Chile's BESS Cyberattack and What It Means for U.S. Projects

BY FRACTAL EMS | NOVEMBER 2026

The Huatacondo Attack in Chile

On August 27, 2026, at 1:10 p.m., the operator of the Huatacondo solar plant in northern Chile asked the national grid operator for a forced outage. It cited a cyberattack on its facilities. Huatacondo is a 103 MW solar farm paired with a 98 MW / 312 MWh battery energy storage system supplied by e-STORAGE, a Canadian Solar subsidiary. Two months later, the grid operator's daily report still listed both at 0% availability.

The logs for the same day also show a forced outage of a transformer at Santa Rita substation, and two thermal plants in Los Vilos lost remote control. The companies reported all of them as cyberattacks. The week before, an engineering and control-systems provider with access to other companies' facilities reported its own incident.

The owners have not disclosed how the attackers got in, and no group has claimed it. The battery system was still in commissioning. In Fractal's experience, that is when the most vendors, integrators and technicians have remote access to a site. The next day, Chile's National Energy Commission opened public consultation on a cybersecurity standard for the electricity sector. It had been in development since 2021.

Coordinated Attacks in Poland

Eight months earlier, on December 29, 2025, attackers hit more than 30 wind and solar farms in Poland, along with a combined heat and power plant serving almost half a million customers. At the renewable substations, they corrupted RTU firmware, wiped controllers and deleted system files. The wind and solar farms lost communication with the distribution system operator and could no longer be controlled remotely, but power output continued. Security software at the heat plant stopped the malware before it affected supply.

Poland's deputy prime minister said everything pointed to Russian sabotage and that the country came close to a blackout. CERT Polska, the national incident response team, linked the attack to an activity cluster tracked as Static Tundra, Berserk Bear or Dragonfly, and called it the first publicly described destructive activity by that cluster.

The attackers got in through internet-facing firewalls and VPNs, many without multi-factor authentication (MFA) and some with known vulnerabilities. Reused credentials likely helped them move from site to site. The substations were unmanned and managed remotely. Fractal finds the same gaps on many of the sites it reviews.

Coordinated Attack Impacts

Poland showed that one group can reach dozens of sites in a day. In September, the security firm Centrii published GRIDLOCK, a study that ran 10,000 simulations of a coordinated attack on battery fleets controlled through cloud and remote platforms. Under current industry practice, the model puts the probability of a major coordinated attack by 2031 at 92%. Moderate improvements lower that to 78%. Mandatory compliance with IEC 62443, the industrial control system security standard, plus regular attack drills lower it to 61%.

An attacker who controls enough batteries has two options. The first is to take them offline, removing the frequency response and capacity the grid depends on. The second is to charge and discharge them in sync, pushing grid frequency and/or voltage outside operating limits, tripping protective relays and risking islanding or blackouts. GRIDLOCK notes that frequency swings of that size can also damage generators and transformers.

> Texas is especially exposed. GRIDLOCK estimates that compromising just 5.4% of connected BESS assets in ERCOT could disrupt power for up to 30 million people and cause $12 billion to $65 billion in economic damage. Implementing IEC 62443 across ERCOT's 28 GW of storage would cost an estimated $800 million to $2.8 billion.

Current Policy and Its Gaps

Federal policymakers have acted this year, and Texas has tightened its rules since 2021, but both have focused on equipment ownership and where it was made.

Executive Order 14421, signed August 26, declared a national emergency in the bulk power system supply chain. It covers inverters, battery storage and control systems, along with the software, firmware and remote access attached to them (when they are tied to China, Russia, Iran or other covered countries). The Department of Energy's (DOE) rules on EO 14421 are due December 24, and they could affect equipment already in service.

In August, the FCC added foreign-made inverters and BESS equipment with remote communications to its Covered List, which blocks new equipment authorizations. It later extended the rule to equipment with wired connections. The test is mainly where final assembly takes place, and models already certified can still be sold and installed.

The Texas Lone Star Infrastructure Protection Act, passed in 2021 and expanded in 2023 and 2025, bars grid contracts that give designated foreign companies remote access or control. Compliance is by attestation. As of July, 261 ERCOT market participants reported buying critical grid equipment from designated companies. All of them attested that the purchases would not allow unauthorized access, and the law allows access for warranty and support.

None of these rules sets baseline requirements for how a site is networked: which protocols it uses, whether traffic is encrypted, how credentials are managed, or who monitors remote sessions. Equipment that passes every ownership and origin test can still be hacked.

Undisclosed Communication Devices

In May 2025, Reuters reported, citing two unnamed sources, that communication devices not listed in product documents had been found in some Chinese-made inverters. One source said they had also been found in batteries from multiple Chinese suppliers.

In Fractal's experience, equipment from foreign and U.S. suppliers alike ships with data acquisition systems and cellular modems that let the manufacturer push remote updates. Most buyers don't know they are there. No one monitors them, and they connect around the owner's firewall (this leads to poor cyber controls).

Supplier-Controlled EMS and PPC

Most foreign equipment suppliers also sell their own energy management system (EMS) and power plant controller (PPC). U.S. buyers usually decline them, but Fractal sees supplier controls on some U.S. projects and on many projects abroad.

The EMS and PPC issue the charge and discharge commands, so a supplier that controls them can control the plant. At Huatacondo, e-STORAGE, a Canadian Solar subsidiary, supplied both the batteries and the EMS.

Battery Management System Risks

Executive Order 14421 does not name battery management systems (BMS),but a BMS is firmware with remote-access capability inside equipment the order covers, and ERCOT already lists BMS among the critical grid equipment market participants report. Fractal expects future rules to cover it as a programmable device.

Fractal sees the same BMS weaknesses repeatedly. Backdoors can be added to firmware during manufacturing, shipping or service. Time signals can be spoofed to line up commands across a fleet. Traffic between devices is unencrypted, authentication is weak, and owners cannot check whether their firmware has been altered.

Common Vulnerabilities on Client Sites

Fractal finds the same problems again and again:

- Vendor and maintenance accounts that are shared, compromised or given more access than they need, with no oversight of technician access.
- One admin login used by everyone, so there is no record of who logged in or what they changed.
- Internet-facing firewalls and VPNs with local accounts, no MFA and unpatched firmware.
- Firewalls with no rules protecting the firewall itself, no geographic blocking, and broad access rules where narrow ones belong.
- Field devices on default passwords, without TLS, with SSH exposed, ports open, and MQTT brokers or REST APIs that anyone on the network can reach.
- Security cameras and other peripheral devices sharing the control network.

- The cheapest security licenses, which limit what can be detected or blocked.
- Patches put off because they affect schedule and support.
- Monitoring and patching that stop when an asset is transferred or sold.

The attackers in Poland used several of these.

Contract Requirements

- No undisclosed cellular modems, data acquisition systems or radio hardware. Suppliers disclose every communication path, and anything not approved is disabled before delivery.
- No vendor remote access except through an EMS-controlled gateway with named accounts, MFA and session logging.
- Encrypted protocols, unique credentials and segmented networks from the start.
- Managed switches, firewalls and other network equipment from domestic sources.
- Monitoring and patching obligations that transfer with the asset when it is sold.
- Suppliers and service providers whose cybersecurity programs follow recognized standards, so the organization behind the equipment has structured practices for its people, processes and products. These include the NIST Cybersecurity Framework (CSF) 2.0, ISO/IEC 27001 for information security management, and the IEC 62443 series, including IEC 62443-2-4 for integrators and maintenance providers and IEC 62443-4-1 for secure product development.
- ISO 9001 quality management certification, so manufacturing, configuration and change control follow documented processes.
- No terms that give a specified foreign entity effective control of the facility, such as unrestricted rights to operate it, exclusive rights to maintain or repair it, or intellectual property licenses. Under the One Big Beautiful Bill Act, signed July 4, 2025, payments under these arrangements can cost the project its Section 48E investment tax credit, including through recapture for 10 years after it enters service.

Fractal's consultants are subject-matter experts in reviewing commercial and technical exhibits and can help buyers secure favorable terms.

Cybersecurity Assessments

Fractal EMS builds cybersecurity into its controls, with its own cyber and IT teams. Fractal's controls, including its three-level BMS, are domestic and free of foreign entities of concern. Fractal's in-house penetration testing team assesses both new and existing assets, remotely or on site.

- Remote assessment: a less intrusive review of the site's network, remote access paths and exposed devices, with no site visit.
- On-site assessment: a full penetration test and cybersecurity assessment of the plant's control systems, network and field devices. This is the most thorough option.

Either way, clients receive an outline of Fractal's findings and the corrective actions needed to close each gap and harden the site.

> Huatacondo was attacked during commissioning and was still offline two months later. If you are buying equipment for 2027, or own assets that came with someone else's network, contact Fractal at info@FractalEMS.com to schedule an assessment. Learn more at https://fractalems.com/cyber-risk-assessment/.

References

CERT Polska. (2026, January 30). *Energy sector incident report – 29 December 2025*. https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

Dragos. (2023, June 7). *Overview of the ISA/IEC 62443 standards & effective IACS security*. https://www.dragos.com/blog/isa-iec-62443-overview

Electric Reliability Council of Texas. (2026, July 30). *[Testimony on Lone Star Infrastructure Protection Act implementation before the Texas House Committee on Homeland Security, Public Safety, and Veterans' Affairs]*. https://www.ercot.com/files/docs/2026/08/04/ERCOT-TXHouse-Homeland-LSIPA.pdf

EnergySage. (2026, August 31). *Grid cybersecurity: Chile's new standard reaches consultation as the sector already reports attacks*. https://energysage.cl/en/analisis/ciberseguridad-electrica-norma-consulta-publica/

Hammond, M. C., Humes, S. J., & Fischer, N. A. (2026, August 28). *New executive order targets foreign-produced equipment across the U.S. bulk-power system*. Pillsbury Winthrop Shaw Pittman. https://www.pillsburylaw.com/en/news-and-insights/eo-foreign-produced-bulk-power-system.html

Ini, L. (2026, October 29). Chile solar and battery system remain offline after cyberattack. *ESS News*. https://www.ess-news.com/2026/10/29/chile-solar-and-battery-system-remain-offline-after-cyberattack/

International Organization for Standardization. (2015). *Quality management systems – Requirements* (ISO Standard No. 9001:2015). https://www.iso.org/standard/62085.html

International Organization for Standardization & International Electrotechnical Commission. (2022). *Information security, cybersecurity and privacy protection – Information security management systems – Requirements* (ISO/IEC Standard No. 27001:2022). https://www.iso.org/standard/27001

Kennedy, R., & Sanchez Molina, P. (2026, August 5). US blocks certification of new foreign-made solar inverters and BESS equipment. *ESS News*. https://www.ess-news.com/2026/08/05/us-blocks-certification-of-new-foreign-made-solar-inverters-and-bess-equipment/

Lang, A. (2026, July 16). The prohibited foreign entity (or FEOC) rules and battery storage. *Energy & Climate Counsel*. Foley Hoag. https://www.foleyhoag.com/news-and-insights/blogs/energy-and-climate-counsel/2026/july/the-prohibited-foreign-entity-(or-feoc)-rules-and-battery-storage/

McFarlane, S. (2025, May 16). Rogue communication devices found in Chinese solar power inverters. *Insurance Journal*. https://www.insurancejournal.com/news/international/2025/05/16/824006.htm

Narezzi, R. (2026). *GRIDLOCK: A Monte Carlo risk assessment of coordinated cyberattacks on battery energy storage systems* [White paper]. Centrii. https://centrii.com/wp-content/uploads/2026/09/GRIDLOCK-Research-Paper.pdf

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Paganini, P. (2026, January 31). Cyberattacks disrupt communications at wind, solar, and heat facilities in Poland. *Security Affairs*. https://securityaffairs.com/187503/apt/cyberattacks-disrupt-communications-at-wind-solar-and-heat-facilities-in-poland.html

Rayner, T. (2026, September 8). Cyberattack on BESS fleets "probable" by 2031, modeling warns. *ESS News*. https://www.ess-news.com/2026/09/08/cyberattack-on-bess-fleets-probable-by-2031-modeling-warns/

Rayner, T., & Kennedy, R. (2026, August 24). US FCC ban updates: Foreign inverters now include wired devices, adds 45X safe harbor for BESS. *ESS News*. https://www.ess-news.com/2026/08/24/us-fcc-ban-updates-foreign-inverters-now-include-wired-devices-adds-45x-safe-harbor-for-bess/

Tilles, D. (2026, January 14). Poland suffers major cyberattack on power grid, says Russia likely responsible. *Notes from Poland*. https://notesfrompoland.com/2026/01/14/poland-suffers-major-cyberattack-on-power-grid-says-russia-likely-responsible/