IGP White Paper #12 [June 2024]

Battery Energy Storage Systems from China:

Being Realistic about Costs and Risks

Juan F. Villarreal, MS Cybersecurity

EXECUTIVE SUMMARY

China has a dominant position in the battery supply chain, limiting the options of procuring Battery Energy Storage Systems (BESS) from US suppliers or other friendly nations. The claim that BESS from China poses a national security risk is making it difficult for utilities, integrators, and contractors to develop renewable energy generation resources. The critics allege that undetectable malware on BESS equipment from China could be activated remotely to cascade into a widespread blackout of the US electric grid. This claim is leading to costly attempts to ban acquisitions of Chinese BESS and to remove ones that are already in place.

Given the tremendous expense involved in these "rip and replace" policies and the major obstacles they place in the path of cleaner energy, it is wise for the United States to investigate the alleged costs and risks. This paper delves deeply into the BESS technology, meticulously examining its components and analyzing potential cyber-attack scenarios. By drawing on existing research literature, conducting interviews with key stakeholders, and applying a customized threat model, this study strives to accurately quantify the risk of implementing a BESS from China in a renewable Distributed Energy Resource (DER).

This paper finds little evidence to support the claim that BESS from China poses a serious national security risk from a cyber event. In the worst case, a cyber event on a BESS from China will impact the battery itself and not the overall grid. To address the risks that might exist, it presents a comprehensive strategy for managing the cyber risks associated with implementing a 100% BESS from China (battery modules plus controls). The risks can be further managed by implementing only the battery modules from China integrated with a domestic or friendly nation control system.

BESS from China is less of a cybersecurity risk and more of an economic issue. Policy advocates who are pursuing a complete decoupling of the U.S. and Chinese economies are exaggerating cybersecurity and national security risks to forestall interdependency with the

Chinese economy. Considering that complete decoupling from Chinese suppliers of battery modules is not possible in the next 5- 10 years, however, policymakers who want to pursue cleaner energy goals should support the adoption of the short and medium-term BESS implementation solutions proposed in this paper.

1. Introduction

The goal of cleaner energy and the threat of climate change are driving the growth of low-emission energy sources, including nuclear and renewables such as solar, wind, and hydro [1]. Much of the growth in renewables will come from the expansion of low-cost solar photovoltaic (PV) generation [1]. To compensate for the intermittency of renewable energy, Battery Energy Storage Systems (BESS) powered by Lithium-Ion batteries play a crucial role. BESS is a mature technology that provides a low cost, rapid response energy storage solution [2]. Recent legislation in the U.S., such as the Infrastructure Investment and Jobs Act [3] and the Inflation Reduction Act [4], will propel the development of renewable energy installations coupled with BESS. The utility-scale BESS market is expected to grow annually at a rate of 29% for the rest of this decade [5].

In addition to compensating for the variability of generation from renewable energy, BESS provides several other services to promote the resilience and efficiency of the electric grid:

- Arbitrage – maximize revenue by storing or discharging energy depending on the fluctuation of electricity prices
- Fast-acting operating reserves when requested by the grid operator
- Ancillary services such as Primary Frequency Response (PFR) and Regulation

To provide these services, BESSs are interconnected to the grid in the transmission network and the distribution network near load centers [6]. This requires the deployment of distributed controls and communications capabilities to adequately sense price, electricity demand, and control signals to perform the above functions.

The connectivity of the BESS increases its vulnerabilities to cyber-attacks that may cause a malfunction or allow unauthorized system surveillance. These attacks can be initially classified into three areas [7]:

1. Data Integrity through false data injection attacks (FDIA) and by introducing a random delay on control commands,
2. Confidentially, unauthorized access through an FDIA attack, and
3. System availability through a denial of service (DoS) attack.

China has a dominant position in the battery supply chain, both in sourcing raw materials and battery manufacturing. The Bloomberg BNEF's global battery supply chain ranking table for 2022 positions China as No. 1 in Raw Materials and Manufacturing [8]. The BESS market's growth exceeds the capacity of domestic or friendly country sources. As a result, project owners, contractors, and integrators need to consider equipment from foreign companies [9], particularly China.

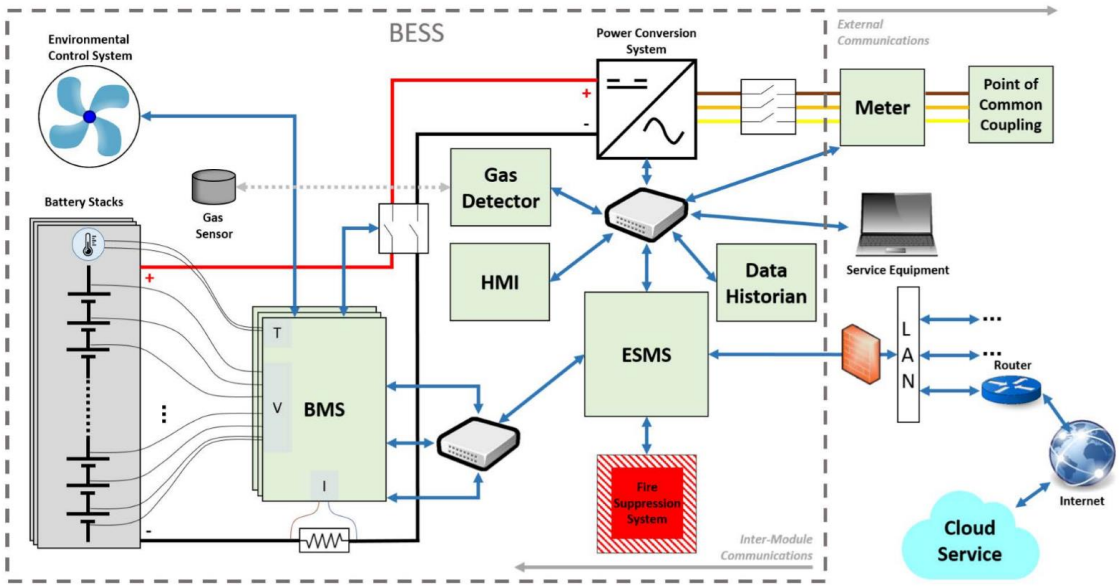
Some argue that the purchase of BESS from China brings geopolitical and cybersecurity risks to the planned grid modification projects. Specifically, the policy think tank Foundation for Defense of Democracies released a report claiming that there were security risks in the use of equipment from Fujian-based Contemporary Amperex Technology Co. Ltd. (CATL), the world's largest manufacturer of lithium-ion batteries [10]. While this report was influential in Washington, it should be noted that the author of the FDD report is a foreign and military policy expert and not an expert in cybersecurity, information technology, or electrical power systems. The article merely speculates about the possibility of undetectable malware on BESS installations that could be activated by foreign entities. Notwithstanding the current state of knowledge on BESS from China, they have been banned for use in military installations by the National Defense Authorization Act for Fiscal Year 2024 [11].

This paper aims to comprehensively evaluate the cybersecurity threats inherent in a BESS [12] and the specific threats from BESS from China and propose mitigation strategies. The paper will include solutions that owners, integrators, and contractors of clean energy projects can apply when considering the deployment of a BESS from China. The proposed solutions will include policy recommendations for de-risking Chinese-supplied batteries in the short term and creating a new supply chain in the US with equipment from trusted nations in the long term.

2. BESS Structure and Components

The main components of a BESS are: 1) battery modules, 2) battery management system (BMS), 3) energy storage management system (ESMS), 4) power conversion system (PCS), and 5) physical hazard protection devices. Figure 2.1 shows the location of the components within the BESS and the power and communications connections (power connections in black and red, data communications in blue) [12].

Figure 2.1 – BESS components and communications [12]



BESSs, while offering various grid reliability functions such as backup power and ancillary services like frequency regulation and voltage support, also present potential risks. To fulfill these functions, BESSs necessitate a high level of internal and external connectivity, thereby expanding vulnerabilities for cyber-attacks. Moreover, batteries, if mishandled or operated, can pose additional safety risks. Damaged or overcharged battery cells can emit toxic and flammable fumes and are prone to thermal events. These three factors combine to make BESSs an alluring target for malicious actors [12]. The potential cyber-attacks against these components are discussed in Section 4 of this paper.

3. BESS Application Use Cases

A Federal Energy Regulatory Commission (FERC) Order paved the way for distributed energy resources (DERs) to participate in wholesale markets [16]. This new role for DERs necessitates digital communications between energy aggregators and the DER assets under their control. The DER interconnection standard IEEE 1547 [15] provides the technical specifications for testing the interconnection and interoperability between utility electric power systems (EPSs) and distributed energy resources (DERs). In this context, BESS will play a pivotal role in facilitating the services that DERs are expected to provide to the electric grid under the FERC order. BESS are not just power systems assets, but flexible ones capable of delivering services for electric energy systems, transmission infrastructure, distribution infrastructure, consumer energy systems, and ancillary services for grid stability and resilience. Recent funding legislation in the U.S. and the transition from fossil generation to clean energy

underscore the increasing importance of low-inertia and intermittent power sources like wind and solar PV. In this evolving energy landscape, BESS will provide energy security and grid stability. This section outlines the significant applications for BESS that provide the required energy production reliability, quality, and stability.

The applications can be divided into two areas. Power applications involve charging and discharging large amounts of power over short periods (seconds to minutes), and energy applications require charging and discharging large amounts of energy over long periods (hours) [16]. This section discusses the primary use cases for BESS and the connectivity required to execute the application. This connectivity will create/expand the BESS attack surfaces and the potential attacks discussed in Section 4. The use cases are Energy Arbitrage, Transmission and Distribution expansion deferral, Renewable Energy Firming, Frequency Regulation, and Voltage Support. Table 3 -1 classifies these use cases and provides a summary definition.

Table 3 -1 BESS use cases

Service Client	BESS Use Case	Definition of Service	Type
Distributed Energy Resource	Renewable Energy Firming	Supply of Energy to cover renewables intermittency	Energy
Utility Grid Service	Frequency Regulation	Supply of active Power for correcting over/under frequency conditions	Power
	Voltage Support	Supply of reactive Power for correcting over/under vlotage conditions	Power
	Black Start	Supply of Power to enable restarting generators after a failure condition	Power
	Transmission and Distribution expansion deferral	Supply of Energy which allows infrastructure investment delay for meeting increased demand	Energy
	Transmission Congestion Relief	Supply of Energy to reduce transmission congestion during peak demand times	Energy

For a more detailed description of all the BESS application use cases, please refer to [16].

4. Cyber Threats on BESS Components and Impacts on the Grid

This section summarizes the potential attacks on the main components of a BESS. Specifically, this section will address 1) Battery Modules, 2) Battery Management System (BMS), 3) Power Conversion System (PCS), and the Energy Storage Management System (ESMS). Figure 2.1 shows the location of the components within the BESS and the power and

communications connections (power connections in black and red, data communications in blue).

There are not many cyber security studies on BESS installations, and to date, there has not been a documented cyber-attack on a BESS installation. Most battery cyber risk analyses and mitigation strategies have been performed for Electric Vehicle (EV) batteries, charging stations, and studies on Smart Grids [17]. This section will leverage the research done on BESS [12] [18], Smart Grids, and Cyber-Physical Systems (CPS) in general to create a threat model for a single BESS supporting a 20MW Solar installation that is connected to the electric grid.

The cyber threats will be grouped into Integrity, Confidentiality, and Availability [7]. The attack vector considered for Integrity and Confidentiality threats is False Data Injection (FDI). In the case of Integrity, the FDI attack is meant to manipulate or modify data. In the case of Confidentiality, FDI is used to access data and construct a more sophisticated eavesdropping attack like the Man-in-the-Middle attack. Finally, in the case of Availability, we consider the Denial of Service (DoS) attack. A DoS attack is targeted to compromise the communication network between the components of a BESS.

Scenario for evaluating the impact on a DER that is supported by a BESS.

A Distributed Energy Resource (DER) comprises a 20MW Solar Generation Facility with one 20MW BESS unit capable of supplying power for 2.5 hours, serving 1500 customers, and is connected to the electric grid. The BESS provides a firming function (backup) to the intermittency of the Solar Generation facility. In addition, the BESS is programmed to provide voltage support and frequency regulation to the grid. The scenario DER is also assumed to be connected to a regional grid with backup spinning reserves that can provide peak power, frequency regulation, and voltage support. The inability of the BESS to deliver these services will have an economic impact on the utility, in some cases resulting in a loss of revenue and extra cost to supply the service from another grid generation source.

The impacts of a cyber-attack on a BESS can be summarized in the following three categories:

1. Grid instability, trips, and load damage due to manipulated PCS and BMS settings [18].
2. Battery Hardware Physical Damage, causing early replacement and, in extreme cases, fire [12].
3. Economic Impact on the utility from being unable to deliver services from the BESS [18].

The impact level (low, medium, high) will depend on the generation asset distribution around the BESS and the network configuration. A low impact would be expected in an electric

grid where devices are available to correct the adverse effects of the attack and well-configured protection devices that will isolate the affected portions of the grid. The lack of the abovementioned configuration and protection may lead to a high impact and cause a local or regional blackout [18]. Quantifying the effects of a large-scale attack on BESSs or other DER components requires modeling the network with methods such as state estimation for power grids [38]. The discussion of wide-area grid cyber-attacks on DERs is left up to future research.

5. BESS Cyber Risk Mitigation Strategies

In principle, a BESS is an industrial control system (ICS) that controls and manages the chemical process inside the battery modules. The following paragraphs address the cybersecurity tactics most efficient for mitigating the risks of the threats described above.

Physical Security

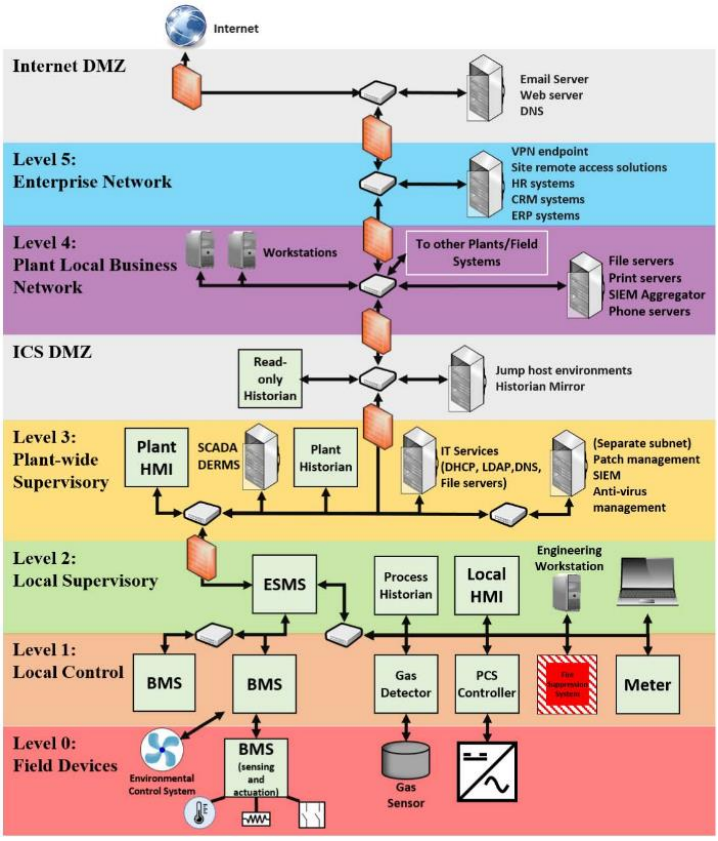
- **Physical Access and Monitoring**. Restrict physical access to the BESS, battery modules, and its monitoring system, including the Data Historian, the HMI, and the internal network switches. These areas should be monitored with cameras or motion sensors to detect threats and respond to threats with local security personnel and law enforcement. The access should be controlled with a fenced perimeter that has controlled access using locks and badge readers. Depending on the location, vehicle barriers can be used to delay any external threat actors [19].

- **Fire Protection.** The risk of fire and explosion is a hazard that needs to be considered for a BESS installation. This hazard may be initiated by a reliability failure or a cyber-induced malfunction of the BMS and its sensors, as discussed in Section 4. The research document “Lithium-ion battery energy storage systems (BESS) hazards” contains a detailed description of the hazards and the mitigating strategies [13]. Some states have created task forces to review existing codes and the required emergency responses to a potential fire in the battery modules [20].

Network Architecture

- **Network Segmentation** [23] is one of the strategies that demonstrate the value of a defense-in-depth strategy. As the CISA infographic [23] shows, adding layers to a network increases the complexity and level of effort an attacker must go through to reach the Industrial Control System, like the BMS for the battery. Figure 6 - 1 shows an example of a communication system connecting a utility-scale BESS to the corporate environment. The network levels are defined by the Purdue Enterprise Reference Architecture, also known as the Purdue Model [24].

Figure 5 -1 – Network Segmentation Applied to a BESS [12]



- Secure Communications [12]. A cryptosystem uses keys and enciphering functions to transform a message (plaintext) into unintelligible information called cyphertext [22]. Many recently developed or updated standard communication protocols, such as IEEE 2030.5, support encrypted communications. Another authentication tactic is to examine and reject messages in the BESS system from a source whose authenticity cannot be verified [18]. Most industrial protocols, like Modbus, DNP3, or CAN, do not provide built-in security features like authentication or encryption. Recent research [18] has successfully tested the addition of tokens and certificates to a Modbus packet along with a firewall that only allows packets to be sent to the battery that has the secure protocol.

- Access Control [21] Controlling who has access to what system or device is the first step for a robust cybersecurity plan. Several internal and external organizations need access to execute their functions and responsibilities for a BESS. Engineers would require access to the engineering workstation to adjust control parameters and setpoints. Utility operations need access to the ESMS to monitor the energy produced from the BESS. A

solution that adds the role parameter to an access control methodology is Role-Based Access Control (RBAC). RBAC is a popular method for limiting or providing access based on the role of the subject with minimum administrative effort.

Perimeter Security

- **Remote Access.** Although a remote access VPN is a critical element of a defense-in-depth strategy, implementing remote and secure connectivity to local components presents technical, cost, and resource allocation challenges. The recent joint NSA/CISA Cybersecurity Information Sheet [40] on VPNs provides some essential items to follow, such as 1) Configuring strong cryptography and authentication, 2) Implementing only necessary features for the specific application, and 3) Protecting and monitoring access to and from the VPN. One of the concerns regarding BESS from China is the potential of remote access by the OEM or another third party with a malicious objective. Hardening and monitoring a VPN for BESS applications is critical for secure implementation at a utility.
- **Software Updates.** Software updates are part of the system's operation and maintenance phase, which includes operations, maintenance, changes, and software upgrades. The Consequence-Focused Design principle from the Cyber Informed Engineering Implementation Guide can be applied to software upgrades by answering the following question: "What anticipated changes, modifications, or upgrades could alter the consequences of system failure, misuse, or compromise?" [37]. In particular, remote software updates should be carefully scrutinized and controlled. The system owner can deny or disable remote software updates for increased security.

Security Monitoring

- Intrusion Detection Systems (IDS) [12] NIST.SP.1800-32, Securing Distributed Energy Resources (DER): An Example of Industrial Internet of Things Cybersecurity, develops a proposed architecture for DER cybersecurity that includes BESS assets and identifies Intrusion Detection Systems (IDS) as a tool for detecting malware in an ICS environment [25]. Signature-based (SID) and anomaly-based detection (AID) are the two techniques for identifying threats. SID identifies known malware and attack patterns through specific data signatures, while AID focuses on unusual patterns and statistical outliers using machine learning algorithms. Figure 6 -2 shows how a Network Intrusion Detection System (NIDS) can be implemented in the local BESS network and the Wide Area Network.

Figure 5 -2 – Network Intrusion Detection System for a BESS [12]

Policy Security Measures

Another defensive strategy is to apply restrictions via policy. Examples of these policies are limiting or disallowing VPN connections by any third party, including the equipment OEM, and executing software updates and patches from the OEM locally through a physical connection and not through external connectivity.

6. Chinese Cyber Threats

The March 2024 joint announcement by the U.S., UK, and New Zealand on Chinese hacking activities targeting politicians, companies, and dissidents [26] is a reminder of the cyber threat that China continues to pose to the Western world. This threat was attributed to the Chinese threat actor APT31. Due to this attribution, the U.S. Department of Justice issued sanctions against APT31 and 8 Chinese individuals [27].

What does the China threat mean to U.S. critical infrastructure, particularly renewable Distributed Energy Resources (DER) in the electric grid and BESS systems backing up the DER? It is important to note that, to date, there has not been a documented attack on the U.S. electric grid from Chinese actors, and no malicious activity has been found in equipment of Chinese origin. The following paragraphs will summarize known Chinese cyber-attacks against critical infrastructure and hypothetical threats from components manufactured in China, including BESS.

Going in reverse chronological order, the most recent Chinese attack on critical infrastructure involved a new actor called Volt Typhoon, a state-supported Chinese cyber operation, announced in February 2024. According to the CISA advisory [28], Volt Typhoon targeted the IT environments of multiple critical infrastructure organizations, including Energy, Water, and Wastewater Systems. This campaign aimed to enable lateral movement to the OT networks to disrupt operations.

In July 2021, CISA revealed an attack on O&G pipelines [29]. According to this advisory, a state-sponsored Chinese group used spear phishing to access the networks of U.S. oil and natural gas (O&G) pipeline companies from December 2011 to 2013. The objective of this unauthorized intrusion was to help China develop cyberattack capabilities against U.S. pipelines and physically damage pipelines or disrupt pipeline operations.

Finally, as far back as 2014, there has been awareness and concern over Chinese cyberattacks identified by the U.S. Defense Department, the State Department, and private research organizations [30].

Regarding components manufactured in China, in March 2024, a congressional probe reported the existence of communications gear in Chinese cranes deployed at several US ports, raising the concern of logistics spying at these ports [31]. The cellular modems used for remote communication were not documented in any contract between US ports and Chinese crane maker ZPMC. It is not clear why or how these modems were included in the delivery of the cranes; however, according to a report from the Wall Street Journal, “it isn’t unusual for modems to be installed on cranes to remotely monitor operations and track maintenance, it appears that at least some of the ports using the ZPMC-made equipment hadn’t asked for that capability” [41]. Earlier in the year, the Biden administration issued an executive order announcing an investment of $20 billion to develop a new port crane supply chain in the US to replace cranes from Chinese manufacturers [32].

BESS equipment from China started attracting lawmakers' attention during the inauguration of an 11-megawatt BESS installation developed by Duke Energy to support Camp Lejeune, a Marine base in North Carolina [33]. The BESS system was purchased from Contemporary Amperex Technology Co. Ltd. (CATL), China's world’s largest lithium-ion battery manufacturer. Lawmakers were concerned that due to CATL’s Chinese domicile, malware could be installed in the equipment at the request of the Chinese Government. Further discussions by lawmakers resulted in a letter from the Senate Foreign Relations Committee to Defense Secretary Loyd Austin [34] requesting “a full accounting of CATL batteries and other products by CCP-aligned companies on U.S. military installations” along with a series of questions related to the implementation of CATL batteries at Military installations. The letter referenced a memo by the policy think tank Foundation for Defense of Democracies (FDD) [10] as a basis for its security and cyber concerns. Shortly after this letter, Duke Energy disconnected and removed the CATL batteries from the Camp Lejeune project [35].

The recent security events [26] [27] and the long history of cyberattacks [22] on our networks attributed to China do indicate that there is a threat of espionage. Government and

private organizations need to consider these risks and take the appropriate countermeasures to mitigate the risk. However, none of these attacks relied on the Chinese origin of an equipment or service supplier. This suggests that general cybersecurity good practice, not national origin restrictions, are the most important defense.

Turning to the focus of this paper – the cyber risks coming from BESS from China – what is the risk, and what countermeasures should utilities and developers be taking to mitigate the risk? Should the approach be a complete decoupling from Chinese equipment, or is there an alternate de-risking approach that permits the use of such equipment with safeguards in the short term, the medium term, and the long term? In the short term, a de-risking approach certainly makes sense since China has a dominant position in the supply chain of the raw materials used to make batteries, and it has an efficient process for manufacturing these components at scale.

The following section will attempt to evaluate the risk to a utility by implementing a BESS from China using a threat model developed for this purpose. Using the results of the risk quantification, the next section will propose risk mitigation strategies that will allow the best of both worlds, using the existing Chinese battery modules and a mix of foreign and local battery management systems with the appropriate cyber countermeasures.

7. BESS Cyber Threat Model

In this section, I will quantify the risk to a utility from implementing a BESS from a Chinese supplier. For this purpose, I developed a simple threat model using a threat model spreadsheet created by SANS as a starting point [36]. The following are the assumptions and initial conditions applied to the threat model:

1. Cyber Threat: False Data Injection or a Denial of Service from hidden malware in the BESS control system or malicious activity by the OEM or another third party through a VPN connection [10].
2. Utility Performance Factors: 1) Battery Modules Physical Damage, 2) Power System Instability on the grid, and 3) Economic Impact (loss of revenue or increased cost) from not delivering BESS grid services [18].
3. Scenario being evaluated: Distributed Energy Resource (DER) composed of a 20MW Solar Generation Facility with one 20MW BESS unit capable of supplying power for 2.5 hours serving 1500 customers connected to the grid.
4. Damage Evaluation Items: 1) Legal, 2) Reputation, 3) Revenue/Cost, and 4) Electric Production. Graded from 0 – 10, None = 0, Low = 3, Medium = 5, High = 7, Worst = 10 [36].

5. The Likelihood that the cyber threat will succeed in impacting the Utility Performance Factors. This factor is evaluated from 0 to 1, considering the difficulty of the exploit. An exploit of high difficulty will be assigned a low likelihood of success, and vice versa; a more straightforward exploit will have a higher probability of success.
6. The total risk on each Utility Performance Factor is calculated by adding all the Damage Evaluation Items and multiplying the result by the likelihood of success. Total Risk = (Legal Impact + Reputation Impact + Revenue/Cost Impact + Electric Production Impact) * Likelihood of Threat Success. For example, in Table 8 -1, the total risk for Battery Hardware Physical Damage equals 5+10+10+7 = 32 * 0.7 = 22.4.

With this threat model, I evaluate two "bookend cases."

1. Worst Case Condition. The utility selects a complete BESS from China, battery modules, and related control systems. In this case, the attacker is assumed to be in the network due to the condition of embedded malware delivered to the system. In addition, policy restrictions were not in place.
2. Best Case Condition. The utility implements only the battery modules from China. The control systems, the BMS, PCS, and ESMS, are integrated from a domestic supplier or a friendly nation. In this case, the attacker is outside the network and has to penetrate the countermeasures mentioned in Section 5. In addition, policy measures are limiting VPN connections and remote software upgrades. This is the best case with the current supply chain, where the battery modules are most likely be procured from China [8].

Threat Model Results Discussion

Table 7-1 illustrates the Threat Model Results for the Worst-Case scenario. As can be seen, damage to the battery itself is the highest level of risk to the utility, with a risk score of 22. The level of damage can range from battery depletion/lower battery life to a thermal runaway that could cause a fire. Battery damage will mainly impact the local DER with a partial or total loss of backup power to the solar field. The effect on the overall grid from one BESS being out of service is low. The probability of the attack causing a malfunction of the Power Conversion System that will create an over/under voltage condition or over/under frequency condition exists. Still, the level of risk is much lower, with a risk score of 16 (30% lower) due to the high difficulty level of executing the exploit. In summary, in the worst case, the highest risk to the utility is the loss of backup power to the single DER.

Table 7–1: Worst-case Scenario

Chinese OEM provides complete BESS - Worst case scenario									
Cyber Threat	Utility Performance Factors	Legal Impact	Reputation Impact	Revenue/Cost Impact	Electric Production Impact	Total Impact	Likelihood of Threat Success (0 - 1.0)	Risk = Likelihood X Total Impact	Comments on Likelihood of Threat Success
		None = 0, Low = 3, Med = 5, High = 7, Worst = 10							
False Data Injection and/or Denial of Service on a BESS system	Battery hardware physical damage - early replacement or fire	5	10	10	7	32	0.7	22.4	Level of difficulty for attacker to adjust battery sensor measurements is medium to low. There is a medium to high probability of success
	Power System Instability - trip protection is disabled causing damage downstream from the DER before backups correct the instability	7	10	5	10	32	0.5	16	Level of difficulty for attacker to adjust complex PCS controls and disable trips is high. There is a medium probability of success
	Economic Impact due to inability to provide grid services	3	3	7	5	18	0.3	5.4	Level of difficulty for attacker for disabling all services is high. There is a low probability of success

Table 7 -2 illustrates the Threat Model Results for the Best-Case scenario where only the battery modules from China are implemented. As can be seen, damage to the battery itself is still the highest level of risk, with a score of 7, but the risk has been reduced by 60%. The probability of the attack causing a malfunction of the Power Conversion System that will create an over/under voltage condition or over/under frequency condition continues to exist with a risk score of 3.2. This score is much lower (80% lower) due to the high difficulty of executing the exploit and penetrating the network.

In summary, in the best case, the significant impact on the utility is localized with the loss of backup power to the DER but with a much lower probability.

Table 7-2—Low-risk scenario

Chinese OEM provides only battery modules - Controls (BMS, PCS, ESMS) domestic or from a friendly nation									
Cyber Threat	Utility Performance Factors	Legal Impact	Reputation Impact	Revenue/Cost Impact	Electric Production Impact	Total Impact	Likelihood of Threat Success (0 - 1.0)	Risk = Likelihood X Total Impact	Comments on Likelihood of Threat Success
		None = 0, Low = 3, Med = 5, High = 7, Worst = 10							
False data Injection and/or Denial of Service on a BESS system	Battery hardware physical damage - early replacement or fire	5	10	10	7	32	0.3	9.6	Level of difficulty for attacker to adjust battery sensor measurements is medium to low. There is a low probability of success due to countermeasures
	Power System Instability - trip protection is disabled causing damage downstream from the DER before backups correct the instability	7	10	5	10	32	0.1	3.2	Level of difficulty for attacker to adjust complex PCS controls and disable trips is high. There is a low probability of success due to countermeasures
	Economic Impact due to inability to provide grid services	3	3	7	5	18	0.1	1.8	Level of difficulty for attacker for disabling all services is high. There is a low probability of success due to countermeasures

Discussion on the Threat Model scoring and assumptions

This attempt at quantifying the risks of implementing a BESS from China is calculated using subjective scoring based on the existing research listed in the references and discussions with key stakeholders from the utilities, OEMs, and government organizations. The interviews executed with critical stakeholders are listed in Appendix A. It is left up to follow-on research to build a more robust scoring system and or apply the Tactics and Techniques from the MITRE ATT&CK ICS Matrix. One possible guide for a future threat modeling approach is the publication Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies [39]. In this publication, the authors build a complex model comprised of two major parts, the adversary model and the attack model, allowing for an inclusive evaluation of malicious attack strategies.

8. China BESS Cyber Risk Mitigation – Solutions for Implementation

Building on the results from the Threat Model Cases, the following implementation solutions are proposed:

Short Term/Immediate - Implement a 100% BESS system from China.

Implement a complete BESS from China (Battery Modules, BMS, PCS, and ESMS) with the following security measures.

- Robust purchase specification with testing and supply chain requirements. The Cyber-Secure Supply Chain Controls from the Cyber Informed Engineering Implementation Guide are proposed as a guideline for applying cyber purchasing requirements [40, Principle 9].
- Defense in Depth measures described in Section 5:
    - Access & Authentication controls
    - Network segmentation
    - Firewall on BESS subnetwork
    - Encryption
    - Modified Modbus protocol with tokens and certificates [18]
- Policy Restrictions
    - OEM remote access limited or denied
    - Remote software upgrades disallowed
- Physical Security and access controls

It is important to emphasize that the essential items that will add security for a BESS from China are the purchase specification and the policy restrictions. In the purchase specification, the buyer can specify that software or hardware that enables external connectivity, either

through a VPN or the Internet, be removed or disabled. It can also request hardware and software factory testing to confirm the removal of the remote connectivity capability or specific penetration testing for security purposes. Section 8B of the Cyber-Secure Supply Chain Controls [37] provides good guidance regarding the questions that should be asked in the supply requirements phase. For example: "What forms of security testing and verification are needed, given the criticality of the product or service to the system under design?" and " What kinds of information about product subcomponents and internals (e.g., hardware bills of materials [HBOMs] and software bills of materials [SBOMs], subcomponent vendors, use of open source) will the organization require for critical system components?".

Finally, the policy restrictions add another layer of security for remote connectivity and software upgrades.

Medium Term/1-5 years – Hybrid Solution

Implement a BESS that only includes the battery modules from China and the control systems (BMS, PCS, and ESMS) from a U.S. supplier or a friendly nation. Security measures would be the same as the short-term solution, with the potential for reconsidering the policy restrictions.

Long Term/5+ years – U.S/Friendly nation 100% supply chain

Implement a BESS sourced 100% from the U.S. or a friendly nation. This solution will provide the maximum reduction of cybersecurity concerns from foreign entities of concern [9]. However, developing sources 100% locally or from a friendly nation has several challenges to overcome. One example is raw materials like Phosphorous and Graphite. These materials are sourced internationally, and 70% of the world's reserves for phosphorus are in Morocco, so domestic manufacturers would compete on a global scale, often finding high prices and short supply [42]. Security measures would be the same as the short-term solution, with the potential for reconsidering the policy restrictions.

The solutions mentioned above should include adopting the recommendations from the recent Department of Energy Cyber Informed Engineering Implementation Guide [37]. This guide describes what it means to engineer systems in a cyber-informed way. It complements—but does not replace—the application of cybersecurity standards or practices within an organization.

9. Recommendations for Policymakers

Cybersecurity is deeply intertwined with geopolitical risk, affecting national security, economic stability, and international relations. This paper proposes that the cyber risks of

implementing a 100% BESS from China (battery modules plus controls) are manageable by applying defense-in-depth countermeasures and policy restrictions. The risks can be further reduced by only sourcing the battery modules from China and integrating a domestic or friendly nation control system. Reducing China's scope of supply to just battery modules reduces the cyber risk; however, the geopolitical supply chain and economic risks remain. Based on the cyber risk analysis results of this paper, it can also be concluded that the national security risks presented in the Foundation for Defense of Democracies [10] article on the risks of implementing EV batteries and BESS from CATL are less of a cyber threat and more of an economic issue.

Considering that complete decoupling from China for the battery modules may not be possible in the next 5- 10 years, policymakers can support the clean energy transition initiatives by encouraging the adoption of the short- and medium-term solutions proposed in Section 8 of this paper.

The long-term solution, which requires creating a new battery module supply chain, should be analyzed along with China's other geopolitical concerns to determine priorities and allocate resources.

10. Conclusions and Recommendations for future work

To execute its functions, BESS requires extensive internal and external data connectivity (Figure 2.1). Internal between components (BMS, PCS, and ESMS) through a local area network and external through the ESMS to the vast area network. The security of a BESS is a complex topic requiring a mix of defense-in-depth strategies, including information security concepts, industrial control systems security, and physical security. The cyber risk analyses presented in this paper show that implementing essential cybersecurity, physical, and policy controls can reduce the cyber risk of a 100% BESS from China to a level that, in the worst case, impacts only the local DER being supported by the BESS. Electric utilities, in the last few years, have become more aware of cybersecurity guidelines and standards and made the cyber and physical security of the grid a priority. Policymakers are encouraged to support the implementation of BESS from China in the short to medium term using the de-risking strategies discussed in Section 8 of this paper.

Cybersecurity of BESS is a new field with just a few comprehensive research papers addressing this topic [12 and 20]. This paper advances this research by applying a simple threat model to calculate the risks of implementing BESS from China on the U.S. electric grid. Keeping in mind that cybersecurity is a continuous improvement activity, the following items are recommended for future work:

- Development of a more objective/robust Threat Model. The publication Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies [39] proposes one possible approach.
- Applying the Threat Model for multiple BESS attacks simultaneously – at scale.
- Executing Hardware & Software testing of Chinese battery modules and controls.

References

[1] IEA report, Electricity 2024, "Executive summary," January 2024, https://www.iea.org/reports/electricity-2024/executive-summary

[2] USAID Grid-Scale Energy Storage Technologies Primer, Thomas Bowen, Ilya Chernyakhovskiy, Kaifeng Xu, Sika Gadzanku, Kamyria Coney, July 2021, https://www.nrel.gov/docs/fy21osti/76097.pdf

[3] H.R.3684 - Infrastructure Investment and Jobs Act, November 2021, https://www.congress.gov/bill/117th-congress/house-bill/3684

[4] H.R.5376 - Inflation Reduction Act of 2022, August 2022, https://www.congress.gov/bill/117th-congress/house-bill/5376/text

[5] McKinsey and Company, Enabling renewable energy with battery energy storage systems, August 2023, https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/enabling-renewable-energy-with-battery-energy-storage-systems

[6] NREL, Grid-Scale Battery Storage - Frequently Asked Questions, Thomas Bowen, Ilya Chernyakhovskiy, Paul Denholm, September 2019, https://www.nrel.gov/docs/fy19osti/74426.pdf

[7] IEEE Xplore, The Cyber Security of Battery Energy Storage Systems and Adoption of Data-driven Methods, Nina Kharlamova; Seyedmostafa Hashemi; Chresten Træholt, February 2021, https://ieeexplore.ieee.org/document/9355460

[8] BloombergNEF: China dominates global battery supply chain again with followers in flux, November 15, 2022, https://www.energy-storage.news/bloombergnef-china-dominates-global-battery-supply-chain-again-with-followers-in-flux/

[9] Federal Register, Interpretation of Foreign Entity of Concern, 12/04/2023, https://www.federalregister.gov/documents/2023/12/04/2023-26479/interpretation-of-foreign-entity-of-concern

[10] Foundation for Defense of Democracies, Beijing's Power Play, Safeguarding U.S. National Security in the Electric Vehicle and Battery Industries, October 23, 2023, https://www.fdd.org/analysis/2023/10/23/beijings-power-play/

[11] National Defense Authorization Act for Fiscal Year 2024, https://www.congress.gov/bill/118th-congress/house-bill/2670/text?s=8&r=1&q=%7B%22search%22%3A%22defense+authorization+act+2024%22%7D

[12] Sandia National Lab, Cyberphysical Security of Grid Battery Energy Storage Systems, Rodrigo D. Trevisan et al., June 2022, https://ieeexplore.ieee.org/abstract/document/9787060

[13] Elsevier, Lithium-ion battery energy storage systems (BESS) hazards, Jens Conzen et al., December 2023, https://www.sciencedirect.com/science/article/pii/S095042302200208X

[14] FERC Order No. 2222 Explainer: Facilitating Participation in Electricity Markets by Distributed Energy Resources, October 2020, https://www.ferc.gov/ferc-order-no-2222-explainer-facilitating-participation-electricity-markets-distributed-energy

[15] IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces, 2018, https://standards.ieee.org/ieee/1547/5915/

[16] IEEE, Energy Management and Optimization Methods for Grid Energy Storage Systems, RAYMOND H. BYRNE, et al. March 2018, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8016321

[17] Elsevier, Cyber-security on smart grid: Threats and potential solutions, Muhammed Zekeriya Gunduz, January 2020, https://www.sciencedirect.com/science/article/pii/S1389128619311235,

[18] Energies, Cybersecurity Considerations for Grid-Connected Batteries with Hardware Demonstrations, Megan Culler and Hannah Burroughs, May 2021, https://www.mdpi.com/1996-1073/14/11/3067,

[19] 2020 U.S. DOE Energy Storage Handbook, Chapter 18: Physical Security and Cybersecurity of Energy Storage Systems, https://www.researchgate.net/publication/348785890_Chapter_18_Physical_Security_and_Cybersecurity_of_Energy_Storage_Systems.

[20] State of New York, New York's Inter-Agency Fire Safety Working Group, https://www.nyserda.ny.gov/All-Programs/Energy-Storage-Program/New-York-Inter-Agency-Fire-Safety-Working-Group

[21] Sandia, Recommendations for Distributed Energy Resource Access Control, Jay Johnson, January 2021, https://www.osti.gov/servlets/purl/1765273

[22] Sandia, Recommendations for Data-inTransit Requirements for Securing DER Communications, Ifeoma Onunkwo, March 2020. https://www.osti.gov/servlets/purl/1813646.

[23] CISA, LAYERING NETWORK SECURITY THROUGH SEGMENTATION, https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf

[24] Purdue Enterprise Reference Architecture - Wikipedia

[25] NIST.SP.1800-32, Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity, February 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-32.pdf

[26] The Economist, What to make of China's massive cyber-espionage campaign, March 26, 2024, https://www.economist.com/china/2024/03/26/what-to-make-of-chinas-massive-cyber-espionage-campaign

[27] U.S. Department of Justice, Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians, March 25, 2024. https://www.justice.gov/usao-edny/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting

[28] CISA, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, February 24, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[29] CISA, Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013, July 21, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a

[30] Foreign Policy, The top 10 Chinese cyber attacks (that we know of), JANUARY 22, 2010, https://foreignpolicy.com/2010/01/22/the-top-10-chinese-cyber-attacks-that-we-know-of/

[31] CNN, Congressional probe finds communications gear in Chinese cranes, raising spying concerns, Sean Lyngaas, March 2024, https://www.cnn.com/2024/03/07/politics/congressional-probe-communications-gear-chinese-cranes/index.html

[32] The White House, Executive order, FACT SHEET: Biden-Harris Administration Announces Initiative to Bolster Cybersecurity of U.S. Ports, February 2024. https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/21/fact-sheet-biden-harris-administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports/

[33] U.S. Marines Website, BATTERY ENERGY STORAGE SYSTEM RIBBON CUTTING, April 2023, https://www.lejeune.marines.mil/News/Article/Article/3362835/battery-energy-storage-system-ribbon-cutting/

[34] Senate Foreign Relations Committee, Letter to Lloyd Austin, December 1, 2023 https://www.rubio.senate.gov/wp-content/uploads/2023/12/12.01.23-Rubio-Gallagher-letter-to-SecDef-re-CATL.pdf

[35] Fox Business News, Duke Energy removes CCP-tied batteries from green energy project at Marine Corps base: report, February 9, 2024 https://www.foxbusiness.com/technology/duke-energy-removes-ccp-tied-batteries-green-energy-project-marine-corps-base-report

[36] Sans, Practical Risk Analysis and Threat Modeling Spreadsheet, Jason Fossen, July 2009, https://www.sans.org/blog/practical-risk-analysis-and-threat-modeling-spreadsheet/

[37] U.S. Department of Energy, Cyber-Informed Engineering Implementation Guide, August 2023, https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf

[38] IEEE Xplore, A method for assessing the impact of cyber attacks manipulating distributed energy resources on stable power system operation, Phillip Linnartz et al., October 2021, https://ieeexplore.ieee.org/abstract/document/9640033/figures#figures

[39] IEEE Xplore, Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies, Ioannis Zografopoulos, et al., February 2021, https://ieeexplore.ieee.org/document/9351954,

[40] NSA/CISA, Selecting and Hardening Remote Access VPN Solutions, September 2021, https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF

[41] WSJ, Espionage Probe Finds Communications Device on Chinese Cranes at U.S. Ports, Dustin Voltz, Mach 2024, https://www.wsj.com/politics/national-security/espionage-probe-finds-communications-device-on-chinese-cargo-cranes-867d32c0.

[42] PV Magazine, Building a U.S. battery supply chain, January 2024, Anne Fischer, https://pv-magazine-usa.com/2024/01/02/building-a-u-s-battery-supply-chain/