain areas of the grid. If attackers manipulate batteries to make them appear unreliable or spoof data that makes the batteries' lifetimes look shorter, then it many not be economic for utilities to delay the upgrades to the systems.
- Transmission Congestion Relief: ISOs charge utilities to use congested transmission corridors during certain times of the day. Deploying batteries downstream of these corridors can prevent the need to use the corridors and reduce congestion. If an attacker can manipulate the battery to maintain a low SOC or reach a low SOC at a peak-demand time of day the utility may be forced to use the transmission corridor and incur increased costs.

3.3.2. Consumer-Owned Battery Assets

- Time-of-Use Bill Management: In some regions customers may select a time-of-use billing structure where electricity rates change based on time of day. Batteries can be utilized to reduce the overall bill by offsetting load at high cost times of day by discharging and by re-charging at lower cost times of day. If the attacker prevents the battery from being used when it is most advantageous, the customer's savings will decrease. In the most extreme case the battery could be used to increase load during high-price times to increase the customer's bill.
- Increased PV Self-Consumption: In some regions, such as Hawaii, there are regulations prohibiting or limiting power exported from a home with a DER (like solar) [77,78]. In these locations residential solar PV is often installed with a battery so that any time the customer's solar PV power output exceeds their local load the excess power can be utilized to charge the battery rather than being curtailed (to prevent violation of non-export rules). The battery can later be discharged to provide power to the customer's loads when PV power is not sufficient. An attack that prevents the battery

from charging when solar PV output exceeds local loads could at worst cause the customer to violate the non-export regulations. If export regulations are not violated and PV is successfully curtailed the customer faces an increased cost of electricity as they will have to purchase electricity later the day that could have otherwise be provided by the battery.

- Demand Charge Reduction: All electricity customers are charged by their utility or power provided for the amount of energy that they use each billing period in kilowatt hours (kWh). However, for customers with loads over a certain threshold, utilities will often include a 'demand charge' in their billing structure. A demand charge is a per-billing-period fee which is proportional to the peak power demand, in kilowatts (kW), that customer uses over the entire billing period. Batteries can be discharged at high load times and recharged at low load times to reduce the overall demand charge. If an adversary prevents the battery from performing this function during just one high load time during the billing period, then the cost savings will be forfeited.
- Backup Power: Batteries with grid forming capabilities have the ability to provide backup power if the main electricity grid is unavailable. To take advantage of this value, the battery needs to have a sufficient stored energy when it is needed for backup. This value is eliminated if malicious commands are sent to the battery to keep it at a low SOC.

4. Materials and Methods

The potential outcomes and impacts of a cyberattack on a grid-connected battery have been described in the previous section. With the exception of battery hardware effects, an attack class that requires overriding internal safety checks, all of the other outcomes could be achieved by manipulating legitimate battery functions. The battery hardware effects attacks would require much more time and resources to develop and likely require physical access to exploit. However, attacks that only require manipulation of normal control functions may be more accessible remotely and through legitimate interfaces. We therefore focus our defense analysis on this class of adversarial manipulation.

There are two levels of defense which we consider. The first is protecting protocol security, exploring what security guarantees can be provided by protocols themselves for authentication and integrity. The second is protecting the controller interface from malicious manipulation of the behavior of the battery.

4.1. Protocol Security

Many batteries are equipped to work with multiple protocols in order to ensure compatibility with many systems. Most industrial protocols, like Modbus, DNP3, or CAN, do not provide built-in security features, like authentication or encryption. Even as the need for secure communications in industrial networks in critical infrastructure is recognized, the need for backwards compatibility and continuity across many systems may continue to drive the use of insecure protocols. When more security features are available, it may be possible to select settings to require that these features be used. However, it may also be possible to use multiple protocols simultaneously without locking in the security features.

We test whether the controller can simultaneously respond to multiple protocols by logging data and sending commands with a more secure protocol while sending contradictory commands via Modbus. We verify if the Modbus commands are accepted by the controller by monitoring the data collected via the secure protocol.

There are two security features that can be provided by an industrial protocol that we explore, token authentication and certificate authentication. When tokens are included in a request, the server may be authorized to give access to certain resources. For the client to verify the authentication of the server, certificates are used. A client verifies a server according to its certificate and the server identifies that client according to a client certificate (so-called mutual authentication). While the roles of these features seem similar,

note that the token grants a certain level of access to the user, and certificates are used to verify identities.

We tested the different levels of security that were added by tokens and certificates independently and together. We verified if the controller rejected messages when these features were enabled but not properly configured, or required but left out.

4.2. Controller Interface Security

If we assume that the adversary can send a syntactically correct, appropriately authenticated message, then we want to know how the adversary could misuse the interface to cause physical and measurable effects to the battery or the grid, as well as what can be done to stop this. Here, we explore the misuse of two common modes: real or reactive power setpoints and Volt-VAR mode setpoints and show how engineering controls can be effective at protecting against the most damaging effects. While it is feasible to test other types of attacks, such as those that have been proposed in related works discussed in Section 2, by showing the feasibility of adverse affects using common modes with real hardware we can infer that more complex adverse mode changes are also possible.

The real and reactive setpoint attack tests the ability of an adversary to directly change the real and reactive power output of a battery. While manipulation of real and reactive power output could be accomplished by manipulation of many modes, we focus on the most simple, and leave demonstrations with other modes to future work. We test whether an adversary can send commands to change the direct power output to values beyond the battery's capacity or beyond the documented limits for power output with and without software controls in place. We also explore how engineering software limits can keep output within certain bounds.

The Volt-VAR setpoints attack tests the ability of an adversary to change the setpoints for a voltage-support curve. This scenario starts by forcing the local voltage to a value below nominal. We attempt to change to different Volt-VAR setpoints and monitor the effects on the local voltage. Both benign (normal) and adverse setpoints are tested. We also test the documented limits for the curve setpoints.

For both of these attacks, we carefully monitored the self-reported status and actual behavior of the device via an external power meter. The alarm logs showed what issues were self-reported by the battery. We measured the severity of the attack and examined any indication that may alert an operator to the attack.

4.3. Experimental Setup

For these experiments, we developed custom programs to interface with the battery controller. All programs were developed in Python 3.8.4 (Python Software Foundation, Fredericksburg, VA, USA). The primary interface was created with authentication features enabled. This was intended to emulate a secure operational deployment of the battery.

One program acted as a historian. The historian communicated using tokens and certificates and polled different system status messages at different intervals based on the expected changes in the data. Power output data was polled at a frequency of 10 Hz. System status data was polled at a frequency of 1 Hz. Mode status, not expected to change often, was polled every 5 min. General configuration and system information was logged at the start of every trial. This information was logged to a SQLite database.

We also developed a controller to send commands that changed settings. The command-line interface allowed the user to specify a mode and the desired changes. If the format did not match the expected format, the command was rejected. The controller also checked the command against the bounds for each mode and returned an error if it was outside the allowed limits.

Finally, we also developed a limited Modbus controller. The primary purpose was to emulate an adversary with the intention to circumvent authenticated protocols. This controller had the ability to send any of the commands that the authenticated controller

was capable of. It did not log any data. The inverter checked the bounds of any proposed setting changes.

For the tests, the battery, which operated at 480 V AC, was grid connected. The wiring and communications setup is shown in Figure 1. The battery had a maximum power output of 111.5 kW and it was configured to operate at 60 Hz. There was bi-directional power flow through the building power connection (both charging and discharging the battery). In addition to the values reported by the battery controller, an external power meter was used to verify the output of the battery.

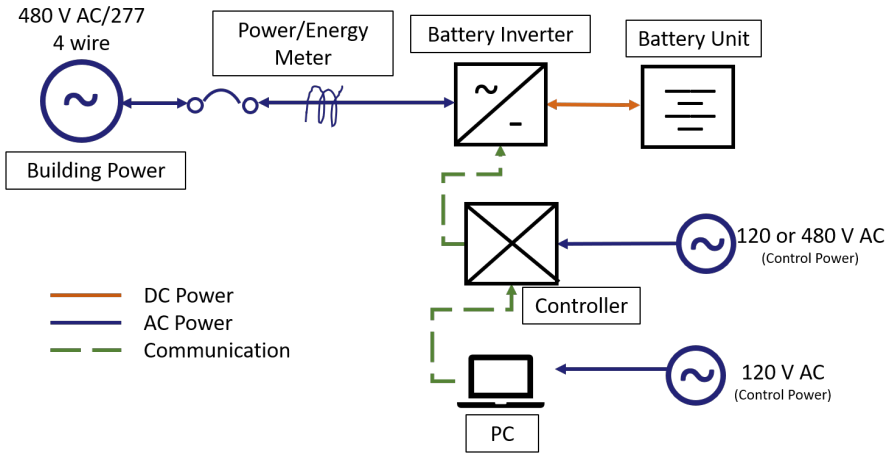

Figure 1. Hardware setup for grid-connected battery tests.

5. Results

5.1. Protocol Security

5.1.1. Circumventing Authentication

Although the system was configured to work with tokens and certificates, and in theory this meant we could use the system as a secure and authenticated system, these features may not have been required to successfully send messages. The system was also outfitted to communicate via simple Modbus. If an attacker was able to craft their own Modbus packets spoofing a valid source and send them on the correct communication channel, the battery controller would accept these commands, assuming authentication features were not locked in.

During testing, a historian using certificates and tokens was used to poll data. The Modbus control interface was used to send commands to change the real power output while the historian was running. We found that the commands were accepted by the battery controller while it was simultaneously responding to the historian's requests for data. The same was possible for direct reactive power output manipulation. This shows that an authenticated and unauthenticated protocol can be used together. Notably, five events were logged by the historian as seen in in Table 1, but nine total events appeared in the power data logged, seen in Figure 2. Those four additional commands were sent via Modbus, stealthily evading record by the authenticated historian. While this input can still easily be detected in the power data logged by the historian, if an adversary sent an unexpected command, it might be difficult to quickly evaluate why the power output was changing.

Both commands that send data and commands that request data were accepted via Modbus, even as the authenticated historian and control programs were also interfacing with the controller. This circumvents any protections afforded by the certificates and tokens, unless there is a way to tell the controller to only accept authenticated messages. One simple way to do this is to make sure that traffic passes through a firewall and only allow packets sent to the battery to pass if they are using the preferred, secure protocol.

Enforcing the use of the authenticated protocol could also be accomplished during setup and installation.

The only way to diagnose this attack would be to monitor the parameter stating the current command source, which is available from the controller. It changed back and forth during these tests depending on what the source of the last received command was. However, depending on the timing of the commands sent, if this parameter was not logged frequently it might not be evident that a Modbus source was also communicating with the controller.

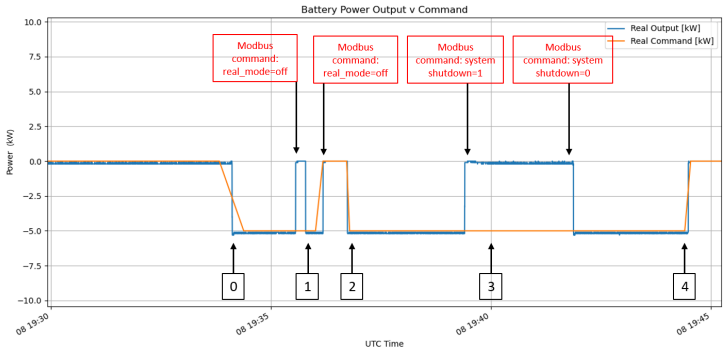

Figure 2. The real power outputs follow the Modbus commands even while being polled through the authenticated interface.

Table 1. Event log captured via authenticated interface while Modbus commands were sent. Indices correspond with authenticated controller events labeled in Figure 1.

Index	Time	Mode	Message
0	19:34:05.055	real power	Submitting: {“power”: −5000}
0	19:34:05.133	real power	Changes accepted
1	19:35:47.070	real power	Submitting: {“power”: −5000}
1	19:35:47.117	real power	Changes accepted
2	19:36:43.934	real power	Submitting: {“power”: −5000}
2	19:36:44.023	real power	Changes accepted
3	19:40:03.180	real power	Submitting: {“power”: −5000}
3	19:40:03.243	real power	Changes accepted
4	19:44:28.617	real power	Submitting: {“mode”: “off”}
4	19:44:28.726	real power	Changes accepted

5.1.2. Probing Authentication Features

The addition of any authentication can be seen as an improvement on the traditional unsecured industrial protocols typically used in power grid applications. We configured the authenticated interface to use both tokens and certificates, and verified that communication worked as expected when the correct token and certificate were used for reading and writing data. We were able to successfully make the battery charge and discharge at different power levels, turn on and different ancillary service modes including Volt-VAR mode. We verified that these mode changes were logged by our authenticated historian. We also verified that the power outputs logged by the battery matched the recordings from the external power meter.

First, we evaluated the benefits added by tokens, which were supposed to make sure a client only had access to resources for which they were approved. We changed a single bit in the token and tried to send both read and write requests. Both requests returned with error messages, signaling that valid tokens had to be used to communicate with the device. Next, we tested the response of the system when no token is included where expected. There were errors raised by the system when write attempts were made, but

read requests were successful without the token. Tokens could therefore protect the system against command-spoofing attacks if the adversary did not have access to the secret token. Although data could be read, it was unlikely that this information could tell an adversary much more about the system then what they would already know if they were at a point where they could intercept the messages. The integrity of the system remained protected.

Next, the token was reintroduced correctly, and the security benefits added by certificates were evaluated. We chose the wrong certificate to send both read and write requests. When starting a new session, both types messages are rejected and an error was returned. However, if a session was already started using the correct certificate, the read requests returned with the data and the write request successfully changed a parameter when a new request was made with the wrong certificate. This is standard behavior for certificates. They are only used to verify identities at the beginning of a session, so if there is a session hijacking attack, the protections provided by a certificate may be evaded. Changing the session cache or timeout process could mitigate this risk. Certificates can certainly offer some protections, but it is important to note that they must be configured correctly to offer full protection. System operators should note the threat of session-hijacking attacks and ensure that if they are expecting additional protections from certificates they have configured their system to require valid certificates for every request.

We tested the response of the system when no certificate was present. There was an error raised for both read and write requests, and the requests were unsuccessful. This implied that the requirements for certificate presence to start a session were strong, and adding this feature added security to the communications. However, this feature could also be evaded if not configured properly. If the packet was crafted with SSL verification explicitly disabled and the certificate left out, both read and write requests were successful. There was a warning raised stating that there was an unverified request being made and that adding certificate verification was strongly recommended, reminding users that this authentication feature was being bypassed. In this case, there was no authentication provided by the certificate, making the communication more like Modbus. If there is intent to use these security features, engineers should ensure that the proper use of the features is enforced.

Tokens and certificates can both add security to command interfaces, helping ensure that unauthorized users cannot access live data or send commands to the controller. Tokens were found to be powerful protections against unauthorized writes. Certificates, when correctly configured and required for each new message, were found to protect against both unauthorized read and write requests. Both features are valuable, but care should be taken to make sure that they do not provide a false sense of security. Operators should ensure that the features are implemented correctly and required for all requests. The use of multiple security features together, i.e., requiring both tokens and certificates, adds layers of security making it even more difficult to spoof commands without access to privileged information.

5.2. Interface Security

5.2.1. Real and Reactive Setpoints

We previously showed that it is possible to configure the system to accept real power commands from properly configured authenticated interfaces and from a separate Modbus source simultaneously. This represents a significant ability that could help an adversary achieve many of the impacts discussed in Section 3. Namely, the ability to control the real and reactive power output gives an adversary the ability to manipulate the SOC. When out-of-band adversarial changes are made, the change is not logged by the historian, but it is not totally hidden. The power setpoint parameters change, and the power output can be monitored via the battery controller and external power meters. Even if the controller's data output could be compromised, the external power meter would be an independent sensor available to measure and communicate the changes.

We found that the controller accepted power setpoints above the documented maximum power output of the battery. Although the battery limited its output to the true

maximum power output, this could be dangerous depending on the system configuration. If the hardware connecting the battery to the grid is rated to handle the maximum power output of the battery this does not present a concern. However, if the interconnection equipment is undersized and is relying on a software-based limit to prevent overloading, then sending maliciously large power commands could result in tripping the breaker which connects the battery to the undersized equipment. An example of this is shown in Figure 3. The real power output was set to 1010 kW. The actual power output reached a maximum of 111.5 kW, which is the listed maximum power output of the battery. If the intent was to operate only to a maximum of 80 kW, software side checks should be introduced to enforce this. These checks would protect against adversarial changes as well as accidental keystrokes.

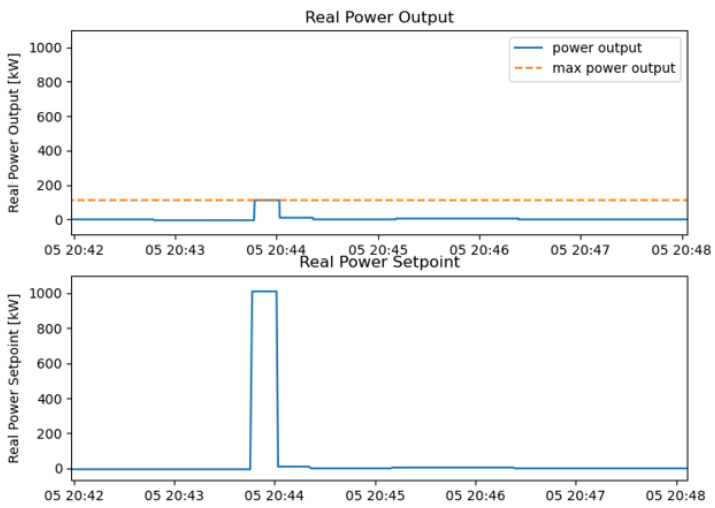

Figure 3. The real power output was set to 1010 kW, far above the 111.5 kW maximum power output.

This experiment reinforces that it's important to use software-side controls specific to the system configuration even when physical limits will stop the battery from exceeding its own safety limits. Documented limits should be carefully tested, and if they are not enforced or proper for the system additional controls should be added.

5.2.2. Volt-VAR Setpoints Attack

The Volt-VAR mode allows for a curve to be specified where reactive power output changes based on the measured local voltage. An adversary can shape the curve arbitrarily, potentially creating a curve that is inverse from a typical support mode. Traditionally, Volt-VAR mode supplies reactive power when the voltage is low and absorbs reactive power when the voltage is high. Setpoints far enough outside the traditional curve have the potential to have adverse effects, as discussed in [79].

Figure 4 shows the results of experiments with the Volt-VAR curve setpoints. Region I shows a mild attack, where the Volt-VAR curve was set to a inverse curve with a maximum of 20% of rated reactive power injection/absorption. Region II shows a more extreme attack, where the Volt-VAR curve was inverse with a maximum of 40% of rated reactive power injection/absorption. These regions showed the adverse effects of the attack; the voltage was depressed instead of raised and reached a minimum voltage of 0.965 p.u.

Region III shows the effects from a traditional Volt-VAR curve. This correctly configured curve brought the voltage back to 0.99 p.u. The difference between Region II and Region III shows the strength of the attack. More extreme attacks are possible, but not demonstrated here. Region IV serves to show what the baseline voltage was without any reactive power support. The baseline low voltage was 0.98 p.u. This clearly showed that the adversarial Volt-VAR curves in Region I and II moved the system away from the desired

state. However, in this experiment the voltage stayed well within the normally allowable range of 0.95–1.05 p.u. Engineering controls, as proposed in [79] could be used to prevent the setpoints for Region I and II from being accepted by the controller.

The adversarial changes to battery setpoints showed that destabilizing effects were possible. The control over real and reactive setpoints gives the adversary near arbitrary control over the battery output. With this ability, many of the adverse impacts described in Section 3 were possible. The effects on grid stability and the economic impacts were more feasible through changes to the battery modes. The potential for adverse manipulation of ancillary service modes was shown through the manipulation of the Volt-VAR curve. We showed that adversarial setpoints could move system voltages further from nominal and desirable values. This experimental setup with real hardware demonstrated the feasibility of a more complete attack path, and revealed the security features that offered the most protection.

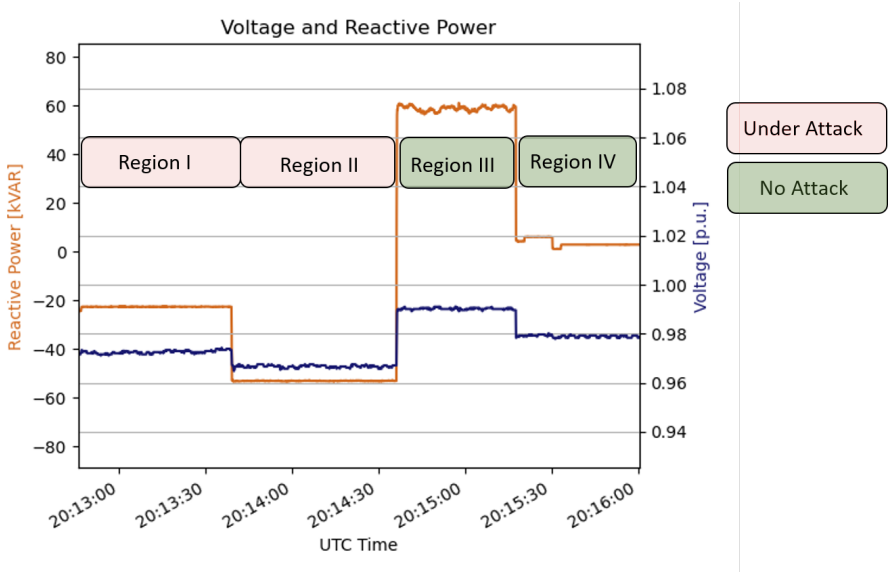

Figure 4. The adverse affects of a malicious Volt-VAR curve are shown in Regions I and II. Region III shows the effects from using a traditional Volt-VAR curve. Region IV shows the system voltage with no reactive power support.

6. Defenses

In light of the specific findings of our experiment, there are a few defenses that would be most valuable to mitigate the effects that were demonstrated. It is desirable to stop an attack before it even reaches the battery controller, in which case network protections are needed. It is also desirable to ensure that all aspects of the controller interface are implemented correctly and provide the safety checks that are expected. Certain engineering controls can also be useful for limiting setpoints to ranges that are not expected to have adverse system effects. These defenses are discussed in more detail in the remainder of this section.

In order to force the system to use the protections provided by authenticated protocols, a firewall can be used to filter out messages that are sent via unauthenticated protocols, like Modbus. It is also desirable to filter packets via their source IP addresses. It is not a huge burden to an attacker to spoof a source IP if they are inserting new traffic on the wire, but all of these protections can help raise the cost of an attack for an adversary. Manufacturers and operators must still ensure the tokens and certificates are properly configured and used. A related defense mechanism could be to accept commands only from the authenticated interface, when it is in use, which would prevent attackers from exploiting an unauthenticated protocol like Modbus.

At the controller level, designers should ensure that all documented limits are properly enforced. We found examples of setpoints that did not have the stated limits enforced, most notably the real and reactive power limits could be set to an arbitrarily large value, positive or negative. In this scenario, the battery tried to meet this value by maximizing its output. On its own, this is not a bad thing, but it is something that operators should be aware of. Reasonable limits should be enforced by the controller, documented by the controller designer and reviewed and verified by the system owner or operator.

In addition, there were certain control parameters that should have had limits enforced that did not. An example of this is the Volt-VAR curve, which could be successfully inverted from a normal support curve to produce destabilizing voltage effects. It is preferable to enforce the limits at the controller level, but it may also be possible to enforce limits outside of that, for example by performing deep packet inspection with system awareness. A control program can be used to perform these checks as well, but there is no guarantee that the adversary will use the internal system program. They may instead use out of band channels and custom craft the control messages themselves.

7. Discussion

As the U.S. grid makes the transition towards cleaner energy, grid operators will have to confront the challenges of integrating new technologies. Grid-connected batteries will be a key part of making solar and wind energy more resilient as combined systems, and they have the potential to perform key grid stability functions, like providing ancillary services. However, security concerns for batteries in particular have not been well studied.

In this work, we presented an in-depth review of potential risks for battery systems. We noted that the wide range of impacts on power quality and economic operation could potentially be accomplished by manipulating standard functions of battery controllers. The major differences were only in how the adversary would change the battery output to cause different targeted outcomes. Additionally, the chemistry of battery technology lends itself to potential safety hazards that could have lasting effects. Though attack paths for this outcome are more complex, similar concepts have been successfully demonstrated for EVs, so it is a valid consideration for battery risk assessments.

With the finding that many adversarial outcomes could potentially be accomplished by manipulating standard functions of a battery controller, we performed novel experiments to show how the controller functions could be compromised, and how they could be protected. The experiments started by examining standard industrial network protocols, and security features that could be added to them, in order to understand the challenges that an adversary would face in order to gain access to the controller. The results showed that standard authentication features had the ability to protect both the integrity and confidentiality of the system when used correctly. Even stronger protection was possible when security features were layered on top of each other. If weak or no security features were used, it was possible for an adversary to access the controller interface. We demonstrated adversarial manipulation of battery features, including arbitrary charge or discharge, or malicious setpoints governing ancillary services. These brief demonstrations show the potential for a wide range of possible outcomes. For example, manipulation of real power output is one way to control the battery SOC. We studied the impact of successful interface manipulation, and proposed engineering controls that could limit any negative effects should an adversary gain access to manipulate the battery functions.

Author Contributions: Conceptualization, M.C. and H.B.; data curation, M.C.; formal analysis, M.C. and H.B.; investigation, M.C. and H.B.; methodology, M.C. and H.B.; project administration, H.B.; resources, H.B.; software, M.C.; supervision, H.B.; validation, H.B.; visualization, H.B.; writing—original draft, M.C.; writing—review and editing, M.C. and H.B. Both authors have read and agreed to the published version of the manuscript.

Funding: This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344 and by the Idaho National Laboratory under Contract DE-AC07-05ID14517. The work was supported by the U.S.

Department of Energy's Grid Modernization Laboratory Consortium. The Lawrence Livermore National Laboratory document number is LLNL-JRNL-819902. The Idaho National Laboratory document number is INL/JOU-21-61817.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to proprietary nature.

Acknowledgments: The authors would like to thank Emma Stewart and Virginia Wright for their extensive support and leadership of this project. They would also like to thank Kurt Myers, Porter Hill, and William Parker for their support in the laboratory, and Tim Yardley for support with initial API development. Finally, they would like to thank Scott McBride for experimental planning advice.

Conflicts of Interest: The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. *Renewable Energy Explained: Portfolio Standards*; US Energy Information Administration: Washington, DC, USA, 2019.
2. Jewell, W.; Hu, Z. The Role of Energy Storage in Transmission and Distribution Efficiency. In *IEEE PES Transmission and Distribution Conference and Exposition 2012, Orlando, FL, USA, 7–10 May 2012*; IEEE: Piscataway, NJ, USA, 2012; pp. 1–4. [CrossRef]
3. Mahmood, A.; Butt, A.R.; Mussadiq, U.; Nawaz, R.; Zafar, R.; Razzaq, S. Energy sharing and management for prosumers in smart grid with integration of storage system. In Proceedings of the 2017 5th International Istanbul Smart Grid and Cities Congress and Fair (ICSG), Istanbul, Turkey, 19–21 April 2017; pp. 153–156. [CrossRef]
4. Atasoy, T.; Akınç, H.E.; Erçin, Ö. An analysis on smart grid applications and grid integration of renewable energy systems in smart cities. In Proceedings of the 2015 International Conference on Renewable Energy Research and Applications (ICRERA), Palermo, Italy, 22–25 November 2015; pp. 547–550. [CrossRef]
5. *FERC Order No. 2222*; Federal Energy Regulatory Commission: Washington, DC, USA, 2020.
6. Angle, M.G.; Madnick, S.; Kirtley, J.L.; Khan, S. Identifying and Anticipating Cyberattacks That Could Cause Physical Damage to Industrial Control Systems. *IEEE Power Energy Technol. Syst. J.* **2019**, *6*, 172–182. [CrossRef]
7. Li, D.; Ramanan, P.; Gebraeel, N.; Paynabar, K. Deep Learning Based Covert Attack Identification for Industrial Control Systems. In Proceedings of the 2020 19th IEEE International Conference on Machine Learning and Applications (ICMLA), Miami, FL, USA, 14–17 December 2020; pp. 438–445. [CrossRef]
8. McLaughlin, S.; Konstantinou, C.; Wang, X.; Davi, L.; Sadeghi, A.R.; Maniatakos, M.; Karri, R. The Cybersecurity Landscape in Industrial Control Systems. *Proc. IEEE* **2016**, *104*, 1039–1057. [CrossRef]
9. Sebastian, D.J.; Hahn, A. Exploring emerging cybersecurity risks from network-connected DER devices. In Proceedings of the 2017 North American Power Symposium (NAPS), Morgantown, WV, USA, 17–19 September 2017; pp. 1–6. [CrossRef]
10. de Carvalho, R.S.; Saleem, D. Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources. In Proceedings of the 2019 Resilience Week (RWS), San Antonio, TX, USA, 4–7 November 2019; Volume 1, pp. 226–231. [CrossRef]
11. Teshome, D.; Xu, W.; Bagheri, P.; Nassif, A.; Zhou, Y. A Reactive Power Control Scheme for DER-caused Voltage Rise Mitigation in Secondary Systems. In Proceedings of the 2019 IEEE Power Energy Society General Meeting (PESGM), Atlanta, GA, USA, 4–8 August 2019; p. 1. [CrossRef]
12. Hussain, S.S.; Ustun, T.S. Smart Inverter Communication Model and Impact of Cybersecurity Attack. In Proceedings of the 2020 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), Jaipur, India, 16–19 December 2020; pp. 1–5. [CrossRef]
13. Duan, N.; Yee, N.; Salazar, B.; Joo, J.Y.; Stewart, E.; Cortez, E. Cybersecurity Analysis of Distribution Grid Operation with Distributed Energy Resources via Co-Simulation. In Proceedings of the 2020 IEEE Power Energy Society General Meeting (PESGM), Montreal, QC, Canada, 2–6 August 2020; pp. 1–5. [CrossRef]
14. Soyoye, O.T.; Stefferud, K.C. Cybersecurity Risk Assessment for California's Smart Inverter Functions. In Proceedings of the 2019 IEEE CyberPELS (CyberPELS), Knoxville, TN, USA, 29 April–1 May 2019; pp. 1–5. [CrossRef]
15. Ustun, T.S. Cybersecurity Vulnerabilities of Smart Inverters and Their Impacts on Power System Operation. In Proceedings of the 2019 International Conference on Power Electronics, Control and Automation (ICPECA), New Delhi, India, 16–17 November 2019; pp. 1–4. [CrossRef]
16. Lee, R.M.; Assante, M.J.; Conway, T. *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*; Technical Report; E-ISAC: Washington, DC, USA, 2016.
17. *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*; Technical Report; Dragos, Inc.: Hanover, MD, USA, 2017.
18. *Threat Analysis: Industrial Control System Technical Report: Dealing with the Threats Posed by Triton / Trisis Destructive Malware*; Technical Report; Accenture Security: New York, NY, USA, 2018.

19. *Framework for Improving Critical Infrastructure Cybersecurity*; Technical Report; National Institute of Standards and Technology, Gaithersburg, MD, USA, 2017.
20. Kure, H.I.; Islam, S. Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber Phys. Syst. Theory Appl.* **2019**, *4*, 332–340. [CrossRef]
21. Lamba, A. Protecting 'Cybersecurity & Resiliency' of Nation's Critical Infrastructure—Energy, Oil & Gas. *Int. J. Curr. Res.* **2018**, *10*, 76865–76876.
22. Jang-Jaccard, J.; Nepal, S. A survey of emerging threats in cybersecurity. *J. Comput. Syst. Sci.* **2014**, *80*, 973–993. [CrossRef]
23. Falco, G.; Caldera, C.; Shrobe, H. IIoT Cybersecurity Risk Modeling for SCADA Systems. *IEEE Internet Things J.* **2018**, *5*, 4486–4495. [CrossRef]
24. Marques, L.; Silva, M.; Vasconcelos, V. CAN Based Network for Modular Battery Bank with Security Features. In Proceedings of the 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), Seville, Spain, 24–27 June 2020; pp. 1–2. [CrossRef]
25. Baumgart, I.; Borsig, M.; Goerke, N.; Hackenjos, T.; Rill, J.; Wehmer, M. Who Controls Your Energy? On the (In)Security of Residential Battery Energy Storage Systems. In Proceedings of the 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Beijing, China, 21–23 October 2019; pp. 1–6. [CrossRef]
26. Onunkwo, I.; Cordeiro, P.; Wright, B.; Jacobs, N.; Lai, C.; Johnson, J.; Hutchins, T.; Stout, W.; Chavez, A.; Richardson, B.T.; Schwalm, K. *Cybersecurity Assessments on Emulated DER Communication Networks*; Technical Report; Sandia National Laboratories: Albuquerque, NM, USA, 2019.
27. Sundararajan, A.; Chavan, A.; Saleem, D.; Sarwat, A.I. A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security. *Energies* **2018**, *11*, 2360. [CrossRef]
28. Dey, S.; Khanra, M. Cybersecurity of Plug-In Electric Vehicles: Cyberattack Detection During Charging. *IEEE Trans. Ind. Electron.* **2021**, *68*, 478–487. [CrossRef]
29. Acharya, S.; Dvorkin, Y.; Pandžić, H.; Karri, R. Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective. *IEEE Access* **2020**, *8*, 214434–214453. [CrossRef]
30. Rahman, S.; Aburub, H.; Mekonnen, Y.; Sarwat, A.I. A Study of EV BMS Cyber Security Based on Neural Network SOC Prediction. In Proceedings of the 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T& D), Denver, CO, USA, 16–19 April 2018; pp. 1–5. [CrossRef]
31. Chandwani, A.; Dey, S.; Mallik, A. Cybersecurity of Onboard Charging Systems for Electric Vehicles—Review, Challenges and Countermeasures. *IEEE Access* **2020**, *8*, 226982–226998. [CrossRef]
32. Qi, J.; Hahn, A.; Lu, X.; Wang, J.; Liu, C.C. Cybersecurity for distributed energy resources and smart inverters. *IET Cyber Phys. Syst. Theory Appl.* **2016**, *1*, 28–39. [CrossRef]
33. Ravikumar, G.; Hyder, B.; Govindarasu, M. Hardware-in-the-Loop CPS Security Architecture for DER Monitoring and Control Applications. In Proceedings of the 2020 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 6–7 February 2020; pp. 1–5. [CrossRef]
34. Gourisetti, S.N.G.; Hansen, J.; Hofer, W.; Manz, D.; Kalsi, K.; Fuller, J.; Niddodi, S.; Kley, H.; Clarke, C.; Kang, K.; et al. A Cyber Secure Communication Architecture for Multi-Site Hardware_in_the_Loop Co_Simulation of DER Control. In Proceedings of the 2018 Resilience Week (RWS), Denver, CO, USA, 20–23 August 2018; pp. 55–62. [CrossRef]
35. Olowu, T.O.; Dharmasena, S.; Jafari, H.; Sarwat, A. Investigation of False Data Injection Attacks on Smart Inverter Settings. In Proceedings of the 2020 IEEE CyberPELS (CyberPELS), Miami, FL, USA, 13 October 2020; pp. 1–6. [CrossRef]
36. Rao, R.; Liu, Z.; Wang, L.; Hou, S.; He, Y. Improved Model Predictive Control for Mitigating False Data Injection on Cascaded H-Bridge Inverters. In Proceedings of the 2019 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Macao, China, 1–4 December 2019; pp. 1–5. [CrossRef]
37. Jafarigiv, D.; Sheshyekani, K.; Kassouf, M.; Seyedi, Y.; Karimi, H.; Mahseredjian, J. Countering FDI Attacks on DERs Coordinated Control System Using FMI-Compatible Cosimulation. *IEEE Trans. Smart Grid* **2021**, *12*, 1640–1650. [CrossRef]
38. Pazouki, S.; Naderi, E.; Asrari, A. Interconnected Energy Hubs including DERs Targeted by FDI Cyberattacks. In Proceedings of the 2020 11th International Green and Sustainable Computing Workshops (IGSC), Pullman, WA, USA, 19–22 October 2020; pp. 1–6. [CrossRef]
39. Gholami, S.; Saha, S.; Aldeen, M. A cyber attack resilient control for distributed energy resources. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Turin, Italy, 26–29 September 2017; pp. 1–6. [CrossRef]
40. Chlela, M.; Joos, G.; Kassouf, M.; Brissette, Y. Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks. In Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 17–21 July 2016; pp. 1–5. [CrossRef]
41. Hosseinzadeh, M.; Sinopoli, B.; Garone, E. Feasibility and Detection of Replay Attack in Networked Constrained Cyber-Physical Systems. In Proceedings of the 2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 24–27 September 2019; pp. 712–717. [CrossRef]
42. Tran, T.T.; Shin, O.S.; Lee, J.H. Detection of replay attacks in smart grid systems. In Proceedings of the 2013 International Conference on Computing, Management and Telecommunications (ComManTel), Ho Chi Minh City, Vietnam, 21–24 January 2013; pp. 298–302. [CrossRef]

43. Lore, K.G.; Shila, D.M.; Ren, L. Detecting Data Integrity Attacks on Correlated Solar Farms Using Multi-layer Data Driven Algorithm. In Proceedings of the 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018; pp. 1–9. [CrossRef]
44. Srikantha, P.; Kundur, D. Denial of service attacks and mitigation for stability in cyber-enabled power grid. In Proceedings of the 2015 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–20 February 2015; pp. 1–5. [CrossRef]
45. Barua, A.; Faruque, M.A.A. Hall Spoofing: A Non-Invasive DoS Attack on Grid-Tied Solar Inverter. In Proceedings of the 29th USENIX Security Symposium (USENIX Security 20), USENIX Association, 12–14 August 2020; pp. 1273–1290.
46. Liu, S.; Hu, Z.; Wang, X.; Wu, L. Stochastic Stability Analysis and Control of Secondary Frequency Regulation for Islanded Microgrids Under Random Denial of Service Attacks. *IEEE Trans. Ind. Inform.* **2019**, *15*, 4066–4075. [CrossRef]
47. Chlela, M.; Mascarella, D.; Joós, G.; Kassouf, M. Fallback Control for Isochronous Energy Storage Systems in Autonomous Microgrids Under Denial-of-Service Cyber-Attacks. *IEEE Trans. Smart Grid* **2018**, *9*, 4702–4711. [CrossRef]
48. Fard, A.Y.; Easley, M.; Amariucai, G.T.; Shadmand, M.B.; Abu-Rub, H. Cybersecurity Analytics using Smart Inverters in Power Distribution System: Proactive Intrusion Detection and Corrective Control Framework. In Proceedings of the 2019 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 5–6 November 2019; pp. 1–6. [CrossRef]
49. Sebastian, D.J.; Agrawal, U.; Tamimi, A.; Hahn, A. DER-TEE: Secure Distributed Energy Resource Operations Through Trusted Execution Environments. *IEEE Internet Things J.* **2019**, *6*, 6476–6486. [CrossRef]
50. Ustun, T.S.; Hussain, S.M.S. A Review of Cybersecurity Issues in Smartgrid Communication Networks. In Proceedings of the 2019 International Conference on Power Electronics, Control and Automation (ICPECA), New Delhi, India, 16–17 November 2019; pp. 1–6. [CrossRef]
51. Johnson, J. Assessing DER network cybersecurity defences in a power-communication co-simulation environment. *IET Cyber Phys. Syst. Theory Appl.* **2020**, *5*, 274–282. [CrossRef]
52. Collins, L.; Ward, J. Real and reactive power control of distributed PV inverters for overvoltage prevention and increased renewable generation hosting capacity. *Renew. Energy* **2015**, *81*, 464–471. [CrossRef]
53. Mansiri, K.; Sukchai, S.; Sirisamphanwong, C. Fuzzy Control for Smart PV-Battery System Management to Stabilize Grid Voltage of 22 kV Distribution System in Thailand. *Energies* **2018**, *11*, 1730. [CrossRef]
54. Wade, N.; Taylor, P.; Lang, P.; Jones, P. Evaluating the benefits of an electrical energy storage system in a future smart grid. *Energy Policy* **2010**, *38*, 7180–7188. [CrossRef]
55. *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*; IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003); IEEE: Piscataway, NJ, USA, 2018; pp. 1–138. [CrossRef]
56. Charalambous, A.; Hadjidemetriou, L.; Kyriakides, E. Voltage and Frequency Support Scheme for Storage Systems in Distribution Grids. In Proceedings of the 2019 21st European Conference on Power Electronics and Applications (EPE '19 ECCE Europe), Genova, Italy, 2–5 September 2019; pp. P.1–P.10. [CrossRef]
57. Oudalov, A.; Chartouni, D.; Ohler, C. Optimizing a Battery Energy Storage System for Primary Frequency Control. *IEEE Trans. Power Syst.* **2007**, *22*, 1259–1266. [CrossRef]
58. Kottick, D.; Blau, M.; Edelstein, D. Battery energy storage for frequency regulation in an island power system. *IEEE Trans. Energy Convers.* **1993**, *8*, 455–459. [CrossRef]
59. Sasaki, T.; Kadoya, T.; Enomoto, K. Study on load frequency control using Redox flow batteries. In Proceedings of the IEEE Power Engineering Society General Meeting, Denver, CO, USA, 6–10 June 2004; Volume 1, p. 580 . [CrossRef]
60. Mercier, P.; Cherkaoui, R.; Oudalov, A. Optimizing a Battery Energy Storage System for Frequency Control Application in an Isolated Power System. *IEEE Trans. Power Syst.* **2009**, *24*, 1469–1477. [CrossRef]
61. Walawalkar, R.; Apt, J.; Mancini, R. Economics of electric energy storage for energy arbitrage and regulation in New York. *Energy Policy* **2007**, *35*, 2558–2568. [CrossRef]
62. Boyes, J.D.; Anda, M.F.D.; Torres, W. Lessons learned from the Puerto Rico battery energy storage system. In *Proceedings of the 6th International Conference Batteries for Utility Energy Storage*; Sandia National Labs.: Albuquerque, NM, USA 1999.
63. Mahat, P.; Chen, Z.; Bak-Jensen, B. Underfrequency Load Shedding for an Islanded Distribution System With Distributed Generators. *IEEE Trans. Power Deliv.* **2010**, *25*, 911–918. [CrossRef]
64. Rudez, U.; Mihalic, R. Analysis of Underfrequency Load Shedding Using a Frequency Gradient. *IEEE Trans. Power Deliv.* **2011**, *26*, 565–575. [CrossRef]
65. Ahshan, R.; Saleh, S.A.; Al-Badi, A. Performance Analysis of a Dq Power Flow-Based Energy Storage Control System for Microgrid Applications. *IEEE Access* **2020**, *8*, 178706–178721. [CrossRef]
66. Rahmoun, A.; Armstorfer, A.; Biechi, H.; Rosin, A. Mathematical modeling of a battery energy storage system in grid forming mode. In Proceedings of the 2017 IEEE 58th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON), Riga, Latvia, 12–13 October 2017; pp. 1–6. [CrossRef]
67. Lee, Y.S.; Cheng, M.W. Intelligent control battery equalization for series connected lithium-ion battery strings. *IEEE Trans. Ind. Electron.* **2005**, *52*, 1297–1307. [CrossRef]
68. Abada, S.; Marlair, G.; Lecocq, A.; Petit, M.; Sauvant-Moynot, V.; Huet, F. Safety focused modeling of lithium-ion batteries: A review. *J. Power Sources* **2016**, *306*, 178 – 192. [CrossRef]

69. Blum, A.F.; Jr, R.T.L. *Hazard Assessment of Lithium Ion Battery Energy Storage Systems*; Technical Report; Fire Protection Research Foundation: Quincy, MA, USA, 2016.
70. Sripad, S.; Kulandaivel, S.; Pande, V.; Sekar, V.; Viswanathan, V. Vulnerabilities of Electric Vehicle Battery Packs to Cyberattacks on Auxiliary Components. *arXiv* **2017**, arXiv:1711.04822.
71. Maleki, H.; Howard, J.N. Effects of overdischarge on performance and thermal stability of a Li-ion cell. *J. Power Sources* **2006**, *160*, 1395–1402. [CrossRef]
72. Lee, H.; Chang, S.K.; Goh, E.Y.; Jeong, J.Y.; Lee, J.H.; Kim, H.J.; Cho, J.J.; Hong, S.T. Li2NiO2 as a Novel Cathode Additive for Overdischarge Protection of Li-Ion Batteries. *Chem. Mater.* **2008**, *20*, 5–7. [CrossRef]
73. Li, H.; Gao, J.; ZHANG, S. Effect of Overdischarge on Swelling and Recharge Performance of Lithium Ion Cells. *Chin. J. Chem.* **2008**, *26*, 1585–1588. [CrossRef]
74. Guo, R.; Lu, L.; Ouyang, M.; Feng, X. Mechanism of the entire overdischarge process and overdischarge-induced internal short circuit in lithium-ion batteries. *Sci. Rep.* **2016**, *6*. [CrossRef] [PubMed]
75. Cho, K.T.; Kim, Y.; Shin, K.G. Who Killed My Parked Car? *arXiv* **2018**, arXiv:cs.CR/1801.07741.
76. Fitzgerald, G.; Mandel, J.; Morris, J.; Touati, H. *The Economics of Battery Energy Storage*; Technical Report; Rocky Mountain Institute: Basalt, CO, USA, 2015.
77. KIUC. *Schedule Q Addendum and FAQs*; Kauai Island Utility Cooperative: Lihue, HI, USA, 2019.
78. HECO. *Customer Renewable Energy Programs Billing and Credit*; Hawaiian Electric (HECO): Honolulu, HI, USA, 2018.
79. Johnson, J.; Quiroz, J.; Concepcion, R.; Wilches-Bernal, F.; Reno, M.J. Power system effects and mitigation recommendations for DER cyberattacks. *IET Cyber Phys. Syst. Theory Appl.* **2019**, *4*. [CrossRef]