centrii

GRIDLOCK: What a Coordinated Battery Attack Would Cost the Grid

A Monte Carlo Risk Assessment of Cyber-Physical Exposure in Battery Energy Storage

By Rafael Narezzi, Centrii August 2026

Battery storage now sits at the center of grid stability - and at the center of a new category of financial risk. This report models the probability and cost of a coordinated attack on battery energy storage systems (BESS) through 2031, using a peer-reviewed Monte Carlo simulation of 10,000 iterations. The findings translate a technical vulnerability into a board-level number.

Visit our website

Executive Summary

Battery energy storage is the fastest-growing asset class in the energy transition, and the least protected. As BESS fleets increasingly are managed through cloud-based control platforms, they introduce a new financial exposure that most portfolios have not yet priced in.

This report presents the findings of a Monte Carlo risk assessment — 10,000 simulations across three industry security postures — quantifying the probability and financial cost of a coordinated attack on battery storage between now and 2031.

The findings:

- **92% probability** of a major attack on battery storage infrastructure by 2031, under today's industry-average security posture — falling to 61% with mandatory IEC 62443 certification in place.
- In Texas, compromising just **5.4% of ERCOT's battery fleet** (1,500 units) is enough to affect 30 million people, with an estimated **$12B–$65B** in economic damage.
- In the GB, compromising **29% of national BESS capacity** (400 units) is enough to trigger a national-scale blackout affecting 67 million people, with an estimated **£2B–£10B** in economic damage.
- Securing that infrastructure is dramatically cheaper than the alternative: our analysis shows a **15x–80x** return on proactive security investment relative to the cost of an attack.

This is not hypothetical. Recent events (a December 2025 compromise attempt on Polish wind infrastructure, and an unexplained 2.5 GW loss in the April 2025 Iberian blackout) show how plausible, and how hard to detect, this failure mode already is.

For asset owners, investors, and risk leaders across the energy sector, the question this report answers is not a technical one. It's financial: what is a coordinated attack on your

About this report

This report is a public-facing summary of Centrii's full peer-reviewed research paper, *Battery Energy Storage Systems — A Monte Carlo Risk Assessment.* The complete paper includes full simulation methodology, input parameters, and academic citations for readers who want the underlying data in detail.

Download the full research paper

Why Batteries Are the New Attack Surface

To understand the financial exposure, it helps to understand the mechanism — in plain terms, without the technical detail that usually keeps this conversation locked inside security teams.

Battery storage exists to balance the grid. Wind and solar generation rise and fall with the weather; batteries absorb the excess and release it back when generation dips, keeping the grid's frequency stable. Its role is like a voltage regulator protecting a piece of sensitive electronics — without it, supply and demand drift out of sync and the system becomes unstable.

Increasingly, that balancing function is managed remotely, through cloud-based control platforms that operate thousands of battery units across a portfolio or a national grid. That connectivity is what makes modern BESS fleets efficient to operate at scale, and it's also what creates a new kind of exposure.

A coordinated attack on battery storage doesn't need to stop power generation to cause a blackout. It only needs to desynchronize the balancing layer — forcing batteries to charge or discharge in a coordinated, disruptive pattern. The effect is closer to a distributed denial-of-service attack than a conventional power outage: instead of overwhelming a website with traffic, the attack overwhelms the grid's ability to stay in balance, using energy itself as the disruptive force.

The result, modeled in this report, is a cascading blackout that can unfold in under two minutes — triggered not by a lack of generation capacity, but by a loss of control over the systems designed to keep that capacity balanced.

This report quantifies how likely that scenario is, what it would cost, and what it would take to prevent it.

Recent Warning Signs — Poland and Iberia

The scenario modeled in this report is not theoretical. In the past year, two events have shown how plausible — and how difficult to detect — a coordinated disruption of grid-balancing infrastructure already is.

Poland, December 2025. State-sponsored actors attempted to destabilize regional grid infrastructure by rapidly cycling wind turbine output on and off. Not by damaging equipment, but by manipulating output in a way designed to push grid frequency out of balance. The attempt was contained, but it demonstrated a working blueprint: an adversary does not need to stop generation to threaten grid stability. Disrupting the balance is enough.

Spain and Portugal, April 28, 2025. At 12:33 CEST, a small number of large solar and wind sites stopped producing at the peak of the day, together shedding 2.5 GW of generation in under 20 seconds — enough to collapse the Iberian grid. The outage lasted roughly 10 hours, and as long as 20 hours in some areas.

Two aspects of the official record are worth noting. First, the affected sites have no usable operational logs from the moment of failure. Investigators cannot reconstruct what the control systems saw or decided in that window. Second, when the documented grid conditions are re-run in simulation, they do not reproduce a blackout. Sources believe something happened at those sites that isn't captured in the official account.

Spanish and Portuguese authorities have attributed the outage to a technical fault, not a cyberattack, and this report does not dispute that finding or claim otherwise. What the Iberian blackout demonstrates is narrower, and arguably more important for risk purposes: a small number of large renewable sites can take a national grid offline in under 20 seconds, through a failure mode that official investigators — using the complete forensic record available to them — have not been able to fully explain or reproduce.

That is the exposure this report quantifies. Not a specific claim about what caused either event, but a demonstrated fact: the balancing layer of a modern renewable grid is fragile enough that a small, coordinated disruption — deliberate or not — can cascade into a blackout affecting tens of millions of people. The Monte Carlo model quantifies: not whether this mechanism works — it has already been validated in peer-reviewed simulation — but how likely someone is to use it, and what happens if they do.

The GRIDLOCK Scenario, Explained

To understand what's being measured in this report, it helps to walk through how a coordinated attack on battery storage would unfold. This is a conceptual overview (enough to understand the exposure, not a technical breakdown.)

It starts with access. Battery fleets are increasingly managed through cloud-based control platforms that issue charge and discharge commands to thousands of units at once. Like any connected system, that control layer can be reached through weak points: remote access credentials that aren't properly secured, outdated device firmware, or vulnerabilities introduced through the hardware supply chain itself — inverters, optimizers, and battery management components sourced from a concentrated group of global manufacturers.

Then it becomes coordination. A single compromised battery unit poses little risk. The threat emerges when an attacker synchronizes commands across many units at once — instructing them to charge or discharge together or introducing a short delay into how they respond to grid signals. Neither action damages a battery. Both actions are enough to disrupt the grid.

The result is frequency manipulation. Electrical grids operate within a narrow frequency band. Deviate too far in either direction, and the imbalance between supply and demand becomes physically unsustainable. A synchronized flood or drain of power across a large enough number of battery units pushes frequency outside that operating band. Introducing even a few seconds of delay into how batteries respond to frequency signals has a similar effect, turning a system designed to stabilize the grid into one that amplifies its instability.

The outcome is cascading failure. Once frequency deviation crosses a critical threshold, protective relays (the safety mechanisms built to protect equipment from damage) begin tripping automatically. That's a feature, not a flaw: relays are designed to isolate parts of the grid before physical equipment is destroyed. But at scale, sequential relay trips cascade into a blackout, unfolding in under two minutes from the moment the attack begins.

The scale required is smaller than most portfolio owners assume. Academic modeling validates that compromising a relatively modest share of a region's total battery capacity — well under a majority — is sufficient to push grid frequency outside safe limits. It is, in effect, the same logic as a traditional denial-of-service attack: many compromised endpoints, coordinated to overwhelm a single system at once.

The difference is what's being overwhelmed. A conventional attack floods a network with data. GRIDLOCK floods a grid with power.

This is the scenario the Monte Carlo model quantifies: not whether this mechanism works — it has already been validated in peer-reviewed simulation — but how likely someone is to use it, and what happens if they do

Quantifying the Risk — The Monte Carlo Model

The findings in this report are not a forecast in the conventional sense. No one can predict exactly when or where a coordinated attack on battery storage might occur. Instead, this analysis uses a Monte Carlo simulation: a modeling technique that runs a scenario tens of thousands of times, each time varying the underlying conditions within realistic bounds, to produce a probability rather than a single prediction. It's the same class of technique used in financial risk modeling, insurance underwriting, and climate forecasting — well established anywhere the question is "how likely, not if."

For this analysis, the model was run **10,000 times** for each of three industry security postures:

- **Baseline** — current, industry-average security practices, with no meaningful improvement over time.
- **Moderate** — voluntary security enhancements, adopted gradually and unevenly across the industry.
- **Aggressive** — mandatory IEC 62443 certification and regular attack-readiness drills, adopted consistently.

Each simulation accounted for the pace at which attackers are likely to improve their capabilities, the pace at which battery storage capacity itself is expected to grow, and a range of realistic success rates for the different ways a system could be compromised — through cloud platforms, remote access tools, or the hardware supply chain. Rather than relying on a single assumption for each variable, the model draws from a plausible range each time it runs, which is what allows 10,000 iterations to produce a probability distribution rather than one fixed answer.

The results:

Security Posture	Probability of a Major Attack by 2031	Earliest Likely Attack Window
Baseline (no improvement)	92%	2027–2028
Moderate improvement	78%	2028–2029
Aggressive improvement (mandatory IEC 62443)	61%	2029–2031

The pattern is the headline finding of this report: security investment doesn't just reduce risk — it buys time. Moving from baseline to aggressive security postures delays the earliest likely attack window by roughly two to three years and reduces the overall probability of a major event by nearly a third.

This isn't a standalone claim. The underlying attack mechanism — that a coordinated, load-altering compromise of a modest share of battery capacity can push grid frequency outside safe operating limits — has been independently validated in peer-reviewed academic research, published separately from this report. This model doesn't assert that GRIDLOCK could theoretically work; it starts from the position that it has already been demonstrated to work in simulation, and asks how likely someone is to attempt it, under what conditions, and by when.

The next section grounds these probabilities in two real-world grids — Texas and the GB — to show what a major attack would mean in terms of people affected and dollars at risk.

What This Looks Like on the Ground — Texas and the GB

Texas — ERCOT

Texas operates roughly 28 GW of grid-scale battery storage — more than half of total US capacity — spread across approximately 28,000 individual battery units. Compromising just **5.4% of that fleet (around 1,500 units)** is sufficient to destabilize the entire ERCOT grid.

The resulting exposure: **30 million people affected**, with economic damage estimated between **$12B and $65B**. Attackers attempting entry through cloud platform vulnerabilities alone have a realistic chance of success — in the 35–70% range, achievable within two to five weeks by an attacker with intermediate-level skill, not the resources of a sophisticated nation-state operation.

Great Britain — National Grid

The GB presents a different — and in some ways more concentrated — risk profile. National battery storage capacity totals roughly 6.8 GW across approximately 1,400 units, with 79% of that capacity concentrated in England. Compromising **29% of national BESS capacity (around 400 units)** is sufficient to trigger a nationwide blackout.

The resulting exposure: **67 million people affected** — effectively the GB's entire population — with economic damage estimated between **£2B and £10B**.

The GB's exposure is proportionally higher than Texas's despite requiring a larger share of total capacity to be compromised, for two structural reasons: the GB operates as a single national grid rather than a set of interconnected regional ones, so there is no equivalent to islanding a single grid operator's territory; and battery deployment is geographically concentrated, meaning a coordinated attack doesn't need to reach every region of the country to affect the whole population.

Why these two markets, side by side

Texas illustrates the risk in a market defined by scale and speed — a fast-growing, deregulated grid where battery deployment is outpacing the security standards applied to it. The GB illustrates the risk in a market defined by concentration and interdependency — a smaller grid where the absence of regional isolation means a localized compromise becomes a national event.

Neither market is an outlier. They represent two of the most common risk profiles present across the battery storage portfolios this report is written for: large, distributed US asset bases, and smaller, tightly coupled European and GB grids. The same underlying math applies to any market with a concentrated or fast-growing battery fleet and cloud-based control infrastructure. These two simply have the public capacity data available to model precisely.

The Cost of Doing Nothing vs. The Cost of Acting

Every figure in this report so far has quantified risk. This section quantifies the alternative — what it costs to close that risk down, and how that cost compares to the price of an attack.

Great Britain

Bringing GB battery storage infrastructure up to IEC 62443 Security Level 2 — the standard this report's modeling shows meaningfully reduces attack probability — is estimated to cost **£400M to £1B** across the national fleet. A single major GRIDLOCK-class attack is estimated to cost **£2B to £10B**. That's a return on security investment of roughly **5x to 25x** — even in the most conservative comparison, the cost of prevention is a fraction of the cost of recovery.

Texas

Securing the ERCOT battery fleet to the same standard is estimated to cost somewhere between **$800M - $2.8B**. Against a single-attack cost of **$12B to $65B**, that produces a return on investment as high as **15x - 80x** in the most severe modeled scenarios.

The pattern holds regardless of market size or structure: the cost of proactive security is measured in the hundreds of millions; the cost of a single successful attack is measured in the billions. For portfolio owners and investors evaluating where to allocate capital, this is not a marginal risk-mitigation decision; it's one of the highest-return investments available anywhere in a battery storage portfolio.

This is also, notably, the inverse of how OT security spending is often perceived. It is rarely framed as a return-generating investment because its value is measured in an event that — if the investment works — never happens. This report's modeling makes that value visible: the return isn't hypothetical, it's calculable, and in the scenarios modeled here, it isn't close.

What Needs to Happen

The findings in this report point to a clear conclusion: the cost of prevention is a fraction of the cost of an event, and the technology to close this gap already exists. What's missing isn't capability. It's urgency and adoption.

For regulators and standards bodies, the case for mandatory action is direct: require IEC 62443 Security Level 2 certification for grid-connected battery storage on a defined timeline, extend existing frameworks like NERC CIP and NIS2 to explicitly cover BESS-specific controls, and introduce supply chain security requirements for battery hardware and firmware given how concentrated global manufacturing is today. Regular, mandated attack-readiness drills — modeled on the exercises already common in aviation and financial services — would meaningfully shorten the gap between a vulnerability being discovered and being fixed.

For asset owners, operators, and investors, the responsibility doesn't wait for regulation to catch up. The practical priorities are consistent regardless of geography: isolate battery control systems from general corporate IT networks, require multi-factor authentication on every remote access point into cloud control platforms, keep firmware current and verified, and build redundancy into frequency measurement so no single sensor or feed becomes a point of failure. None of these are novel security concepts — they are the same fundamentals that have hardened other categories of critical infrastructure. Battery storage has simply outpaced their adoption.

This is worth treating with the same seriousness as physical safety. Energy operators already have deeply embedded processes for physical risk. A worker injury on site triggers investigation, reporting, and accountability up to the board level. A cyber event with the potential to affect the power supply of millions of people warrants the same posture. This isn't a compliance checkbox to be satisfied once a year; it's an operational duty of care that must be demonstrated continuously.

Every recommendation in this section reduces the probability of a major attack, delays its likely timing, and does so at a fraction of the cost of the alternative. The industry does not need new technology to close this gap. It needs to act on what already exists, before the model stops being a probability and becomes a headline.

Closing - The Sovereignty and Timing Question

Every finding in this report traces back to one underlying shift: as more of the grid's balancing capacity moves into cloud-controlled battery systems, more of the grid's stability depends on who controls that software layer — not who owns the physical asset beneath it.

That's the real question this report raises, beyond probability and cost. If a remote vendor portal, a compromised credential, or a piece of unpatched firmware can influence the frequency of a national grid, then operational control of that grid is no longer fully defined by ownership. It's defined by whoever controls the systems in between.

This report has modeled the probability of that control being taken (92% by 2031 under current industry conditions, falling meaningfully with proactive investment) and the financial exposure that follows. What it can't model is timing with certainty. The conditions for a major attack on battery storage already exist today, and every year of delay in closing this gap is a year the probability compounds rather than resets.

The question for every asset owner, investor, and risk leader reading this isn't whether a coordinated attack on battery storage is possible. The research in this report (and the events already unfolding in Poland and Iberia) settle that question. The real question is whether the industry closes this gap before the first attack, or after.

For organizations ready to understand their own exposure (by asset, by portfolio, or across an entire fleet), Centrii's platform translates this same class of risk into board-ready financial terms, specific to your infrastructure.

Download the executive summary **Get your risk profile**

Methodology & Sources Appendix

This report is a public-facing summary of a peer-reviewed Monte Carlo risk assessment. Readers seeking full methodological detail, complete input parameters, and the underlying academic citations are encouraged to download the complete research paper. The sources below support the specific claims made throughout this report.

Primary Research

Narezzi, R. Battery Energy Storage Systems — A Monte Carlo Risk Assessment. Centrii, London, 2026.

Full paper

Academic Validation

The load-altering attack mechanism modeled in this report — including the finding that compromising roughly 15% of battery power in a target region can push grid frequency outside safe operating limits — is independently validated in: "From Balance to Breach: Cyber Threats to Battery Energy Storage Systems," arXiv:2501.05923v1 [cs.CR], Cornell University, January 2025.

Regulatory and Industry Sources

- International Energy Agency (IEA), Grid-Scale Battery Storage: 2026 Market Update, IEA Publications, Paris, 2026.
- North American Electric Reliability Corporation (NERC), Supply Chain Risk Assessment for Energy Storage Systems, NERC Technical Report, Atlanta, 2025.
- U.S. Department of Energy (DOE), Energy Storage Grand Challenge Roadmap, DOE Office of Electricity, Washington, DC, 2024.
- European Union Agency for Cybersecurity (ENISA), Guidelines for Securing Smart Grid, Heraklion, 2025.
- National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0, Gaithersburg, 2024.
- International Electrotechnical Commission (IEC), IEC 62443-3-3: Security Technologies for Industrial Automation and Control Systems, Geneva, 2023.

Incident Sources

- Ministerio para la Transición Ecológica y el Reto Demográfico (MITECO), official report on the 28 April 2025 Iberian Peninsula blackout, published 17 June 2025.
- European Network of Transmission System Operators for Electricity (ENTSO-E), factual report on the 28 April 2025 incident, published October 2025.
- Poland, 29 December 2025 incident: CERT Polska incident report (29 Dec 2025) and DOE CESER (10 Feb 2026) .

Methodology Note

The Monte Carlo simulation underlying this report's probability findings was run 10,000 times per security posture, incorporating projected attacker capability growth, battery storage deployment growth, and a range of realistic compromise success rates across cloud, remote-access, and supply chain attack paths. Full input parameters and statistical methodology are available in the peer-reviewed paper.

centrii

Centrii, Experts in renewable OT cybersecurity

Centrii exclusively focuses on renewables, offering a cybersecurity SaaS platform, CEntrii , designed specifically for the unique complexities of renewable energy operational technology (OT). Unlike generic, one-size-fits-all solutions, Centrii delivers a tailored approach through an intuitive dashboard that consolidates critical functions such as regulatory compliance, OT asset inventory, cyber risk assessment, financial impact risk assessment, incident response, and vulnerability management.

Learn More

Please visit: https://centrii.com

+1 346 471 3614
+44 20461 44800

info@centrii.com

British Assessment Bureau
UKAS MANAGEMENT SYSTEMS 8289
ISO 27001 INFORMATION SECURITY MANAGEMENT