Component Criticality in BESS for Cybersecurity

Battery energy storage systems (BESS), inverters, and associated digital equipment are integral pieces of interdependent energy delivery systems. When considering the supply chain security of such systems, there is often a misplaced focus on the origin of energy generation and storage materials like battery cells, overlooking the more significant cyber risks that stem from digital power electronics control systems. Part of this misplaced focus is due to the relative costs of these components, with more attention given to expensive raw materials rather than the impactful digital elements themselves.

The Idaho National Laboratory (INL) is addressing this gap in supply chain security through a systems-of-systems approach that considers the impact various components in digital energy systems can have should misoperation occur. Therefore, **INL assigns a cyber criticality score based on quantitative analysis, which enables informed prioritization of mitigations and allows operators to reduce risk** in light of the prevalence of a BESS and associated systems foreign supply chain.

Supply Chain Security Considerations

The global energy evolution has inadvertently woven the United States and its allies into a complex web of dependence on foreign entities for critical components like inverters and batteries. While this reliance on globalized expertise and economies of scale can offer cost-saving benefits and technological advancements, it also introduces a layer of cyber vulnerability. The potential for geopolitical tensions, supply chain disruptions, and intellectual property theft cast a shadow on the path of energy independence. Potential consequences include:

- **Hardware or software that could introduce backdoors or security flaws;**
- **Counterfeit and poor-quality components;**
- **Lack of transparency regarding software components and their origins that hinder vulnerability assessments;**
- **Weak vendor security practices, such as insufficient security measures at component manufacturers that increase susceptibility to cybersecurity attacks;**
- **Hard-coded passwords; and**
- **Persistent and unsanctioned communications.**

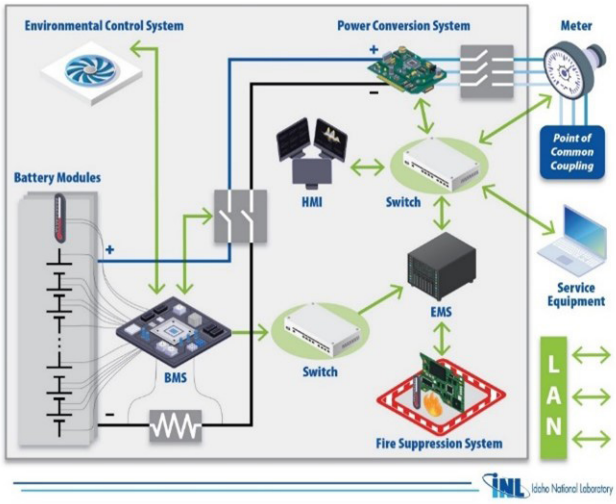

Figure 1. Key components and communications in a BESS deployment.

This reliance on foreign entities, particularly for high-consequence and critical infrastructure components, demands a careful balancing act: leveraging the strengths of foreign entities while mitigating the inherent risks through strategic diversification, robust cybersecurity measures, cyber-informed engineering, and fostering domestic innovation in key areas.

For additional information, please visit or email:

inl.gov/national-security/csdet

csdet.ta@inl.gov

Idaho National Laboratory

Defining Component Function and Consequence

INL has identified the **BESS critical enabling functions and the components** that contribute to these functions throughout the supply chain. Several components may have a role in enabling a function, and each component may play a role in several functions, making them interdependent. For example, the Battery Management System (BMS) controls the current, voltage, and state of charge, monitors the level of charge in the battery modules and optimizes usage to prevent overcharging or discharging, and performs temperature monitoring.

After identifying what each component supports, the INL approach is used to define and evaluate the worst-case scenario for BESS installations in various modes of operation. This requires awareness of the critical functions, the system-of-systems dependencies, and the undesired consequences that must be prevented. These possible repercussions include safety, local grid impact, local equipment damage, bulk grid impact, bulk grid damage, reputation, and community impact.

Another essential nuance in analyzing risk and component failure impact is the use of ownership. There's a notable move towards direct ownership of BESS components. These companies are transitioning from merely supplying battery cells to offering integrated energy systems with advanced features. Therefore, it is common to have multiple organizations maintain communications with the BESS site, creating attack exposure where these entities could be used as a point of entry to connect to the BESS. Additionally, this gateway could make the companies a secondary target as adversaries use BESS communications architecture to penetrate new networks.

The rapid interconnectivity and need for cost reduction remain dominant goals in BESS deployment. While these objectives are crucial for scalability and economic viability, there is a risk of overlooking cybersecurity concerns in favor of achieving efficiency targets. Some entities are employing inventive interconnecting methods to avoid cumbersome generator registration processes.

A full breakdown of the consequence and operations analysis and the criteria by which the consequence is assessed against, can be found in the whitepaper, "Application of Cyber Informed Engineering for Protecting BESS."

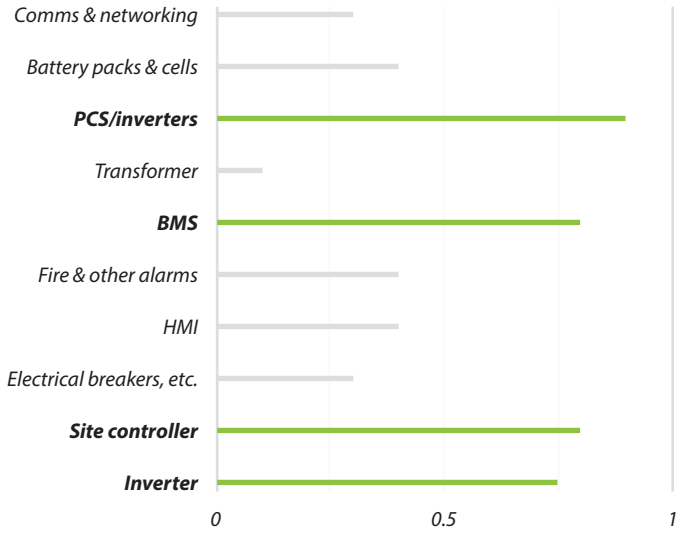

Figure 2. Prioritization of BESS components based on function criticality

Criticality Scoring of BESS Components

INL calculated a total score for each BESS component in relation to its misoperation impact across cyber and physical domains and assigned each component a **functionality consequence priority level.** This score can be used to prioritize the most critical components to streamline solutions for securing systems in the short- and long- term.

Using this approach, INL concludes that Power Conversion System (PCS), BMS, and inverters should be prioritized at the BESS level, and site controllers should be prioritized at the fleet level. This is because the PCS 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, through the nature of its functionality to decide when to charge and discharge, must communicate with higher-level systems. As a result, the combined exposure and criticality of the device leads to its high criticality score.

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