



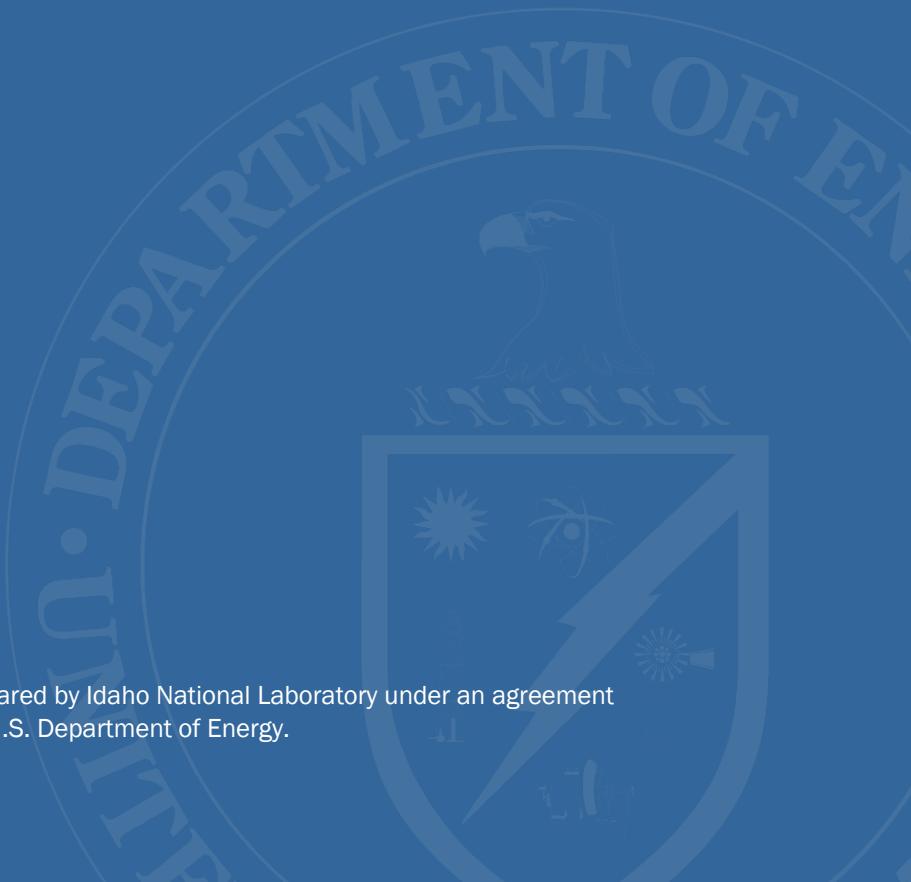
Office of
Cybersecurity, Energy Security,
and Emergency Response

Battery Energy Storage Systems Report

November 1, 2024



This document was prepared by Idaho National Laboratory under an agreement with and funded by the U.S. Department of Energy.



DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

Table of Contents

Introduction	11
Methodology	12
Use Cases, Penetration, and Functions of Grid Scale BESS.....	13
Interconnection Timelines	16
Selected Use Cases for BESS	17
Overall Summary of Functions.....	17
Regional Performance - California.....	20
Regional Performance - Hawaii.....	22
Regional Performance - Texas	22
Known Operational Issues and Events.....	23
Moss Landing.....	23
Western Electricity Coordinating Council (WECC) Heat Event	24
Failure Data Analyses and Root Cause for BESS	25
Technical BESS Architecture, Components, and Functions.....	25
Component Functions.....	27
Battery Management Systems and Environmental Control.....	27
Inverters	28
PCS	28
Power Electronic Transformers and Inverters	29
Sensors and Monitoring	29
Grid Transformers.....	30
Site Control and EMS.....	31
Communications and Cloud	32
DERMS, Software, and Fleet Controllers.....	34
Human-Machine Interface (HMI)	34
Supply Chain for BESS Components	35
Battery Cell/Modules	37
Battery Cell and Integrator Relationships	38
BMS.....	39
PCS.....	40
Inverters.....	41
Summary: Presence of PRC in Combined BESS Supply Chain	43
Supply Chain Analysis Challenges: Commonality and Sources	43

Threats, Vulnerability, and Attack Exposure for BESS.....	46
Threats.....	46
Vulnerability.....	47
Attack Exposure	52
Common Digital and Communication Features in BESS and Power Electronics:	
Risk vs. Benefit.....	54
Communications and Inverters.....	54
Condition Monitoring	54
Supply Chain Threat of PRC Influence for Digital Energy Infrastructure: Evaluating the Technical Risk Landscape.....	55
Grid and Utility-Scale Operational Consequence of BESS Functions	57
DERMS, Software, and Mass Orchestration	60
Integrator Risk Evaluation	61
Scaling Integrator and Aggregator Risk at a Systems Level	62
Supply Chain Threat of PRC Influence for Digital Energy Infrastructure: Business Model and Policy Landscape	65
Roles and Responsibilities in the BESS and Inverter Sector	65
Potential Impact by Stakeholder.....	67
Decentralization of Ownership, Operations, and Maintenance.....	68
Expanding Markets for BESS Suppliers.....	70
Legitimate Persistence within Communications Networks.....	71
Mitigation Planning and Relevant Initiatives.....	74
National Strategies and Policy	74
Legislation	74
Rip-and-Replace.....	75
Limitations of Ban Lists.....	76
Prior Rip-and-Replace Initiatives.....	77
Technical Solutions.....	78
Solution Stakeholders and Targets	78
Cyber-Informed Engineering (CIE) and Technical Assistance Programs	81
Strategic Component Assessment	81
Standards and Regulations.....	82
Develop Hardware and Firmware Citizenship.....	82
Most-Critical Location Analysis	82
Long-Term Strategic Monitoring and Information Sharing.....	83
Contracting and Procurement Guides	83

Key Programs for Solutions.....	83
Summary and Conclusions.....	85
Appendix A: BESS Components and Functions	87
Appendix B: Consequence Ranking and Scoring.....	89
Appendix C: Critical Component Prioritization	90

Figures

Figure 1. Strategic framework for supply-chain risk assessment and mitigation.	13
Figure 2. 2023 U.S. energy storage installations by region (2.0 GW) ⁹	14
Figure 3. U.S. energy storage installations by market share ¹¹	15
Figure 4. U.S. West has 95% of U.S. battery storage capacity additions in Q2 2023 ¹²	15
Figure 5. Annual U.S. cumulative installed battery capacity (as of November 2023).	16
Figure 6. Capacity in interconnection queues as of the end of 2023 ¹⁴	17
Figure 7. Battery-storage capacity and functions in CAISO, from the 2022 Event Report.	20
Figure 8. Total capacity of CAISO-participating battery storage as of May 2023.	21
Figure 9. Texas emergency discharge in February 2024, showing a close to 1 GW ramp in storage.	23
Figure 10. Western area outage of BESS caused by a misconfiguration and performance issue.	24
Figure 11. Global grid-scale BESS deployment and failure statistics.	25
Figure 12. Global grid-scale BESS failure rates from 2018-2023.	25
Figure 13. BESS system architecture.	26
Figure 14. Integrated strategy for component supply for an integrator.	27
Figure 15. Transformer components.	31
Figure 16. BESS communication interconnections.	33
Figure 17. Purdue diagram summary for BESS.	33
Figure 18. U.S. lithium-ion battery imports during Q1 2023.	38
Figure 19. Li-ion battery manufacturing planned (blue) or under construction (red).	38
Figure 20. U.S. PCS providers vs. Chinese PCS providers.	41
Figure 21. Global inverter companies ⁴⁵	42
Figure 22. Supply chain linkages for BESS.	45
Figure 23. Criticality of BESS components to cyber, physical, and safety consequence outcomes.	57
Figure 24. Criticality of BESS functions in grid connection and operation.	60

Figure 25: Assessment Matrix for Suppliers of BESS and integrators.....	63
Figure 26. Use case and comparison of a PRC-based integrator versus a U.S. one.	65
Figure 27. Utility as owner, operator, and maintainer of BESS site.	68
Figure 28. An example of third-party ownership; site in Texas.	70
Figure 29 - List of DOE programs relevant to securing BESS.	85

Tables

Table 1. BESS measurements and performed actions.....	29
Table 2. Barriers and associated hazard types.	30
Table 3. HMI functionalities and connections in BESS.	34
Table 4. Energy storage manufacturers meeting Bloomberg's NEF Tier 1 criteria as of Q2 FY 2024.	36
Table 5. Companies and their main products supplied.	40
Table 6. Specificity of BESS components to supply chain vertical.	44
Table 7. Attack types and potential outcomes	51
Table 8. Ability and negative impact of component misoperation.	56
Table 9. CCE criteria scoring threshold.	59
Table 10: Integrator risk solutions on analysis scale.....	63
Table 11. Roles and responsibilities in the BESS ecosystem.....	66
Table 12. Potential impact by stakeholder.	67
Table 13. Scenarios and correlating solution policies and technical approaches.....	80
Table 14. BESS components and their functions.....	87
Table 15. Example of a consequence matrix.....	89
Table 16. Categorization of BESS components and their capabilities.....	90

Acronyms

AC	Alternating Current	DOE	Department of Energy
AOO	Asset Owner and Operator	DOS	Denial of Service
BABA	Build America Buy America Act	EIA	Energy Information Administration
BESS	Battery Energy Storage Systems	EMS	Energy Management System
BIL	Bipartisan Infrastructure Law	EV	Electric Vehicle
BMS	Battery Management System	FEOC	Foreign Entity of Concern
BNEF	Bloomberg New Energy Finance	FOCI	Foreign Ownership, Control, or Influence
CAISO	California Independent System Operator	G&T	Generation and Transmission
CATL	Contemporary Amperex Technology Company, Limited	GDO	Grid Deployment Office
CCE	Consequence-driven Cyber Informed Engineering	GW	Gigawatt
CIE	Cyber-Informed Engineering	GWh	Gigawatt Hours
CIP	Critical Infrastructure Protection	HBOM	Hardware Bill of Materials
CMC	Chinese Military Company	HMI	Human-Machine Interface
CyTRICS	Cyber Testing for Resilient Industrial Control Systems	IBR	Inverter-Based Resource
DC	Direct Current	IIJA	Infrastructure Investment and Jobs Act
DER	Distributed Energy Resources	INL	Idaho National Laboratory
DERMS	Distributed Energy Resource Management System	IPP	Independent Power Producer
DOD	Department of Defense	IRS	Internal Revenue Service
		ISO	Independent System Operator
		IT	Information Technology
		LLC	Limited Liability Company
		LOTO	Lockout/Tagout

MW	Megawatt	PPA	Power Purchase Agreement
MWh	Megawatt Hour	PRC	People's Republic of China
NDAA	National Defense Authorization Act	PV	Photovoltaic
NERC	North American Electric Reliability Corporation	SBOM	Software Bill of Materials
NGR	Non-Generator Resource	SCADA	Supervisory Control and Data Acquisition
NREL	National Renewable Energy Lab	SEC	Securities and Exchange Commission
O&M	Operation and Maintenance	SIS	Safety Instrumented System
OEM	Original Equipment Manufacturer	SOC	State of Charge
OT	Operational Technology	SOH	State of Health
PCS	Power Conversion System	VPP	Virtual Power Plant
		WECC	Western Electricity Coordinating Council

Introduction

The Bipartisan Infrastructure Law and other federal programs¹ are driving the essential modernization and digitization of U.S. energy infrastructure. Still, the United States faces a key challenge in this grid transformation: our renewable and clean energy supply chains have limited capacity to source necessary digital assets through U.S. or allied sources.²

Batteries and their associated power electronic interfaces are key components to delivering clean and more resilient energy delivery, providing much-needed fast ramping, emergency discharge, generation, and operations support to the electric grid. These services have grown to be invaluable over the past 10 years and will soon be an irreplaceable component of energy delivery.

While there have been significant strides to move supply chains for raw and critical materials to the United States and allied nations,³ the control and power electronic industry has lagged, in part because of lower cost margins. For example, the United States now has a growing capacity to manufacture solar photovoltaic (PV) panels, but 90% of the inverters—which are essential to the conversion of direct current (DC) to alternating current (AC) for grid connection and controls—are made in or source parts from the People's Republic of China (PRC).⁴ A large number of the product integrators who leverage batteries, inverters, and associated devices are U.S.-based companies, employing American people in well-paying jobs and creating hundreds of thousands of jobs in the past five years.⁵ Yet the sourcing of control equipment from Chinese-based entities has an inherent geopolitical concern.⁶

The United States can strategically address battery supply chain risks by pairing short-term steps to operate securely through today's risks with long-term steps to shape the supply chain over the coming years. Federal investments in semiconductors through the CHIPS Act⁷

¹ U.S. Department of Energy, "Grid Resilience and Innovation Partnerships (GRIP) Program," Grid Deployment Office, accessed April 24, 2024, <https://www.energy.gov/gdo/grid-resilience-and-innovation-partnerships-grip-program>.

² National Renewable Energy Laboratory (NREL), "NREL Fall Solar Industry Update FY23," last modified October 26, 2023, <https://www.nrel.gov/docs/fy24osti/88026.pdf>.

³ U.S. Department of Energy (DOE) Loan Programs Office, "Sector Spotlight: Critical Materials," last modified July 9, 2024, <https://www.energy.gov/lpo/articles/sector-spotlight-critical-materials>.

⁴ California Energy Commission, "Solar Equipment Lists," accessed April 24, 2024, <https://www.energy.ca.gov/programs-and-topics/programs/solar-equipment-lists>.

⁵ Gardner, Timothy. "Jobs in US energy grew 3% in 2022, led by work in clean energy," Reuters, June 28, 2023, <https://www.reuters.com/business/energy/jobs-us-energy-grew-38-2022-led-by-work-clean-energy-2023-06-28/>.

⁶ Pandolfo, Chris, "Duke Energy removes CCP-tied batteries from green energy project at Marine Corps base: report," Fox Business, February 9, 2024, <https://www.foxbusiness.com/technology/duke-energy-removes-ccp-tied-batteries-green-energy-project-marine-corps-base-report>.

⁷ The White House, "FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China," last modified August 9, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/>.

and other manufacturing programs⁸ will result in U.S. supply chains for batteries and power electronics that will begin to mature over the next 5 to 10 years. In the meantime, U.S. asset owners must also leverage available battery and electronics equipment to meet their goals and maintain cost. The demand signal for these components must be maintained to continue domestic industry growth at a sufficient pace to realize the economic benefit of these federal supply chain investments.

Addressing the current push and pull between our accelerating energy transition and the cybersecurity of our future energy infrastructure will require a suite of policy, technical, and organizational approaches. Determining the optimal decisions requires an end-to-end assessment of the supply chain to identify and prioritize risks. This report details that assessment, including key findings on the state of risk and recommendations informed by quantifiable cyber-informed engineering and data-driven solutions.

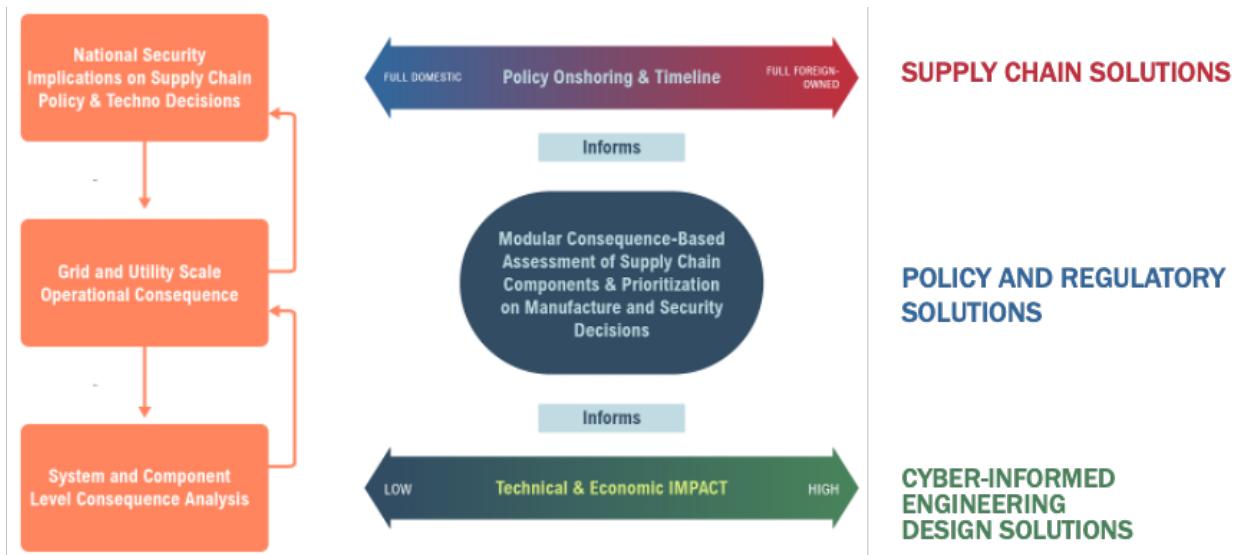
Methodology

Our approach is a systemic analysis that evolves from a macro to a micro perspective, focusing on the tasks the systems are expected to perform and the penetration levels and use cases in the evolving energy-delivery system. Figure 1 represents the paper's analytical framework, illustrating the interdependencies between national security implications on the supply chain and subsequent policy and technological decisions, as well as the flow of consequences from grid and utility-scale to individual system and component levels. The analysis presented evaluates the national security implications of policy and technical and supply chain decisions through a series of consequence-driven components and a system of systems functionality study. Categorizing these risks on multiple levels enables a framework of decisions to be made, which optimize both technical and economic supply chain investment decisions for U.S. manufacturing and the prioritization of mitigations using Cyber-Informed Engineering⁹ and alternative types of tooling in development at the Department of Energy and other industry capabilities. The study can then be used to identify gaps in tooling and resources for future research and development as the policy changes to the supply chain take shape.

⁸ Department of Energy, “Biden-Harris Administration Announces \$3.5 Billion to Strengthen Domestic Battery Manufacturing,” last modified November 15, 2023, <https://www.energy.gov/articles/biden-harris-administration-announces-35-billion-strengthen-domestic-battery-manufacturing>.

⁹ Department of Energy, “Cyber-Informed Engineering,” <https://www.energy.gov/ceser/cyber-informed-engineering>

Figure 1. Strategic framework for supply-chain risk assessment and mitigation.



This report offers a strategic plan for evaluating battery system components from end to end, employing methodologies and subject matter expertise to measure the magnitude of current challenges and benefits of a new evaluative approach—a system of systems approach. This requires not only a comprehensive assessment but also a strategic allocation of resources to bolster both the supply chain and the operational security of battery energy storage systems (BESS) and their associated systems.

Use Cases, Penetration, and Functions of Grid Scale BESS

Battery systems fulfill a variety of important roles in the electric grid contingent upon the unique market demands and specific challenges of regional grid infrastructures. These roles also vary due to the differing business models for ownership and operation and they are often adapted to regional capabilities and requirements.

The Storage Futures Study conducted by the National Renewable Energy Laboratory (NREL)¹⁰ forecasts significant growth in national storage capacity over the coming decades. In the reference case, it is projected to increase from approximately 25 gigawatts (GW) in 2020 to around 200 GW by 2050. Within this capacity, battery storage is anticipated to constitute approximately 175 GW, with the remaining amount supplied by pumped hydropower. The surge in demand for lithium-ion batteries is chiefly attributed to electric vehicles (EVs), although stationary storage is also expected to increase substantially, reaching approximately 1,000 gigawatt hours (GWh) by 2030. Projections for utility-scale BESS indicate a decline in energy prices by 2–3 times their 2020 levels by the year 2050. Figure 2 shows the potential for BESS installed and planned capacity in the United States.¹¹

Figure 2. 2023 U.S. energy storage installations by region (2.0 GW)⁹.



The market has accelerated with a 10-fold increase in energy capacity (in megawatt hours) installed from 2018 to 2020.¹² The U.S. Energy Information Administration (EIA)¹³ reports that the United States will install approximately 4 GW of new storage in 2023 (Figure 3), with 35% installed in California and 27% in Texas (Figure 4). The EIA also reported that as of January 2024 (Figure 4), installed storage capacity is predicted to double between 2024 and 2025 (Figure 5).

¹⁰ National Renewable Energy Laboratory (NREL), "Storage Futures Study," accessed April 24, 2024, <https://www.nrel.gov/analysis/storage-futures.html>.

¹¹ Jorgenson, Jennie A., Frazier, Will, Denholm, Paul, and Nate Blair, "Grid Operational Impacts of Widespread Storage Deployment," National Renewable Energy Laboratory (NREL), NREL/TP-6A40-80688, last modified 2022, <https://www.nrel.gov/docs/fy22osti/80688.pdf>.

¹² S&P Global Commodity Insights, "Powering Decisions," accessed April 24, 2024, <https://www.spglobal.com/commodityinsights/en>.

¹³ U.S. Energy Information Administration, "Battery Storage in the United States: An Update on Market Trends," last modified July 24, 2023, <https://www.eia.gov/analysis/studies/electricity/batterystorage/>.

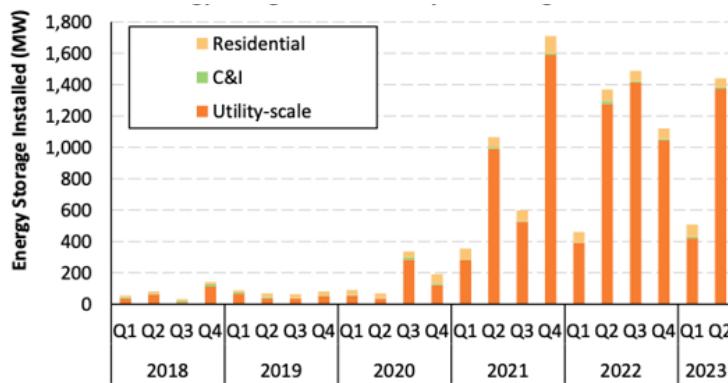
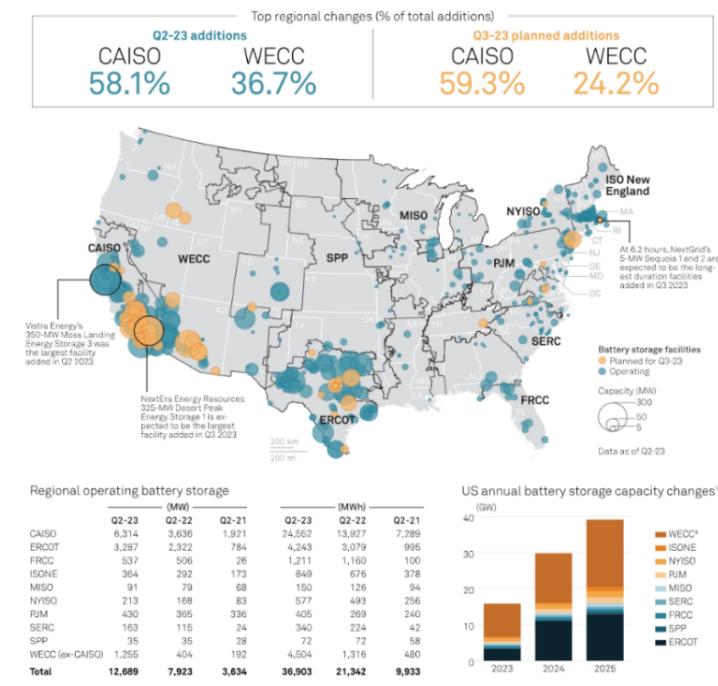
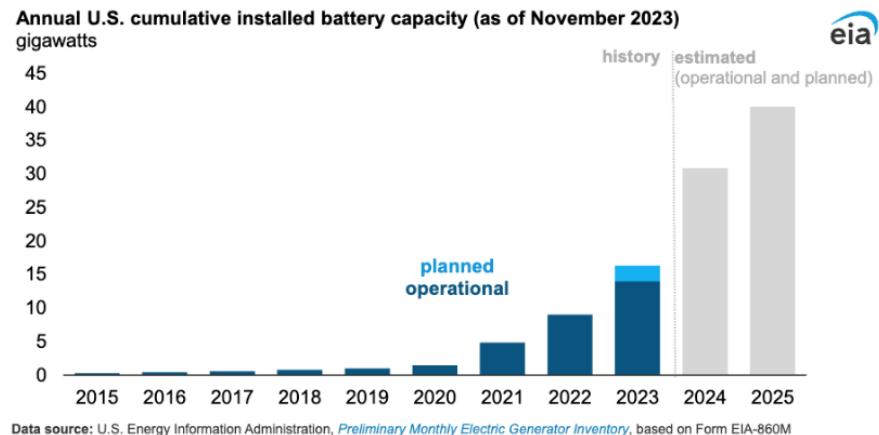
Figure 3. U.S. energy storage installations by market share¹¹.**Figure 4. U.S. West has 95% of U.S. battery storage capacity additions in Q2 2023¹².**

Figure 5. Annual U.S. cumulative installed battery capacity (as of November 2023).



Interconnection Timelines

Interconnection to the electric grid for energy delivery products—especially inverter-based resources such as BESS—requires a detailed set of power flow, environmental, operational, and dynamic studies to ensure they can operate reliably and beneficially.

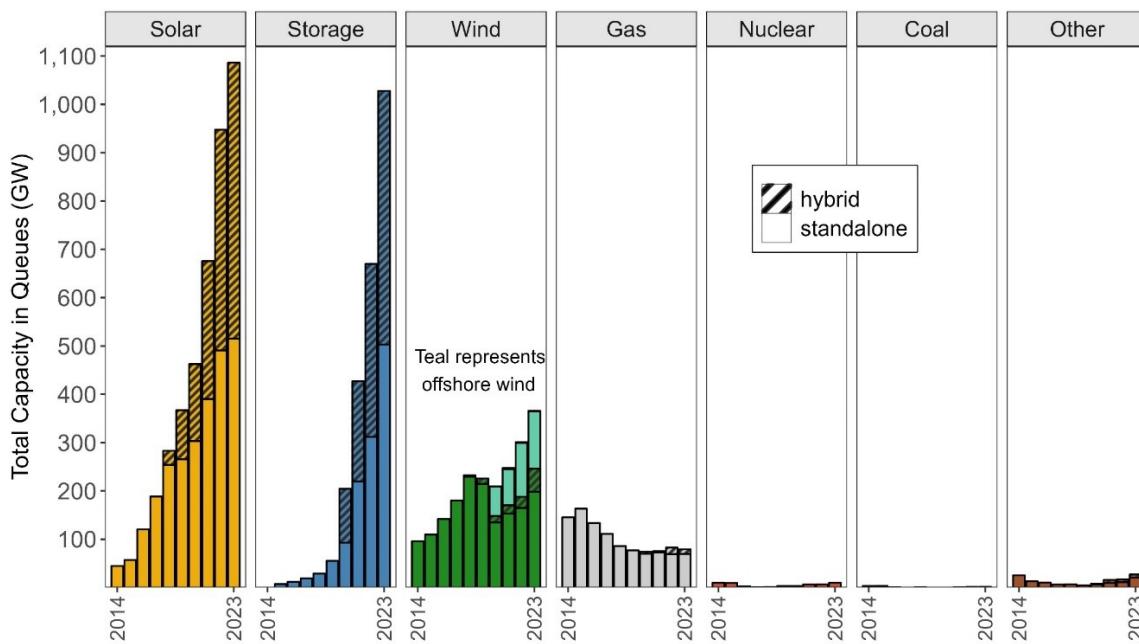
The process tests system and operational scenarios, such as different load conditions and emergency scenarios in a power flow model of the electric site to which it is connecting. While crucial, this interconnection process presents a set of challenges to getting new projects online:

- The recommendations of the interconnection studies often require cost estimates to interconnect grid upgrades or mitigations such as a max output requirement to a particular line;¹⁴ these are often performed by consultants and the utilities themselves.
- During the interconnection process, equipment selection is often performed to ensure the right models are selected, which requires that inverter functions and battery operational requirements be known.
- Additionally, interconnection queues form for sites waiting for these studies so they may begin building. In fact, as illustrated in Figure 5, as of the end of 2023, there is approximately 1030 GW of storage and hybrid storage in the queue—enough to serve all U.S. customers for 1 hour¹⁵.

¹⁴ Savion Energy, “Energy Storage Development Process,” accessed April 2024, <https://savionenergy.com/energy-storage-and-development/>.

¹⁵ Rand, Joseph, Manderlink, Nick, Gorman, Will, Wiser, Ryan, Seel, Joachim, Mulvaney, Julie Kemp, Jeong, Seongeun, and Fritz Kahrl, “Queued Up: Characteristics of Power Plants Seeking Transmission Interconnection,” last modified April 2024, <https://emp.lbl.gov/queues>.

Figure 6. Capacity in interconnection queues as of the end of 2023¹⁴.



- As of 2023, an interconnection takes a maximum of 50 months from request to agreement, at which point the requestor can proceed with the full build, which then can take more than 3 years to complete (Figure 6). Therefore, projects coming online in 2024 likely received interconnect agreements in 2021 and joined the interconnection queue between 2017 and 2018. Supply chain variations during this time have had an enormous impact on the bankability of these projects.

To be successful, projects must have a strong supply chain plan, consistent information and funding stability, and technical viability. However, most proposed projects have been withdrawn for a variety of reasons.

Selected Use Cases for BESS

Overall Summary of Functions

Batteries, particularly utility-scale batteries, provide a range of essential services to the power grid in the United States—services that are vital for maintaining the stability, efficiency, and reliability of the grid. To evaluate the risk associated with their growing penetration, including the impact of the supply chain and risk of foreign control, the functions of these systems and the services they provide must be well understood. Key grid services performed by batteries include:

1. **Frequency and Voltage Regulation:** Batteries help maintain the grid's electric frequency on a millisecond-to-second basis. This is one of their most common uses and is crucial to preventing deviations in frequency that can lead to system instability; batteries are ideal as they can quickly respond to changes without the need for startup time. Because they can quickly absorb surges and release energy, maintaining grid frequency close to its target value, batteries are well suited for frequency regulation. Similarly, they can help maintain a constant voltage on the power system by injecting or absorbing reactive power, which can correct voltage drops at the end of lines or help maintain voltage stability during transient events with droop control. Voltage support also requires a quick response time, which is a feature that batteries provide via their control systems and power electronics in the inverters.
2. **Energy Arbitrage:** Batteries can store electricity when prices are low and release it back into the grid when prices are high. This process, known as energy arbitrage, helps to balance electricity supply and demand and can lead to economic benefits by capitalizing on variable energy prices. The timeframe for energy arbitrage can vary widely, from a few hours to a full day. Batteries charge during periods of low electricity prices (often during low-demand times) and discharge when prices are higher (typically during peak-demand periods).
3. **Ramping or Spinning Reserve:** Ramping or spinning reserve involves quickly responding to sudden changes in the grid, such as a rapid change in demand or the sudden loss of generation; batteries used can typically respond within minutes to these sudden changes in grid conditions. This is particularly valuable in regions with a high proportion of renewable energy sources, such as wind and solar, where output can fluctuate based on changing weather conditions.
4. **Load Following:** Batteries can adjust their output to match changes in electricity demand. This capability is valuable for more efficient load change response, putting less stress on the grid compared to mechanical systems. Batteries performing load following adjust their output to match changes in electricity demand, generally operating on a scale of minutes to hours, responding to more gradual changes in load throughout the day.
5. **Peak Shaving and Congestion Relief:** By discharging during peak demand periods,¹⁶ batteries can reduce the need for higher-cost, seldom-used generation capacity, leading to overall lower wholesale electricity prices and a more balanced demand on the grid. For peak shaving, batteries discharge during periods of peak demand, which can last for several hours, usually in the late afternoon or early evening when electricity demand is highest. For congestion relief, the batteries are discharged to serve a local load and reduce the perceived demand for the transmission system. This occurs at times of high

¹⁶ U.S. Energy Information Administration, "Peak Hourly U.S. Electricity Demand In July was the Second Highest Since 2016," October 5, 2023, <https://www.eia.gov/todayinenergy/detail.php?id=60602>.

load when significant power has to be transferred from generation sources to load centers, putting stress on the capacity of the transmission system.

6. **Storing and Smoothing Renewable Generation:** Batteries can store excess electricity generated from renewable sources such as solar and wind and then supply it back to the grid or to local loads as needed. This reduces curtailments and helps in managing the intermittency of renewable sources. The timeframe depends on the variability of the renewable energy source. For solar energy, this could involve storing excess energy during midday and releasing it in the evening, while for wind energy, it could involve longer or more variable periods, depending on wind patterns.
7. **Deferring Infrastructure Investment:** Batteries can be used strategically to manage growing electricity demand in specific areas, largely by reducing peak loads over time, to help defer or delay the need for costly new grid infrastructure such as upgraded substations or additional distribution lines. This is a longer-term application where batteries might be used intermittently, depending on local demand growth patterns.
8. **Reducing End-Use Consumer Demand Charges:** For commercial and industrial facilities, onsite energy storage used during peak demand times can lower electricity demand charges, which are based on the highest rates of consumption observed during peak periods. This application typically targets peak demand periods, which can last for a few hours each day, particularly during times when electricity prices are highest.
9. **Backup Power:** For outages or to support electric reliability, batteries can provide backup power to households, businesses, and parts of the distribution grid. They are also integral to advanced microgrid setups, helping maintain power flow during temporary separations from the main grid. The duration for backup power can vary significantly based on the capacity of the battery system and the energy needs of the connected load, ranging from a few hours to days, especially in advanced microgrid setups.
10. **Black Start and Grid Forming:** In some cases, when an outage is experienced, immediate detection of the outage can allow local generation sources to quickly pick up the load and support a seamless transition to backup power. However, this is often not the case, and it may even be dangerous to do so at the risk of creating unintentional islands (i.e., powering loads that are not intended to be run on the backup power). After the outage begins, batteries can be used to black start the system, powering first local loads, then increasing output or supporting other generation sources as they come online to bring power back to the entire system. Because batteries cannot support as much inrush current as traditional synchronous generators of the same capacity, the re-energization of loads must be done with care and consideration. Batteries acting as a grid-forming source can enable other resources, such as wind and solar, to come online in a grid-following mode, which is often better suited for variable resources. The primary duty of a grid-forming source is to dynamically adjust its output to ensure that the load

and generation are balanced at all times, which can be done using local feedback of voltage and frequency.

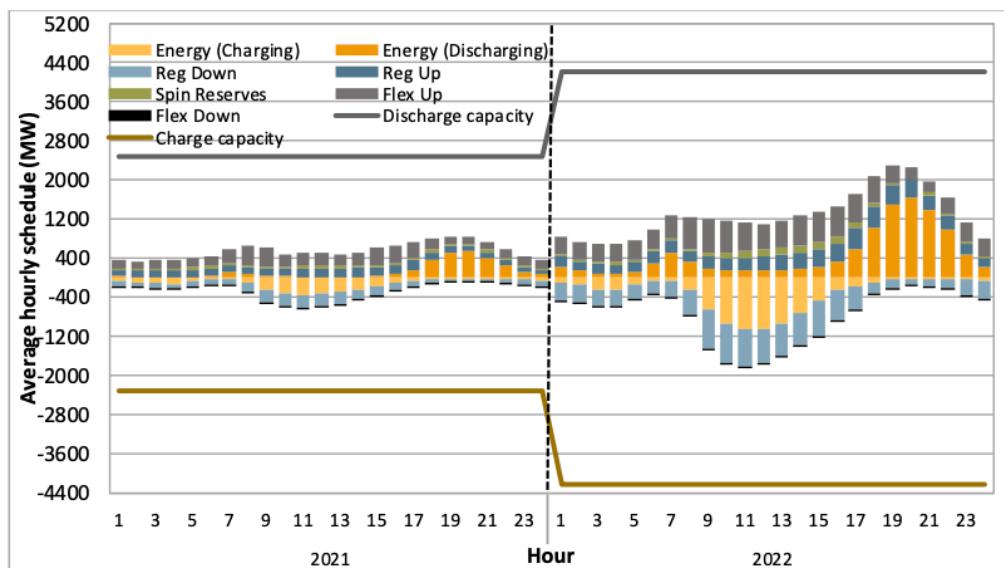
These services illustrate the growing importance of battery storage in enhancing the grid's resilience, flexibility, and ability to integrate renewable energy sources. As the deployment of battery storage continues to increase, its role in the U.S. energy grid is likely to expand and evolve, offering new solutions for energy management and grid stability.

Regional Performance - California

In California, BESS play a significant role in helping the state meet its ambitious clean energy goals and provide critical support in emergencies:

- By storing excess energy generated from renewable sources during periods of low demand, BESS help optimize the utilization of clean energy resources, thereby reducing reliance on fossil fuels.
- Their rapid response and ramping capabilities make BESS invaluable assets during heat emergencies¹⁷, in which spikes in energy demand can strain the grid. By providing additional power when needed most, BESSs enhance grid stability and help prevent disruptions in critical services.

Figure 7. Battery-storage capacity and functions in CAISO, from the 2022 Event Report.



As illustrated in Figure 7, the California Independent System Operator (CAISO) has experienced a significant expansion in battery storage capacity and related functions. By

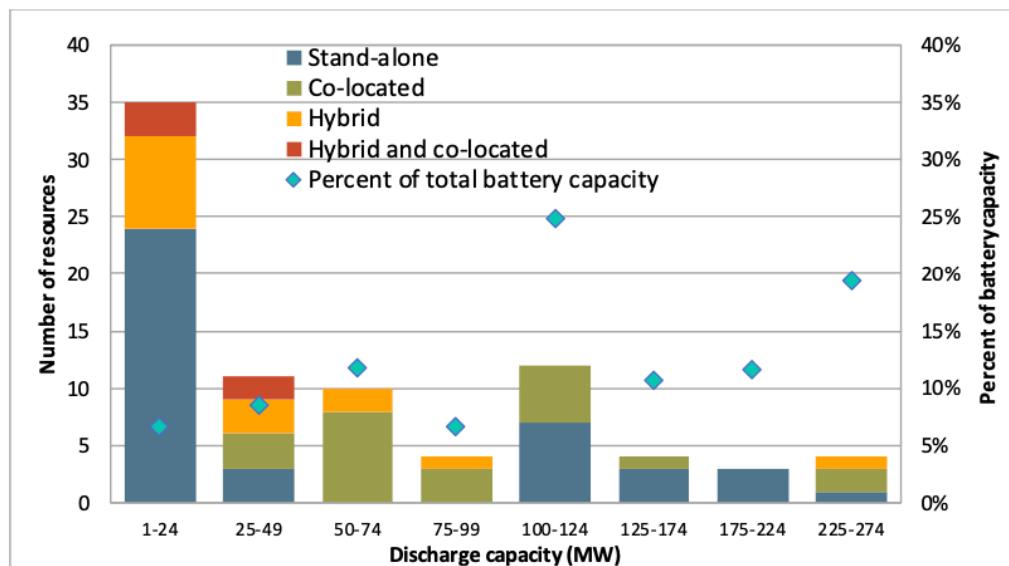
¹⁷ California Independent System Operator (CAISO), "Special Report on Battery Storage," last modified July 7, 2023, <http://www.caiso.com/Documents/2022-Special-Report-on-Battery-Storage-Jul-7-2023.pdf>.

May 2023, the total active battery capacity reached 5,000 megawatts (MW). Figure 8 details how the capacity expansion is distributed across various project types:

- Standalone projects contributed 2,200 MW
- Co-located projects added 2,000 MW
- Storage components of hybrid resources accounted for 700 MW
- Storage components of co-located hybrids contributed 100 MW

At the same time, the total active hybrid capacity, including generation components, reached 2,300 MW. This surge in battery-storage capacity reflects the increasing importance of energy storage in California's grid infrastructure, facilitating grid stability, renewable integration, and overall system reliability.

Figure 8. Total capacity of CAISO-participating battery storage as of May 2023.



During the 2022 heatwave, batteries showcased their flexibility, offering a significant portion of both charging and discharging capacity to the market. Early in the day, average output schedules—including energy discharging, regulation, reserves, and ramp—intentionally decreased to allow the batteries to charge. During peak hours, both charging and discharging schedules increased compared to usual trends, though charging remained low on average. Batteries provided a large share of total regulation, including full coverage for some intervals. On average, scheduled battery output was about 82% of available capacity. In both real-time and day-ahead markets, batteries actively sought to charge during mornings and early afternoons. Discharge bids in the day-ahead market remained constant throughout the day. Interestingly, despite high bids, batteries averaged below the peak-demand nodal price. Notably, real-time discharge bids even decreased during peak hours. CAISO operators leveraged exceptional dispatches (out-of-market manual interventions) for unit commitments and energy dispatches, when deemed necessary, to address reliability.

issues or constraints. Battery-storage resources received exceptional dispatches throughout the heatwave, primarily to encourage charging in anticipation of peak demand hours.

With careful planning and investment, BESS can be a valuable asset to the CAISO grid. In CAISO's market, BESS operate under the Non-Generator Resource (NGR) model, allowing them to function both as generation resources when discharging and as load resources when charging. This unique framework enables BESS to participate in the market using a single supply curve that encompasses both charging and discharging prices. This streamlined approach enhances market efficiency and simplifies the dispatch process for BESS operators.

Regional Performance - Hawaii

Commissioned in 2023, a 185 MW BESS has been successfully deployed in Hawaii to replace coal on the island of Oahu, marking a significant milestone in Hawaii's transition to 100% renewable energy.¹⁸ This cutting-edge BESS, operated by Hawaiian Electric, is a key component in accelerating the state's renewable energy goals. With a storage capacity of 185 MW and capable of discharging 565 megawatt hours (MWh) of energy, the system enhances grid stability and facilitates the integration of renewable energy sources like solar and wind power. Its advanced capabilities enable efficient energy management, supporting Hawaii's ambitious targets for reducing carbon emissions and reliance on fossil fuels.

Hawaiian Electric's BESS is equipped with state-of-the-art technology, including advanced lithium-ion batteries and sophisticated control systems, ensuring optimal performance and reliability. The system's deployment underscores Hawaii's commitment to sustainable energy solutions and resilience against climate change impacts.

Regional Performance - Texas

The recent solar eclipse in Texas sheds light on the crucial role of battery storage in maintaining energy supply reliability during periods of intermittent renewable generation. As solar output dropped significantly during the eclipse, the grid faced challenges in balancing supply and demand (see Figure 9). However, battery storage systems helped bridge the gap by providing stored energy when solar generation was unavailable, demonstrating their importance in enhancing grid resilience and ensuring uninterrupted energy supply, especially in regions heavily reliant on renewable energy sources.

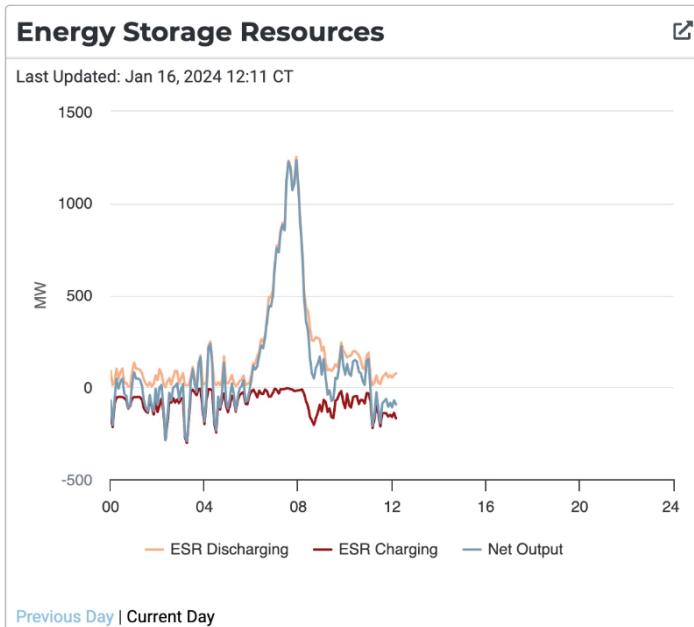
The eclipse event, coupled with another 17+ emergency dispatch events for BESS in 2022–2024,¹⁹ illustrates the need for further investment and expansion of battery storage infrastructure to mitigate the impacts of renewable energy intermittency on grid stability and

¹⁸ Spector, Julian, "Hawaii to Replace Coal on the Island of Oahu," Canary Media, last modified January 10, 2024, <https://www.canarymedia.com/articles/energy-storage/a-huge-battery-has-replaced-hawaiis-last-coal-plant#:~:text=Plus%20Power's%20Kapolei%20battery%20is,fueled%20plants%20to%20clean%20energy.>

¹⁹ Carter, David and Tu Nguyen, "Texas Energy Supply During Eclipse Highlights Importance of Battery Storage," April 10, 2024, <https://realeconomy.rsmus.com/texas-energy-supply-during-eclipse-highlights-importance-of-battery-storage/>.

enhance overall system reliability.²⁰ It also underscores the importance of adopting innovative energy storage solutions to support the transition towards a more sustainable and resilient energy system capable of meeting the evolving demands²¹.

Figure 9. Texas emergency discharge in February 2024, showing a close to 1 GW ramp in storage.



Known Operational Issues and Events

Moss Landing

While the 2022 fire incident involving a Tesla grid battery at Moss Landing in California raised concerns about the safety of grid-scale battery systems, it also served as a learning opportunity for stakeholders to address the industry's growing pains.²² The incident demonstrated the importance of stringent safety protocols and regulatory oversight in ensuring the reliability and security of energy storage deployments. Despite the setback, the incident also showcased the resilience of Tesla's battery technology, as the affected unit continued to function even after sustaining significant damage, preventing a potentially more severe outcome.

²⁰ Fred Lambert, "Tesla Megapacks are About to Replace Hawaii's Last Remaining Coal Plant," *Electrek*, June 27, 2022, <https://electrek.co/2022/06/27/tesla-megapacks-replace-hawaii-last-remaining-coal-plant/>.

²¹ Balaraman, Kavya, "California Sets 7 GW Load Shift Goal for Demand Response," *Utility Dive*, June 6, 2023, <https://www.utilitydive.com/news/california-7-gw-load-shift-goal-demand-response/652135/>.

²² Australian Associated Press, "Tesla Lithium Battery Fire Hits 'Landmark' Queensland Energy Project, Sparking Political Debate," *The Guardian*, last modified September 26, 2023, <https://www.theguardian.com/australia-news/2023/sep/27/tesla-lithium-battery-fire-bouldercombe-energy-storage-site-project-rockhampton>.

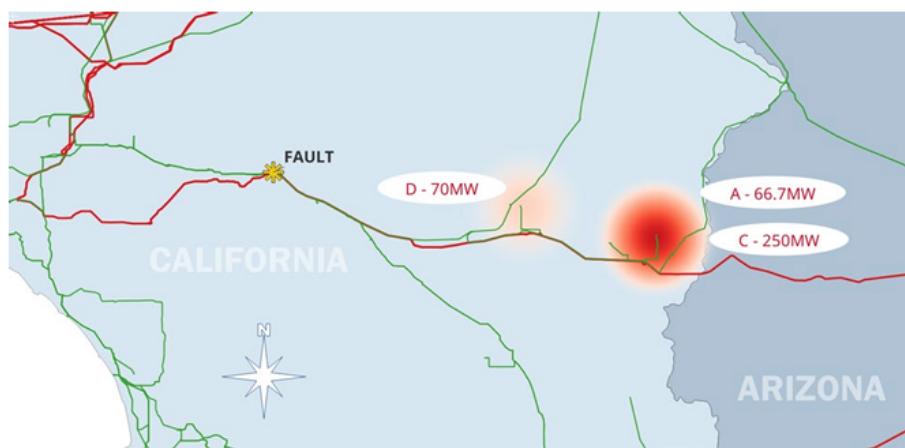
The Tesla grid battery fire brings attention to the need for continued innovation and improvement in energy storage technology and safety standards. As the industry matures, stakeholders must collaborate to develop robust safety measures and emergency response protocols to mitigate risks and ensure the long-term viability of energy storage deployments.

Western Electricity Coordinating Council (WECC) Heat Event

Several incidents—including BESS trips, reduced capacity, and thermal issues—occurred due to the extreme heat experienced by BESS in the Western Interconnection region (see Figure 10). As temperatures soared, BESS units struggled to manage thermal loads, resulting in degraded performance and, in some cases, complete shutdowns²³. The root cause of these failures was primarily attributed to the inability of BESS to effectively dissipate heat under extreme temperature conditions, together with poor commissioning, miscoded inverters, and bad data.

One of the key contributing factors to the heat-related failures was the design limitations of BESS cooling systems. Many BESS installations were not adequately equipped to handle the intense heat levels experienced during the event, leading to thermal stress on critical components. Additionally, operational practices such as reduced charge and discharge rates were implemented to mitigate thermal issues, further impacting BESS performance and grid reliability. The software was updated in both the CAISO 2022 and WECC 2023 events and tested to prevent a similar issue from occurring.

Figure 10. Western area outage of BESS caused by a misconfiguration and performance issue.



²³ North American Electric Reliability Corporation, (NERC), “2022 California Battery Energy Storage System Disturbances,” last modified September 2023, https://www.nerc.com/comm/RSTC/Documents/NERC_BESS_Disturbance_Report_2023.pdf.

Failure Data Analyses and Root Cause for BESS

While there is discussion of BESS with regards to fires and other events²⁴, tracked data indicates a reduction in fires, particularly those attributed to thermal runaway in the battery cell material. Overall catastrophic failures are lessening, now mostly driven by controls and power conversion systems (PCS). Material quality has improved; even with the majority of the material being produced in China. This runs counter to many assumptions of offshoring risk. The majority of fires are attributed to the controls and faults in the battery management system (BMS) and battery optimization system, along with the PCS (Figure 11 and Figure 12).

Figure 11. Global grid-scale BESS deployment and failure statistics.

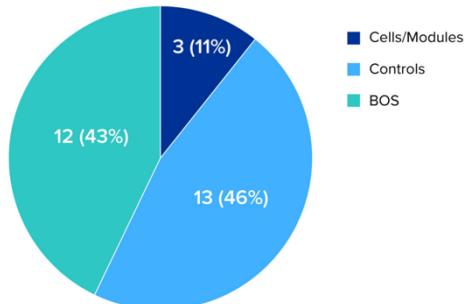
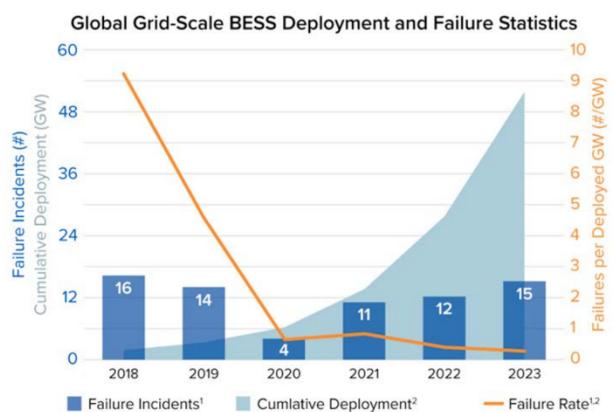


Figure 12. Global grid-scale BESS failure rates from 2018-2023.



Courtesy EPRI and Wood Mackenzie.

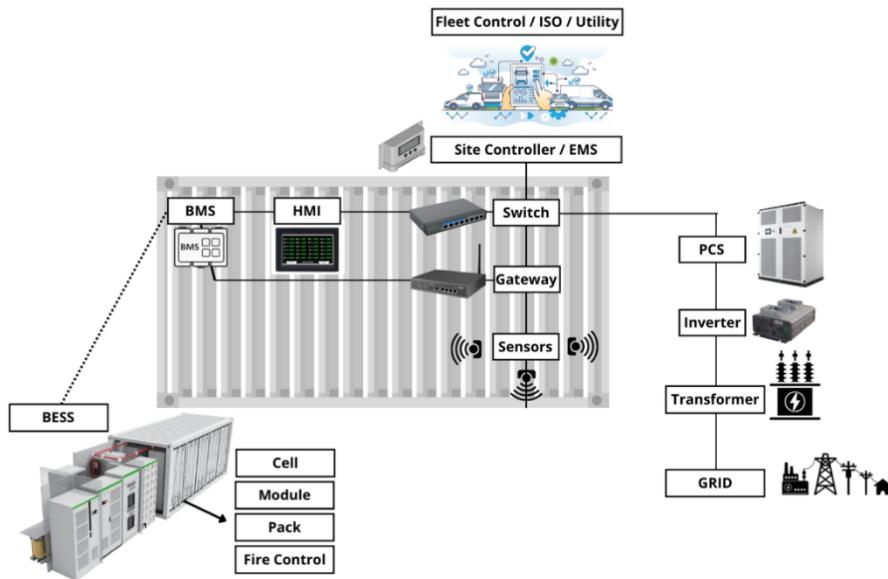
Technical BESS Architecture, Components, and Functions

Different architectures for BESS can have various configurations and components, ranging from fundamental cell-level setups to comprehensive systems encompassing controls and

²⁴ Jones, Willie D., “Extinguishing the EV Battery Fire Hype: The Numbers Don’t Support Persistent Fears of Lithium-Ion Conflagrations,” IEEE Spectrum, December 4, 2023, <https://spectrum.ieee.org/lithium-ion-battery-fires>.

additional functionalities. Batteries are but one component, with configuration dependent on features including size and utilization, as illustrated in Figure 13.

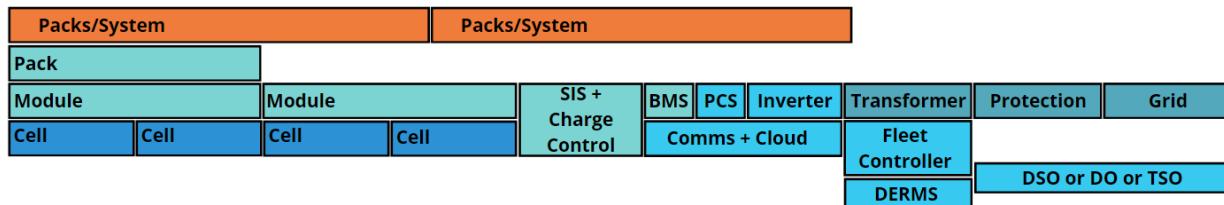
Figure 13. BESS system architecture.



- **Cell level:** At the most basic level, BESS architecture revolves around individual battery cells. These cells form the foundational building blocks of the energy storage system. They are typically connected in series and parallel configurations to achieve the desired voltage and capacity requirements.
 - This architecture focuses primarily on the electrochemical performance and characteristics of the battery cells themselves, including factors such as energy density, cycle life, and safety features.
- **Integrated controls and components:** A more comprehensive approach involves integrating various controls and additional components into the BESS. This includes incorporating BMS to monitor and manage the performance, state of charge, and health of the battery pack. Additionally, safety mechanisms (e.g., thermal management systems and protective enclosures) are implemented to ensure safe operation under diverse conditions.
 - Integration with power conversion systems, inverters, and grid interfaces enables bidirectional power flow and seamless integration with renewable energy sources or electrical grids.
- **Integrated hardware and software:** In more advanced BESS architectures, there is a focus on integrating the hardware components with sophisticated software solutions. This involves the deployment of intelligent control algorithms, predictive analytics, and optimization strategies to maximize the performance and efficiency of the energy storage system. Integrators play a crucial role in designing and implementing these

software-driven functionalities, tailoring them to specific use cases and operational requirements (Figure 14).

Figure 14. Integrated strategy for component supply for an integrator.



Component Functions

Battery Management Systems and Environmental Control

The BMS is both a hardware and software component, which connects to the energy management system EMS and PCS to manage the system's charge and discharge and provide environmental monitoring of the battery cells. Common architectures and functions within the BMS play an important role in ensuring operational safety, efficiency, and reliability. These functions include signaling mechanisms, fire alarms, emergency stop functionalities, insulation breakdown detection, temperature monitoring, and management of over and under current. Each function safeguards against potential failures²⁵ that could lead to adverse outcomes. For example:

- Failure in signaling mechanisms could result in delayed responses to operational issues.
- A malfunctioning fire alarm system could lead to delayed detection of fire hazards, potentially causing extensive damage or endangering lives.
- Failure in emergency stop functionalities could impede the ability to quickly halt operations in hazardous situations, increasing the risk of accidents.
- Insulation breakdown detection failures might lead to electrical faults or short circuits, posing fire risks or damaging equipment.
- Malfunctions in temperature monitoring and management systems could result in overheating, reducing the lifespan of components, or even causing thermal runaway events.
- Inadequate protection against overcharging could lead to battery degradation, reducing performance and longevity.
- Voltage imbalances, if left unaddressed, can cause uneven distribution of energy within the system, potentially leading to inefficiencies, reduced performance, or even damage to sensitive components.

²⁵ EPRI, “Insights from EPRI’s Battery Energy Storage Systems (BESS) Failure Incident Database: Analysis of Failure Root Cause,” May 2024, <https://www.epri.com/research/products/000000003002030360>.

When well-managed, advanced BMS can help optimize performance, improve lifetimes, and prevent runaway failures or catastrophes.

Inverters

The inverter is responsible for converting DC electricity from the battery into AC electricity, enabling integration with the electrical grid or other AC loads. It connects to both the battery system and the electrical grid or loads, forming a bidirectional link for energy flow. In BESS architecture, the inverter is typically positioned between the battery storage unit and the grid or loads, serving as an intermediary for power conversion and control. The inverter uses various measurements—including voltage, current, frequency, and temperature—to ensure efficient and stable operation. It is often combined with the power conversion system.

Actions performed by the inverter include:

- Performing frequency droop control and voltage droop control to regulate grid frequency and voltage levels, respectively
- Establishing voltage and frequency references
- Implementing virtual generator inertia to mimic the behavior of traditional generators
- Managing real power vs. reactive power output
- Supporting the utility grid during voltage or frequency disturbances through utility support mode
- Facilitating black start capabilities to restore power in the event of a grid outage

Inverters can be supplied as three-phase, single-phase, or micro. Many companies that sell inverter hardware also sell BMS and other devices as an interlinked system. In large BESS, three-phase inverters are the most common, but solar may also include microinverters if combined in hybrid configurations. Home storage units are usually single-phase or micro.

PCS

Power conversion systems are essentially the larger parent of the inverters, comprised of conversion and power conditioning equipment and potentially small transformers; they are often larger-scale systems that encompass multiple inverters, together with additional control and protection components. PCS refers to the combined system used to convert and manage the quality of power from one form to another within an electrical power grid. Functions and attributes of the PCS include the following:

- Controls the power flow, integration, and synchronization among various power sources and loads, generally for large sites rather than distributed energy resources DER. This coordination enables efficient and reliable operation of diverse sources, as well as loading.

- Has significant processing power to allow advanced control algorithms to optimize power management.
- Monitors grid conditions, regulates voltage and frequency, and facilitates smooth transitions between power sources or operational modes.
- Includes vital safety features such as fault detection, isolation, and protection mechanisms.
- Accounts for the wider perspective of system-level integration, control, and monitoring.

Power Electronic Transformers and Inverters

Many inverters also include a small transformer, often a solid-state transformer in more modern systems, to enable consistent power supply and connection to the electric grid. These transformers are embedded in the inverters themselves and separate from the on-site grid transformer.

Sensors and Monitoring

The BESS and its BMS rely on critical measurements such as state of charge (SOC), battery temperature, voltage and current levels, power output and input, and grid frequency and voltage. These measurements enable the system to perform actions such as controlling charging and discharging processes, managing thermal conditions, detecting and isolating faults, regulating grid frequency and voltage, and balancing loads and shaving peaks to ensure optimal performance and safety (Table 1. BESS measurements and performed actions.).

Table 1. BESS measurements and performed actions.

Measurements	Actions Performed
State of charge	Charge and discharge control
Battery temperature	Thermal management (cooling/heating)
Voltage and current levels	Fault detection and isolation, charge and protection
Power output and input	Grid frequency and voltage regulation
Grid frequency and voltage	Load balancing and peak shaving

There is also significant sensoring required for safety, environment and physical security, as summarized in Table 2. Barriers and associated hazard types.. Most of these share data with the BMS or Environment Manager. Some perform manual actions with no cyber components, while others are connected with larger required fire protections.

Table 2. Barriers and associated hazard types.

Barriers	Hazard Type	Function	Connected to
BMS monitoring	Electrical, thermal	Current, voltage, SOC, and temperature monitoring	BMS to EMS
Cooling system	Thermal	Temperature regulation of BESS	Fire and Environmental Safety - EMS
Thermal insulation	Thermal	Minimize heat transfer between battery modules/racks	BMS
Fire and smoke detector	Fire	Detect smoke and produce visual and audible alerts at the control center	Fire Safety and Control Center
Active fire suppression	Fire	Fire suppression, extinguishment, and cooling	Manual action detects manual conditions
Gas detection	Explosion	Early detection for accumulation of flammable gases before reaching explosive	Fire and environmental safety - EMS
Emergency ventilation	Explosion	Removal of gas before reaching explosive concentration	Fire and environmental safety - EMS
Emergency shutdown	Electrical/fire	Electrical isolation	Manual and Automated
Circuit breaker	Electrical	Electrical isolation	Manual and Automated
Intrusion detection	Physical	Detect unauthorized physical access and open doors of BESS	Emergency response and control center

Grid Transformers

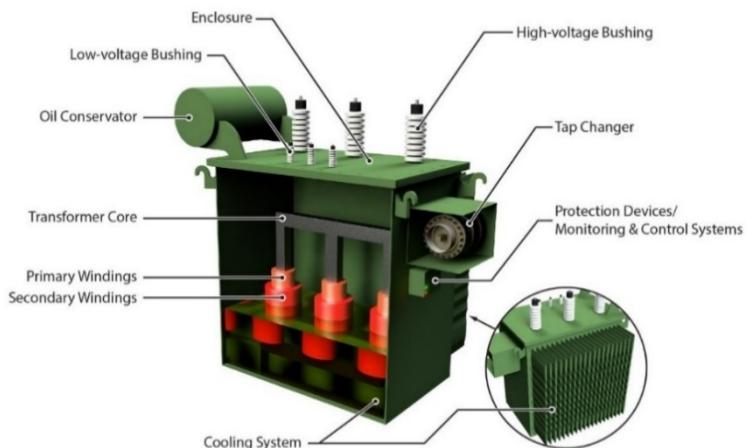
BESS connected via grid scale transformers are key components in energy storage systems that help manage the flow of electricity between the battery system and the grid. Below is a breakdown of the main components typically found in BESS site transformers (illustrated in Figure 15. Transformer components.):

- Transformer Core:** The BESS transformer core is typically made of high-permeability materials such as iron or steel; it provides a low reluctance path for the magnetic flux generated by the transformer, facilitating efficient energy transfer.
- Windings:** Windings are conductive wires wound around the transformer core. In BESS transformers, there are typically two sets of windings: primary and secondary.

The primary windings are connected to the battery system, and the secondary windings are connected to the grid.

3. **Tap Changer:** A tap changer is a mechanism used to adjust the transformer's voltage ratio. In BESS transformers, tap changers may be used to accommodate variations in grid voltage or to optimize the performance of the battery system. They are more common in larger sites and substations than in BESS.
4. **Cooling System:** Since BESS transformers may experience varying loads and operating conditions, a cooling system is essential to dissipate heat generated during operation. Cooling may be achieved through natural convection, forced air, or liquid cooling.
5. **Protection Devices:** Protection devices are installed to ensure the safety and reliability of the transformer as well as the overall BESS system. These may include overcurrent protection, overvoltage protection, temperature sensors, and insulation monitoring systems.
6. **Monitoring and Control Systems:** Monitoring and control systems are integrated into BESS transformers to enable remote monitoring, data logging, and control of transformer parameters. These systems allow operators to optimize the performance of the transformer and respond quickly to changes in operating conditions.
7. **Enclosure:** Transformers are often housed in enclosures designed to protect them from environmental factors such as moisture, dust, and temperature extremes. The enclosure also provides mechanical protection for the transformer and its components.

Figure 15. Transformer components.



Site Control and EMS

Architecture designs for Site Control may vary depending on the specific design and requirements of the BESS. Common architectures include centralized control, distributed

control, and hierarchical control, with each offering different levels of flexibility, scalability, and redundancy:

- Centralized control involves a single controller managing all aspects of the BESS operation.
- Distributed control distributes control functions across multiple controllers for improved fault tolerance and responsiveness.
- Hierarchical control combines elements of both centralized and distributed control, allowing for centralized coordination of high-level functions while delegating lower-level control tasks to distributed controllers.

In a BESS, Site Control or the EMS serves as the central hub for managing and coordinating the operation of various components within the system. It establishes a parent-child relationship with other control elements, acting as the master controller. Site Control connects to both the battery storage units and the grid, facilitating bidirectional communication and control.

Measurements used by site control typically include:

- **Voltage:** Monitoring grid voltage levels to ensure stability and compatibility with the BESS operation
- **Frequency:** Tracking grid frequency for frequency regulation and synchronization purposes
- **State of Charge:** Monitoring the level of charge in the battery storage units to optimize usage and prevent overcharging or discharging
- Environmental monitoring
- Physical and safety monitoring

Communications and Cloud

External to the BESS, a cloud connection to DERMS or fleet control is often used. The growth and maturation of cloud computing have facilitated a transformative shift across various industries, with the energy sector at the forefront. Many, if not all BESS sites, aggregations, and OEMs use cloud and remote communications to monitor and manage their fleets. These cloud connections can vary from data storage to fully implemented DER management systems and mass orchestration. Figure 16. BESS communication interconnections. below illustrates the communication pathways and points of coupling for a BESS, while Figure 17 outlines the OT and IT interconnections.

Figure 16. BESS communication interconnections.

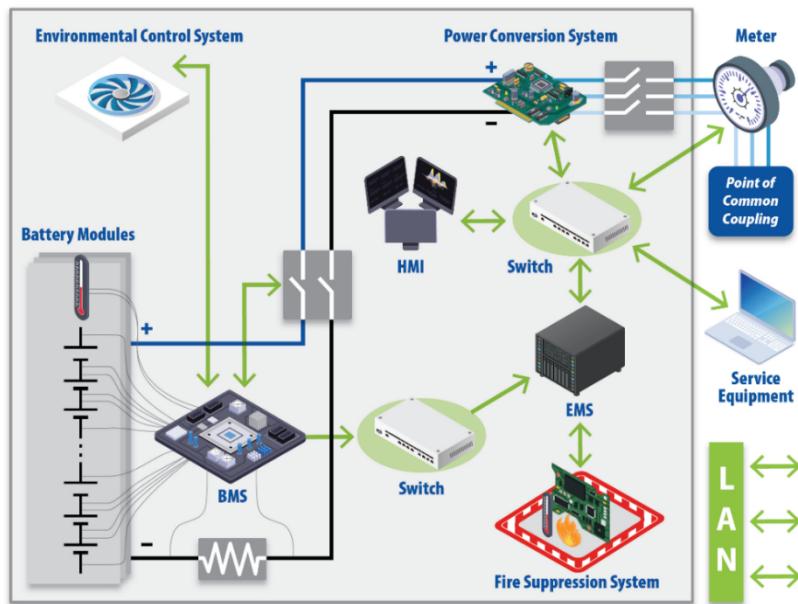
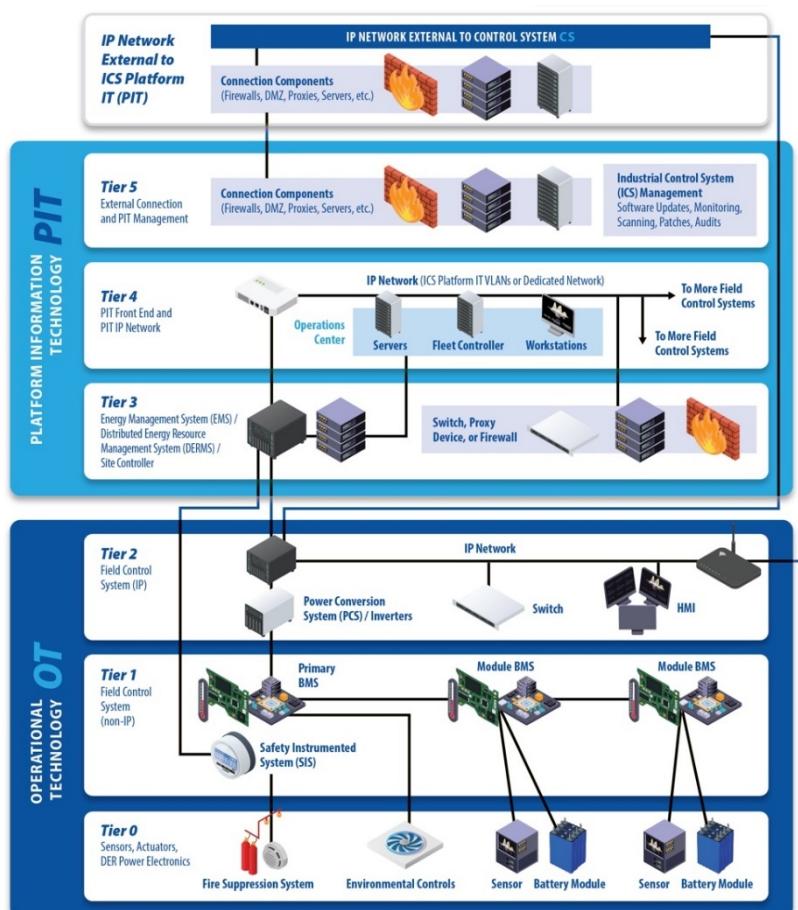


Figure 17. Purdue diagram summary for BESS.



DERMS, Software, and Fleet Controllers

While Site Control acts as the centralized management system for the BESS, it connects to DERMS and fleet controllers to manage and optimize the performance of the BESS, ensuring efficient energy storage and distribution. Within a fleet or network of BESS units, DERMS and other distributed control and mass orchestration platforms serve as central management systems that enable the coordination and optimization of multiple energy resources, providing crucial capabilities such as real-time monitoring, control, and coordination of energy storage assets to maintain grid stability, manage peak demand, and integrate renewable energy resources effectively. In the hierarchical structure, Site Control is the parent system, located at the top tier of the BESS architecture, overseeing multiple child subsystems, including individual battery modules and inverters; it coordinates operations and communications across all subordinate components. A fleet usually has one owner or operator, whereas mass control could confer across different boundaries of ownership in regions where that function is aggregated.

Beyond their functional roles in coordinating with the BESS, DERMS and mass control also contribute to grid stability, system reliability, and safety, enabling utilities and aggregators to visualize and control widely dispersed resources. Therefore, the accessibility and reliability of DERMS and mass control are paramount for ensuring the overall performance and safety of BESS deployments, particularly in large-scale operations within independent system operators (ISOs) with high resource penetration. Any disruption or failure in these components could have cascading effects on system operation, potentially compromising grid stability, energy supply reliability, and overall safety. Therefore, robust access and security controls between DERMS and fleet control functionalities, either through on-site management systems or cloud-based platforms, are essential for optimizing BESS performance and mitigating risks associated with misoperation or failure scenarios.

Human-Machine Interface (HMI)

The HMI is the interface between the operator and the BESS, connecting to the supervisory control and data acquisition (SCADA) system for monitoring and control. Facilitating local manual operations, such as resets and emergency stops, helps ensure compliance with safety protocols and offers direct interaction with the system components.

As shown in Table 3, the HMI serves as a child component under the SCADA system (parent) and interacts with various local subsystems (child), facilitating real-time data exchange and control within the BESS.

Table 3. HMI functionalities and connections in BESS.

Connections and Functions	Description
SCADA to local via HMI	Enables SCADA system to communicate and control local subsystems through the HMI

SCADA to local/manual disable – lockout/tagout (LOTO) compliance	Ensures LOTO compliance by allowing manual disable functions via SCADA
HMI manual reset	Provides the capability to manually reset system components
HMI local only	Restricts operations to local control, ensuring security and operational integrity
HMI local emergency stop	Facilitates immediate shutdown of the system in emergencies
Fire alarm	Integrates with the fire alarm system for safety and emergency response

Supply Chain for BESS Components

A key supply chain risk was highlighted recently with the removal of the Contemporary Amperex Technology Co (CATL) battery from Camp Lejeune.²⁶ The battery system, owned and operated by Duke Energy and located on Camp Lejeune, was disconnected in December 2023 after being commissioned in April 2023.²⁷ CATL is publicly acknowledged as one of the top suppliers of cells and other integrated equipment or built systems in the United States. The company asserts itself to be the world's largest battery manufacturer.²⁸ While CATL's origin as a PRC-based manufacturer of cells and an integrator is now a focus of discussion, it is not an isolated case. The BESS market is largely dominated by PRC-based companies and components. Reviewing this supply chain is challenging and intricate – but overall, the dominance of PRC manufacture and supply is significant. Breaking it down into key components and leading companies forms a more complete picture for deriving solutions.

Reviewing common supply chain sources and ranking for energy delivery, the Bloomberg New Energy Finance (BNEF) Tier 1 Storage list²⁹ for the second quarter of fiscal year 2024 (FY24 Q2), shown in Table 4 below, documents the top manufacturers and integrators globally of energy storage products. The Tier 1 list is identified from the BNEF Energy Storage Assets database, which included 9,000 energy storage projects worldwide as of June 2023 that are above 1 MW or 1 MWh in size and for which a supplier has provided battery storage systems in the last two years. The criterion to be listed as Tier 1 is that the

²⁶ Martina, Michael, "Exclusive: Duke Energy to Remove Chinese Battery Giant CATL from Marine Corps Base," Reuters, February 9, 2024, <https://www.reuters.com/business/energy/duke-energy-remove-chinese-battery-giant-catl-marine-corps-base-2024-02-09/>.

²⁷ CATL, "CATL Obtains the World's First Access Certification under the New Regulation of the UN Economic Commission for Europe (UNECE)," last modified May 19, 2022, <https://www.catl.com/en/news/951.html>.

²⁸ Maisch, Marija, "CATL: Staying on Top of the Battery Game," PV Magazine, December 1, 2023, <https://www.pv-magazine.com/2023/12/01/catl-staying-on-top-of-the-battery-game/>.

²⁹ BloombergNEF, "BloombergNEF Tier 1 Solar Module Maker Methodology," last modified January 11, 2024, <https://assets.bnef.com/public/tiering/solarmodules.pdf>.

vendor must have supplied or be firmly contracted to supply products to six different eligible projects within two years.

Table 4. Energy storage manufacturers meeting Bloomberg's NEF Tier 1 criteria as of Q2 FY 2024.

Firm/Brand	Headquarters	Firm/Brand	Headquarters
Xuji Electric	China	JD Energy	China
Wartsila	Finland	Invinity	UK
Trina Storage	China	Hyperstrong	China
Tesla	United States	Hyosung Heavy Industries	South Korea
Sungrow	China	Huawei	China
Sermatec	China	Hithium	China
Samsung SDI	South Korea	Gotion High Tech	China
Saft	France	Fluence	United States
Robestec/Shanghai Ronghe	China	FlexGen Power Systems	United States
REPT BATTERO	China	Eve Energy	China
RelyEZ	China	Envision Energy/AESC	China/Japan
Powin Energy	United States	Cubenergy	China
Pinggao Group	China	CRRC Zhuzhou	China
NHOA Energy	Italy	CLOU Electronics	China
Narada	China	CATL	China
LG Energy Solution	South Korea	Canadian Solar e-STORAGE	Canada
Kehua	China	BYD	China
Jinko	China	Fluence	United States

*Blue highlights signify most common in the U.S.

Of this list:

- 65% of the vendors have a Chinese headquarters
- 11% of those listed have a U.S. headquarters
- All the suppliers have a Chinese supplier for either the BMS, PCS, or inverter product

The National Defense Authorization Act (NDAA) FY24 Section 154³⁰ lists 6 BESS companies as prohibited from being sourced through DOD funds. They include:

- CATL
- BYD Company, Limited
- Envision Energy, Limited
- EVE Energy Company, Limited
- Gotion High Tech Company, Limited
- Hithium Energy Storage Technology Company Limited

The most common integrators in the U.S. are highlighted in blue, as of 2023 and 2024, combined from multiple media and supply chain reports^{31 32}. These integrators and their presence vary considerably each year, and some are new to the market or a company evolving from supplying components to fully integrated units³³.

Note that both cell providers and system integrators are considered battery manufacturers or brands eligible for this list. The inclusion of integrators allows for national companies to be listed as the primary brand despite sourcing components from other manufacturers.

Battery Cell/Modules

Illustrated by Figure 18 and Figure 19, the interplay of global trade highlights the current dependence of the United States on international battery suppliers, particularly from China, to the surging demand for lithium-ion batteries amidst the ongoing energy transition.

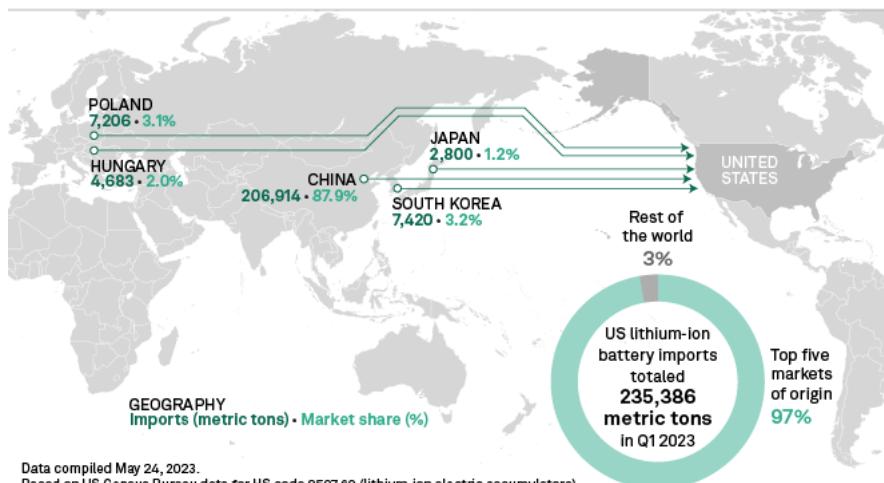
³⁰ U.S. Congress, “National Defense Authorization Act for Fiscal Year 2024,” Section 154, 118th Cong., April 18, 2023, <https://www.congress.gov/bill/118th-congress/house-bill/2670>.

³¹ Wood Mackenzie. *Smart Energy International*. Retrieved from <https://www.smart-energy.com/regional-news/north-america/sungrow-fluence-and-tesla-leading-bess-integrators-says-wood-mackenzie/#:~:text=The%20North%20American%20BESS%20integrator,an%20downstream%20supply%20chain%20participants>.

³² Guidehouse Insights. (2021). Guidehouse Insights Leaderboard: Utility-Scale Energy Storage Systems Integrators. Retrieved from <https://guidehouseinsights.com/reports/guidehouse-insights-leaderboard-utility-scale-energy-storage-systems-integrators>

³³ Shi, A., & Wilkinson, S. (2023, September 29). The five largest battery energy storage system (BESS) integrators have installed over a quarter of global projects. Retrieved from <https://www.spglobal.com/commodityinsights/en/ci/research-analysis/the-five-largest-battery-energy-storage-system-bess-integrator.html>

Figure 18. U.S. lithium-ion battery imports during Q1 2023.



Data compiled May 24, 2023.
Based on US Census Bureau data for HS code 8507.60 (lithium-ion electric accumulators).
Only includes countries that report monthly data to the US Census Bureau.
Map credit: Mahnoor Haider
Source: Parjiva, the supply chain research unit of S&P Global Market Intelligence, a division of S&P Global Inc.
© 2023 S&P Global.

Figure 19. Li-ion battery manufacturing planned (blue) or under construction (red).

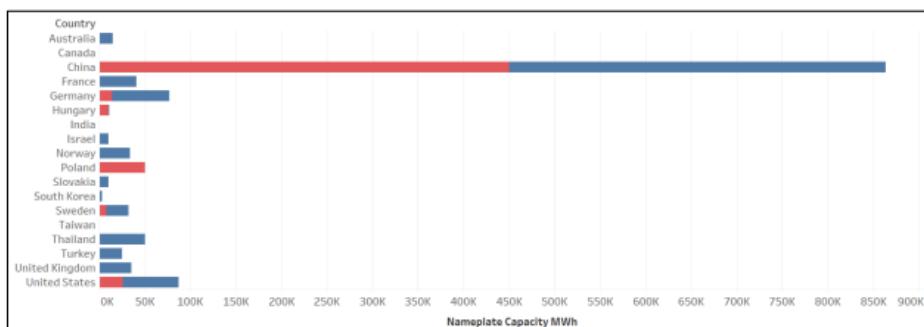


Figure 16. Li-ion battery manufacturing planned (blue) or under construction (red)

Source: [15] Bloomberg New Energy Finance, "Storage Data Hub, Cell Manufacturers," BloombergNEF, New York, 2020. Available:
<https://about.bnef.com/>

Battery Cell and Integrator Relationships

Batteries suppliers also ship receivers, communications equipment, primary cells, enclosed full units with sensors, inverters, and other power electronics. Modular shipping and manufacturing are common practices. This is further discussed in Section 4 (Supply Chain for BESS Components) above. The supply chain is complex. Considering the complex relationships in integration and battery cell provision, we consider CATL to be the use case. There are at least 10 primary buyers of CATL technology in the US and global integrator market³⁴ based on export and import records linking their operation³⁵. The top 10 relationships from a shipping perspective, while indistinguishable from the EV Battery Market, are many of the top BESS product vendors in the US.

³⁴ Ferguson, Mark, "Infographic: The Big Picture 2024—Energy Transition Outlook," S&P Global, December 6, 2023, <https://www.spglobal.com/marketintelligence/en/news-insights/blog/infographic-the-big-picture-2024-energy-transition-outlook>.

³⁵ Derived from research performed on Import Yeti throughout 2024: <https://www.importyeti.com/>.

Evaluating commonly used battery cell providers, including other major PRC based companies such as Hithium [reference] there are a varied set of cell suppliers for some of the major integrators, and removal of these 6 will leave another set of 70 behind them. Many have limited safety records and low maturity³⁶. If CATL is removed from this picture, along with others on the NDAA FY24 List, there would be a shift to a set of suppliers that may have lower performance or less mature products and operations. It is unlikely the shift would be to fully onshore manufactured options, as there are none currently. The California Battery Supply List,³⁷ is a list of suppliers eligible for tax credits in California who have passed rigorous safety checks. On this list, over 80 BESS and Battery Cell providers are included in varied configurations. Most companies on the list are PRC-owned and operated and meet the required performance specifications. Given this, integrators would likely not shift to a more costly U.S. manufacturer but to a different PRC-manufactured system.

BMS

The BMS supply chain has become increasingly more complex as many BMS are integrated with battery sensors and even cells. Often, if buying or contracting for cell supply, a BMS will be an integrated choice. The BMS manufacturer for a BESS is commonly not disclosed, and many BMS have the same supplier and hardware as the inverter. It is not usually possible in today's market, with BESS sold as a system of linked components, to replace the BMS with one not offered by the BESS vendor.

There are independent companies in the U.S. market, including Nuvation³⁸. Fluence and Flexgen have recently announced new U.S. onshore manufacture and software for BMS³⁹. Penetration of Chinese versus other entities cannot be ascertained with confidence individually, but based on the investigation of most common integrators, it is most likely the same penetration as inverters and other power electronics components. Often in literature, the BMS is discussed in terms of the software manufacturer, but hardware is likely the same vendor as the inverter. The independent providers of BMS are listed in Table 5 as of February 2024. Many of these are part of other parent companies or also sell to EVs, given the tied markets. The majority of independent BMS developers are non-PRC-based companies. Separating the Cell manufacture from BMS is a challenge as they are often integrated. Therefore this list does not necessarily represent penetration in the US Market.

³⁶ Ren, D., & Xu Klein, J. (n.d.). China's battery makers burnish their safety image as they grab the lion's share of the world's market for powering electric cars. South China Morning Post. Retrieved from https://www.scmp.com/business/companies/article/3154120/how-do-electric-vehicle-batteries-work-and-why-do-they-sometimes?module=perpetual_scroll_1_RM&pgtype=article

³⁷ California Energy Commission, "Energy Commission's Solar Equipment Lists Home," accessed April 2024, <https://solarequipment.energy.ca.gov/>.

³⁸ Nuvation Energy, "Accelerating Sustainable Energy," 2024, <https://nuvationenergy.com/>.

³⁹ Fluence. (September, 10 2024). Fluence Initiates U.S. Manufacturing of Battery Modules for Energy Storage Products. Retrieved from <https://ir.fluenceenergy.com/news-releases/news-release-details/fluence-initiates-us-manufacturing-battery-modules-energy>

Table 5. Companies and their main products supplied.

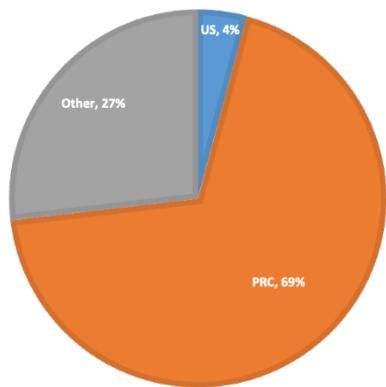
Company	Location	Main Products
Leclanché	Switzerland	BMS/Cell/Modules
MOKOEnergy	China	BMS/PV Inverter
Nuvation	California	BMS
Intel	United States	BMS
Bosch	Germany	battery management & thermal management system/e-axel/module
Denso	Japan	battery monitoring integrated IC
SK Innovation	South Korea	BMS/energy system
BYD	China	BMS
Panasonic	Japan	BMS/lithium-ion batteries
LG Chem	South Korea	BMS/energy system

PCS

PCS are a highly critical component in the BESS, combining inverters and other conversion systems to operate a consistent system. It is worth noting where PCS are sourced. Analysis of the California inverter⁴⁰ allow lists indicate that there are 517 PCS models used either with or combined with the allowed inverters. Because manufacturers are eager to be on the allow list for California—which has the largest installed capacity of BESS and plans for continued growth—it can be assumed that even systems installed outside of California have a similar breakdown. As illustrated in , just 4.2% of PCS are from the U.S., while 69.4% are from China. The remaining 26.3% come from a country other than the U.S. or China.

⁴⁰ California Energy Commission, “Solar Equipment Lists Program,” accessed April 2024, <https://www.energy.ca.gov/programs-and-topics/programs/solar-equipment-lists>.

Figure 20. U.S. PCS providers vs. Chinese PCS providers.



Understanding the penetration of foreign-manufactured components offers insight into the full supply chain beyond the primary named supplier.

Inverters

In addition to BESS, inverters are foundational components for clean energy sources such as hybrid systems, solar, and hydrogen fuel cells. Involving microchips, electronic switches, and PLCs, the inverter supply chain is complex. This complexity and the growing digitization associated with these components create supply chain cyber risks. For example, in solar environments—a related market often tied closely to BESS—the manufacturing market for solar panels and inverters is dominated by China.^{41,42} According to the IEA,⁴³ global solar PV manufacturing capacity has increasingly moved from Europe, Japan, and the United States to China over the last decade.^{44,45} For panel manufacturing—which includes the development of polysilicon, ingots, wafers, cells, and modules—China's share exceeds 80%. Perhaps more concerning from a cyber security perspective, the top five vendors of solar inverters, based on GW capacity shipped, are all foreign entities of concern (FEOCs), accounting for 71% of total global solar inverter shipments in 2022,⁴⁶ as illustrated in Figure 21.⁴⁷ The strong dependence on FEOC-manufactured solar PV systems requires a

⁴¹ Wiki-Solar, “Inverters,” accessed April 24, 2024, <https://wiki-solar.org/company/inverters/>.

⁴² Statista, “Market Share of The Solar PV Inverter Market Worldwide In 2022, Based On Shipments,” last modified September 2023, <https://www.statista.com/statistics/1003705/global-pv-inverter-market-share-shipments/>.

⁴³ International Energy Agency (IEA), “Special Report on Solar PV Global Supply Chains,” Executive Summary, revised August 2022, <https://www.iea.org/reports/solar-pv-global-supply-chains/executive-summary>.

⁴⁴ Global Market Insights, “Utility Scale PV Inverter Market Size,” last modified June 2023, <https://www.gminsights.com/industry-analysis/utility-scale-pv-inverter-market>.

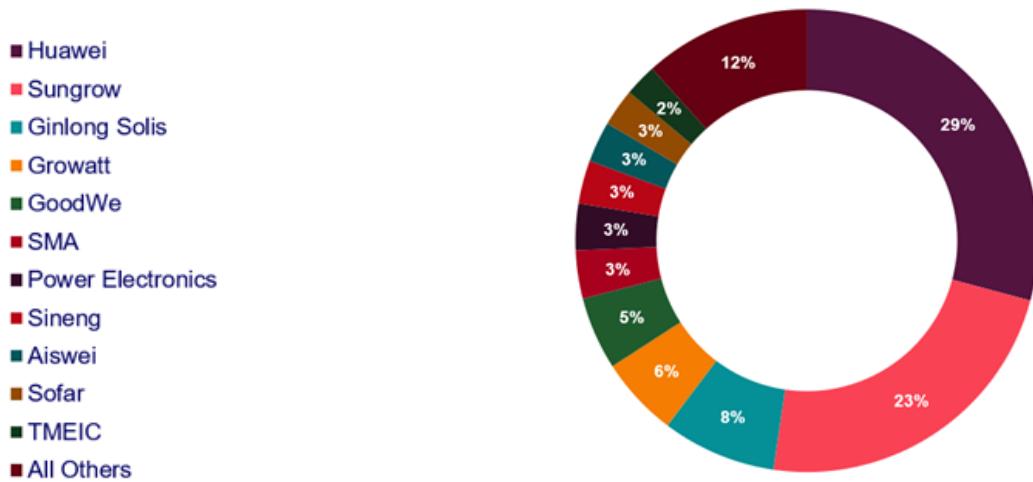
⁴⁵ UnivDatos Market Insights, “US Solar Inverter Market: Current Analysis and Forecast (2023-2030),” last modified November 2023, <https://univdatos.com/report/us-solar-inverter-market/>.

⁴⁶ Grand View Research, “PV Inverter Market Size, Share & Trends Analysis Report By Product (String PV Inverter, Central PV Inverter), By End-use (Commercial & Industrial, Utilities), By Region, And Segment Forecasts, 2024 – 2030,” last modified January 2024, <https://www.grandviewresearch.com/industry-analysis/pv-inverters-market>.

⁴⁷ Wood Mackenzie, “Top 10 Solar PV Inverter Vendors Account For 86% Of Global Market Share,” August 14, 2023, <https://www.woodmac.com/press-releases/top-10-solar-pv-inverter-vendors-account-for-86-of-global-market-share/>.

better understanding of the risk these systems pose to U.S. energy security. Following the tariff application to solar cells and modules in 2018, and extension in 2020⁴⁸, and the injection of federal infrastructure funds, panel manufacturing has slowly but steadily been moving to the United States and allied countries, but inverters have not followed the same path;⁴⁹ many now have primary sourcing from China.

Figure 21. Global inverter companies⁴⁵.



Source: Wood Mackenzie

Below is a list of the most commonly sourced large three-phase large inverters in the United States:

- FIMER SPA (ABB)
- Power Electronics
- Schneider Electronics
- SMA
- Siemens
- Delta Electronics
- Sungrow Power Supply
- Huawei Technologies Co
- Ginlong Solis
- Yaskawa Solectria Solar
- Toshiba Mitsubishi-electric Industrial Systems Corporation (TMEIC)
- Hitachi

⁴⁸ Office of the United States Trade Representative, “Section 201 – Imported Solar Cells and Modules,” accessed April 2024, <https://ustr.gov/issue-areas/enforcement/section-201-investigations/investigation-no-ta-201-75-cspv-cells>.

⁴⁹ Daly, Matthew, “New US tariffs on Chinese Electric Vehicles, Batteries and Solar Cells Could Raise Consumer Prices,” Associated Press, updated May 14, 2024, <https://apnews.com/article/biden-china-tariffs-electric-vehicles-solar-254546e92f823a78220c195a0a42a10e>.

On the California State Allow List alone, there are 96 manufacturers and over 1500 eligible inverter models; an even greater number of inverters are available for purchase in the United States beyond the list. Therefore, it would be nearly impossible to conduct a thorough analysis of either the supply chains and components of each model or all the manufacturers. Based on this vast scope, coupled with their importance in BESS security The primary criterion used to drive the analysis was inverter manufacturers with the largest potential impact to the grid based on deployed capacity.

Summary: Presence of PRC in Combined BESS Supply Chain

In evaluating the presence of PRC manufacture overall in the supply chain for battery energy system components, the dominance is clear. There are significant efforts to move this supply chain, through BIL funding, but this to date has focused on the cell material.

If we consider that at the lowest level, components and manufacture for electronics are sourced from a PRC-manufactured or imported material in the range of 70 to 100%^{50,51,52,53}, we can estimate that 90 to 100% of the BESS will have 1+ PRC component (from above analysis 70% inverters and PCS, with over 90% having PRC linked businesses, and 100% of cells) . With the top 10 suppliers in the market PRC-owned and operated, it is likely that BESS systems have at least 1 control component sourced from China. This estimate indicates that it is unlikely that the core control supply chain can exclude PRC-manufactured electronics without significant actions driving change.

Supply Chain Analysis Challenges: Commonality and Sources

There are significant overlaps in supply chains between power electronic components, inverters, BMS, and industry verticals, such as solar, wind, EVSE. This adds additional risk and complication in disaggregating the entangled relationships and ownership models for these entities. Table 6 outlines the functions of critical BESS components, indicating, as well, if they are also used in other renewables or inverter-based resources, and where the supply chain overlaps, both in components and company roles. Similar functions offer insight as to where the supply for these components may be interlinked with another industry vertical, such as solar, wind, or electric vehicles. For example, inverters provided for

⁵⁰ Thadani, A., & Allen, G. (2023, May 30). Mapping the Semiconductor Supply Chain: The Critical Role of the Indo-Pacific Region. Center for Strategic and International Studies. Retrieved from <https://www.csis.org/analysis/mapping-semiconductor-supply-chain-critical-role-indo-pacific-region>

⁵¹ Observatory of Economic Complexity (OEC). (n.d.). Parts of electronic integrated circuits etc in China. Retrieved from <https://oec.world/en/profile/bilateral-product/parts-of-electronic-integrated-circuits-etc/reporter/chn>

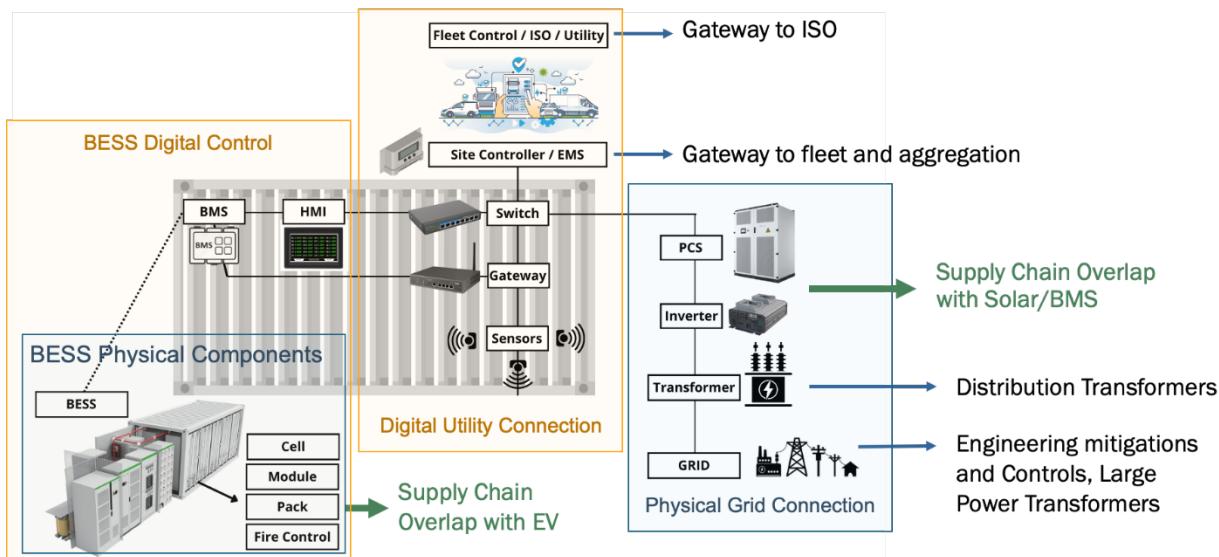
⁵² Semiconductor Industry Association. (2021, July 31). Taking Stock of China's Semiconductor Industry. Retrieved from <https://www.semiconductors.org/taking-stock-of-chinas-semiconductor-industry/>

⁵³ Trading Economics. (2024, November). United States Imports from China of Electrical, electronic equipment. Retrieved from <https://tradingeconomics.com/united-states/imports/china/electrical-electronic-equipment>

solar or hybrid plants, use similar if not identical components in many cases, potentially with different software or configuration of functions enabled on the same hardware. Battery modules developed for stationary storage are likely the same cells used in electric vehicle batteries, and the Supervisory Control Systems are not often specific to BESS alone. This indicates the complex web that should be considered in analyses of any one supply chain vertical. This is also illustrated graphically in Figure 22.

Table 6. Specificity of BESS components to supply chain vertical.

Item	Description of Functions	BESS Specificity
Battery modules, packs, and cells	Core energy storage functions and electrochemistry	Stationary and Mobile Systems
PCS	Convert between AC and DC power, bidirectional and often combined with inverter in BESS (specific to BESS – not other IBR)	Specific to BESS
Inverters	Convert DC power from battery cells to AC power	Solar, wind, EV other IBR – can be a combined or separate
BMS	Monitor and control battery SOC, state of health (SOH), and environmental safety	Stationary and mobile (EV) systems, along with other types of batteries
Supervisory control systems and EMS	Coordinate and manage BESS system level functions	EMS and SCADA are common in IBR
Environment control systems	Regulate temperature and air quality within BESS facilities	Specific to BESS
Fire suppression or fire control	Detect and suppress fires	Specific to BESS
Transformers	Step up or down voltage levels as needed	Common in power systems, new solid state integrated with inverters are specific to BESS
HMI	Provide user interface for monitoring and control on site	Common components
Electrical disconnects, circuit breakers, and switches	Protect components from overloads or faults	Common components
Communications and modems	Facilitate data exchange between components and external systems and controls	Common components

Figure 22. Supply chain linkages for BESS.

Multiple open-source and commercial references were used in this report to help identify the top vendors in the United States. Business models for OEMs and integrators vary more widely than traditional electric vendors, with common problematic elements including changing vendor names, changes in parent or holding companies, companies that have merged or separated,⁵⁴ entries into new markets, withdrawal from the U.S. market (Huawei),⁵⁵ and development of new business lines such as storage or electric vehicle supply equipment.⁵⁶ In the U.S. market, published company penetration lists often leverage “pay-to-play” as inclusion criteria, leading to bias.

⁵⁴ Africa CEO Voices, “US solar company SunPower to splits into two business units to enhance efficiency,” last modified November 12, 2019, <https://www.africaceovoices.com/us-solar-company-sunpower-to-splits-into-two-business-units-to-enhance-efficiency/>.

⁵⁵ Roselund, Christian, “Reports Huawei has Exited US Solar Inverter Market,” PV Magazine, last modified June 26, 2019, <https://www.pv-magazine.com/2019/06/26/reports-huawei-has-exited-us-solar-inverter-market/>.

⁵⁶ SolarEdge, “SolarEdge Acquires Wevo Energy, EV Charging Optimization and Management Software Startup,” last modified April 4, 2024, <https://investors.solaredge.com/news-releases/news-release-details/solaredge-acquires-wevo-energy-ev-charging-optimization-and>.

Threats, Vulnerability, and Attack Exposure for BESS

Threats

Threat actors interested in battery targets may range from nation-state actors to cyber-criminal organizations to individuals with limited capabilities and physical criminals. For FEOC components, the threat over the lifecycle of the system, as an integrated unit is as important to consider as the threat actors for systems in operation, exploiting vulnerabilities from outside. Organizations should track the manufacturing country and the influence of the local government on their critical components. For example, the influence of the Chinese government on CATL includes the appointment of government workers to key positions within their corporate structure, as well as the use of specific mining locations⁵⁷.

Even more difficult to track than the original component manufacturers are additional organizations with access to equipment during the assembling, shipping, and construction phases. The U.S. Department of Commerce found that some Chinese solar producers were shipping products through Cambodia, Malaysia, Thailand, or Vietnam to avoid payment of U.S. duties⁵⁸. Similar actions could be taken by battery companies to avoid tariffs or bans on Chinese-manufactured components. Even if done legally (i.e., significant assembly or manufacturing occurs in a different country), intermediary companies and countries should be held to the same level of scrutiny as core component manufacturers to maintain trust in the security of the supply chain.

Operation of the battery may also expose it to a wide range of potential threat actors. Batteries used in critical applications may be seen as valuable targets for nation-state actors. Even those not used in critical applications may be seen as “low-hanging fruit” easily targeted by cybercriminals. In recent years there has been a rise in both nation-state actors and criminal actors targeting not only the energy sector in general but also specific renewable targets.⁵⁹

⁵⁷ Homeland Security Committee, “House Homeland Republicans Join Chairman Moolenaar in Demanding Immediate Blacklist for Chinese Battery Companies Gotion, CATL Amid Shocking New Evidence of Slave Labor Links,” last modified June 6, 2024. <https://homeland.house.gov/2024/06/06/house-homeland-republicans-join-chairman-moolenaar-in-uncovering-shocking-new-evidence-of-slave-labor-links-at-chinese-battery-companies-gotion-catl-demand-immediate-blacklist/#:~:text=CATL%20sources%20electrolytic%20nickel%20from,by%20Yibin%20Tianyuan%20Group%20Co.>

⁵⁸ U.S. Department of Commerce, “Department of Commerce Issues Final Determination of Circumvention Inquiries of Solar Cells and Modules from China,” last modified August 18, 2023. <https://www.commerce.gov/news/press-releases/2023/08/department-commerce-issues-final-determination-circumvention-inquiries>.

⁵⁹ Federal Bureau of Investigation, “Expansion of Renewable Energy Industry Increases Risk of Targeting by Malicious Cyber Actors,” last modified July 1, 2024. <https://s3.documentcloud.org/documents/24788637/fbiwarning.pdf>.

Vulnerability

Vulnerabilities may exist in either individual components in the battery or within the overall system. Flaws may exist at the design, execution, system assembly, or at any layer, including firmware, software, hardware, and communications. Vulnerabilities may occur in key BESS components:

- **Battery modules, packs, and cells:** While cells are free of integrated digital components, flaws in the manufacturing process could lead to degraded performance over time, eventually causing the battery to fail when performing key functions. Failure of a single cell can lead to failure of the entire module through thermal propagation.
- **PCS/Inverters:** Widespread use and application of BESS increases the potential for functions to be affected by vulnerabilities in the PCS. As with battery modules, poor manufacturing could create hardware vulnerabilities that affect performance. Another hardware vulnerability is intentional tampering with the manufacturing or shipping process. China has been accused of tampering with computing equipment destined for the United States⁶⁰ and even installing backdoors on chips used for military applications, nuclear power plants, and power distribution.⁶¹ Additionally, PCS communicate with the fleet, BMS, and outside world, often requiring firmware updates like the BMS and inverters. Vulnerabilities such weak password policies, hard-coded passwords, improper authentication, or improper storage of critical information may create attack paths for adversaries.

⁶⁰ Department of Justice, “Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians,” Office of Public Affairs, March 25, 2024. <https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived>.

⁶¹ Allen, Gregory C., “China’s New Strategy for Waging the Microchip Tech War,” Center for Strategic and International Studies, May 3, 2023. <https://www.csis.org/analysis/chinas-new-strategy-waging-microchip-tech-war>.

- **BMS:** Both firmware (operating system and setup of the computing system) and software (programs running on the system to perform operational tasks) may have vulnerabilities, with weaknesses created by features similar to those for inverters and PCS. Many vulnerabilities are simply flaws in the design or execution of the code that lead to unintended functionality, such as memory overflows that allow for the insertion of arbitrary code. However, particularly for FEOC devices, malicious code insertion can cause undocumented activity to occur, such as leaving a backdoor open or sending beaconing signals. Though purchasers can require tracking of all software subcomponents on a device through an SBOM, the intentions of code authors and the execution and effectiveness of code quality reviews must also be considered. While it is extremely difficult to track the origin of every single line of code on a device, requiring vendors to submit their SBOMs to customers and show proof of code review processes can provide some visibility into the maturity of the digital supply chain for the product. The SolarWinds hack of 2020⁶² occurred because nation-state hackers were able to add malicious code into the SolarWinds software that was not detected before the code was certified and distributed to customers. In addition to intentional attacks on the software supply chain, vulnerabilities may occur through poor code-writing practices or the use of open-source (and often unsupported) code in enterprise applications.
- **Supervisory control system and EMS:** The supervisory control system collects data and may send control signals to batteries based on the conditions of the grid. At this level of the BESS, key considerations include who has access to what data and functionalities, and how that access is managed.
- **Electrical disconnects, circuit breakers, and switches (protection):** Historically, circuit breakers and switches were manual or electromechanical devices triggered by local sensor readings. However, with digital relays often being used as primary protection for grid systems, vulnerabilities in these devices have been shown to cause misoperation of devices.⁶³
- **Communications networking switches and cables:** In addition to battery-specific hardware, the supplementary equipment used in these systems—including IT and communications equipment—must be considered. The first publicly disclosed attack that affected U.S. renewables exploited a known vulnerability in Cisco firewalls, which caused them to reboot repeatedly, blocking the flow of data from several wind and solar sites to the aggregator, sPower.⁶⁴ More recently, both disclosed and zero-day vulnerabilities were exploited on systems belonging to several small Danish utilities⁶⁵.

⁶² Jake Williams, “What You Need to Know About the SolarWinds Supply-Chain Attack,” SANS Institute, December 15, 2020, <https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/>.

⁶³ Idaho National Laboratory, “Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector,” Department of Energy, last modified August 2016. <https://energy.gov/epsa/downloads/cyber-threat-and-vulnerability-analysis-us-electric-sector>.

⁶⁴ Kovacs, Eduard, “Cisco Firewall Exploited in Attack on U.S. Renewable Energy Firm,” Cybercrime, November 1, 2019. <https://www.securityweek.com/cisco-firewall-vulnerability-exploited-attack-us-renewable-energy-provider/#:~:text=It%20appears%20that%20the%20firewall,would%20not%20cause%20other%20problems>.

⁶⁵ Nelson, Nate, “Danish Energy Attacks Portend Targeting More Critical Infrastructure,” Dark Reading, November 14, 2023. <https://www.darkreading.com/ics-ot-security/danish-energy-attacks-portend-targeting-more-critical-infrastructure>.

Common technical issues that can increase risk of cyber events for all source inverters, BMS, and PCS include:

- Hardcoded and weak passwords
- Direct connection to OEM for firmware management
- Direct connection to OEM for quality monitoring
- Application security issues
- Weak or limited access controls
- Mass orchestration via cloud and third-party platforms

While technical issues with power electronic-based control equipment may lead to significant challenges and areas for exploitation, solutions are in place to enable U.S. and non-FEOC operators to secure these components. Many non-FEOC vendors have robust reporting mechanisms or are growing their product security teams and have disclosed vulnerabilities in inter-nation inverters and related applications⁶⁶, indicating a willingness to resolve challenges in the technology.

There are greater concerns, however, with FEOC vendors.⁶⁷ While vendors must perform and certify tests for safety and evolving tests for cyber safety (UL 2941)⁶⁸, technical testing to standard (by UL or Electrotek, for example) is authorized to be performed by PRC companies and, therefore, may not adhere to U.S. disclosure or reporting requirements. Future work will be required in geolocating testing and certification.

Technical issues with PRC-sourced power electronic conversion/management products include:

- Direct connection to offshore site for firmware management
- Direct connection to offshore site for quality monitoring, not segmented from control per standards
- Hardcoded passwords
- Poor chip quality
- Insecure support software to manage security features
- Bad documentation
- No vulnerability disclosures to U.S. or international governments
- Providing white labeling of products

Additionally, many inverters, BMS, and PCS sourced in the United States are governed by third-party contracts with integrators and suppliers with specific provisions forbidding

⁶⁶ Enphase, “Cybersecurity Reporting Policy,” accessed April 24, 2024. <https://enphase.com/cybersecurity>.

⁶⁷ Jewett, Michelle M., Kiely, Daniel T., Park, Kyoolee C., and Warren S. Payne, “Final Guidance Issued on “Foreign Entity of Concern” Criteria,” Mayer Brown, last modified May 28, 2024. <https://www.mayerbrown.com/en/insights/publications/2024/05/final-guidance-issued-on-foreign-entity-of-concern-criteria>.

⁶⁸ Cryar, Ryan, “Cybersecurity Certification Standard for Distributed Energy Resources, North American Electric Reliability Corporation (NERC), last modified December 14th, 2022. <https://www.nrel.gov/docs/fy23osti/84709.pdf>.

reverse engineering or inspecting components, leaving an extremely limited ability to identify or manage the vulnerabilities. This is true even with equipment sourced through U.S. companies. For example, an integrator may buy a shipment/set of inverters to incorporate into their BESS. This may be a long-term contract. To receive that supply, the integrator must sign an agreement with the OEM, which often enforces clauses on the integrator to not inspect, reverse engineer, or evaluate the internal workings of the device, creating a barrier to improving security within the integrators. So, while they may build their own software, they have limited ability to inspect the underlying hardware and firmware.

Some examples of reported vulnerabilities in BESS and other renewable components include:

- Enphase Envoy
 - CVE-2020-25754: Custom privilege access management module uses password derived from the MD5 hash of the username and serial number. Serial number can be retrieved by an unauthenticated remote user⁶⁹.
 - CVE-2020-25753: Default admin password for certain versions set to the last 6 digits of the serial number, which can be retrieved by an unauthenticated remote user⁷⁰.
 - CVE-2020-25752: Hardcoded web-panel login passwords for the installer and Enphase accounts. Users are unable to change these passwords⁷¹.
 - CVE-2019-7676: Weak password vulnerability discovered in Envoy R3⁷².
- Contec SolarView
 - CVE-2023-27512 use of hard-coded credentials may allow remote authenticated attacker to login with administrative privilege.⁷³
- Fronius
 - CVE-2019-19228: Solar inverter allows attackers to bypass authentication because the password is stored in a plaintext file.⁷⁴

⁶⁹ MITRE, CVE-2020-25754 Detail, NIST National Vulnerability Database, last modified June 28, 2021.
<https://nvd.nist.gov/vuln/detail/CVE-2020-25754>.

⁷⁰ MITRE, CVE-2020-25753 Detail, NIST National Vulnerability Database, last modified June 28, 2021.
<https://nvd.nist.gov/vuln/detail/CVE-2020-25753>.

⁷¹ MITRE, CVE-2020-25753 Detail, NIST National Vulnerability Database, last modified June 28, 2021.
<https://nvd.nist.gov/vuln/detail/CVE-2020-25752>.

⁷² MITRE, CVE-2019-7676 Detail, NIST National Vulnerability Database, last modified August 24, 2020.
<https://nvd.nist.gov/vuln/detail/CVE-2019-7676>.

⁷³ MITRE, CVE-2023-27512 Detail, NIST National Vulnerability Database, last modified May 30, 2023.
<https://nvd.nist.gov/vuln/detail/CVE-2023-27512>.

⁷⁴ MITRE, CVE-2019-19228 Detail, NIST National Vulnerability Database, last modified December 16, 2019.
<https://nvd.nist.gov/vuln/detail/CVE-2019-19228>.

Table 7. Attack types and potential outcomes

Attack type	Potential enabling attack paths	Potential Outcomes
Reconnaissance	Network scans Stolen credentials (social engineering) hardcoded credentials Pivoting Spyware	Leaked system configurations Leaked operational data
Exfiltration	File transfer vulnerabilities via cloud or DERMS	Leaked performance data Leaked personal data
False data injection	Access to PCS, Access to Inverter Access to meters Access to data in transit Unencrypted protocols Lack/no authentication	Misoperation of BESS based on bad data Hide further adversary activity
Wiper malware	Access to devices of interest	Destroyed forensics Delayed cyber recovery Bricked devices
Botnets	Internet exposure via applications or unpatched systems Vulnerabilities enabling remote takeover	Degraded performance
Denial-of-critical-functionality	Flooding Network equipment DoS Power equipment DoS	Disable safety features Prevent operation in mission-critical scenarios

Command injection	Malicious firmware LotL Backdoor	Local Outage Reverse Operation
Escalation & Pivot	Pivot into cloud mass orchestration, wider impact	Mass outage Financial Loss Loss of Load

Attack Exposure

Normally, the introduction of remote management systems for distributed resources increases the attack surface. For BESS and other inverter-based resources, however, remote management is necessary to maintain secure features through software and firmware updates which would be unlikely to be applied manually.

The United States' increasing reliance on batteries and their associated power electronics also increases the number of stakeholders requiring access to both data collection and command permissions, which in turn increases the potential attack surface. If any one of the authorized stakeholders were compromised, it could lead to an adversary using that stakeholder's level of access to perform malicious actions. This increasing access is a growing trend in renewables, where entities with third-party access (e.g., OEMs and maintenance providers) have ongoing connections to devices. In March 2022, an attack on Viasat SATCOM infrastructure interrupted satellite communications⁷⁵, knocking out remote communications for over 5,800 ENERCON wind turbines⁷⁶.

Many third-party stakeholders may not be subject to the same level of regulation as a utility or power provider. If these companies are hacked, there is potential attack exposure to the BESS through these third-party entities. Recent incidents have shown that affected organizations tend to cut off their remote access to renewable systems in the event of a compromise to prevent spread, but it remains unclear whether these incident response actions occur sufficiently quickly or completely. In another example, wind turbine manufacturers Nordex and Vestas and maintenance company Deutsche Windtechnik⁷⁷ were forced to deactivate remote data monitoring capabilities for several days while they

⁷⁵ Page, Carly, "Viasat cyberattack blamed on Russian wiper malware," TechCrunch, March 31, 2022. <https://techcrunch.com/2022/03/31/viasat-cyberattack-russian-wiper/>.

⁷⁶ Reuters, "Satellite outage knocks out thousands of Enercon's wind turbines," February 28, 2022. <https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/>.

⁷⁷ Deutsche Windtechnik, "Cyber attack on Deutsche Windtechnik," April 22, 2022. <https://www.deutsche-windtechnik.com/us/news/news/detail/cyber-attack-on-deutsche-windtechnik/#:~:text=During%20the%20night%20between%20April,switched%20off%20for%20security%20reasons>.

responded to ransomware attacks on their enterprise systems⁷⁸. While none of these incidents resulted in a loss of power production capability, they highlight the susceptibility of third parties to attacks with potential operational impacts, even if OT equipment is not directly affected.

As with threat actors, the attack exposure of the system must be considered throughout its lifecycle. Manufacturing, shipping, assembly, and development all represent potential points of exposure where vulnerabilities could be introduced or illegitimate access to systems gained prior to operation. Major challenges of remote BESS maintenance can include:

- **Connectivity:** Remote maintenance relies on robust communication networks. Any connectivity issues can hinder real-time monitoring and timely intervention.
- **Security:** Remote systems are potential targets for cyberattacks. Ensuring secure data transmission and access control is critical.
- **Diagnostics and Response:** Remote diagnostics can be limited compared to onsite inspections, and remote response capabilities might not be adequate for all types of maintenance issues.

Examples of exploited vulnerabilities in recent years include:

- Enphase Envoy vulnerabilities (2023)⁷⁹
 - Enphase Envoy is a communications gateway that transmits home solar energy system performance data to the MyEnlighten portal
 - Wired connection to microinverter, connected through user's router or cell modem to MyEnlighten
 - Used for monitoring and automatic software updates
 - Control features include power export limiting and zero-export applications
 - OS Command Injection in the gateway allows root access
- Mirai Botnet leveraging CONTEC vulnerabilities (June 2023)⁸⁰

⁷⁸ Petkauskas, Vilius, “Deutsche Windtechnik hit with a cyberattack, a third on Germany’s wind energy sector,” April 27, 2022, Cybernews. <https://cybernews.com/news/deutsche-windtechnik-hit-with-a-cyberattack-a-third-on-germanys-wind-energy-sector/>.

⁷⁹ Cybersecurity & Infrastructure Security Agency (CISA), “Enphase Envoy (Update A),” July 13, 2023. <https://www.cisa.gov/news-events/ics-advisories/icsa-23-171-01>.

⁸⁰ Cadzow, Emma, “Why We’ll Be Seeing More Mirai-Like DDoS Attacks This Year,” Corero Network Security, 2024. <https://www.corero.com/mirai-like-ddos-attacks/>.

- Palo Alto Networks Unit 42 describes threat actor activity leveraging IoT vulnerabilities to spread a variant of Mirai botnet
- Contec SolarView vulnerabilities included, but not the only ones
- Bots used to execute additional attacks, including denial of service (DOS)

Common Digital and Communication Features in BESS and Power Electronics: Risk vs. Benefit

Some common features in Power Electronics and BESS, which provide benefit, but also risk include persistence in communications and condition monitoring:

Communications and Inverters

BESS often require key digital components from non-domestic suppliers, which could give PRC-backed companies the ability to impact domestic energy resources. These supplier relationships enable the PRC to establish delivery mechanisms that, if exploited, could cause downstream impacts on regional energy infrastructure.

Some technical features of digital infrastructure enhance risk of adversary access. Distributed systems, for example, require communications and remote maintenance to manage security fixes, patches, and updates which enable secure operation. Because cyber safety may be compromised by out-of-date firmware and software, remote management is often the only practical path, given the volume of devices affected. However, componentry configured to accept updates from an OEM with negative influences can create a pathway to intrusion and a supply chain style attack.⁸¹ Furthermore, if service control is retained by the OEM, suppliers could dictate service provisions and potentially exert control over essential functions (e.g., Volt/Var management for Tesla). While OEM service control is a current business standard, efforts should be made to prioritize adding controls.

Condition Monitoring

Battery companies, in particular cell manufacturers, as common practice, collect condition and performance data across the operational fleet to identify early warnings of failure and degradation. For this communication, best practices and IEC requirements⁸² suggest segmenting it from the command and control and limiting transmissions with a one-way diode; however, if segmented, it could also pose a limited risk in normal and medium consequence operational systems. In most installations, these communication interfaces are poorly documented. For example:

⁸¹ Bart Lenaerts-Bergmans, “What Is a Supply Chain Attack?” CrowdStrike, September 27, 2023, <https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/>.

⁸² International Society of Automation (ISA), “ISA/IEC 62443 Series of Standards,” accessed April 24, 2024, <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>.

“After a project is put into operation, CATL continues to monitor its operational status through AI-powered risk monitoring and an intelligent early warning system. It calculates the failure rate of energy storage products throughout their life cycle, and thus verifies the safety design goals while continuing to optimize them.” – CATL Publication May 2024⁸³

To facilitate the data exchange, the BESS must communicate outside the firewall of its utility or integrator connection. While many large vendors—including Tesla, Fluence, and Flexgen—operate this way, the risk is mitigated via the separation of communications and control, along with other features to isolate it from other networks.

Supply Chain Threat of PRC Influence for Digital Energy Infrastructure: Evaluating the Technical Risk Landscape

As part of this report’s supply chain analysis, the criticality of the BESS functional components, together with the systemic consequence of their cyber or physical misoperation, were evaluated to identify their priority relevant to solution development. The evaluation considered the system functions, modes in which each can or should operate, and modes by which each can mis-operate. The operational functions of concern are shown in Table 8.

The BESS functionality’s various critical aspects include communications ability (comms), charge and discharge control, and safety for equipment functions.

- Comms facilitates communication within the BESS, enabling control over the charge rate and limiting the ability to turn the system on or off fully or trip it completely.
- Comms also allows incremental generation or discharge within predefined limits.
- Safety measures are paramount to preventing equipment damage and ensuring life safety by averting potential risks of escalating damage or harm to personnel (e.g., electrocution).

BESS also has cybersecurity impact potential both through its connection with other cybersecurity components within a single system as well as its connections to external cybersecurity components, including site, fleet, or utility networks, amplifying cybersecurity risks and implications.

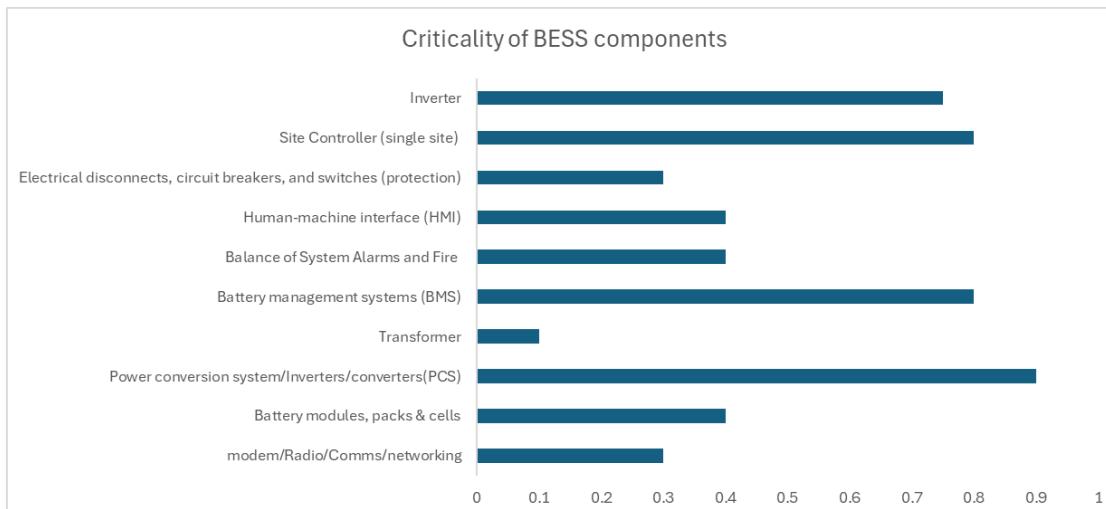
⁸³ PR Newswire, “CATL Unveils TENER, the World’s First Five-Year Zero Degradation Energy Storage System with 6.25MWh Capacity”, last modified April 12, 2014. <https://www.prnewswire.com/news-releases/catl-unveils-tener-the-worlds-first-five-year-zero-degradation-energy-storage-system-with-6-25mwh-capacity-302115412.html>

Table 8. Ability and negative impact of component misoperation.

Component Name	Function	Negative Impact of Misoperation	Can Operate in Isolation?
PCS/Inverter	Charge and discharge management	Power system coordination (meeting the load), ability to provide emergency and backup support, power system stability, two-way power flow	No
	Turning the system on and off	Power system coordination (meeting the load), ability to provide emergency and backup support, power system stability	No
	Voltage support	Power system stability	No
	Frequency support	Power system stability	No
PCS	Coordination of power and control functions for two-way power flow, communication from internal to external components	Cyber escalation can manage both the flow and the charge protections in the Battery Management System, stability, safety	No
EMS	Coordination of batteries in a site	Coordinated cyber impact (connection to other cyber components within one BESS)	No
Comms system	Connection of field system to operations center or other field systems	Cyber escalation (connection to other cyber components outside the single BESS)	No
BMS	Battery health monitoring and control	Escalating damage to components	Yes
Safety Instrumented System (SIS)	Fire prevention	Fires, equipment damage	Yes
	Temperature control	Runaway fires, equipment damage	Yes
	Life safety	Electrocution, harm of personnel	Yes

Analysts applied a Cyber-Informed, Consequence-Driven Engineering approach, generating a total consequence score for each component in the BESS, leveraging the impact of misoperation across cyber and physical domains to assign a priority to the consequence of the functions illustrated in Table 8. These scores were then used to identify the most critical components for both long- and short-term security solutions. These results are shown in Figure 23. This prioritization represents a technical, validated assessment of the capabilities of these devices and the potential impact of their exploit on the wider network (scores and functions for each item may be found in the appendices).

Figure 23. Criticality of BESS components to cyber, physical, and safety consequence outcomes.



Analysis of function, consequence, and cybersecurity capability concludes that PCS, BMS, and inverters should be prioritized at the BESS level, and site controllers prioritized at the fleet level. The PCS is the critical digital technology that allows the BESS to perform both charging and discharging, enabling a two-way flow of energy. The BMS, while critical to BESS health and safety, can be isolated from a communications standpoint, but the PCS, by nature of its function to decide when to charge and discharge, must communicate with higher level systems. The combined exposure and criticality of the PCS leads to its high criticality score.

Based on this analysis, resources and efforts should be allocated towards replacing or strengthening the protections and controls for the most critical components first. This may include implementing security measures such as encryption, access controls, intrusion detection systems, and regular security assessments and updates.

Grid and Utility-Scale Operational Consequence of BESS Functions

When prioritizing protections and controls for BESS, significant risks must be mitigated first. By first identifying and understanding the vulnerabilities and threats facing the BESS infrastructure, the risks can then be assessed, and policy actions prioritized based on replacing or enhancing the most consequential components of the system.

To assess the consequences of misoperation and failure scenarios for BESS in a large ISO with high resource penetration, criteria encompassing various aspects of system performance, safety, and reliability should be considered. Some potential criteria include:

1. **Grid Stability Impact:** Evaluate how misoperation or failure affects the stability of the grid, including voltage and frequency control, power quality, and overall system reliability.

2. **Energy Supply Disruption:** Assess the extent to which misoperation or failure disrupts energy supply to consumers, considering factors such as load shedding, blackouts, and curtailment of renewable resources.
3. **Safety Risks:** Determine the level of safety risk posed by misoperation or failure, including potential hazards to personnel, equipment damage, and environmental impact.
4. **Economic Consequences:** Evaluate the economic impact of misoperation or failure, considering costs associated with lost revenue, system repairs, compensation claims, and market penalties.

Once the criteria are established, they can be incorporated into a decision matrix ranking the consequences of misoperation and failure scenarios. Each scenario can then be evaluated against these criteria to determine its overall impact on system performance, safety, and economic viability.

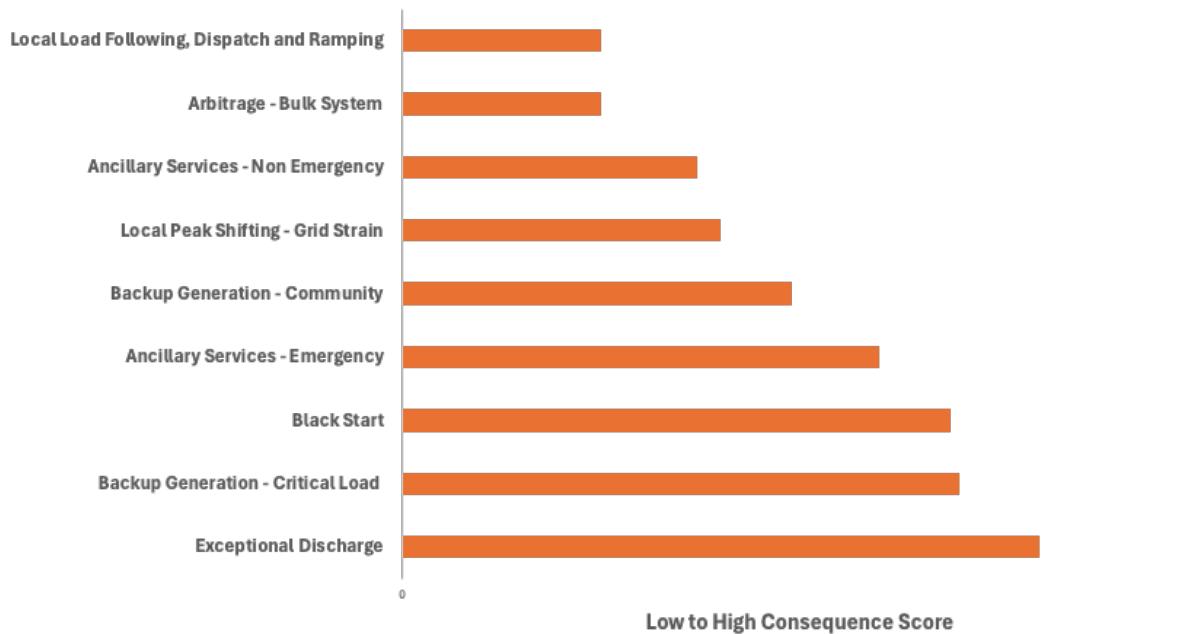
The Consequence-driven Cyber-Informed Engineering's (CCE)⁸⁴ criteria scoring threshold is illustrated in Table 9 below, with additional factors added specifically to BESS and its role in the national landscape. Environmental and reputational damage in this space are significant factors to consider in addition to the standard criteria for bulk energy systems. Many BESS and new generation components are supporting energy resilience upgrades, and the loss of these components via cyber attacks and supply chain issues would result in a significant impact on the communities they are connected to.

By systematically assessing the consequences of potential failures, stakeholders can prioritize mitigation measures and enhance the resilience of BESS deployments in high-resource penetration environments within large ISOs.

⁸⁴ Idaho National Laboratory, “Consequence-Driven Cyber-Informed Engineering,” accessed April 24, 2024, <https://inl.gov/national-security/cce/#:~:text=CCE%20is%20a%20rigorous%20process.most%20effective%20means%20of%20removing>.

Table 9. CCE criteria scoring threshold.

Criteria	None	Low	Medium	High
Area/load impact	Inconsequential	Loss of failure to service firm load of less than 300 MW (or) load supply loss of MSC or 2,000 MW, whichever is lower	Loss of failure to service firm load between 301 and 1,500 MW (or) load supply loss of between 2,000 MW (or MSC, whichever is lower) and 3,000 MW	Loss of failure to service firm load greater than 1,500 MW (or) load supply loss of greater than 3,000 MW
Duration	Inconsequential	Return of all service in less than 1 day (inability to serve firm load) (or) supply outage for less than 1 week	Return of all service 1 – 5 days (inability to serve firm load) (or) supply outage for 1 week – 1 month	Return of all service >5 days (inability to serve firm load) (or) supply outage >1 month
Safety	Inconsequential	Risk onsite	Definite safety risk offsite	Loss of life potential
Asset owner/system integrity	Inconsequential	Can restore with confidence in integrity	Owner has knowledge but no resources (money, time, personnel) to restore	Asset owner can restore but no confidence in integrity
Cost	Inconsequential	Significant but can recover	Multiple years to financially recover	Trigger of liquidity crisis/potential bankruptcy
Reputational damage	Inconsequential	—	—	Customer loss of faith in utility
Environmental damage	Inconsequential	—	—	Environmental damage
Breadth	Inconsequential	Impact to single unit nearby through attack	Impact to distribution operations through attack	Impact to critical BESS operations through networked attack

Figure 24. Criticality of BESS functions in grid connection and operation.

The technical functions of the BESS and the potential scale of impact of disruption of its performance in its role on the grid, are then scored against the Criteria priority and impact to develop a prioritization and solutions list. This is outlined further in Appendix A: BESS Components and Functions. This prioritization, showing types of BESS performance that can lead to the most consequential events, enables strategic deployment of solutions across the national fleet. For example, if a BESS is performing a critical role in backup generation, a more focused approach on its supply chain provenance, and a high assurance security package would be considered. In normal or small-level operations, the impact of a disruption would be lower and a more limited but still applicable set of solutions could be considered.

DERMS, Software, and Mass Orchestration

In assessing the importance of components to site operation and safety for BESS, it is essential to consider their broader implications beyond individual system functions. While DERMS and mass control play significant roles in BESS operation, their importance extends beyond mere functionality to encompass broader implications for grid stability, system reliability, and safety. The theory underlying the assessment of component importance emphasizes the critical role of DERMS and mass control in enabling the seamless integration and operation of BESS units within broader energy systems. Any disruption or failure in these components could have cascading effects on system operation, potentially compromising grid stability, energy supply reliability, and overall safety. Therefore, ensuring robust access to DERMS and fleet control functionalities, whether through on-site management systems or cloud-based platforms, is essential for optimizing BESS performance and mitigating risks associated with misoperation or failure scenarios.

The DERMS and US marketplace for DERMS is an opportunity to secure the upper layers of a mass-orchestrated power electronic system. With a US vendor landscape, software design practices, and programs to assist with this can be implemented quickly and to US guidelines. DERMS is currently a \$1.2B market in the US.⁸⁵ The key market leaders include GE Vernova, Siemens, Schneider Electric, and ABB. Secure by Design,⁸⁶ and integrated practices could use this mature market to deploy solutions. A key consideration in the DERMS marketplace is the use of open-source software packages, and programs to evaluate this are a supply chain security option.

The DERMS and Mass Orchestration evaluation will be considered in later studies, given the cross-cutting applications of DERMS and the Cloud Functions.

Integrator Risk Evaluation

The concept of integrators versus component suppliers for BESS was introduced earlier in this report (Section 4: Supply Chain for BESS Components). As a final piece to the analysis, the integrator model is evaluated, which effectively is a company which sells a combination of products in a complete unit and ties the components together. Integrators can be also manufacturers and OEMs, or independent companies. An integrator is essentially a system of systems and offers opportunities for secure solutions in communications and software with the turnkey unit, or integrated BESS.

Evaluating the risk, or scale of risk in the integrator space, we consider the Source of Components, Integrator Country of Origin, and other features including their maturity and operations and maintenance model. Integrators that are PRC-owned, operated and connected offer little opportunity to develop secure US-based systems, as the software and hardware will all be from the one PRC entity. One of the biggest spaces for solutions is the US integrators, while they cannot purchase many of the US solutions, or have long term agreements in place, they can develop software packages, integrate OT monitoring solutions and create other secure design solutions which do not violate the terms of their contracts with suppliers.

As illustrated in

Transitioning from this detailed examination of roles, it is essential to understand the comparative use cases of integrators based in the PRC versus those in the U.S. (Figure 26).

Figure 26, a U.S. integrator can deploy BESS systems branded under the domestic company's name but which still use battery packs (e.g., via CATL), BMS, and inverter hardware (e.g., Sungrow) provided by PRC manufacturing companies. Comparing the risk factors a US integrator using the same components may present, in comparison to a PRC

⁸⁵ Mordor Intelligence, "Distributed Energy Resource Management System Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029)", accessed April 24, 2024, <https://www.mordorintelligence.com/industry-reports/distributed-energy-resource-management-system-market>.

⁸⁶ Cybersecurity & Infrastructure Security Agency (CISA), "Secure by Design," accessed April 24 2024, <https://www.cisa.gov/securebydesign>.

based integrator, illustrates the difference in solutions and challenges we can address. However, the software components, (e.g., firmware), related to communications and data, both concerns mentioned in the CATL statement on security concerns, are made by the U.S. integrator, rather than a PRC integrator who would use software developed by CATL or partners in the PRC. Additionally, long-term O&M may also be provided by the U.S. integrator but require CATL parts. One disadvantage of this approach, which provides more visibility and control in the cyber domain in the long term than a PRC integrator, is that supplier agreements are long-term and enforce requirements that an integrator cannot inspect or analyze supplied equipment firmware.

Scaling Integrator and Aggregator Risk at a Systems Level

To comprehensively address these concerns, a systematic evaluation framework is essential for assessing and mitigating risks at both the component and integrator levels. Through this approach, the analysis has addressed and evaluated a series of factors by which a company or systemic supply chain risk, can be assessed against consequence. This strategy enables a rapid assessment of suppliers and integrators, to address the most applicable solutions and resources for supply chain threats as they occur or new systems are being designed. This scale means that foreign equipment, and integrations can be assessed apples to apples rapidly for key factors such as willingness to comply with safety and security requirements, maturity of company and record of equipment supply. This can be assessed from public records and would enable a strategic assessment of vulnerability against dominance in the global markets.

Integrators in this assessment can be placed on the matrix, and rapidly reassessed based on new information periodically. Solutions are then designed on this framework, for targeted industry engagement.

Figure 25: Assessment Matrix for Suppliers of BESS and integrators

		All FEOC	All US/Trusted Partner
		Dominant	Vulnerable
Dominant	All FEOC	PRC Integrator, PRC Equipment Mature Meets sec requirements Good safety record	US integrator, PRC equipment Mature Meets sec requirements Good safety record
	All FEOC	PRC Integrator, PRC Equipment Mature Won't meet sec requirements Unknown safety record	US integrator, PRC equipment Mature Meets some security and safety requirements
	Vulnerable	PRC Integrator, PRC Equipment Immature Won't meet sec requirements Poor safety record	US integrator, PRC equipment Immature Won't meet sec requirements Poor safety record
		All FEOC	All US/Trusted Partner
Dominant	All FEOC	Integrator A 	Integrator E 
	Vulnerable		
	Vulnerable		Integrator C 
Vulnerable	All FEOC		Integrator D 
	Vulnerable	Integrator B 	
	Vulnerable		

Nonetheless, such a strategy may provide a way to obtain the benefits of BESS systems while mitigating attack surface exposure and long-term access to BESS facilities. Such a strategy should consider the observation that companies such as Hithium are executing multi-year supplier agreements with U.S. companies that develop EMS, and there is a challenging landscape for growing the U.S. power electronics supply. These solutions are defined in the final section and presented here (Table 10) as part of the evaluation.

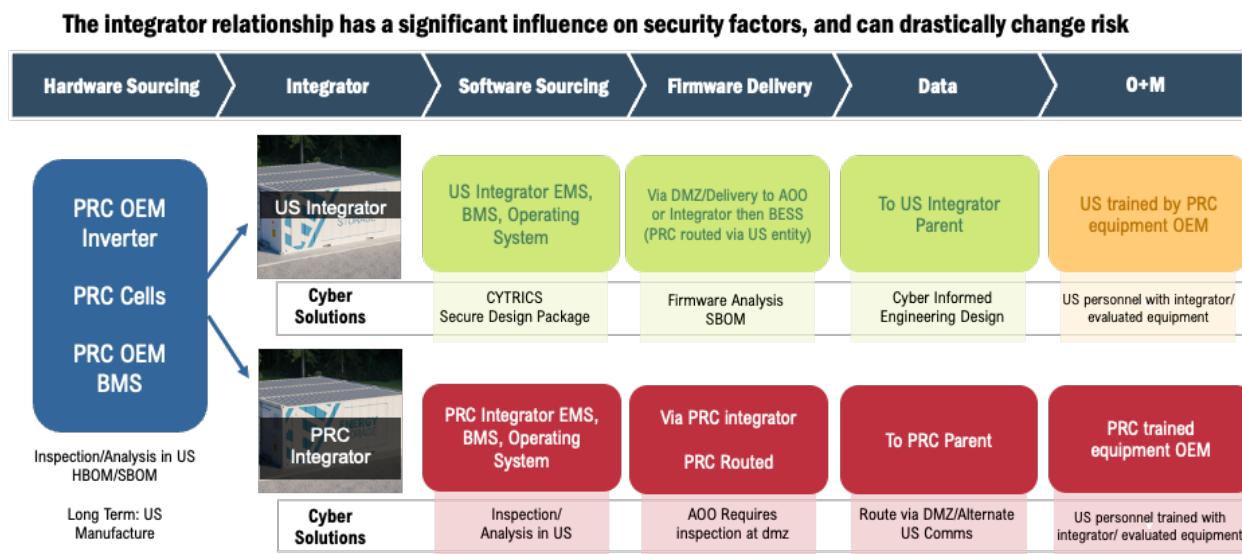
Table 10: Integrator risk solutions on analysis scale.

 PRC Owned, Operated, Connected	U.S.-Owned, Operated, Connected 
--	---

	All FEOC, High Risk, more PRC Control and Connection, Less Ability to Evaluate	May Have Non-FEOC Equipment, Emerging Tech Relationships, Financial Ownership	Less Risk, All U.S. Connection. Higher Ability to Evaluate
Policy Solutions	Right to inspect/evaluate for vulnerability and control	Develop U.S. integrator and international cybersecure manufacture agreements	U.S. supply chain incentives for power electronics
Technical Solutions	<ul style="list-style-type: none">• Procurement/contract guide• Configuration and inspection• OT monitoring and specific detections for PRC controller/actors• CIE design	<ul style="list-style-type: none">• Configurations & inspection• Secure by design for U.S.-made software• Secure comms• Vulnerability assessment program• Clean Energy Defenders Training	<ul style="list-style-type: none">• Secure comms• Secure equipment manufacture• CIE design• Clean Energy Defenders Training
Coordination Required From	U.S. AOO, Buyer of PRC Product	U.S. AOO, U.S. Integrator, International OEM	U.S. AOO, Integrator, U.S. OEM

Transitioning from this detailed examination of roles, it is essential to understand the comparative use cases of integrators based in the PRC versus those in the U.S. (Figure 26).

Figure 26. Use case and comparison of a PRC-based integrator versus a U.S. one.



Supply Chain Threat of PRC Influence for Digital Energy Infrastructure: Business Model and Policy Landscape

Supply chain risk management often focuses analysis of manufactured devices on individual companies and components. BESS and the business model landscape in which they are manufactured, built, installed, maintained, and operated are complex and often obfuscated by many layers of process, which impacts the attack surface exposure of regional energy infrastructure and its downstream dependencies.

The recent focus on cyber supply chain risk management underscores how inter-organizational relationships, just like cyber-physical dependencies, can be used to provide access, persistence, and unexpected and potentially adversarial impacts to energy sector systems. As a result, we must consider business models surrounding BESS as a source of long-term operational risk.

Roles and Responsibilities in the BESS and Inverter Sector

Various entities within the BESS ecosystem, with distinct roles and specific responsibilities, contribute to the system's functionality and efficiency. Unlike conventional utilities in which ownership, operation, and maintenance are typically consolidated within a single entity, the

BESS ecosystem features diverse stakeholders with specialized functions. As captured in Table 11, all these stakeholders—including builders and commissioners, owners, operators, maintenance providers, communicators with site infrastructure, and power sellers—fulfill crucial roles in the deployment and operation of BESS infrastructure, and all are affected by supply chain risk.

Table 11. Roles and responsibilities in the BESS ecosystem.

Item	Builds and Commission s	Owner	Operator	Physical Location and Electrical Interconnect	Maintains Communications with Site	Sells Power	Data Access
Distribution or G&T Utility		X	X	X	X	X	X
Third-Party Independent Power Producer/Virtual/Aggregator		X	X		X	X	X
Third-Party O&M Company			X		X		X
BESS OEM					X		X
ISO					X		X
Third-Party Retail Sales						X	X
Engineering, Procurement, and Construction	X						X
Interconnect Analysis Party							X

Because multiple organizations may maintain communications with the site, appropriate management or security procedures (e.g., multi-factor authentication, role-based access) is crucial; these measures help to reduce attack exposure by which the organizations could be used as an entry point to connect to the BESS or become a secondary targets as adversaries

use BESS communications infrastructure to pivot into new networks.⁸⁷ While utilities (distribution and G&T) are responsible for maintaining system reliability and may experience the highest consequences of BESS misoperation, other stakeholders—such as third-party IPPs, or VPP operators—may have more direct control over the BESS operation and should take an active role in cybersecurity risk mitigation.

Limited liability companies (LLCs) are a business structure that combines elements of both a corporation and a partnership or sole proprietorship.⁸⁸ In an LLC, owners have limited liability, meaning their personal assets are typically protected from the debts and liabilities of the business. An LLC approach can help compartmentalize risks and legal obligations associated with individual installations.

Potential Impact by Stakeholder

We can also consider the potential impact by stakeholder, utilizing the potential vectors for issue. While all stakeholders may not be impacted by a system power outage, or cyber event, they may face impacts through the organizational relationship structures, shown in Table 12.

Table 12. Potential impact by stakeholder.

Potential Impact by Stakeholder			
Event	Utility (Non-Operator)	Operator (Facility, Aggregator, Utility)	Manufacturer, Integrator, or Installer
Loss of Control	<ul style="list-style-type: none">• Energy imbalance	<ul style="list-style-type: none">• Propagated failures• Injury• Equipment damage	<ul style="list-style-type: none">• Reduce reputation• Financial liability
Manipulation of View	<ul style="list-style-type: none">• Improper control decision	<ul style="list-style-type: none">• Improper control decision	<ul style="list-style-type: none">• Reduce reputation• Financial liability
Manipulation of Safety	<ul style="list-style-type: none">• Extended restoration time• Failure of regulatory compliance	<ul style="list-style-type: none">• Injury or death• Loss of intellectual property• Technical investigation	<ul style="list-style-type: none">• Devalue brand name• Reduce market share• Decommission product from market• Financial liability

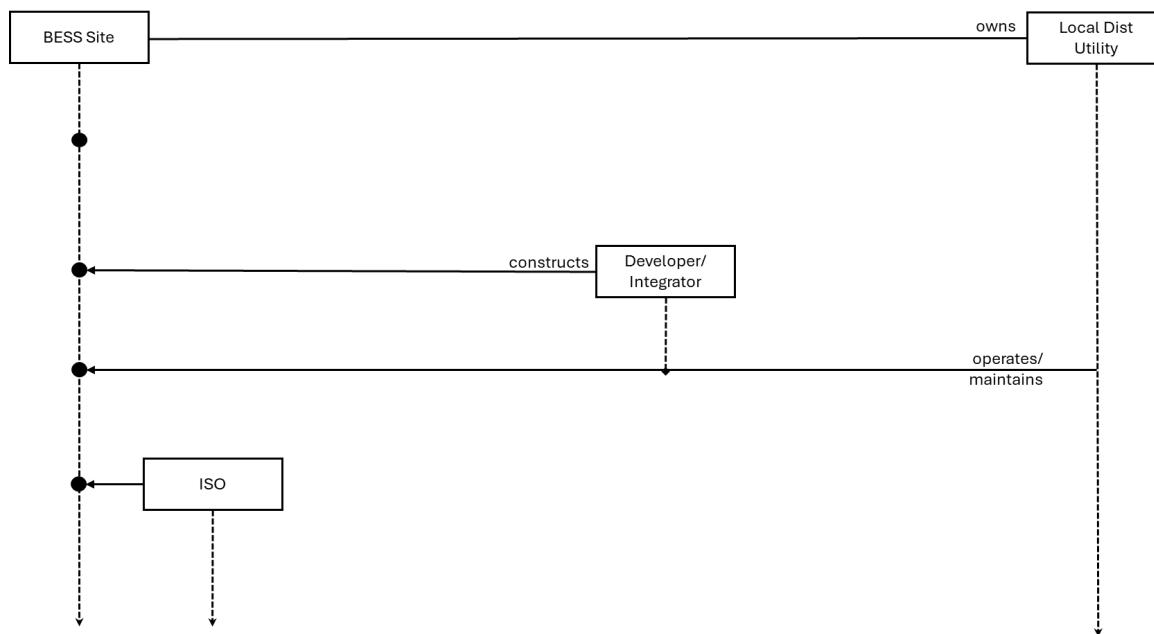
⁸⁷ BoHyun, Ahn, Seerin, Ahmad, Mazumder, Sudip Kumar, Johnson, Jay, Mantooth, Alan H., Farnell, Chris, "An Overview of Cyber-Resilient Smart Inverters Based on Practical Attack Models," *IEEE Transactions on Power Electronics*, 39, no. 4 (April 2024): 4657-4673, <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10360278>.

⁸⁸ Internal Revenue Service (IRS), "Limited Liability Company (LLC) - Small Businesses/Self-Employed," accessed April 24, 2024, <https://www.irs.gov/businesses/small-businesses-self-employed/limited-liability-company-llc>.

Decentralization of Ownership, Operations, and Maintenance⁸⁹

Just as communications and computer networks have enabled physical decentralization of generation via DER, decentralization is increasingly a trend in clean energy business models, motivated by specialization and economies of scale. For example, offering BESS O&M as a service is gaining traction.⁹⁰ But while specialized services can reduce costs and spur investment within the sector by decoupling ownership from operational expertise, they also decouple financial ownership from operational control. Additionally, to realize economies of scale, these services must be widely adopted, which increases the potential impact of a disruption.

Figure 27. Utility as owner, operator, and maintainer of BESS site.



Case Study 1: Utility as Owner, Operator, and Maintainer

Traditionally, utilities have been the primary owners of BESS installations. As illustrated in Figure 27, a distribution utility with a Generation and Transmission (G&T) component is approached to host a BESS site to bolster generation and distribution support. The site is owned and operated by the G&T entity, which assumes responsibility from both a cyber and a physical standpoint. Each site is interconnected at 69 KV and falls under 10 MVA capacity

⁸⁹ Weaver, G., Culler, M., Stewart, EM., "Organizational Influence on Supply Chain for Digital Energy Infrastructure: Business Models, and Policy Landscape" Proceedings of The Sixth IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, Oct 28 – 30 2024

⁹⁰ CAMS Technology, "Battery Energy Storage System - CAMS Technology," accessed April 2024, <https://camstex.com/tag/battery-energy-storage-system/>.

so that in the future it will be registered as a generator under NERC CIP,⁹¹ and subject at a minimum to Low Impact Generator owner requirements—that is, the asset owner and operator (AOO) must follow the NERC CIP requirements for this site (when implemented). In this case, the AOO is the utility itself, which retains control over the interconnect process, performance monitoring, and cybersecurity measures and ensures comprehensive oversight and management of the BESS site.

Case Study 2: Third-Party Ownership

In contrast, there has been a noticeable shift towards third-party ownership, primarily driven by financiers seeking investment opportunities in energy infrastructure. In this case study example, as illustrated in Figure 28Figure 28. An example of third-party ownership; site in Texas.

, a third-party independent power producer (IPP) secures rights and interconnect agreements for site development. The site is then sold to another IPP before sourcing and construction commences. This second IPP finalizes interconnect agreements with the local distribution utility. The utility secures a Power Purchase Agreement (PPA) with the site but does not assume ownership, operation, or maintenance responsibilities. Instead, the IPP enters into a 4th party O&M contract.⁷⁷ The site is interconnected with both the O&M site and the ISO. The site operates within the ISO market pool and is connected at 138 kilovolts (KV) with a capacity of 2x100 MVA. Following an acquisition in 2023, all assets are owned by a French company.⁹²; physical location requirements are overseen by the distribution utility, with the ISO serving as the market controller and defining interconnect standards.

While the model in which the utility owns the unit preferable from a management and responsibility standpoint (i.e., one clear asset owner and operator who will fall under a standard for cybersecurity), the potential for the AOO to have limited staffing resources and understanding of the system, coupled with increased management costs, may lead to security vulnerabilities and/or a limited or minimal application of required standards. In this scenario, the primary impact of a failure on the electric grid or local area and the responsibility for managing it are held by the same entity.

In the third-party model, the utility is still receiving electricity from the site, but is not managing its security, as there is a different owner and operator. There are many more points of connection that could impact the cyber risk of this site that must be managed. Additionally, the AOO or Generator Owner is not a U.S. company, and if there was a need to register under NERC CIP, it would not be clear exactly who would be registered. The impact of an attack will still be with the physical device and connection to the electric grid.

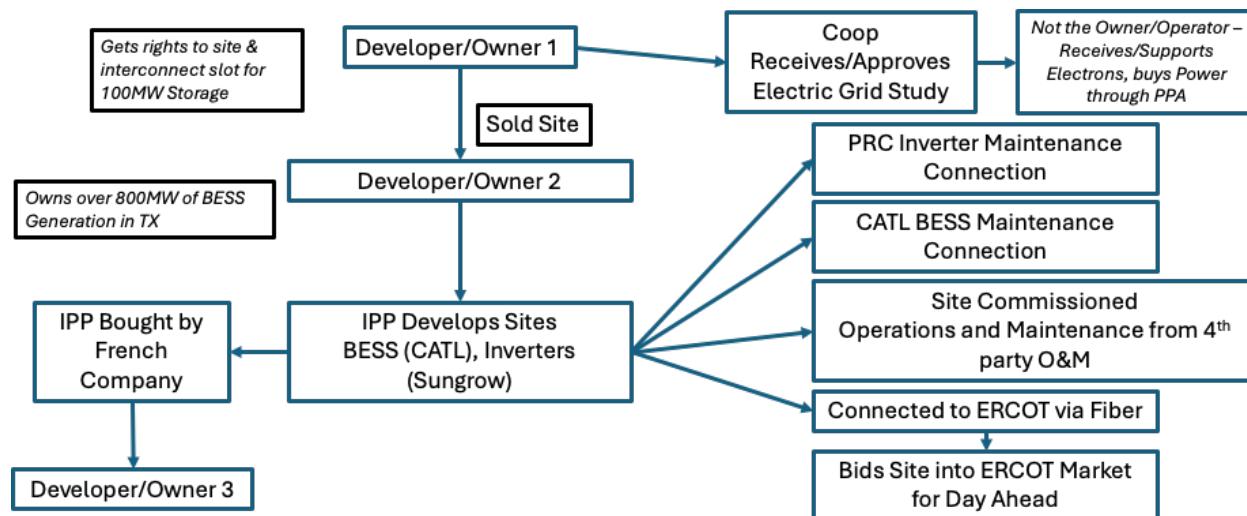
The trend toward decentralization of ownership, operations, and maintenance of a BESS facility, results in more complex business relationships that may increase operational risk.

⁹¹ North American Electric Reliability Corporation (NERC), "NERC Launches IBR Registration Initiative Resources to Highlight Progress and Keep Stakeholders Informed," last modified February 29, 2024, <https://www.nerc.com/news/Pages/NERC-Launches-IBR-Registration-Initiative-Resources-to-Highlight-Progress-and-Keep-Stakeholders-Informed.aspx>.

⁹² Enix Power Solutions, "White Label Batteries," accessed April 24, 2024, <https://www.enix-power-solutions.com/white-label-batteries/>.

While there is limited choice in manufacture from non-PRC locations there are business models and technical configurations which reduce the risk of that influence. Domestic integrators may reduce the long-term attack surface exposure for turnkey BESS installations.

Figure 28. An example of third-party ownership; site in Texas.



Expanding Markets for BESS Suppliers

BESS facilities and other clean-energy technologies require key digital components, but the supply chains for many, if not all, these digital components are dominated by foreign-owned suppliers. As a result, these foreign-backed suppliers can reduce risk by indirectly entering a newer market via a domestic partner, with the potential over time to compete with that partner and/or become vital to the operation and maintenance of increasingly prevalent clean-energy systems. This may occur by leveraging the distribution channels of U.S.-owned companies through long-term supplier agreements, gaining access to key digital technologies through strategic partnerships, leveraging clean-energy tax incentives available to partners, and participating in U.S.-hosted industry groups, conferences, and standards bodies.

Case Study 1: White Label, Integrated Component Suppliers Expanding Up the BESS Vertical

Suppliers of BESS digital components can pivot from a manufacturer role to an integrator and turnkey provider role—currently a common shift in the clean energy industry. The entity can enter and learn about an emerging market via long-term supplier agreements with U.S. companies, providing either a component, such as a battery cell or chip to be integrated into other devices, or a white-labeled device, such as a basic inverter, which is then relabeled as a different provider. Over time, as the supplier learns more about the market, they may be able to expand their business model up the vertical and become an integrator; for example,

renowned battery cell manufacturers CATL⁹³ and SYL Ningbo are transitioning from simply supplying battery cells to offering integrated systems with advanced features including sensors, often branded under their own names.⁹⁴

Case Study 2: Suppliers Expanding Across the BESS and Clean Energy Infrastructure Lifecycle

Alternatively, suppliers of digital components for BESS can expand their influence across the BESS lifecycle by becoming a service provider. For example, in Tesla's EV model, service control is retained by the OEM,⁹⁵ illustrating the significance of the OEM in dictating service provisions and potentially exerting control over essential functionalities such as Volt/Var management. Additionally, the integration of sensors necessary for operation, optimization, and safety systems can provide an opportunity for legitimate, legal, continuous monitoring as a service.

Case Study 3: Integrators and Turnkey Products

The choice of a domestic integrator may provide an approach to decreasing the attack surface exposure of a BESS site. In its December 2023 rebuttal to security concerns, CATL noted that integrators "manage connections to the grid and the grid operators set up an additional layer of security measures."⁹⁶ These connections include those for electrical power, and integrators also make facility design choices that impact network architectures to enable long-term operations and maintenance. Therefore, choosing a U.S. rather than a PRC-based integrator may help mitigate long-term attack surface exposure within the BESS site, while still enabling commerce and integration of cutting-edge technology.

Legitimate Persistence within Communications Networks

Clean energy systems depend upon reliable communications to coordinate and optimize generation via renewables and BESS to help stabilize the grid. The clean energy transition promises increased dependency on such systems; such dependencies, if not explicitly managed, have the potential to erode national sovereignty via legal, grey-zone business practices.

As noted earlier in this report, DER require communications to coordinate generation across a wide geographic area. While such technologies drive efficiencies and enable some security features such as regular patching, they also increased risk. Supplier entity influence or

⁹³ Amy Hawkins, "CATL, The Little-Known Chinese Battery Maker That Has The US Worried," *The Guardian*, March 18, 2024, <https://www.theguardian.com/world/2024/mar/18/catl-chinese-battery-maker-evs-electric-vehicles>.

⁹⁴ Cameron Murray, "Hithium and US developer Perfect Power in 1GWh battery MOU," *Energy Storage News*, November 10, 2023, <https://www.energy-storage.news/hithium-and-us-developer-perfect-power-in-1gwh-battery-mou/>.

⁹⁵ Tesla, Inc., "Tesla Owners Manual," accessed April 2024, <https://www.tesla.com/ownersmanual>.

⁹⁶ CATL, "CATL Statement on Security Concerns", last modified on December 7, 2023. <https://www.catl.com/en/news/6154.html>

insertion of a firmware vulnerability into their supply chain, like the SolarWinds incident,⁹⁷ are key risks in this architecture—risk that is enhanced by a foreign business ownership model. While the risk may be mitigated technically, often negotiated via contracts with the OEM, many maintain the connection for ease. Similarly, many battery companies, under enhanced scrutiny for safety and fire risk, also maintain connections across their fleet to gather data on battery performance and develop early warning systems for faults and fires⁹⁸. In many cases, the BESS company has been required to provide that data to investigators, so removing that connection may be a challenge, with the benefit of safety outweighing the cyber risk.

Even after installation, operation and maintenance of physical systems is an area in which the OEM can have influence. Adversarial manufacturers and integrators that provide O&M as a service to BESS may be able to apply living-off-the-land and data collection tactics, often seen in the cyber domain, via connectivity required by Service-Level Agreements (SLAs) or enabled by strategic partnerships. Such services can increase the complexity of underlying network architectures, further complicating network configuration and maintenance, implementation of access and security controls, and development of incident response plans. For example, in 2018 at the AWEA Conference, a technician working for a manufacturer, used a poorly maintained laptop which had downloaded malware from hotel internet and uploaded that malware upon physically connecting to the renewable energy infrastructure.⁹⁹

Case Study 1: Pivoting from Multi-Year Supplier Agreements to Design

Suppliers of digital components for BESS may leverage multi-year supplier agreements to gain access to and potentially influence emerging technologies. Securities and Exchange Commission (SEC) filings from late 2023 and early 2024 show the existence of three-year supplier agreements between Hithium and U.S. companies that develop energy management systems¹⁰⁰¹⁰¹¹⁰². In the EV space, CATL has multi-year supplier agreements

⁹⁷ Oladimeji, Saheed and Sean Michael Kerner, "SolarWinds Hack Explained: Everything you Need to Know," last modified November 3, 2023. <https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>.

⁹⁸ Zhao, Jingyuan, Feng, Xuning, Tran, Manh-Kien, Fowler, Michael, Ouyang, Minggao, and Andrew F. Burke, Battery Safety: Fault Diagnosis from Laboratory to Real World, *Journal of Power Sources*, 598, 234111, (April 2024). <https://doi.org/10.1016/j.jpowsour.2024.234111>.

⁹⁹ Davidson, Ros, "AWEA 2018: Increase in Cyber Security Attacks 'Inevitable,' Expert Warns," *Windpower Monthly*, May 8, 2018, <https://www.windpowernonthly.com/article/1464061/awea-2018-increase-cyber-securityattacks-inevitable-expert-warns>.

¹⁰⁰ ELM Microgrid, "Utility Scale MicroGrid ESS Packages," accessed April 24, 2024. <https://elmmicrogrid.com/utility-ess/>.

¹⁰¹ BusinessWire, "Hithium and FlexGen Sign Cooperation Agreement," last modified November 21, 2023, <https://www.businesswire.com/news/home/20231121630058/en/Hithium-and-FlexGen-Sign-Cooperation-Agreement>.

¹⁰² Hithium, "Hithium to Supply Powin with 5GWh Battery Cells," last modified January 16, 2024, <https://hithium.com/en/news/hithium-to-supply-powin-with-5gwh-battery-cells>.

with several auto companies^{103 104 105}. These agreements between private U.S. business entities are likely difficult to legally dissolve.

Case Study 2: Influencing Network Architecture via Service Level Agreements

Moreover, OEMs that can pivot to provide operation and management services gain legitimate, persistent access to a BESS facility across its lifecycle. These O&M services are expressed within a BESS facility's communication network architecture (an instance of Conway's Law).¹⁰⁶ Visibility and telemetry over operations, accessible via a management dashboard, become part of the value proposition that customers expect. As noted by a 2021 DOE EERE SETO article, “[a] solar-plus-storage system can help you to better track the energy your system is generating through monitoring capabilities, providing an enhanced level of transparency and precision. These systems allow you to track the energy your home is producing and using in real time.”¹⁰⁷ Moreover, a 2017 report by Sandia notes that “remote access to DER equipment from foreign companies is permitted.”¹⁰⁸ In other words, many DER systems have a design-level dependency on telemetry and monitoring, services that suppliers are naturally able to provide following an installation. For example, Sungrow, a foreign-owned manufacturer and supplier of BESS components for the Chisholm Grid in Fort Worth, Texas, maintains this facility under a long-term service agreement¹⁰⁹.

¹⁰³ Honda Motor Co., LTD, “Form 6-K for the Month of April 2022 (filed April 2022),” Securities and Exchange Commission (SEC), accessed April 24, 2024.

<https://www.sec.gov/Archives/edgar/data/715153/000119312522102310/d294649d6k.htm>.

¹⁰⁴ Securities and Exchange Commission (SEC), Ford News, “Ford Releases New Battery Capacity Plan, Raw Materials Details to Scale EVs; On Track to Ramp to 600K Run Rate by '23 and 2M+ by '26, Leveraging Global Relationships,” last modified July 21, 2022, <https://www.sec.gov/Archives/edgar/data/37996/000003799622000044/exhibit99-pressrelease.htm>.

¹⁰⁵ Securities and Exchange Commission (SEC), Tesla, “Annual Report 2023,” last modified January 2024, https://www.sec.gov/Archives/edgar/data/1318605/000110465924053372/tm2412112d4_ars.pdf.

¹⁰⁶ Martin Fowler, “Conway's Law,” MartinFowler.com, last modified October 20, 2022. <https://martinfowler.com/bliki/ConwaysLaw.html>.

¹⁰⁷ Office of Energy Efficiency & Renewable Energy (EEFE), “Should I Get Battery Storage for My Solar Energy System?,” Department of Energy, last modified November 22, 2021, <https://www.energy.gov/eere/solar/articles/should-i-get-battery-storage-my-solar-energy-system>.

¹⁰⁸ Johnson, Jay Tillay, “Roadmap for Photovoltaic Cyber Security,” Sandia National Lab, last modified December 1, 2017. <https://www.osti.gov/biblio/1782667 page 62>.

¹⁰⁹ Colthorpe, Andy, “Sungrow Awarded Supply Contract for One of Texas' Largest Battery Projects So Far,” Energy Storage News, last modified January 25, 2021. <https://www.energy-storage.news/sungrow-awarded-supply-contract-for-one-of-texas-largest-battery-projects-so-far/>.

Mitigation Planning and Relevant Initiatives

National Strategies and Policy

Legislation

- Multiple stakeholders—including utilities, regulators, and independent system operators—make up the complex ownership and operation models of the U.S. grid and its digital energy components. Coordination of cybersecurity efforts across these diverse entities is challenged by different priorities, resources, and levels of cybersecurity maturity. Legislation provides one mechanism for coordinating action across the industry. The NDAA, the Build America Buy America Act (BABA), and tax credit limitations for equipment manufactured by Foreign Entities of Concern (FEOC) offer strategies relevant to securing the digital supply chain for BESS.
- Several versions of the NDAA seek to mitigate supply chain risks by creating and enforcing lists of banned companies. Section 889, signed into law via the NDAA FY19, applies to federal agencies, their contractors, and grant or loan recipients. Section 889 within the NDAA prohibits agencies from procuring equipment, doing business with companies that use covered equipment, or funding the purchase of covered equipment using federal money.¹¹⁰ While the original NDAA applied to telecommunications and video surveillance equipment that were critical technologies or essential system components, the NDAA for FY21 directed the Secretary of Defense to list Chinese Military Companies (CMCs) annually until the end of 2030.¹¹¹ Most recently, the Pentagon provided an updated list of CMCs with NDAA FY24.^{112,113}
- The Buy America standards for equipment and materials used in federally funded projects are designed to prioritize the use of domestically produced items. These standards are part of the Buy America Act and BABA¹¹⁴, enacted as part of the

¹¹⁰ National Defense Industrial Association (NDIA), “Section 889,” accessed April 2024.
<https://www.ndia.org/policy/issues/cyber/section-889>.

¹¹¹ U.S. Department of Defense, “Notice of Designation of Chinese Military Companies Under the William M. (Mac) Thornberry NDAA for FY21,” Federal Register, 86, no. 121 (June 28, 2021): 33994,
<https://www.govinfo.gov/content/pkg/FR-2021-06-28/pdf/2021-13753.pdf>.

¹¹² U.S. Department of Defense, “DOD Releases List of People’s Republic of China (PRC) Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021,” October 5, 2022,
<https://www.defense.gov/News/Releases/Release/Article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/>.

¹¹³ U.S. Congress, National Defense Authorization Act for Fiscal Year 2024, 118th Cong., last modified April 18, 2023, <https://www.congress.gov/bill/118th-congress/house-bill/2670>.

¹¹⁴ U.S. Environmental Protection Agency (EPA), “Build America - Buy America (BABA),” last modified June 12, 2024.
<https://www.epa.gov/cwsrf/build-america-buy-america-baba>.

Infrastructure Investment and Jobs Act (IIJA)¹¹⁵ or Bipartisan Infrastructure Law (BIL).¹¹⁶ BABA applies a domestic content procurement preference requirement to federally funded, public infrastructure projects. Various agencies, including the U.S. Department of Agriculture¹¹⁷ and Department of Energy (DOE)¹¹⁸ have implementation guidelines, which aim to promote domestic manufacturing and reduce reliance on foreign suppliers. Key points of these standards include Domestic Content Preference, Specific Requirements for Construction Materials, Exceptions and Waivers, Rolling-Stock Requirements, and Waivers for Specific Situations.

The IIJA provides tax credits for infrastructure projects. For example, in May 2023, the Internal Revenue Service (IRS) issued preliminary directives for entities aiming to be eligible for the domestic-content tax credit. The IRS sets thresholds for the total direct costs of manufactured products that originated from within the United States: 40% of total direct costs through 2024 and 55% of those costs by 2027.¹¹⁹ The BIL also imposes limits when the project includes FEOC. DOE's Office of Manufacturing and Energy Supply Chains provided guidance relevant to their Battery Materials Processing and Manufacturing grant¹²⁰ as well as their Clean Vehicle tax credit.¹²¹

Rip-and-Replace

A common high-level approach to concerns about dependence on a non-U.S. supply chain for critical energy infrastructure is to replace the equipment with a U.S. supply. However, rip and replace is unrealistic in the immediate and short term but also the long term.

- **Immediate Term:** As previously noted, there was approximately 16 GW of BESS capacity installed by the end of 2023, with plans to reach 30 GW by the end of 2024. Both the existing systems and the systems under construction have already selected suppliers and procured equipment. Even if a domestic supply chain were immediately available, it would be prohibitively costly to replace all this equipment. Additionally, the labor needed to make substitutions and the downtime that operators would

¹¹⁵ U.S. Congress, "H.R.3684 - Infrastructure Investment and Jobs Act," 117th Cong., last modified November 15, 2021. <https://www.congress.gov/bill/117th-congress/house-bill/3684/text>.

¹¹⁶ The White House, "A Guidebook to the Bipartisan Infrastructure Law," last modified January 2024. <https://whitehouse.gov/build/guidebook/>.

¹¹⁷ U.S. Department of Agriculture, "USDA Implementation Framework for A Plan to Enable the Bioeconomy in America: Building a Resilient Biomass Supply," last modified March 2024. <https://www.usda.gov/sites/default/files/documents/usda-implementation-framework.pdf>.

¹¹⁸ U.S. Department of Energy (DOE), Office of Manufacturing and Energy Supply Chains (MESC), "Foreign Entity of Concern Interpretive Guidance," accessed April 24, 2024. <https://www.energy.gov/mesc/foreign-entity-concern-interpretive-guidance>.

¹¹⁹ Internal Revenue Services (IRS), "Notice 2024-41," last modified May 17, 2024. <https://assets.law360news.com/1837000/1837423/notice%202024-41.pdf>.

¹²⁰ Office of Manufacturing and Energy Supply Chains, "Battery Manufacturing and Recycling Grants," accessed April 24, 2024. <https://www.energy.gov/mesc/battery-manufacturing-and-recycling-grants>.

¹²¹ Energy Saver, "New and Used Clean Vehicle Tax Credits," Department of Energy, accessed April 24, 2024. <https://www.energy.gov/energysaver/new-and-used-clean-vehicle-tax-credits>.

experience during the process would be unacceptable for an industry that prioritizes high availability and reliability.

- **Short Term:** In the short term (5–10 years), it will be difficult to create a fully domestic supply chain. Manufacturing costs must be reduced to make supply competitive with non-U.S. manufacturers. Battery cells require rare minerals (e.g., lithium), for their production, which requires access to mining operations. Maturity in manufacturing, security, and support operations can only be gained via execution over time. The development of a domestic supply chain may face opposition from large, foreign-owned stakeholders in the BESS market. While steps can be taken in the near term to promote U.S. manufacturing, it will take time to develop a domestic industry.
- **Long Term:** A robust U.S. supply chain for BESS can be built up in the long term. Even with the requirement for mined materials to create battery cells and the environmental impacts of production, government incentives, and industry support can drive the development of domestic manufacturing. While there are many benefits of a fully domestic supply chain for energy security, cybersecurity concerns can be addressed in the long term by developing and requiring better component interoperability standards. Rather than a BESS requiring a custom BMS, PCS, and EMS, likely all developed by the same manufacturer, interoperability requirements could allow for the integration of trusted digital components with the battery cells and modules that may still be manufactured outside of the United States.

Although these challenges exist, risk mitigations to address the supply chain's existing systems and systems installed in the short term must be put in place while long-term solutions for a domestic supply chain are developed. The most consequential functions can be protected while longer term supply chain mitigations happen. For existing systems, the scope of risk on a system can be assessed, and protective measures put in place to limit the impacts of potential misoperation. For systems designed and installed in the near term, mitigations can be included in the system design, and thoughtful selection of suppliers can limit association with FEOCs and prioritize monitoring, redundancy, and protection of high-impact components.

Limitations of Ban Lists

The policies outlined above define strategies for reducing reliance on foreign suppliers within federally funded infrastructure projects. At a high level, these policies primarily impact the BESS supply chain through procurement and expensive post-procurement mitigations. However, procurement is just one stage within the lifecycle of critical infrastructure components. Based on publicly available information about domestic BESS projects, policymakers should consider the direct and indirect impacts of actions across the entire BESS component lifecycle to employ a defense-in-depth strategy.

Another currently employed strategy with significant limitations and obstacles is the creation and maintenance of banned lists to drive federal infrastructure funding and tax credits.

Controlling Procurement: The federal government must be able to create and maintain banned lists to implement the NDAA as well as BIL-based tax credits. While bans on certain equipment under the NDAA aim to mitigate supply chain risks, implementing and enforcing these bans effectively is challenging. To be useful, blacklists put enforcing departments—whether those working in procurement in industry or federal agencies—in a reactive position because they must continually check contracted business relationships against the blacklist as part of a vendor risk assessment. This overhead in time and resources increases in accordance with the size of the blacklist. Moreover, blacklists must be updated at a frequency consistent with the adversarial behavior they seek to mitigate; the business operations of banned companies, and their names, can change dramatically over even a few months. In contrast, updating such lists annually via the NDAA, is too slow for an agile approach that keeps pace with the threat cadence of the threat and again encourages a reactive posture.

Prior Rip-and-Replace Initiatives

There is significant movement at present to remove, ban, or otherwise replace PRC infrastructure, including the NDAA Prohibited Battery List from FY24.¹²² The precedence for this includes the ban of Huawei and ZTE by the FCC via the Secure and Trusted Telecommunications Networks Act,¹²³ which required and funded a rip-and-replace budget for both civilian critical infrastructure, and military. Huawei at the time was also the second largest manufacturer globally of inverters,¹²⁴ but in 2019, following the FCC implemented Act, it announced its exit from the U.S. Market.¹²⁵ The Secure Networks Act also enabled funding for entities to replace that infrastructure, many of whom were small and medium-sized rural electric cooperatives and municipalities. Those entities were limited from participating in the Broadband funding program without performing the rip and replace of Huawei equipment. It was estimated that this replacement would take approximately \$4B and 4 years.¹²⁶ The UK followed suit with a similar order.¹²⁷ While it was expected that order, and funding would dent Huawei and decrease their hold over this market, in 2024, they are the number 1 inverter manufacturer in the world. In 2023, Huawei reported

¹²² H.R.2670 - 118th Congress (2023-2024): National Defense Authorization Act for Fiscal Year 2024. (2023, December 22). <https://www.congress.gov/bill/118th-congress/house-bill/2670>.

¹²³ H.R.4998 - 116th Congress (2019-2020): Secure and Trusted Communications Networks Act of 2019. (2020, March 12). <https://www.congress.gov/bill/116th-congress/house-bill/4998>.

¹²⁴ S&P Global, “Global PV inverter market surpassed \$9 billion in 2019 following record shipments”, 2019, [Online] <https://www.spglobal.com/commodityinsights/en/ci/research-analysis/global-pv-inverter-market-surpassed-9-billion-in-2019.html>.

¹²⁵ PV Magazine International, “Huawei has exited US solar inverter market”, 2024, [Online] <https://www.pv-magazine.com/2019/06/26/reports-huawei-has-exited-us-solar-inverter-market/>.

¹²⁶ Reuters, “Telecom firms need more funding to replace Huawei,” 2024, [Online] <https://www.reuters.com/business/media-telecom/many-us-telecom-firms-need-more-funding-replace-huawei-zte-equipment-fcc-says-2024-05-02/>.

¹²⁷ Data Center Dynamics, “UK begins ripping out Huawei”, 2024, [Online], <https://www.datacenterdynamics.com/en/news/bt-begins-ripping-out-huawei-hardware-from-uk-mobile-network/> <https://www.bbc.co.uk/news/business-55269879>.

a strong economic status, with revenue increasing 9% to over \$99 billion,¹²⁸ and net profit more than doubling. This was despite the company being a focus of the rivalry between Washington and Beijing. Huawei's revenue growth was attributed to a stronger-than-expected performance in its electronics business, particularly its smartphone handsets, and its Enterprise Business Group, which includes cloud, IoT, and private networks.

In 2024, the FCC (who funded the rip and replace), was estimated to have a budget shortfall of over \$3B.¹²⁹ and the rip-and-replace effort was not expected to continue or be successful as most affected entities had not replaced the technology or been able to access the allocated funds. The Pentagon, citing a risk to national security from removing technology without effective replacement, also requested a waiver to the NDAA Ban on Huawei until effective technology could be sourced.¹³⁰

The replacement of existing equipment and enabling new sources of battery technology will cost many more times the funding than the Huawei example, with the current stock of BESS installed being over \$10B of equipment. It is unlikely a replacement will be sourced rapidly despite investment. Therefore, following a similar path to the FCC's rip and replacement of Huawei is likely to be ineffective.

Technical Solutions

Solution Stakeholders and Targets

Manufacturers: Manufacturers are an important aspect of BESS supply chain security that impacts many downstream systems. Recent efforts have sought to increase domestic manufacturing of critical BESS components, which in turn increases U.S. jobs. Although the direct impacts of such a strategy are beneficial to communities in the short term, if not carefully managed over time, domestic manufacturing plants can introduce long-term dependencies on foreign entities and technologies near the base dependencies within the BESS supply chain network. For example, several domestic manufacturing sites for EVSE equipment components have the potential to provide U.S. jobs at the expense of dependence on business processes and technologies under foreign influence. Tesla is currently working on a factory to manufacture and operate CATL batteries domestically.¹³¹

¹²⁸ The economist, "Americas Assassination Attempt on Huawei," 2024, [online] <https://www.economist.com/briefing/2024/06/13/americas-assassination-attempt-on-huawei-is-backfiring>.

¹²⁹ Washington Post, "Huawei Rip and Remove Order," 2024, [Online] <https://www.washingtonpost.com/technology/2024/05/02/huawei-rip-remove-order-threatens-service/>.

¹³⁰ Bloomberg, "Pentagon has a Huawei Dilemma", 2024, [online] <https://www.bloomberg.com/news/articles/2024-07-03/pentagon-has-a-huawei-dilemma-congress-doesn-t-want-to-solve?embedded-checkout=true>

¹³¹ Coppola, Gabrielle and Edward Ludlow, "Tesla to Open US Battery Plant With Equipment From China's CATL," Bloomberg, January 31, 2024. <https://www.bloomberg.com/news/articles/2024-01-31/tesla-to-open-new-us-battery-plant-with-equipment-from-catl>.

In addition, Ford recently halted work on a \$3.5B EV battery factory which included \$1.7B in state incentives and could have employed approximately 2,500 workers.^{132 133 134}

Integrators: Integrators and O&M service providers offer opportunities for long-term, indirect influence over a BESS site. Integrators integrate the technical and physical infrastructure that enables decentralization of the ownership, operations, and maintenance in BESS systems. As acknowledged within CATL's December 2023 rebuttal to security concerns, integrators "manage connections to the grid and the grid operators set up an additional layer of security measures."¹³⁵

Operations and Maintenance: O&M activities also provide an opportunity for long-term influence over BESS. For example, Sungrow pivoted from being a supplier of BESS components for the Chisholm Grid in Fort Worth, Texas, to providing maintenance under a long-term service agreement. This privately funded project, not dependent on federal funding, falls outside of the scope of the NDAA and BABA. Furthermore, Sungrow components were purchased for the Revolution project in Texas¹³⁶ via a \$92M tax equity investment enabled via the Inflation Reduction Act.^{137 138} Table 13 highlights some of the riskier scenarios and the correlating potential policy and technical solutions.

¹³² Securities and Exchange Commission (SEC), Ford News, "Ford Releases New Battery Capacity Plan, Raw Materials Details to Scale EVs; On Track to Ramp to 600K Run Rate by '23 and 2M+ by '26, Leveraging Global Relationships," last modified July 21, 2022. <https://www.sec.gov/Archives/edgar/data/37996/000003799622000044/exhibit99-pressrelease.htm>.

¹³³ UpNorthLive, "Gotion Wins Court Ruling to Continue Development of Electric Vehicle Battery Factory," last modified May 20, 2024, <https://upnorthlive.com/news/local/company-wins-court-ruling-to-continue-development-of-michigan-factory-serving-ev-industry>.

¹³⁴ Smith, Jake, "Chinese Communist-Linked Battery Maker Breaks The Bank on Lobbying Amid Congressional Scrutiny," *Daily Caller*, last modified May 1, 2024, <https://dailycaller.com/2024/05/01/chinese-communist-party-battery-gotion-lobbying/>.

¹³⁵ CATL, "CATL Statement on Security Concerns," last modified December 7, 2023, <https://www.catl.com/en/news/6154.html>.

¹³⁶ Sungrow, "Sungrow Supplies a 100 MW Energy Storage Project in Texas," last modified January 22, 2021. <https://en.sungrowpower.com/newsDetail/2127/sungrow-supplies-a-100-mw-energy-storage-project-in-texas>.

¹³⁷ U.S. Department of the Treasury, "Inflation Reduction Act," last modified August 16, 2022. <https://home.treasury.gov/policy-issues/inflation-reduction-act#:~:text=On%20August%202016%2C%202022%2C%20President,made%20in%20the%20nation's%20history>.

¹³⁸ BusinessWire, "Spearmint Energy Completes 300 MWh Battery Energy Storage System in ERCOT Power Market; Revolution Commences Commercial Operation," last modified January 4, 2024, <https://www.businesswire.com/news/home/20240104494094/en/Spearmint-Energy-Completes-300-MWh-Battery-Energy-Storage-System-in-ERCOT-Power-Market-Revolution-Commences-Commercial-Operation>.

Table 13. Scenarios and correlating solution policies and technical approaches.

Risky Scenario	Solution Policy	Solution Technical
PRC integrator/PRC equipment	<ul style="list-style-type: none">• Firmware Analysis• Communications Ban• Equipment Ban/Sanctions• AOO is not the integrator• FOCI requirement to operate/maintain warranty batteries in U.S.• Tariffs on control and most consequential equipment	<ul style="list-style-type: none">• Full hardware/software/• AOO is not the integrator• Secure communications research
Non-U.S. Integrator/PRC Equipment	<ul style="list-style-type: none">• Firmware Analysis• Communications Ban• Equipment Ban/Sanctions• AOO is not the integrator• FOCI requirement to operate/maintain warranty batteries in U.S.• Tariffs on control and most consequential equipment	<ul style="list-style-type: none">• IR plan framework with third-party battery owner-operators
U.S. integrator/PRC Equipment	<ul style="list-style-type: none">• Firmware Analysis• Communications Ban• Equipment Ban/Sanctions• Secure by Design in Software and Interconnection	<ul style="list-style-type: none">• IR plan framework with third-party battery owner-operators

	<ul style="list-style-type: none">FOCI requirement to operate/maintain warranty batteries in U.S.	
U.S. integrator/U.S. equipment	<ul style="list-style-type: none">Secure by Design in Manufacturing	

Cyber-Informed Engineering (CIE) and Technical Assistance Programs

CIE is an innovative approach developed by DOE CESER, INL, and NREL to integrate cybersecurity principles into the engineering life cycle. This challenges practitioners to go beyond the traditional IT-centric perspective of cybersecurity to embed security considerations and engineered controls directly into the design, operation, and maintenance of industrial control systems and OT. The goal is to achieve a cybersecurity protection scheme from both engineering controls and digital controls as well as to ensure that cybersecurity is not just an afterthought but an intrinsic part of the engineering process; all of this is further encouraged in the Cyber-informed Implementation Guide¹³⁹ ¹⁴⁰.

CIE focuses on identifying and protecting against high-consequence events that could result from cybersecurity adversaries exploiting the digital components of process systems. It emphasizes a proactive and preemptive strategy, whereby potential pathways for cyberattacks are eliminated or mitigated during the design phase. This strategy reduces the likelihood of successful exploitation which could impact critical operations.

Existing federal secure-by-design initiatives¹⁴¹ could focus upon long-term needs for key software packages and global adherence to better standards, whereas CIE can provide direct engineering solutions for existing integrations and guidance for interconnection.¹⁴² In a subsequent BESS report, we will delve further into the application of CIE for protecting BESS.

Strategic Component Assessment

A Strategic Component Assessment initiative entails evaluating critical components and systems within the energy supply chain to identify potential vulnerabilities and risks and should focus on the prioritized components of the BMS, inverters, and PCS. This involves

¹³⁹ Cyber, Energy, Security and Emergency Response (CESER), “Cyber-Informed Engineering Implementation Guide,” Department of Energy, last modified August 7, 2023. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf.

¹⁴⁰ We note that Sungrow also received a Department of Agriculture grant (\$20,000) via the Rural Energy for America Program, from 2017-2019. See Grant Summary: USASpending, “10.868 Rural Energy for America Program,” accessed April 2024, https://www.usaspending.gov/award/ASST_NON_CLSS00000053963_12E4.

¹⁴¹ Cybersecurity and Infrastructure Security Agency (CISA), “Secure by Design”, accessed October, 27, 2024. <https://www.cisa.gov/securebydesign>.

¹⁴² Idaho National Laboratory, “Cyber-Informed Engineering,” last modified 2024. <https://inl.gov/national-security/cie/>.

employing metrics and methodologies to assess the cybersecurity of various components, including supply chain dependencies, reliability, and resilience. If a battery is designated as FEOC, measures will be taken to ensure that the inverter is not similarly affected.

Collaboration with integrators will facilitate adjustments to component models and configurations to align with cybersecurity requirements and mitigate supply chain risks.

Standards and Regulations

BMS, inverters, and PCS are combinations of hardware and software. Development of U.S.-controlled, secure software packages in addition to non-domestic components can mitigate risk significantly and enable continued operation in adverse conditions. The development of standards for renewable energy and power electronics can sometimes lag technological advancements, posing challenges for their widespread adoption. Key standards in progress include IEEE 1547.3 for energy storage integration,¹⁴³ UL 2941 for system safety,¹⁴⁴ and SunSpec Modbus for communication protocols.¹⁴⁵ Despite their importance, standards development can be slow due to consensus-building and regulatory processes. Nonetheless, these standards are vital for ensuring safety, reliability, and interoperability in renewable energy systems. Collaboration among stakeholders is crucial to expedite the development and implementation of these standards, keeping pace with evolving technologies. Additionally, scale-up of testing “in country” would be required.

Develop Hardware and Firmware Citizenship

The Develop Firmware and Hardware Citizenship initiative focuses on the security and integrity of firmware and hardware components within energy infrastructure systems through proactive measures. This initiative includes replacing parts during installation to ensure authenticity and mitigate the risk of compromised hardware. Additionally, a process is implemented wherein firmware is validated upon installation or update, enabling the detection and removal of any malicious or faulty firmware components. Furthermore, extra monitoring systems are installed for critical components, such as fire and environmental condition sensors, to provide real-time monitoring and early detection of abnormalities or potential security threats.

Most-Critical Location Analysis

Installation should be optimized for "non-FEOC non-waivered" equipment, particularly in critical locations or functions. For example, in hospitals or high-risk regions where functions are essential for emergency response, no waivers should be granted, even if higher costs

¹⁴³ IEEE Standards Association, “IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems,” IEEE 1547.3-2023, last modified December 11, 2023. <https://standards.ieee.org/ieee/1547.3/10173/>.

¹⁴⁴ UL Solutions, “UL Solutions and NREL Announce Distributed Energy and Inverter-Based Resources Cybersecurity Certification Requirements,” last modified April 18, 2023. <https://www.ul.com/news/ul-solutions-and-nrel-announce-distributed-energy-and-inverter-based-resources-cybersecurity>.

¹⁴⁵ SunSpec Modbus, “A Clear Path to Compliance With The IEEE 1547-2018 Communications Mandate,” last modified 2024. <https://sunspec.org/sunspec-modbus-initiative/>.

result. By prioritizing the security of critical infrastructure, this approach ensures greater resilience against cyber threats and enhances emergency preparedness.

Long-Term Strategic Monitoring and Information Sharing

Advanced sensors in key sites can be strategically placed to evaluate data in near-real-time and historical contexts, establishing a Renewable Energy Security Operations Center, or integrating with the DOE Energy Threat Analysis Center (ETAC). This allows for enhanced monitoring capabilities and documentation of sources.

Contracting and Procurement Guides

Outline procedures for evaluating vendors, negotiating contracts, and implementing cybersecurity clauses to ensure suppliers meet specified security standards. By standardizing contracting and procurement practices, organizations can enhance the security of their supply chains and mitigate risks associated with third-party vendors.

Long-Term Supply-Chain Moves: Relocating or building capacity to produce control equipment onshore or in allied locations to enhance cybersecurity resilience. Effective risk mitigation strategies can reduce the risk of high-consequence events without requiring total replacement or redesign of existing systems. By focusing on protecting the core functions of the BESS, operators and utilities can feel confident in their reliance on BESS, even with the presence of untrusted components.

To achieve this goal, several key steps need to be taken:

- **Cost Assessment:** Conduct a thorough evaluation to determine the financial implications of moving control equipment onshore.
- **Identification of Components:** Identify which components, from a technical consequence and techno-economic analysis of the control equipment need to be relocated onshore.
- **Prioritization Based on Security and Consequence:** Prioritize components based on their security implications and potential consequences of supply chain disruptions.
- **Focus on Techno-Economic Factors:** Emphasize a holistic approach that considers both technical and economic factors in decision-making and policy.

Key Programs for Solutions

DOE and the national laboratories offer several management best practices and mitigation measures that can be applied to currently installed projects or projects under development (Figure 29).

- CESER is working to address existing systems with a CIE strategy (see previous section). In this approach, systems are evaluated to understand the largest possible

impact of malicious cyber activity, and engineering controls are put in place to mitigate the impact of these high-consequence events.

- GDO is utilizing tools developed through IIJA and in partnership with CESER to support and assist more robust security measures being placed around systems currently under development. As organizations apply for funding from GDO to support new projects, GDO can offer applicants CIE resources, including a playbook for applying CIE to BESS systems, complete with recommended controls, to help them mitigate the risk of their proposed systems. GDO is releasing procurement guidance and contracting language, a key risk factor for integration, and will be partnering with other offices to extend these comprehensive solution sets in the coming months.
- The national laboratories have advanced subject matter expertise in supply chain and component analysis. Through programs like Cyber Testing for Resilient Industrial Control Systems (CyTRICS), risks or vulnerabilities associated with specific equipment can be discovered, and appropriate responses or mitigations put in place. CyTRICS leverages best-in-class test facilities and analytic capabilities at six DOE National Laboratories and strategic partnerships with key stakeholders to perform expert testing, share information about vulnerabilities in the digital supply chain, and inform improvements in component design and manufacturing.

Figure 29 - List of DOE programs relevant to securing BESS.

1. Cyber Informed Engineering – <https://www.energy.gov/ceser/cyber-informed-engineering>
 - a. Products in IBR, Interconnection, Microgrids, and BESS to guide secure configuration
2. Cyber Testing for Resilient Industrial Control Systems (CyTRICS) – <https://cytrics.inl.gov/>
3. Energy Cyber Sense - <https://www.energy.gov/ceser/energy-cyber-sense-program>
 - a. Principles Targeted as Guidelines for IBR and BESS Manufacture
 - b. Analysis and Assessment Combined
4. Cyber Labeling (Inverters) - <https://energy.sandia.gov/programs/electric-grid/cyber-security-for-electric-infrastructure/cyber-labeling-research-initiative/>
5. CECA - <https://www.nrel.gov/security-resilience/cybersecurity-accelerator.html>
6. DER AI Work - <https://www.energy.gov/ceser/articles/doe-announces-39-million-research-funding-enhance-cybersecurity-clean-distributed>
7. Liberty Eclipse – <https://www.energy.gov/ceser/liberty-eclipse>
 - a. Battery Assessments in GMLC
8. CyberStrike (STORMCLOUD) – <https://inl.gov/national-security/cyberstrike/>
9. Energy Threat Analysis Center (ETAC) – <https://www.energy.gov/ceser/energy-threat-analysis-center-0>
10. RESCUE - <https://www.energy.gov/ceser/articles/doe-nrel-and-clean-energy-industry-stakeholders-partner-address-cybersecurity-hybrid>
11. CESER OT Defender – <https://otdefender.inl.gov/>
12. Cyber Security through Hardware Integration, Education, and Layered Defense (CyberSHIELD) – <https://resilience.inl.gov/inlcybershield/>
13. GDO TA for GRIP – <https://www.energy.gov/gdo/grid-resilience-and-innovation-partnerships-grip-program-technical-assistance-resource-center>
14. CESER BESSIE – development of strategic mitigations for BESS security challenges

Summary and Conclusions

This report describes a detailed examination of battery supply-chain risks and the complex interplay between energy security and sustainable energy transition within the United States. Key findings include the following:

1. **Supply Chain Analysis:** The evaluation of regional battery system functionalities and their security considerations highlighted the importance of understanding and adapting to local market demands and grid challenges. The diversity of utility models across regions necessitates tailored strategies for ownership and operation.
2. **Legislative Impact:** The influence of the NDAA for Fiscal Year 2023¹⁴⁶ and related legislation, on the battery supply chain was identified as a critical factor in shaping future supply-chain strategies.
3. **Cybersecurity Integration:** The adoption of CIE methodologies emerged as essential for embedding cybersecurity in the life cycle of battery systems, from design through operation.
4. **Geopolitical Concerns:** Incidents involving FEOC and reports of cybersecurity threats in the energy sector underscore the geopolitical complexities affecting the supply chain. These events necessitate a vigilant and responsive approach to supply-chain management.
5. **Supply-Chain Diversification:** The report advocates for a compartmentalized strategy in supply-chain management, prioritizing the components deemed highest risk or most impactful on control and communication systems.
6. **Consequence-Based Prioritization:** A modular consequence-based assessment framework was employed to prioritize supply-chain components and, in turn, influence strategic manufacturing and security decisions.
7. **Recommendations for Resilience:** A set of strategic initiatives was proposed, targeting both immediate and long-term mitigation strategies to address supply-chain vulnerabilities. These initiatives were evaluated against their cost implications and potential to enhance FEOC.
8. **Operational and Regional Consequence Assessment:** The report highlighted the need to address consequences sensitive to regional and seasonal variations, who and what the battery is serving, and the availability of emergency resources.

¹⁴⁶ NDAA - National Defense Authorization Act, House Armed Services Committee, last modified December 7, 2022.
<https://armedservices.house.gov/ndaa>.

Appendix A: BESS Components and Functions

Table 14. BESS components and their functions.

Component	Description	Function
Cell	Electrochemical cells, cathodes, and anodes	Primary electrochemical reaction
Module	Collection of cells	Combines cells to make a deployable unit within the battery at the right voltage
Pack	Collection of modules with fire suppression and BMS integrated	Modules, which connect to supply the kW needed for the pack
System	Integrated multiple packs for larger sites	Can contain BMS, EMS, PCS Transformers and Inverters – along with the packs, cells and modules – the system is the grid connected piece
PCS	Power control/conversion system	Used to connect the inverter and the BMS, often used in DC coupled systems to couple – also to help with charge and discharge regulation
Inverter	Power conversion and grid connection	Sometimes combined with PCS, converts DC to AC, to synchronize with the electric grid, can be grid forming, can control charge rates or switch
BMS	Battery management system	Connects cell measurements to control on state of charge and safety against overcharge, state of health and state of charge, along with environmental sensing. Can actuate the fire protection and other protection for the cells, primary purpose is safety controls.
EMS	Supervisory control	Overarching management of the system and combination of sensors and components. Above the PCS and Inverters – not always present
Transformer	Voltage step up or step down	Can be combined with the PCS and Inverter in various cases

Component	Description	Function
Fleet Controller	Controls multiple sites/systems	Overarching monitoring of all BESS in an owner's fleet or sphere of operations
Fire Suppression	Suppresses fire	Mechanical actuation of fire protection based on response from BMS and other sensing
Modem	A device that modulates and demodulates signals	Facilitates communication between a computer or digital device and an internet service provider, enabling internet connectivity
Cloud	Remote servers accessed over the internet	Provides scalable and flexible storage, computing resources, and services to users and organizations.
DERMS	Software platform for monitoring and controlling distributed energy resources	Optimizes the operation of resources like solar panels and energy storage systems to enhance grid stability and efficiency
DO/ADMS	Software platform for managing the distribution grid	Monitors, analyzes, and controls grid operations in real time, improving asset performance and grid reliability

Appendix B: Consequence Ranking and Scoring

Each consequence is weighted, and the impact is ranked and then scored using the CCE methodology. List of consequences include:

- Load Impact (0 to Bulk)
- Duration of Load Impact (0 to over 3 days)
- Safety Human (0 to death)
- Safety Fire/Discharge (0 to wildfire)
- System Cyber Integrity (0 to complete loss of trust)
- Cost (0 to bankruptcy)
- Environmental Damage
- Climate Change
- Single Site Does Not Perform/performs the opposite action
- Geographically/Grid Local/State Fleet Does Not perform
- Geographically dispersed

Table 15. Example of a consequence matrix.

Service	Timeframe	Normal	Strained	Emergency	Associated Inverter Capability
Arbitrage	Hours	x	—	—	Price signal response
Operating Resource (OR) - Primary frequency response	4+ Hrs	x	—	—	Price signal response
OR - regulation	seconds		x	x	Frequency and voltage droop control
OR - contingency spinning	15 min - 1 hr	—	x	—	Voltage and frequency reference
OR - replacement/supplemental	30 in to 2 hr	—	x	x	Virtual generator inertia
OR - ramping/load following	hrs	x	x	x	Utility support mode
T + D Deferral	30 mins to hrs	x	—	—	Utility support mode
Black Start	hrs	x	—	—	Real power vs. reactive power limiting

Exceptional Discharge	hours	—	—	x	Black start/grid forming
-----------------------	-------	---	---	---	--------------------------

Appendix C: Critical Component Prioritization

Using Table 16 shown below, the total score for each component has been calculated to determine its impact of misoperation and assign a priority to the consequence of the function marked in top row. This is then used to prioritize the most critical components for style of solutions that can be applied to secure them in both the short and long term. This is performed for a single site or BESS initially.

Table 16. Categorization of BESS components and their capabilities.

	Comms	Charge / Discharge Control	On / OFF	Gen – incremental	Equipment Safety	Life Safety	Cyber Access Potential to Impact Other Functions in BESS	Cyber Access Potential Mass Control/Orchestration
Device (Single Site)								
Battery modules, packs & cells			x			x		
Power conversion system/Inverters (PCS)	x	x	x	x	x		x	x
Inverter	x	x	x	x				x
Battery management systems (BMS)	x	x	x		x		x	x
Environmental control system (heating, ventilation and air-conditioning system)								
Fire suppression system or fire control system		x	x			x		
Transformer			x					

Human-machine interface (HMI)		X				X	X	
Electrical disconnects, circuit breakers, and switches (protection)		X	X		X	X	X	
Communications networking switches and cables.	X						X	
Modem	X						X	X
Site Controller (single site)/EMS			X	X	X			