Battery Management System Security in Grid Energy Storage

June 17, 2024

Introduction

Over the last several years concerns have been expressed by both industry and U.S. lawmakers about the potential risks in using utility grid equipment manufactured in nations which are not strategic allies. In May 2020, a presidential Executive Order was issued restricting utilities from buying power grid equipment from "foreign adversaries."[i] Due to a lack of clarity (no specific nations or equipment were identified), while the Order did raise concerns within the power generation industry it did not result in a concrete response. That order was set aside by the following administration, but the scrutiny it spurred into the issue of the security of US electricity grids has continued. In March 2023, Duke Energy decommissioned an energy storage system (ESS) provided by China-based CATL (Contemporary Amperex Technology Co Ltd) in response to pressure from the US Senate Select Committee.[ii] No specific written guidance or regulation precipitated this, and that energy storage system had been installed at a military base as opposed to at a public utility, but electricity providers and battery energy storage suppliers are nevertheless taking notice.

Any battery energy storage system, whether it is designed and manufactured within the United States or in a country of concern to US legislators, contains components sourced from around the world – there is no way to avoid this. For example, Nuvation Energy provides battery management systems that are designed and manufactured in the US and Canada. All our software is developed in-house, and our manufacturing is performed within Canada and the US by Canadian and US manufacturers. We are nevertheless as subject to global supply chain realities as any other technology company, which means that components used in our products, including those sourced from US companies, are not all produced in the United States.

Given the realities of global supply chains in energy storage system production, how does an energy storage company provide solutions that address the concerns of industry and legislators? Would "domestic" sourcing of an ESS fully resolve security risk concerns? What meaning can we assign to the term "domestic" considering the globally integrated supply chain used to develop the ESS? How does one determine what is and what is not a "security risk?"

The Battery Energy Storage Supply Chain

In November of 2023 Senate Intelligence Committee members asserted that the United States was over a decade behind China in the commercialization of battery technology.[iii] The Inflation Reduction Act passed in August of 2022 is spurring in the US what is essentially a catch-up technology race against industry-leading countries in Asia in the fields of battery production.[iv] Leading battery manufacturers from several of those nations are now building battery plants in the US, and US companies are developing new battery technologies and ramping them up to volume production. The transition from battery cell prototype to volume production however is expensive, time consuming, and not always successful. It is likely to take multiple years for American battery companies to catch up to their Asian counterparts.

Battery energy storage systems need to be competitive on price, measured in $/kWh (dollars per kilowatt-hour), and batteries manufactured in Asia still lead in the current price race to the bottom. While US manufacturers are continuously optimizing their processes to reduce cost, the world's leading battery manufacturers are also doing the same, delivering ever-higher energy densities at ever-lower prices.

While batteries are the bulk of the cost of an energy storage system, there are significant additional cost drivers. Other major parts include thermal management, steel containers, climate controls, cabling, power conversion systems and energy management controllers.

Of the items listed above, the key distinction to be made regarding security is one of passive components versus control systems. Battery cells are passive components; while they inherently have safety issues due the innate volatility of chemical energy storage (e.g. fire, off-gassing), it is far more difficult to tamper with a battery cell than with a control device. Other passive components such as cables, racking, metalwork, and fuses for example, are also unlikely to provide security vulnerabilities to a bad actor.

The Battery Management System (BMS)

The BMS is a battery cell data collection and management device that connects directly to battery cells. It is a computing device that includes multiple ICs (integrated circuits / semiconductors) and sophisticated software algorithms that ensure batteries are being charged and discharged by the PCS (Power Conversion System) in a safe and performant manner. The operational safety profile of the specific cells being managed (i.e. min/max voltage, temperature, etc.) are stored as configuration values in the BMS.

An intelligent BMS will dynamically change performance threshold data provided to the PCS in response to changing voltage and temperature in the cells. For example, if cells begin to surpass their optimal temperature range, the intelligent BMS will reduce the current threshold setting and the PCS can respond by reducing the level of current being applied to the cells. The interaction between the control systems will typically result in a drop in cell temperature and restore the batteries to a safe state. If the cells do not respond to initial corrective actions, the BMS will initiate additional protection measures. If problems escalate beyond safe thresholds despite these actions, the BMS will open contactors to disconnect the batteries.

Various computing devices, both local and remote, can potentially access the BMS as part of their routine operation. For example, an energy management system can access the BMS to make operational decisions based on State of Charge. The PCS uses data pulled from the BMS to manage the charging and discharging of the ESS. A system operator can log into the BMS from a remote location to view the condition of the batteries and assess maintenance requirements.

Any energy storage installation can have network security such as firewalls and other forms of protection. A utility grid may even operate on a private network that is separate from the Internet. But security risks do exist and can include:

1. Compromising features designed into the BMS. A network firewall is designed to prevent a bad actor from “getting in” to the ESS, but the BMS, as with any computing device, could potentially have hidden features added with the intention of compromising the system from the inside (e.g. a ‘backdoor’ that allows remote access).
2. Counterfeit or tampered-with BMS component. A bad actor might physically replace a BMS component with a counterfeit or tampered part.
3. Cybersecurity / hacking. This risk occurs if the cybersecurity protocols of the energy storage system have failed and a bad actor has “gotten in,” which would expose the BMS (along with other control systems) as a potential target.

Assessing the risks of counterfeiting, tampering, and compromising features involve determining that something has not been done to the BMS before it has been installed in the ESS. Cybersecurity or hacking vulnerability assessments on the other hand involve evaluating what has been done to harden the BMS against intrusion.

Avoiding a BMS with Hidden Compromising Features

The easiest way to avoid purchasing a battery management system that has hidden compromising features designed in is to deal with a trusted BMS supplier. What is a “trusted BMS supplier?” First, we must recognize that this emerging security concern is being driven mostly by government agencies, and that their current criteria revolve more around the country of origin than of protecting the BMS against intrusion. Nuvation Energy battery management systems address country of origin concerns as follows:

- Nuvation Energy is wholly North American owned and managed, with facilities in Canada and the United States. All our software development and product design are performed within Canada and the United States.
- Our products are manufactured at trusted facilities in North America and under the supervision of Nuvation Energy personnel.
- Manufacturing data is securely transferred and stored on servers hosted in the US.

Avoiding Counterfeit or Tampered BMS Components

Since a battery management system within an ESS is modular, (i.e. it consists of many separate pieces of hardware that are connected to each other), one counterfeit component could conceivably be substituted by a bad actor to compromise the BMS. Alternately, a BMS module could conceivably be tampered with during or after the manufacturing process. Nuvation Energy has taken the following steps to prevent counterfeiting and tampering:

- Cloud-based manufacturing and test management systems (MTMS) verify the authenticity of components being integrated during manufacturing.
- Tamper protection and continuous authenticity checks of our hardware and software ensures changes cannot be made after manufacturing and/or commissioning of systems with the relevant (UL) certifications.

Avoiding Cybersecurity / Hacking

To reduce the risk of intrusion by bad actors after the BMS has been installed in an energy storage system, Nuvation includes the following security measures into our battery management systems:

- Nuvation Energy has taken steps to harden our Multi-Stack Controller and nController EMS (energy management system) against intrusion. Our internet-connected products employ security protocols for secure and authenticated communication and data transfer.
- BMS firmware updates are encrypted and digitally signed to ensure that only updates developed by Nuvation Energy are accepted by the BMS hardware.
- Disk encryption and hardware security features are included on Nuvation Energy's Multi-Stack Controller (which aggregates battery stacks in parallel), and nController EMS (energy management system) to protect the hardware from physical tampering and intrusion.

The Role of Collaboration

The current state of cybersecurity in the energy storage industry is reminiscent of that of functional safety ten years ago; industry and regulators worked together until UL 1973 (battery stacks), UL 9540 (energy storage systems), and UL 1741 (PCS) became the most widely recognized functional safety standards for battery energy storage in North America. Shortly afterwards, Nuvation Energy's BMS became the first battery management system in the world to become UL 1973 Recognized. Today we are collaborating with industry regarding what approaches or standards will become as widely accepted for cybersecurity as UL 1973 has for functional safety.

Regardless of all the technical solutions one can add to an energy storage controller for security, the most important one is transparency. This is why we work collaboratively with system integrators to ensure seamless integration of our battery management products into their energy storage solutions and cybersecurity strategies.

References

[i] May 1, 2020. *"Executive Order on Securing the United States Bulk Power System."* Retrieved 2024-04-26 from https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/

[ii] February 9, 2024, Michael Martina. *"Duke Energy to remove Chinese battery giant CATL from Marine Corps Base."* Reuters. Retrieved 2024-04-26 from https://www.reuters.com/business/energy/duke-energy-remove-chinese-battery-giant-catl-marine-corps-base-2024-02-09/

[iii] November 6, 2023, David Shephardson, *"Senators urge US to take steps to boost battery production, citing China."* Reuters. Retrieved 2024-04-30 from https://www.reuters.com/technology/senators-urge-us-take-steps-boost-battery-production-citing-china-2023-11-06/

[iv] August 16, 2023, Rebecca Bellan, *"Tracking the EV battery factory construction boom across North America."* TechCrunch, Retrieved 2024-04-30 from https://techcrunch.com/2023/08/16/tracking-the-ev-battery-factory-construction-boom-across-north-america/