247 ENERGY

Cybersecurity in Battery Energy Storage:

A Risk That Cannot Be Ignored

What every BESS owner and operator needs to understand.

James Troch
Chief Executive Officer
247 Energy NV
January 2026

FOREWORD

Why I Write About This Now

Energy storage has entered the mainstream of infrastructure investment, and that is a development I welcome. But as the asset class has grown, a dimension of risk that deserves far more serious attention from owners, operators, and investors has remained underexamined. I am referring to cybersecurity, and specifically to the cybersecurity of the battery energy storage systems that are now being connected to critical grid infrastructure around the world.

I write about this not to alarm, but to inform. The energy sector has a long tradition of treating physical security with the gravity it deserves, while treating digital and software security as a secondary concern. That asymmetry made sense in an era when energy assets were largely analogue and isolated. It makes no sense today, when a utility-scale battery energy storage system is a sophisticated digital platform connected to grid control systems, cloud monitoring infrastructure, and in many cases to the public internet. The attack surface of a modern BESS installation is large, the consequences of a successful attack are serious, and the level of awareness among many asset owners remains insufficient.

This paper is addressed to BESS owners, operators, and the investors who fund them. It does not assume a technical background in cybersecurity. It does assume a willingness to think seriously about a risk category that the energy industry has been slow to address and that regulators in several jurisdictions are now beginning to mandate. Understanding the nature of the threat, the specific vulnerabilities of battery storage systems, and the architectural principles that determine whether a system is more or less resistant to attack is, I believe, now a basic requirement for responsible operation of grid-connected storage infrastructure.

James Troch, Chief Executive Officer, 247 Energy

Energy Infrastructure Has Become a Target

A New Category of Critical Risk

The targeting of energy infrastructure by hostile actors is not a hypothetical future scenario. It is a present reality that has been documented in incident reports, regulatory warnings, and post-event analyses across multiple continents. The motivations of attackers vary considerably. Nation-state actors seek to map, penetrate, and in some cases pre-position within energy control systems for strategic purposes, maintaining the capability to disrupt supply during a period of geopolitical tension. Criminal organisations target energy operators for ransomware attacks, seeking payment in exchange for restoring access to systems that have been encrypted or locked. Ideologically motivated actors aim to disrupt energy supply as a form of protest or to cause economic damage to specific sectors or jurisdictions.

What all of these actors share is an interest in systems that are both valuable and vulnerable. Energy infrastructure is valuable as a target because disruption has immediate, visible consequences for large populations. It is vulnerable because it was designed and built over decades in an era when connectivity and digital control were not primary design considerations, and because the pace of digitalisation in the sector has consistently outrun the pace of security investment. The combination of high value and structural vulnerability creates an environment where sophisticated attackers operating with patience and resources can find paths into systems that their operators believe to be secure.

Battery energy storage systems occupy a particular position in this threat landscape. They are new enough that their security characteristics have not been thoroughly tested in adversarial conditions. They are connected enough that they present a meaningful attack surface. They are critical enough that a successful attack on a grid-connected storage asset could have consequences that extend well beyond the facility itself. And they are proliferating rapidly enough that the aggregate risk they present to grid stability is growing faster than the security standards that govern their deployment.

> ***Energy infrastructure has become a strategic target. Battery storage systems, as new nodes in grid control networks, are entering this threat environment at precisely the moment when the sophistication and frequency of attacks is increasing.***

The regulatory response to this situation is beginning to take shape. In Europe, the Network and Information Security Directive, known as NIS2, extended the scope of mandatory cybersecurity requirements to include energy infrastructure operators and introduced substantially more rigorous obligations around risk management, incident reporting, and supply chain security. In North America, the

NERC CIP standards for critical infrastructure protection have been progressively tightened to address storage and distributed energy resources. In Asia, several jurisdictions have introduced grid security frameworks that explicitly address software-controlled grid assets. The direction of travel is clear: regulators are moving toward mandatory minimum cybersecurity standards for energy storage, and the assets that are not built and operated to meet those standards will face increasing compliance risk, operational restrictions, and in some cases liability exposure.

THE SPECIFIC RISK

Why Battery Storage Systems Are Different

More Than a Battery

A utility-scale battery energy storage system is not simply a large battery. It is a sophisticated digital platform in which the physical storage capability is managed, controlled, and communicated by multiple layers of software and hardware. A modern BESS installation typically includes a Battery Management System responsible for cell-level monitoring and protection, an Energy Management System that coordinates dispatch decisions and communicates with the grid operator, a Power Conversion System with its own embedded control software, remote monitoring and diagnostics capabilities accessed over network connections, and in many cases a cloud-based analytics and optimisation platform. Each of these layers represents a potential entry point for an attacker, and each interacts with the others in ways that a security compromise in any one of them can propagate across the rest.

The Battery Management System is particularly sensitive. It monitors and controls the fundamental operating parameters of the battery cells: state of charge, temperature, voltage, and current. If an attacker gains access to the BMS and can manipulate these parameters, the consequences range from degraded performance and premature ageing of the battery to, in the most serious cases, forced operation outside of safe boundaries. The nature of those consequences depends on the chemistry of the battery cells involved, which is a point we will return to when discussing how the choice of technology affects the risk profile.

The Energy Management System presents a different category of risk. Its role is to communicate with the grid operator and to dispatch the storage asset in response to grid signals. An attacker who gains access to the EMS can potentially manipulate the timing and magnitude of charge and discharge cycles in ways that are not immediately visible to either the operator or the grid. In a frequency response context, this could mean that the storage asset fails to respond when called upon, or worse, responds in the wrong direction, injecting power when the grid needs it absorbed or absorbing power when the grid needs it

injected. In a grid that is already stressed, a coordinated manipulation of multiple storage assets could amplify rather than dampen frequency deviations.

Remote access and cloud connectivity introduce further complexity. The ability to monitor and manage a storage asset remotely is operationally valuable and in many cases essential for assets in locations without continuous on-site staffing. But remote access creates a network path between the asset and the wider internet, and every such path is a potential attack vector. The security of that path depends on the implementation of authentication, encryption, and access control, none of which can be assumed without explicit verification. Many storage systems deployed today use vendor-provided remote access platforms whose security architecture is not fully transparent to the asset owner. In those cases, the owner is trusting the vendor's security practices without the means to verify them.

THE WEAPONISATION RISK

Can a Battery Be Turned Against the Grid?

A Question Worth Taking Seriously

The concept of weaponising an energy storage asset may seem extreme, but it is taken seriously by the security agencies and grid operators who have examined the question in technical detail. The concern is not that a single storage asset could be used to cause catastrophic damage in isolation. It is that a coordinated attack on multiple assets, or on the software systems that control a portfolio of assets managed by a single platform, could cause disruptions to grid stability that are difficult to attribute and difficult to correct in real time.

The mechanism of weaponisation in a storage context typically operates through the dispatch logic rather than through the physical hardware. An attacker who can influence the dispatch decisions of a storage asset can, in principle, cause that asset to behave in ways that are harmful to the grid without triggering the protection systems that are designed to prevent physical damage. A storage system that charges aggressively at the moment of peak demand, or discharges into a grid that is already experiencing an oversupply condition, is performing actions that are individually within its technical capability but collectively harmful if coordinated across multiple assets or timed to coincide with other stress events.

The physical safety characteristics of the battery technology used in a storage system are directly relevant to the weaponisation risk. Lithium-ion batteries, which are the dominant technology in utility-scale storage today, present a specific vulnerability: thermal runaway. Thermal runaway is a self-sustaining exothermic reaction that can occur in lithium-ion cells when they are operated outside of their safe

operating parameters, whether as a result of overcharging, external impact, or internal fault. A sophisticated attacker with access to the Battery Management System and the ability to manipulate cell-level parameters might, in principle, create conditions that initiate thermal runaway in one or more cells, with consequences that can range from localised damage to fire. The historical record of lithium-ion battery fires, in grid storage, electric vehicles, and consumer electronics, demonstrates that this risk is real even in the absence of deliberate manipulation.

Technologies that are not susceptible to thermal runaway by their fundamental physical nature present a categorically different risk profile in this regard. If an attacker cannot cause a physical catastrophe through software manipulation of operating parameters, a significant dimension of the weaponisation risk is eliminated. The attacker may still be able to cause the asset to behave suboptimally or to extract data that should be protected, but the worst-case physical outcome is bounded in a way that it is not for thermally unstable chemistries. This is not a theoretical distinction. It is a design consideration that should be part of the technology selection process for any BESS asset where security is taken seriously.

> ***The weaponisation risk of a battery storage system is shaped by two factors: the security of its software and the physical behaviour of its cells under fault conditions. Both need to be addressed. Neither alone is sufficient.***

SUPPLY CHAIN AND SOFTWARE RISK

The Problem With Black Boxes

Where Vulnerabilities Hide

One of the most significant and least discussed cybersecurity risks in the battery energy storage sector is the opacity of the software and hardware supply chain. A typical BESS installation integrates components from multiple suppliers: battery cells from one manufacturer, a Battery Management System from another, an Energy Management System from a third, power conversion hardware from a fourth, and cloud connectivity and monitoring services from a fifth. Each of these components contains software, and in many cases that software is proprietary, meaning that the asset owner has no ability to inspect its code, verify its security properties, or audit the practices of the organisation that developed and maintains it.

This opacity creates what security professionals call a black box risk. The asset owner is trusting that each supplier has developed their software securely, maintains it with appropriate security updates, and does not introduce vulnerabilities through the update process itself. None of these assumptions can be verified without access to the software source code and the development practices of the supplier. In the worst

case, a vulnerability introduced by a single supplier affects every BESS asset that uses their software globally, creating a systemwide exposure that can be exploited simultaneously across thousands of installations.

The risk is compounded by the geographic origin of components. A significant proportion of the battery hardware and embedded software in utility-scale storage systems today originates from suppliers in jurisdictions where the regulatory environment for software security is different from that of the markets where the assets are deployed. This is not an argument for protectionism. It is an observation that the security practices and regulatory obligations of a software supplier in a given jurisdiction reflect the standards of that jurisdiction, and that those standards vary materially. For asset owners and grid operators in Europe and North America who are subject to increasingly stringent cybersecurity regulations, the security properties of software originating from less regulated environments are difficult to verify and potentially difficult to defend to regulators in the event of an incident.

The NIS2 Directive in Europe has introduced explicit supply chain security requirements that place the burden of due diligence on the operator rather than the supplier. An energy operator subject to NIS2 is expected to assess the cybersecurity practices of every supplier whose products or services are part of their critical infrastructure, and to document the basis on which they have satisfied themselves that those practices are adequate. For operators whose BESS systems rely on multiple proprietary software components from suppliers in different jurisdictions, meeting this requirement is genuinely challenging. For operators whose BESS systems run on software that they or a trusted partner have developed and can inspect, the task is considerably more tractable.

Hardware supply chain risk operates on a parallel track. Embedded computing components, communication modules, and control hardware that originate from suppliers with limited traceability create a risk that is more difficult to mitigate than software risk, because hardware cannot be patched after deployment in the way that software can. An operator who cannot trace the origin and specifications of the hardware components in their BESS control systems has limited ability to assess whether those components contain vulnerabilities at the silicon or firmware level, and even more limited ability to address them if they do. Component traceability, the ability to document the origin, specification, and chain of custody of every significant piece of hardware in a system, is increasingly recognised as a basic requirement for secure infrastructure operation, and it is one that many current BESS installations cannot meet.

Compliance Is Becoming Mandatory

The Direction of Travel

Until recently, cybersecurity in the energy storage sector was treated primarily as a matter of good practice, with guidance documents and voluntary frameworks available to those who chose to use them. That era is ending. Regulators in Europe, North America, and a growing number of other jurisdictions have concluded that voluntary frameworks are insufficient for infrastructure whose failure could affect the security and welfare of large populations, and they are moving to replace guidance with mandatory requirements backed by enforcement powers and significant financial penalties.

In Europe, the NIS2 Directive that came into force in late 2024 represents the most comprehensive mandatory cybersecurity framework the continent has seen. It applies to operators of essential services, a category that explicitly includes electricity distribution, transmission, and related infrastructure. It requires these operators to implement risk management measures, report significant incidents within defined timeframes, and demonstrate that their supply chains meet appropriate security standards. The penalties for non-compliance are material: fines of up to ten million euros or two percent of global annual turnover, whichever is higher, for entities in the highest risk category. Equally significant, NIS2 places personal liability on the management of non-compliant organisations, creating an incentive for boards and executive teams to take the requirements seriously in a way that does not apply when the consequences fall only on the corporate entity.

The EU Cyber Resilience Act, which applies to connected hardware and software products, adds a further layer of requirement for the manufacturers and importers of BESS components sold into European markets. Products subject to the CRA must meet minimum security requirements before they can be placed on the market, must be supported with security updates for a defined period, and must be accompanied by documentation that enables buyers to assess their security properties. The practical implication for BESS buyers is that the regulatory compliance of the components in their systems is becoming part of the procurement decision in a formal and documented way, not simply an informal preference.

In the United States, the NERC CIP standards have been extended and tightened progressively to address new categories of grid-connected assets, including battery storage. The Federal Energy Regulatory Commission has directed revisions to the standards specifically to address the security of inverter-based resources, a category that includes virtually all utility-scale storage. Several individual states have

introduced their own requirements that go beyond the federal baseline. The trajectory in North America mirrors that in Europe: mandatory, increasingly specific, and increasingly enforced.

For BESS investors, the regulatory trajectory has direct financial implications. Assets that are not designed and operated to meet current and foreseeable regulatory requirements carry compliance costs that can be substantial: retrofitting security controls, engaging external assessors, managing incident reporting processes, and potentially paying fines if incidents do occur. Assets that are built from the outset with security as a design requirement rather than an afterthought are better positioned to meet evolving standards without major capital expenditure and with less operational disruption. Regulatory compliance is not the primary reason to take BESS cybersecurity seriously, but for investors focused on the long-term financial performance of their assets, it is a reason that belongs in the investment analysis.

BUILDING SECURE SYSTEMS

Principles of Secure BESS Design

Architecture That Reduces Exposure

Cybersecurity in a complex system like a battery energy storage installation is not a single product or a single decision. It is the aggregate of many architectural choices made at the design stage and many operational practices maintained throughout the life of the asset. Understanding what good looks like requires some engagement with the principles that determine whether a system is more or less resistant to attack, more or less transparent to its operators, and more or less capable of containing the consequences of a breach when one occurs.

Network segmentation is among the most fundamental of these principles. A secure BESS architecture separates the control systems that manage cell-level battery operations from the communications systems that connect to grid operators and monitoring platforms, and separates both of these from any connectivity to the public internet. Each segment is governed by rules that define precisely what traffic can pass between them, implemented in hardware rather than in software wherever possible. Hardware firewall boundaries between segments cannot be reconfigured remotely by an attacker who has compromised a software component, which provides a meaningful and verifiable limit on lateral movement within a breached system.

The principle of dedicated hardware firewalling deserves particular emphasis because it is frequently misunderstood. Software firewalls and virtual network controls are valuable tools, but they share the vulnerability of the software environment in which they run. A sufficiently sophisticated attacker who has

compromised the underlying operating system can potentially bypass or reconfigure software-based security controls without those changes being visible to external monitoring. A hardware firewall that enforces network boundaries at the physical layer does not share this vulnerability. Its configuration cannot be changed by software running on the same system, and its behaviour can be verified independently of the software components it protects. For BESS systems connected to critical grid infrastructure, this distinction is not a theoretical nicety. It is the difference between a security boundary that holds under pressure and one that does not.

Software transparency is a principle that is easy to state and difficult to achieve in a sector where most control software is proprietary. The underlying requirement is that the operators and owners of a BESS system should be able to understand what their software is doing, verify that it is doing only what it is supposed to do, and audit any changes made to it through the update process. This requires either that the software be developed by a party who shares their source code and development practices openly, or that the operator has contractual rights of audit that they can and do exercise. In neither case is trust alone a substitute for verification. Systems whose behaviour is opaque to their operators create dependencies that are not merely operationally inconvenient. They are security liabilities.

Authentication and access control represent a further dimension of secure design. Every access path to a BESS control system, whether from a local terminal, a remote management platform, or an automated process, should require strong authentication and should be logged in a way that supports post-incident forensic analysis. Privileged access, the ability to change configuration, update firmware, or modify dispatch parameters, should be subject to multi-party authorisation rather than resting on a single credential. These requirements are straightforward to state and widely understood in the cybersecurity community, but they are not consistently implemented in energy storage systems deployed today, partly because the operational convenience of simpler access arrangements has historically outweighed the security argument for more rigorous controls.

Cybersecurity as an Asset Quality Dimension

What Diligence Should Cover

For investors conducting due diligence on battery energy storage assets, cybersecurity has traditionally occupied a small and often formulaic section of the technical assessment. This is changing, and it is changing for reasons that are directly relevant to the financial performance of the assets being assessed. The regulatory costs of non-compliance, the operational consequences of a successful attack, the reputational damage associated with a publicly reported incident, and the increasingly explicit requirements of institutional investors with environmental, social, and governance mandates are all converging to make cybersecurity a material consideration in BESS asset valuation.

The direct financial exposure from a cybersecurity incident can take several forms. Regulatory fines for failure to meet NIS2 or equivalent national requirements are the most obvious. Business interruption losses, the revenue foregone while an asset is taken offline following an incident, can be substantial for grid services assets that are compensated on an availability basis. Third-party liability claims, potentially from a grid operator whose operations were affected by the behaviour of a compromised storage asset, represent a further category of exposure that is difficult to quantify in advance but cannot be dismissed as remote. And the cost of incident response, forensic investigation, system restoration, and remediation following a breach can be significant even where the direct operational impact was limited.

Beyond direct financial exposure, there is a subtler dimension of investor risk that relates to the long-term competitiveness of assets with weak security profiles. As mandatory standards tighten and as grid operators become more discriminating about the security credentials of the assets they contract with, storage systems that cannot demonstrate compliance with relevant frameworks will face increasing difficulty in accessing the highest-value contracted positions in the market. A storage asset that has been built without adequate attention to security may be operational today but may find itself excluded from capacity markets, black start contracts, or other high-value services as the eligibility requirements for those services evolve. The security architecture of an asset is therefore not only a present compliance question. It is a factor in the long-term revenue potential of the investment.

For institutional investors with sustainability frameworks, there is an additional dimension. ESG assessments of infrastructure assets are increasingly sophisticated, and the governance pillar of ESG is being interpreted more broadly than it once was. Cybersecurity governance, the frameworks, practices, and accountability structures through which an organisation manages digital risk, is beginning to appear explicitly in the assessment criteria of some of the largest infrastructure investors. An asset whose

security practices cannot be documented and defended against these criteria is at a disadvantage relative to one that has made security governance a visible and demonstrable part of its operational framework.

> ***Cybersecurity is no longer a technical footnote in BESS investment analysis. It is a dimension of asset quality with direct implications for regulatory compliance, revenue access, liability exposure, and long-term competitiveness.***

247 ENERGY

Security by Design, Every Day

At 247 Energy, cybersecurity is not a certification we point to or a policy document we keep on file. It is a daily discipline that shapes the way we design systems, select components, develop software, and operate assets. I want to be specific about what that means in practice, because the energy sector has a tendency to use security language loosely, and I think the distinction between stated intent and verifiable practice matters enormously when the assets involved are connected to critical grid infrastructure.

The most fundamental expression of our security commitment is the decision to develop all Energy Management System and monitoring software in-house. This is not the most commercially convenient approach. Third-party software platforms are available that would reduce our development costs and accelerate our time to market. We have chosen not to use them because we believe that the security properties of a system are only as verifiable as the software that controls it, and we are not willing to operate critical infrastructure on a black box that we cannot inspect, audit, and modify. Every line of code in our control systems was written by engineers who work for 247 Energy, reviewed within our security framework, and tested before deployment. We know what our software does because we built it. That transparency is not incidental to our security posture. It is the foundation of it.

Our hardware architecture implements dedicated physical firewall boundaries between the cell-level management systems, the site-level control systems, and any external communications paths. These boundaries are enforced in hardware, not in software, which means they cannot be reconfigured by a remote attacker who has compromised a software component. The design principle is that a breach in the external communications layer should not be able to propagate to the Battery Management System, because the two are separated by a boundary that software cannot cross. We test this boundary as part of our commissioning process and verify it as part of our periodic security assessments.

The physical safety characteristics of the supercapacitor technology we use in our storage systems are directly relevant to our security profile. Supercapacitor cells are not susceptible to thermal runaway. This is a consequence of their fundamental electrochemical architecture, not a feature that depends on the correct operation of any management system. An attacker who gains access to our Battery Management System and attempts to create dangerous physical conditions by manipulating operating parameters will find that the attack vector that works against lithium-ion chemistry simply does not exist in our technology. The worst-case outcome of a software-level attack on our systems is operational disruption, not physical danger. That boundary matters to us and, we believe, it should matter to anyone who operates storage infrastructure in proximity to people.

Our component sourcing practices reflect a commitment to supply chain security that goes beyond compliance with current regulatory requirements. Approximately 70 percent of the components in our storage systems are sourced from European suppliers, and we maintain detailed records of the origin, specification, and chain of custody of every significant component category. This level of traceability is not required by any regulation we are currently subject to. We maintain it because we believe it is the responsible way to operate critical infrastructure, and because we are confident that the regulatory direction of travel will make it a formal requirement for all operators in our sector within a planning horizon that is relevant to the assets we are building today.

Our software update process is governed by a formal change management framework that requires security review of all updates before deployment, testing in a non-production environment, and documentation of the change rationale and expected behaviour. We do not push updates to operational assets automatically or without prior notice to the asset operator. We do not accept updates from third-party components that have not been reviewed by our security team. These practices are operationally conservative and they add overhead to our development process. We accept that overhead because the alternative, a fast but opaque update process that could introduce vulnerabilities or unpredictable behaviour into a grid-connected asset, is not consistent with the standard of care we apply to infrastructure that matters.

We engage regularly with the cybersecurity research community, with grid operators on the security requirements they expect from connected assets, and with the regulatory frameworks that are shaping the mandatory standards in our operating markets. We do not wait for regulations to tell us what good security looks like. We try to be ahead of the regulatory curve, because we believe that the assets that will perform best over the long term are those built to a higher standard than the minimum that any current regulation requires. Security, like safety, is not a destination. It is a practice, and it requires constant attention as the threat environment evolves.

At 247 Energy, we are committed to building storage infrastructure that our grid operator partners, our co-investors, and the communities whose grids we help stabilise can trust. That commitment is expressed not in marketing materials but in the architecture of our systems, the practices of our engineers, and the standards we hold ourselves to every day.

---

247 Energy NV

Schaarbeekstraat 20E/11 | 9120 Beveren, Belgium

+32 3331 0000 | storage@247.energy | 247.energy