Securing Energy Storage for a Resilient Future:

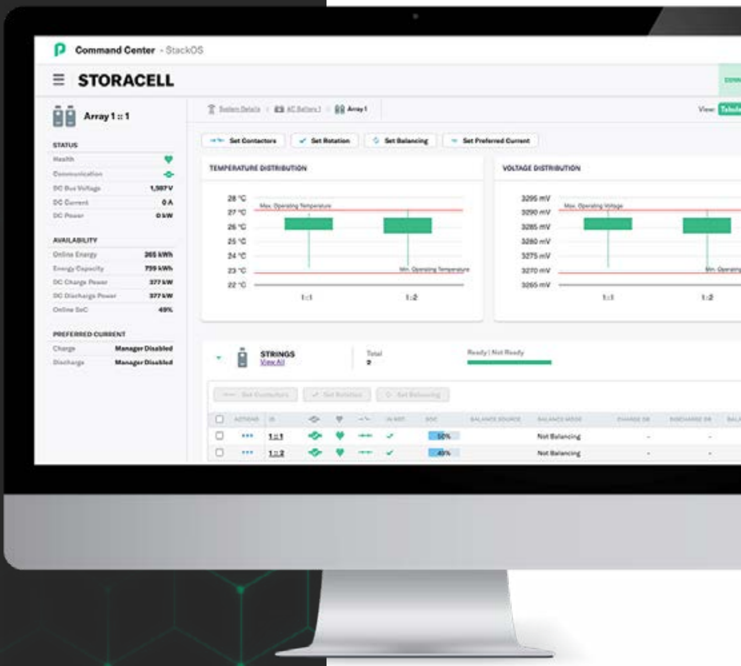
POWIN'S CYBERSECURITY SOLUTIONS

Generating clean, carbon-neutral energy is among mankind's greatest achievements. As the demand for it grows, so do the complexities of increased distribution and interconnectivity within the bulk electric system. This can open asset operators to threats from malicious entities looking to thwart safety protocols and destabilize grid operations, the results of which can be devastating: Widespread outages, massive financial losses, and damage to public safety to name just a few.

A Commitment to Cybersecurity

At Powin, cybersecurity is of the utmost importance and is our number one defense against potential attacks to our Battery Energy Storage Systems (BESS). Like cyber-attacks themselves, our approach to cybersecurity is constantly evolving and helps ensure that our BESS continue to deliver secure, resilient, and compliant energy storage solutions.

The safe and secure operation of the bulk electric system is a cornerstone of national security policies, and the growing deployment of Powin systems mean our cybersecurity efforts have a material impact. To help ensure our hardware systems cannot be compromised by bad actors, Powin's Enterprise Cybersecurity Program exists to fortify and standardize our approach to cybersecurity.



Array 1 :: 1

STATUS

Health	♥
Communication	
DC Bus Voltage	1,387V
DC Current	0 A
DC Power	0 kW

AVAILABILITY

Online Energy	365 kWh
Energy Capacity	739 kWh
DC Charge Power	377 kW
DC Discharge Power	377 kW
Online SoC	49%

PREFERRED CURRENT

Charge	Manager Disabled
Discharge	Manager Disabled

STRINGS View All

Total 2

□	ACTIONS	ID				IN ROT.	SOC	BALANCE SOURCE	BALANCE MODE	CHARGE DR	DISCHARGE DR
□	•••	1::1		♥		✓	50%		Not Balancing	-	-
□	•••	1::2		♥		✓	49%		Not Balancing	-	-

A COMPREHENSIVE APPROACH WITH **IT AND OT CONVERGENCE**

Our thoughtful approach to OT infrastructure ensures safe, secure BESS operation throughout the lifespan of the system. Through implementation of secure industrial control systems (ICS), strategic network segmentation, and 24/7 real-time monitoring, we safeguard our energy storage systems from intruders.

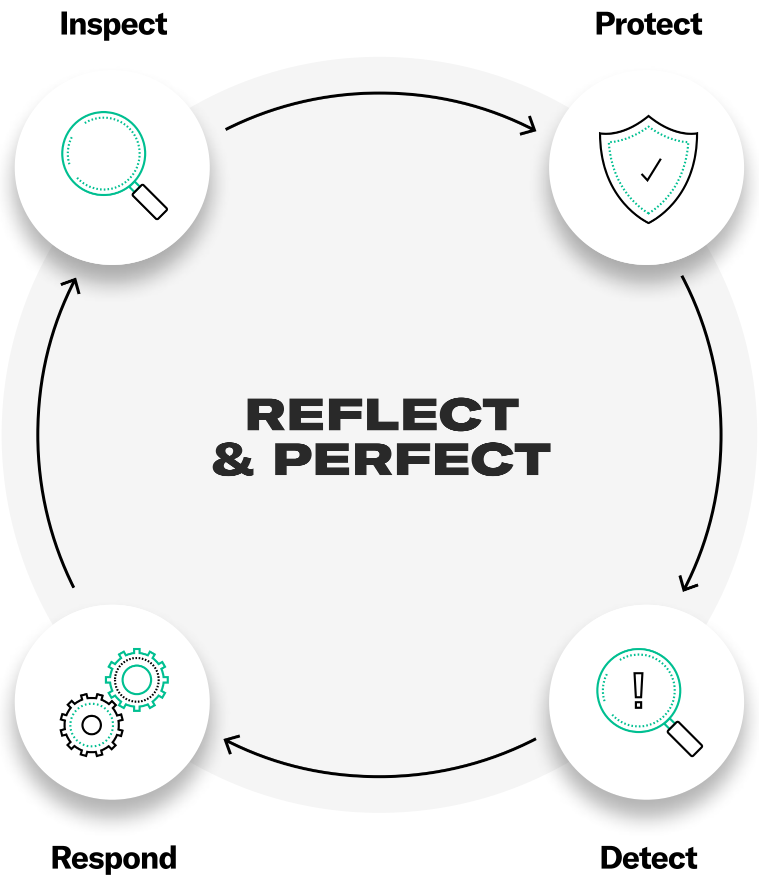
Our IT security measures complement this by protecting customer data through encryption, access controls, and adherence to industry-standard cybersecurity frameworks. By eliminating silos and merging IT and OT cybersecurity efforts, we enhance the overall security of both data and physical systems, ensuring operational integrity, reliability, and protection against cyber threats. While others may not invest at this level, we see it as fundamental to maintaining a secure and resilient environment.

By converging IT and OT, we streamline operations, reduce redundancies, and enhance real-time decision-making. This unified approach provides end-to-end visibility, enabling faster responses to potential threats, improved system reliability, and optimized asset performance. Integrating secure IT and OT frameworks not only strengthens our cybersecurity, it also simplifies the management of our energy storage systems, allowing us to scale operations without compromising safety or efficiency. This convergence drives operational efficiency by ensuring smoother workflows, reducing downtime, and creating a scalable foundation for future growth.

There is no Finish Line in Cybersecurity

INSPECT. PROTECT. DETECT. RESPOND.

Cyber criminals continue to learn and evolve which means we must do the same in our defenses against them. We are continually auditing and improving our cybersecurity posture. This perpetual loop of continuous improvement helps ensure customer BESS and data are always in their control.



INSPECT

Vigilant Auditing and Compliance

At Powin, cybersecurity is woven into every layer of our operations, driven by a proactive and holistic approach to safeguarding our systems. We conduct thorough **gap and vulnerability analyses** to identify potential weaknesses and ensure they are addressed before they can become threats. Regular **third-party audits** provide an external perspective, keeping us accountable and ensuring our defenses are always up to date.

Our approach includes **software threat modeling** using the **STRIDE framework**, which helps us assess risks and develop effective mitigation strategies. We conduct real-world simulations including cloud failure infrastructure remediation and ongoing **penetration testing**. We continually push the limits of our defenses to ensure they can withstand any attack.

But our commitment doesn't stop at testing and evaluation. We are dedicated to **constant self-reflection and improvement**, regularly refining our security practices, adopting **new tools** and **standards**, and evolving our approach to align with emerging threats and regulations. Cybersecurity at Powin is a continuous, organization-wide effort that adapts and strengthens in response to the dynamic landscape of cyber risks.

PROTECT

Grid Stability & Resiliency at Powin

In order to combat these threats, we employ a multi-layered approach to protecting system security from cyberattacks that is unmatched in the industry. It all begins with our fundamentally sound building blocks:

Proprietary firmware, Battery Management System (BMS), and Energy Management System (EMS)

Each of these systems is developed and tested in the U.S. with no third-party sourcing our outside involvement. The control starts and stops with Powin.

Our proprietary, patented firmware, BMS, and EMS controls comply with robust localized cybersecurity standards and regulations, emphasizing data privacy and system integrity. This helps guarantee the security of our customers' data and that their system is operated in a safe, secure manner.

Connection system with built-in redundancy

In the event that network connectivity is lost, each Powin BESS enclosure is designed to operate independent of the larger system. This helps guarantee safe, uninterrupted operation while isolated and avoid costly downtime.

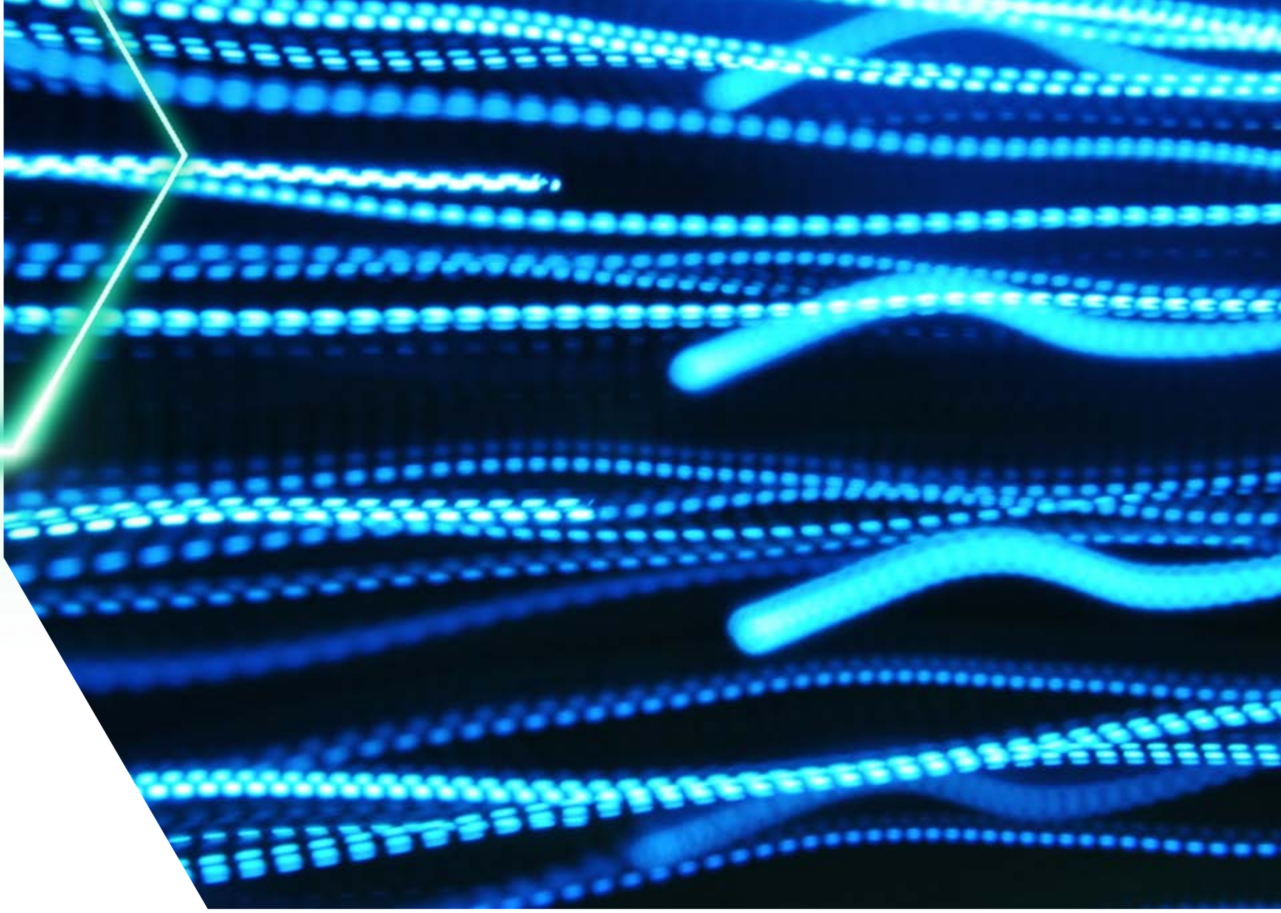
The Purdue model for Industrial Control Systems (ICS)

Powin follows the tried-and-true Purdue model in all of our BESS systems. This industry-standard model, developed by the Purdue Laboratory for Applied Industrial Control (PLAIC) of Purdue University, provides a conceptual framework for the hierarchy of system components. We employ this approach to micro-segmentation which defines and separates ICS architecture into two zones, IT and OT, then further separates OT into six zones. This micro-segmentation between layers creates "air gaps" and is one of many ways we embody Zero-Trust Architecture in our IT/OT systems.

BESS Control Security

Powin StackOS Gatekeeper screens and blocks unauthorized commands far before they reach critical components, ensuring BESS systems are exclusively in customer control. Each instance of Gatekeeper is custom-tailored to the customer's security needs to ensure the system is always operated safely, securely, and predictably.

Designed for flexibility, the system integrates seamlessly with customers' IT and OT infrastructures. Gatekeeper is supported by comprehensive documentation of possible software commands and their expected outcomes, giving customers the ability to build their own OT defense layer to further reinforce the inherent security of Powin's platform. This adaptability has been proven in over 6 GWh of deployments across utility, developer, and IPP customers, offering tailored protection and reducing the risk of malicious tampering by bad actors.



Secure Controls

Powin ensures that the source of remote controls and the control signals themselves are protected from bad actors. All control signals are protected through robust encryption whether they're in transit or at rest. All control systems employ no-trust fundamentals, leveraging multi-factor authentication and application-specific user roles preventing unauthorized access.

Customer Data and Data Security

Protecting our customers' personal and operational information is paramount at Powin. Part of our commitment to that is following widely known regulations such as NERC-CIP, AESCSF, and NIS2, local compliance regulations, as well as helping our customers be part of the security solution.

We apply robust encryption both in transit and at rest to help protect privacy, limiting access through role-based controls and ensuring compliance with data protection standards. Powin uses these methods to secure all customer data, maintaining its confidentiality and protection from unauthorized access or breaches.

Internally at Powin, we remain vigilant. Examples of this include security events such as randomized phishing tests, ongoing employee training, and ensuring the security of mobile devices that contain Powin data.

Physical Security Integration

To help prevent sabotage or unauthorized control by bad actors, our energy storage systems include 24/7 monitoring and access logging, multi-tiered system access controls, and tamper-proof enclosures. Security measures such as these are essential to protecting your critical assets. They are like safety belts and air bags in a vehicle. You hope you never need them, but you wouldn't go anywhere without them.

Supplier Vetting: Ensuring Security and Integrity in the Supply Chain

While we employ a supplier-agnostic approach to offer greater flexibility, higher quality, and better pricing, we maintain strict standards for every supplier we work with. Each one is subject to a rigorous vetting process to ensure compliance with high ethical and cybersecurity standards. We source components only from top-tier, trusted, secure manufacturers, maintaining complete transparency and control over the supply chain to prevent vulnerabilities.

DETECT

Identifying threats in real-time

At Powin, our approach to cybersecurity includes continuous **real-time threat detection** to identify and neutralize vulnerabilities before they escalate. We utilize **advanced event logging** to monitor system activity, capturing detailed data on operations and interactions. This allows us to detect suspicious behavior, unauthorized access attempts, and system anomalies in real-time, providing us with the ability to take swift corrective action.

Our systems also employ **automated alerts and responses** to handle compromised or offline systems, ensuring seamless **failover and recovery**. In the event of a system failure or cyber threat, automated alerts trigger immediate responses to restore functionality and mitigate risks. This proactive approach minimizes downtime and keeps our systems running smoothly, even under adverse conditions.

In addition to real-time monitoring, Powin performs **codebase vulnerability scanning and correction** to protect against emergent malware and exploits. These scans ensure that any vulnerabilities in the code are promptly identified and addressed, helping to safeguard our systems from both known and unknown cyber threats. This layer of protection is critical for defending against sophisticated malware and ensuring the ongoing security of our infrastructure.

By blending these advanced detection strategies with automated failover systems and real-time vulnerability scanning, Powin ensures that our BESS remain secure, reliable, and resilient against both internal and external threats. With 24/7 visibility, our cybersecurity defenses are always ready to detect, respond, and recover.

RESPOND

Prepared for the Unexpected

Times of emergency are no time to panic. We continually prepare for and respond to emerging threats, systems vulnerabilities, and even acts of nature. Keeping physical locations safe, protecting customer data, minimizing downtime, and restoring systems to normal requires prescient planning.

Our **cloud services** are engineered for rapid recovery, ensuring our control center's remote monitoring and control systems can be restored quickly in the event of an incident affecting cloud infrastructure. Even when services are disrupted, our BESS remain fully operational and responsive to grid operator dispatch. With restoration of cloud services and data warehousing in 24 hours or less, we minimize downtime to help ensure continuous, reliable performance for our customers.

Additionally, **localized controls** provide redundancy by enabling systems to operate independently if external networks fail. This helps ensure continuous operation, even in isolated mode, preventing costly disruptions to energy storage functions.

Powin's real-time incident response protocols, supported by continuous monitoring by dedicated teams and **incident management tools**, enable us to swiftly identify, contain, and eliminate threats. Additionally, we provide customers with a documented incident response plan that clearly defines key roles and responsibilities, ensuring a coordinated and effective response in the event of any incident.

REFLECT & PERFECT

Continuous Improvement for Future-Ready Security

Being cybersecure is a journey, not a destination, and at Powin, we are committed to **continuous improvement** to stay ahead of evolving threats. We are perpetually **evaluating new tools and standards** and testing the security of our systems so that they are prepared to combat all outside threats. We actively test our defenses through emergency **simulations** and **penetration testing**, identifying/remedying potential vulnerabilities and strengthening our response strategies.

By embracing a culture of continuous improvement, Powin not only keeps its BESS secure today, we also help ensure they are prepared for the cybersecurity challenges of tomorrow.

COMPLIANCE WITH INDUSTRY STANDARDS

Powin's commitment to robust cybersecurity is demonstrated by our adherence to the most respected industry standards and frameworks. By aligning with NERC CIP, SOC2, NIST800, and ISO27001, we further demonstrate that our systems are secure, resilient, and capable of mitigating both current and emerging threats.

NERC CIP

The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards focus on securing critical infrastructure by enforcing strict controls over operational technology (OT). Powin complies with NERC CIP to protect the reliability of energy systems, ensuring robust access controls, real-time monitoring, and effective incident response protocols.

NIST-800

The National Institute of Standards and Technology (NIST-800) framework provides comprehensive guidelines for managing cybersecurity risks. It focuses on areas such as identity management, continuous monitoring, and incident response, helping Powin ensure its systems are resilient and adaptable to emerging threats.

SOC2

Service Organization Control 2 (SOC2) is a framework designed to secure customer data by evaluating the effectiveness of controls in five key areas: security, availability, processing integrity, confidentiality, and privacy. SOC2 is essential for ensuring that Powin's systems safeguard sensitive information and meet industry expectations for data protection.

ISO27001

ISO/IEC 27001 is an internationally recognized standard for information security management. It sets the requirements for establishing, implementing, maintaining, and continuously improving an organization's information security management system (ISMS). Powin is currently in the process of achieving compliance with ISO27001.

Compliance Matrix

KEY INDUSTRY STANDARDS AND POWIN'S APPROACH

Below is a summary of how these standards overlap across key cybersecurity topics and how Powin emphasizes cybersecurity in all aspects of our products and larger organization.

CORE SECURITY REQUIREMENT	SUMMARY	POWIN
Electronic and Physical Access Control	Control and monitor access to digital systems and physical infrastructure to prevent unauthorized entry.	• Leverages Zero Trust Architecture through items like: Least Privilege Access and Strong Identity Management (MFA, identify management) • 24/7 surveillance and facility access management (performed through Powin Remote Operations Center)
Network Security	Protect IT and OT systems by securing networks and controlling access to them.	• ICS micro-segmentation • Third party audits • Constant automated system scanning for vulnerabilities • Purdue model, the industry standard that separates ICS architecture into two zone, creating "air gaps" for safe collaboration
Risk Management	Identify, assess, and mitigate cybersecurity risks across IT/OT environments.	• StackOS Gatekeeper provides customer safeguards, preventing any bad actor from controlling system through the internet • All Powin software/firmware engineered, designed, and managed in the US • Regular penetration testing by internal and external CISSP/eCPPT certified professionals • Perpetual scanning of all Powin-created software to identify emerging and existing exploits
Incident Response and Recovery	Detect, respond to, and recover from cybersecurity incidents to minimize or eliminate disruption.	• Incident response plans tailored to customer needs • Routine exercises simulating security and major infrastructure emergencies
Data Protection	Prevent unauthorized access to all IT/OT data.	• Industry-standard encryption of all data both in transit and at rest • GDPR, UKGDPR, APP, CCPA compliant data management program
Asset and Change Management	Tracks and manages hardware and software assets, ensuring they are updated and protected. Controls and documents changes to systems, ensuring they are tested and authorized to prevent disruptions.	• StackOS Patch Management organization works with customers to safely update systems to minimize disruption • All patches automatically verified for malware and exploits • Comprehensive inventory and firmware management program of networked devices (switches/routers etc.)

By viewing cybersecurity through the lens of proven frameworks, we prove our commitment to ensuring that systems meet customer requirements and demonstrate our willingness to go above and beyond. We continuously refine our processes through regular audits, vulnerability assessments, and the adoption of new technologies, making sure our cybersecurity posture remains strong in the face of emerging threats. This proactive approach allows us to deliver secure, reliable energy storage solutions to our customers, safeguarding both their operations and their data.

UNRELENTING **CYBERSECURITY**

The need for vigilance in cybersecurity is abundantly clear, as evidenced by the constant barrage of new threats adding to those that are already out there. As our security measures grow more sophisticated, so too, do the attacks themselves, which is why we are committed to continual investment, assessment, and innovative solutions to protect our customers' data.

There are far too many examples of inadequate cybersecurity out there for us to ever let our guard down, particularly in the energy storage industry where safety and financial risks are so high. It is an ongoing endeavor, one in which we claim to be future ready, never future proof.

POWIN

For additional information about our Enterprise Cybersecurity Program, as well as sales and partnership inquiries, please reach out at **www.powin.com**