



CYBERSECURITY IN BATTERY ENERGY STORAGE SYSTEMS:

A Strategic Imperative for Resilient Energy Infrastructure

With the rapid growth of digitalization and the increasing interconnectedness of energy systems, cyber security has become one of the most critical challenges facing modern infrastructure. Battery Energy Storage Systems (BESS), as key enablers of the energy transition, are increasingly exposed to these risks.

Across the European Union (EU), energy assets are classified as critical infrastructure – the NIS2 Directive reinforces this by designating energy providers as essential entities, requiring robust cyber security risk management and incident response capabilities. National regulations are further strengthening these requirements, with countries such as Lithuania and Latvia, for example, introducing additional controls on system access and security.

At the same time, the adoption of smart grids, connected devices, and remote operation continues to expand the attack surface. As a result, cyber security is no longer a purely technical concern – it directly impacts system availability, operational control, asset lifetime, and long-term investment value.

Why cyber security matters in BESS

Since battery energy storage systems bring together multiple interconnected components – including battery management systems (BMS), energy management systems (EMS), and grid connection interfaces – both operational capability and system complexity increase significantly.

Connectivity and remote access are essential for efficient operation, but they also introduce additional security exposure if they are not properly controlled and secured. In multi-vendor environments, the interaction between components must be carefully managed to avoid vulnerabilities.

Supply chain considerations add another dimension: the origin of components, system architecture, and data handling practices can influence not only technical performance, but also regulatory compliance and geopolitical risk.

Cyber security in BESS therefore goes beyond data protection – it is about maintaining operational control, ensuring availability, and safeguarding the integrity and secure operation of the entire system.

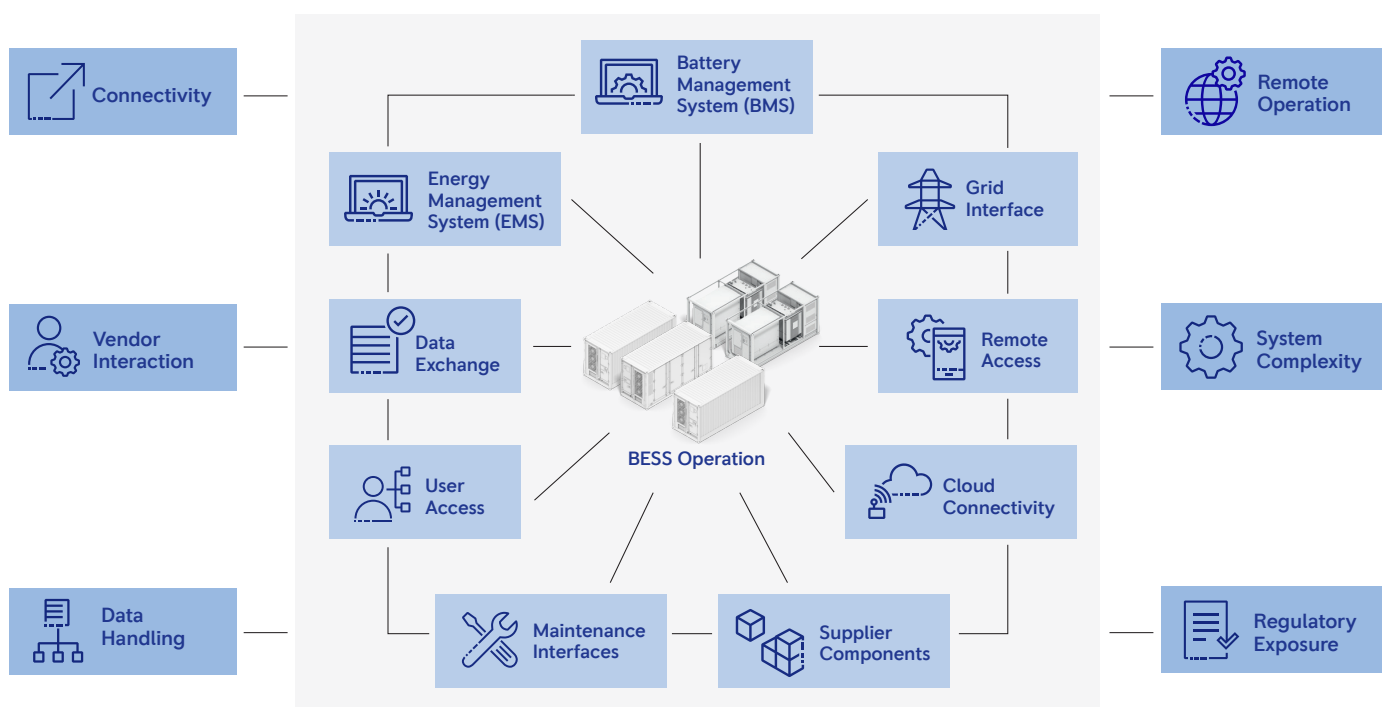


Figure 1: BESS attack surface

Key cyber exposure points in a connected BESS ecosystem.

Business impact & strategic considerations

Thus, cyber security has become a key decision factor in BESS projects as technical design choices now have direct implications for risk exposure, compliance, and long-term resilience.

This includes limiting exposure to high-risk external interfaces and ensuring that systems are designed with security, transparency, and traceability in mind.

Organizations that address these aspects early benefit from greater operational stability, improved compliance readiness, and stronger protection of their investments. A structured cyber security approach delivers tangible benefits:

- It reduces the likelihood of disruptions by identifying vulnerabilities early and applying targeted mitigation measures – this contributes to higher system availability and more stable operations.
- It also supports cost efficiency by preventing incidents that lead to downtime and associated financial losses. Improved system performance enhances productivity, and a strong security posture can help reduce liability exposure.
- At the same time, it strengthens overall security maturity, enabling organizations to protect sensitive data, meet regulatory expectations, and respond effectively to evolving threats.

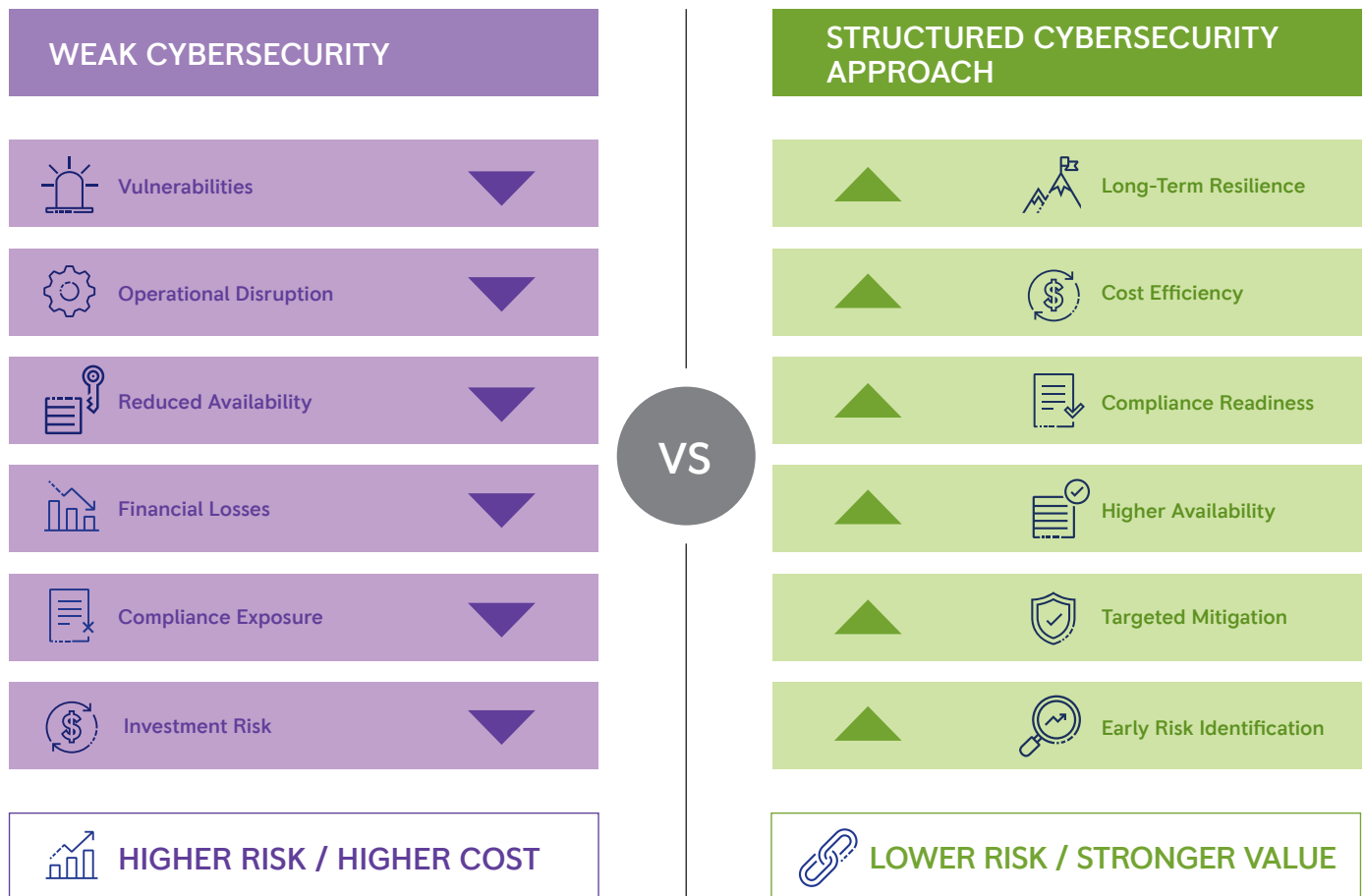


Figure 2: Cyber risk to business impact
How cyber weaknesses affect availability, cost, compliance, and resilience.

Core requirements for secure BESS

Effective cyber security in BESS, therefore, requires a structured and consistent approach across all levels of the system through:

1. Governance & risk management

A strong foundation for cyber security includes the use of structured frameworks, such as an Information Security Management System (ISMS), to identify critical assets, assess risks, and implement appropriate controls across both IT and operational technology (OT) environments.

2. Secure-by-Design development

Cyber security must also be embedded throughout the product lifecycle. Secure-by-design development ensures that risks are addressed early through threat modeling, defined security architectures, and continuous vulnerability management. This approach is typically guided by recognized industrial cyber security standards such as IEC 62443, including system-level requirements defined in IEC 62443-3-3.

3. Testing

Validation plays a key role in ensuring security effectiveness. Regular penetration testing and vulnerability scanning help identify potential weaknesses, while system-level validation ensures that defined security requirements are met prior to deployment.

4. Data & system control

Control over data and system access, including secure data transmission, controlled storage environments, and clearly defined access mechanisms – is equally important. In many cases, regional data hosting and on-premise solutions provide additional assurance and control.

5. Supply chain security

Finally, supply chain security must be considered from the outset. The use of trusted components and structured supplier management processes reduces exposure to external risks and supports the integrity of the overall system.

Cyber security at Rolls-Royce Power Systems

To translate these principles into practice, we at Rolls-Royce Power Systems apply a structured approach to cyber security across both organizational and product levels.

- Rolls-Royce Power Systems operates an up-to-date Information Security Management System (ISMS), drawing on recognized frameworks such as ISO/IEC 27001 and the NIST Cyber security Framework
- A certified development process in accordance with IEC 62443-4-1 supports the implementation of cyber security requirements throughout the product lifecycle
- System design and development are guided by recognized standards for industrial cyber security, with a focus on robust and state-of-the-art security controls
- Dedicated cyber security teams, including product and E/E cyber security functions, work closely with customers to address specific security needs and requirements
- Customers are supported by services including:
 - Threat and risk assessments
 - Product cybersecurity concepts
 - Security architecture design
 - Vulnerability management
- Products undergo regular penetration testing and vulnerability scanning
- Cyber security-focused Factory Acceptance Testing (FAT) is performed to validate customer-specific or classification-based security requirements
- Supply chain management processes are in place to ensure the integration of trusted and cybersecure components
- For applications with elevated security requirements, including governmental use cases, solutions are developed and adapted to meet specific customer needs

Conclusion

Cyber security is a fundamental requirement for the reliable and compliant operation of battery energy storage systems. As system complexity increases and regulatory expectations continue to evolve, a holistic approach that combines governance, secure design, and operational resilience becomes essential.

By embedding cyber security across the entire lifecycle and aligning organizational and technical measures, energy systems can be operated securely, reliably, and with confidence even in the presence of evolving cyber threats.

Rolls-Royce Power Systems is headquartered in Friedrichshafen in southern Germany and employs around 11,000 people. The product portfolio includes **mtu**-brand high-speed engines and propulsion systems for ships, heavy land, rail and defence vehicles and for the oil and gas industry. The portfolio also includes diesel and gas systems

and battery solutions for mission critical, standby and continuous power, combined generation of heat and power, and microgrids. With its climate friendly technologies, Rolls-Royce Power Systems is helping to drive the energy transition.

Rolls-Royce Group
www.mtu-solutions.com

The Rolls-Royce name, Rolls-Royce Badge and Rolls-Royce Monogram logos are registered trade marks of Rolls-Royce plc

