

# Railroad Operating Technology Cybersecurity Safety Alert

2026-01

**SUBJECT: Power Inverters and Batteries**

---

**Power inverters and batteries integrated into railroads' critical infrastructure environments could contain unexplained communication devices introduced via the supply chain. Railroads can help prevent unintended access by identifying power inverters in their operating environment and applying appropriate mitigations.**

Recent open-source news reporting, corroborated by a U.S. Department of Energy report, has asserted that unexplained communication devices have been found inside Chinese-made power inverters and batteries, which make up a large portion of the renewable components used in global critical infrastructure.<sup>1,2</sup> Given that Chinese state-affiliated cyber actors present a persistent threat to U.S. critical infrastructure—conducting espionage, intellectual-property theft, and disruptive intrusions that have been documented by U.S. government and global intelligence agencies, these devices could provide nation-state actors access to put U.S. critical infrastructure at risk.<sup>3</sup>

Common uses of inverter-based resources across U.S. railroads include wayside signaling and communication equipment, train stations and depots, yards and maintenance facilities, and specialized locomotives and freight cars. Wayside solar systems in dark territory, e.g., track segments without wayside signaling or centralized traffic control, often use power inverters and batteries to power autonomous equipment, such as grade crossings, hazard detectors, communications, and switch heaters, where commercial grid power is unavailable or costly to source.

In addition to complying with current standards and regulations, railroads and other entities should consider treating inverters and battery managements systems in railroad operating environments as networked operational technology (OT) systems, not as passive appliances. Mitigations to consider include inventorying and segmenting these as OT, disabling and removing unused services and communication devices, enforcing identity management such as multi-factor authentication, and using secure logging and monitoring for unusual activity related to connections.

Issued: January 29, 2026

Prepared by: Office of Railroad Safety

---

<sup>1</sup> McFarlane, Sarah, *Reuters*, “Rogue communication devices found in Chinese solar power inverters” (May 14, 2025), available at <https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/>.

<sup>2</sup> U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, *Battery Energy Storage Systems Report* (Nov. 1, 2024), available at [BESSIE\\_supply-chain-battery-report\\_111124\\_OPENRELEASE\\_SJ\\_1.pdf](https://www.energy.gov/eere/energy-storage/bessie-supply-chain-battery-report-111124-openrelease-sj-1.pdf).

<sup>3</sup> National Security Agency and International Partners, *Joint Cybersecurity Advisory: Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System* (Sept. 3, 2025), available at [https://media.defense.gov/2025/Aug/22/2003786665/-1/-1/0/CSA\\_COUNTERING\\_CHINA\\_STATE\\_ACTORS\\_COMPROMISE\\_OF\\_NETWORKS.PDF](https://media.defense.gov/2025/Aug/22/2003786665/-1/-1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF).

*This alert does not have the force or effect of law and is not meant to bind the public in any way. FRA will not rely upon this alert as a separate basis for enforcement action or other administrative penalty. Conformity with this alert (as distinct from existing statutes and regulations) is voluntary only, and nonconformity will not affect rights and obligations under existing statutes and regulations.*