Zero Trust OT Cybersecurity Protection for Battery Energy Storage Systems

In May 2025, the revised NERC CIP framework requires that lower capacity BESS systems rated at 20 MVa or greater with a connection at 60 kV or higher be subject to NERC CIP. These newly regulated assets must demonstrate compliance by May 2026 or face fines of up to $1M per day for non-compliance. BlastWave's approach to delivering NERC CIP security solutions for the BESS market focuses on operational simplicity for critical infrastructure at scale.

BlastWave protects Battery Energy Storage Systems (BESS) with a unique overlay Zero Trust Protection architecture. It supports key foundational security requirements with less operational complexity and lower TCO than traditional OT security offerings. BlastWave's solution addresses key NERC CIP requirements faster and more economically than conventional "bolt-on" OT security solutions.

BlastWave's solution supports :
Secure Remote Access: Passwordless remote access is phishing-resistant and removes credential theft as a risk factor.

Network Segmentation: Software-defined segmentation allows BESS networks to be segmented by risk factors and ensures least privilege access to each segment.

Network Cloaking: Create a secure overlay to protect legacy systems from vulnerabilities, shield them between patch windows, and limit downtime by creating segmentation for BESS systems.

BlastShield solutions require only 10% of the installation time, need 50% less maintenance, and cost 25% of traditional OT security solutions. BlastWave's solutions are optimized for OT and built with Secure-By-Design principles from Day 1. These comprehensive protection solutions deliver:

Enhanced Operational Uptime: Reduces downtime associated with patching vulnerable operational systems with network cloaking

Enhanced Resilience: BESS networks and systems are undiscoverable to hackers, preventing targeted cyberattacks and cloaking Zero Day vulnerabilities.

Enabling secure BESS operations: With geographically dispersed assets and greater reliance on remote maintenance, BlastWave prevents unauthorized access or manipulation of BESS systems.

Lowered Operational Costs: Existing staff can install and maintain systems without adding costly OT cybersecurity hires.

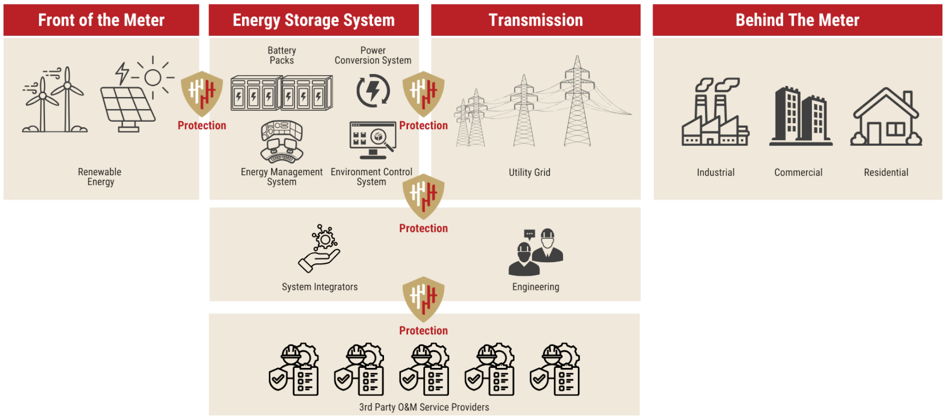
BlastShield

Increase Uptime by eliminating cybersecurity risks before they can gain a foothold in your network.

Improve Safety by ensuring that all connectivity to the BESS systems is secure and encrypted, preventing the modification of sensor data in flight.

Lower Costs by not requiring expensive IT personnel or platforms and simplifying the installation, operation, and management of OT cybersecurity solutions

Figure 1 BlastWave in Battery Energy Storage Networks



BlastShield™: Zero Trust OT Protection for Battery Energy Storage Systems

BlastWave in Battery Energy Storage Networks

Supports key NERC CIP security requirements with minimal impact or downtime to existing operations.

Extending patch cycles while mitigating security controls increases uptime. Securing and encrypting all BESS system connectivity improves resilience, preventing sensor data modification in transit.

Lower Total cost of ownership with decreased capital expense, lower maintenance labor due to decreased complexity of maintaining multiple OT security integrations, and reduced requirements for specialized OT security expertise to own and operate.

BlastWave Use Cases for Battery Energy Storage Systems (BESS):

Securing Battery Management Systems (BMS)

- Protect BMS from unauthorized access and manipulation.
- Ensure secure remote monitoring and control of battery health and performance.

Protecting Inverter Control Systems

- Secure inverter control systems from cyberattacks.
- Ensure secure communication between inverters and grid control systems.

Securing Grid Integration Systems

- Protect communication and control systems integrating BESS with the power grid.
- Mitigate the risk of unauthorized manipulation to grid frequency and voltage.

Securing Remote Monitoring and Control

- Enable secure remote access for maintenance personnel and operators.
- Limit access to necessary systems and data, enforcing least privilege.

Protecting Data Acquisition Systems

- Safeguard sensor data (e.g., temperature, voltage, current).
- Ensure secure data transmission to control centers and analytics platforms.

Protection Against AI-Powered Reconnaissance

- Hide critical network assets from AI reconnaissance tools.

Phishing Protection

- Use passwordless MFA to prevent phishing attacks on employees and contractors.

Segmentation and Microsegmentation

- Limit cyberattack blast radius through network segmentation.

Zero Trust Architecture

- Implement Zero Trust to protect the entire network with minimal impact on existing operations.

Protecting Legacy Systems

- Provides mitigating controls for end-of-life systems that can no longer be patched.

Securing DER Communication

- Protect communication between BESS and other distributed energy resources (DERs).

Protecting Frequency Regulation Market Participants

- Protect systems that control BESS and bid devices into frequency regulation markets.

BlastShield Deployment Benefits:

- Helps energy networks achieve regulatory compliance.
- Simple migration – no changes to existing IT/OT architecture.
- Faster installation and administration vs. traditional solutions.
- Consumer-grade UX: simple biometric authentication, access only to required devices.

BlastShield's Unique Features:

- Reconnaissance-proof Network Cloaking
- Phishing-Resistant Secure Remote Access
- Software Defined Segmentation

These features help BESS systems comply with NERC CIP requirements effectively.

v20250408

Front Cover banner image © Sig. Chiocciola. Creative Commons

About BlastWave

BlastWave securely connects Industrial Control Systems, Operational Technology, and Critical Infrastructure networks with Zero Trust Protection and delivers industrial-grade cybersecurity with consumer-grade ease-of-use. Visit **www.blastwave.com** to learn more.

BlastWave

1045 Hutchinson Ave.
Palo Alto, CA 94301 USA
T: +1 650 206 8499