Battery Energy Storage System (BESS) Supply Chain Analysis

The United States faces a significant challenge in keeping pace with the evolving and increasingly digitized grid. Batteries and their power electronic interfaces are essential for delivering resilient energy and providing critical support to the electric grid. Despite progress in relocating supply chains for raw materials from home or allied countries, the control and power electronic industry has lagged, in part due to lower profit margins and cost-based domestic supply chain incentives. Many U.S. companies rely on People's Republic of China (PRC)-sourced control equipment, raising geopolitical concerns. To support domestic industry growth and maintain economic benefits from federal investments, it is crucial to ensure a consistent demand for these components. Addressing the delicate balance between energy modernization and cybersecurity necessitates comprehensive policy, technical, and organizational approaches, with a thorough assessment of supply chain risks to identify and prioritize them effectively.

BESS Threats, Vulnerability, and Attack Exposure

Cyber threats to BESS encompass a range of actors, from nation-states to cybercriminals, targeting critical components throughout their lifecycle, including manufacturing, shipping, and operation. Vulnerabilities can arise at multiple levels, such as design, firmware, software, hardware, communications, and configuration, affecting key BESS components like battery modules, power conversion systems (PCS), inverters, and battery management systems (BMS). Common issues include weak passwords, hardcoded credentials, and unsecured communication pathways. Attack exposure is heightened by the need for remote management and the increasing number of stakeholders with access to these systems, potentially leading to cascading impacts on grid stability and energy supply reliability.

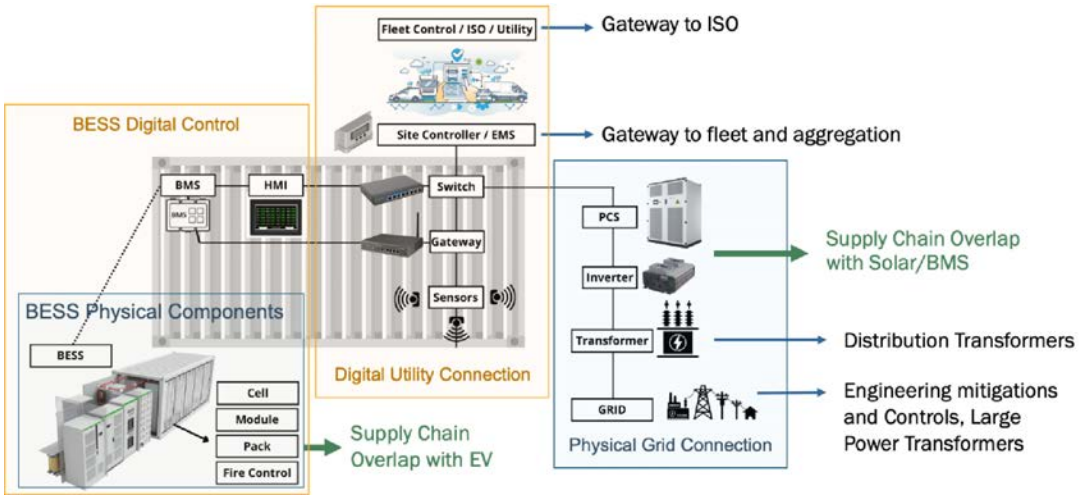

Figure 1. Supply chains for BESS are complex and interconnected with other key energy infrastructure.

For additional information, please visit or email:

inl.gov/national-security/csdet

csdet.ta@inl.gov

Idaho National Laboratory

Supply Chain Threat of Foreign Influence for Digital Energy Infrastructure

Supply chain risk management for BESS must consider the complex business models and policy landscape influencing the sector, particularly the significant presence of PRC-based companies. For example, 90% of inverters in the U.S. are made in or sourced from the PRC and nearly 70% of PCS in inverters on the California battery allow list are from China. The dominance of PRC manufacturers in the supply chain poses long-term operational risks due to potential adversarial influences. Intricate inter-organizational relationships within the BESS ecosystem, from manufacturing through integration, installation, and ongoing operations and maintenance, highlight the supply chain's vulnerability to exploitation should one of these stakeholders be compromised. The diverse roles and responsibilities within the BESS sector further complicate the risk landscape. Multiple entities maintain communications with the site, increasing the potential attack surface for external threat actors. Addressing these risks requires a multifaceted approach that includes robust access and security controls, comprehensive policy interventions, and the establishment of stringent standards and regulations to mitigate the influence of foreign entities and enhance the resilience of digital energy infrastructure.

Mitigation Planning and Relevant Initiatives

Mitigating supply chain risks for BESS encompasses several national strategies, policy and regulatory actions, and technical solutions. Many federal policies aim to incentivize domestic manufacturing and reduce reliance on foreign suppliers, but implementation challenges exist, especially concerning the enforcement of banned lists and effective management of procurement processes. The rip-and-replace strategy, although promising, is complex and costly, requiring significant investment and time.

Technical solutions focus on securing the supply chain through proactive measures, such as Cyber-Informed Engineering (CIE) and implementing secure-by-design practices. The Department of Energy (DOE) and national laboratories have initiated programs like Cyber Testing for Resilient Industrial Control Systems (CyTRICS) to identify vulnerabilities in digital components and implement security enhancements. Additionally, strategic component assessments prioritize critical components for security interventions, while long-term initiatives aim to relocate or build manufacturing capacity onshore or in allied nations to enhance cyber resilience.

Collaborative efforts among stakeholders are essential for addressing the complexities of the BESS supply chain. This includes developing robust contracting and procurement guidelines, ensuring compliance with standards and regulations, and fostering information sharing through advanced monitoring systems. By focusing on both immediate and long-term strategies, the goal is to secure the most consequential BESS functions while supporting the growth of domestic industry and enhancing the overall resilience of the U.S. energy supply chain.

BESS-related reports and resources: https://inl.gov/national-security/csdet/

Full report: https://www.energy.gov/sites/default/files/2025-01/BESSIE supply-chain-battery-report

This work is sponsored by the U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response (CESER), and Grid Deployment Office (GDO).

U.S. Department of ENERGY