The SunSpec Modbus Threat Vector

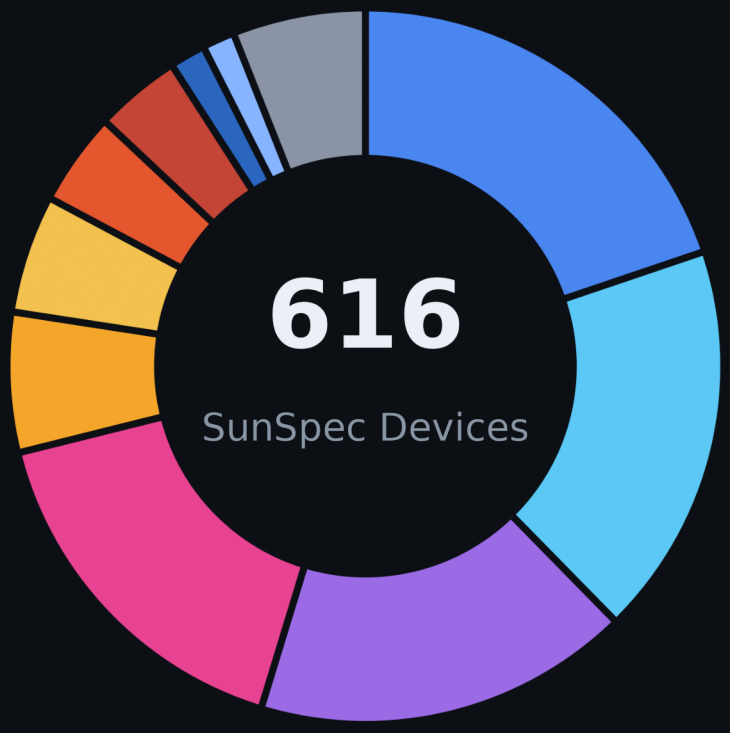
An Open Door to Our Power Systems

DER Security Research · June 2026

Solar inverters, battery systems, and other distributed energy resources increasingly speak SunSpec Modbus, an open, self-identifying register mapping schema, designed for trusted local networks. We performed SunSpec discovery on 265k internet-reachable Modbus (port 502) endpoints to better understand the power system risk from internet-connected grid-edge assets. The scan confirmed 616 internet-exposed SunSpec DER devices at 442 reachable sites in 46 countries and 29 manufacturers, representing 22.1 MW of generation and storage whose grid-control set-points are unauthenticated and writable from the public internet today.

265,583	616	22.1 MW	46
Modbus Endpoints Scanned	Unique SunSpec Devices	Remotely Controllable	Countries

Identified Devices by Manufacturer



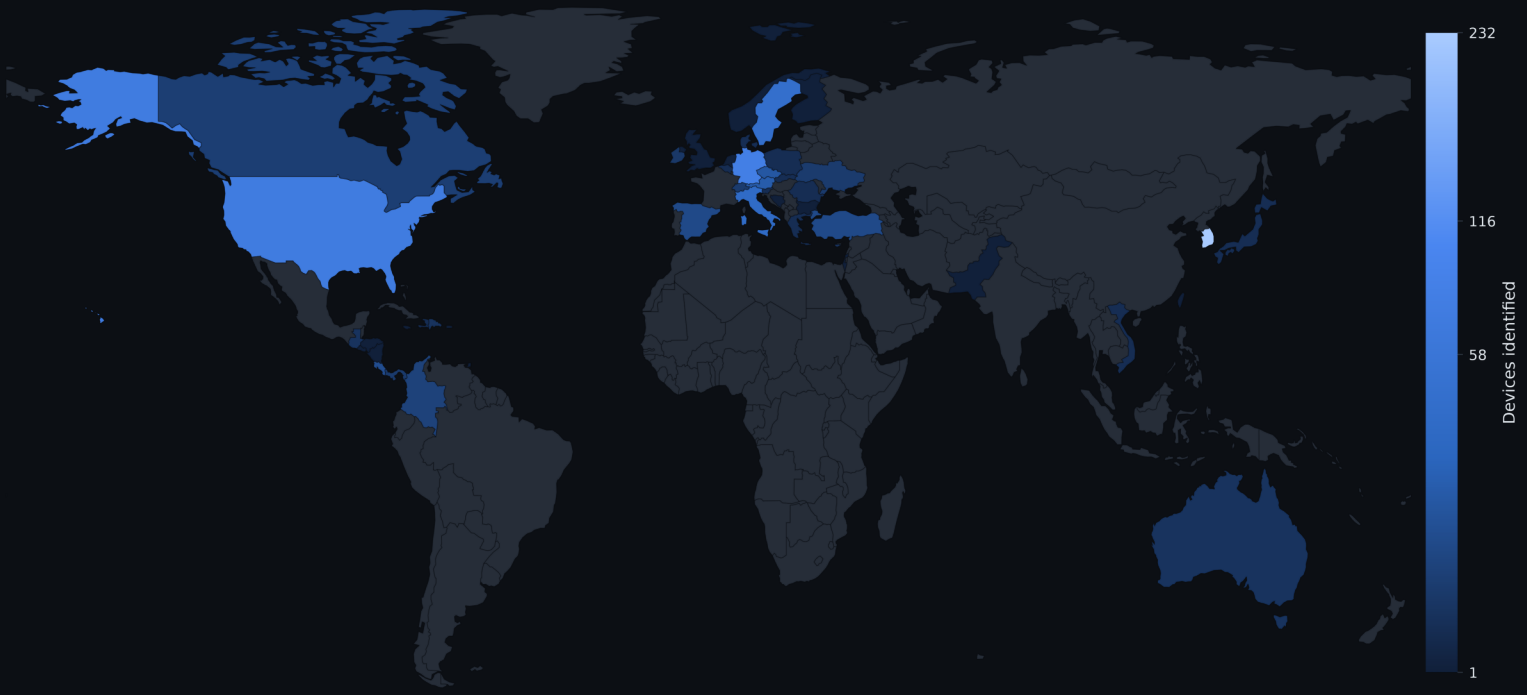
- CPS (122 · 20%)
- HYUNDAI (110 · 18%)
- ACCUENERGY (105 · 17%)
- FRONIUS (101 · 16%)
- ABB/FIMER (39 · 6%)
- SOLAX (33 · 5%)
- SMA (26 · 4%)
- SUNGROW (24 · 4%)
- KOSTAL (10 · 2%)
- KACO (9 · 1%)
- OTHER (37 · 6%)

NOTE: These are not product vulnerabilities; they represent insecure networking configurations.

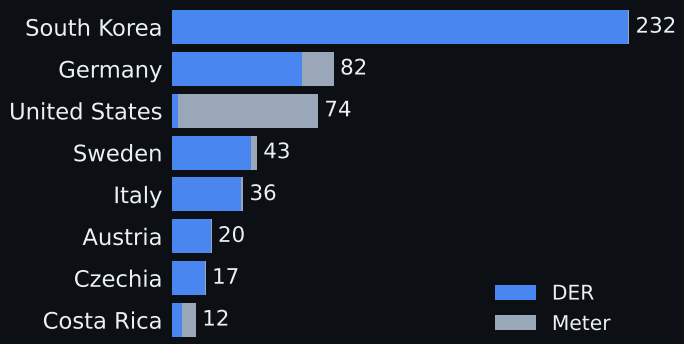
Methodology

This was read-only SunSpec probing; no registers were written. The scan was daylight-gated based on location to ensure the solar inverters were powered. There were 108 unique device models observed. Enumerating Modbus unit IDs revealed 86 multi-inverter sites (up to 22 inverters behind one gateway), so the device count is a lower bound.

Identified SunSpec Devices by Country



Top Countries — DER vs Meter



Top Countries — Controllable Power

Device Mix

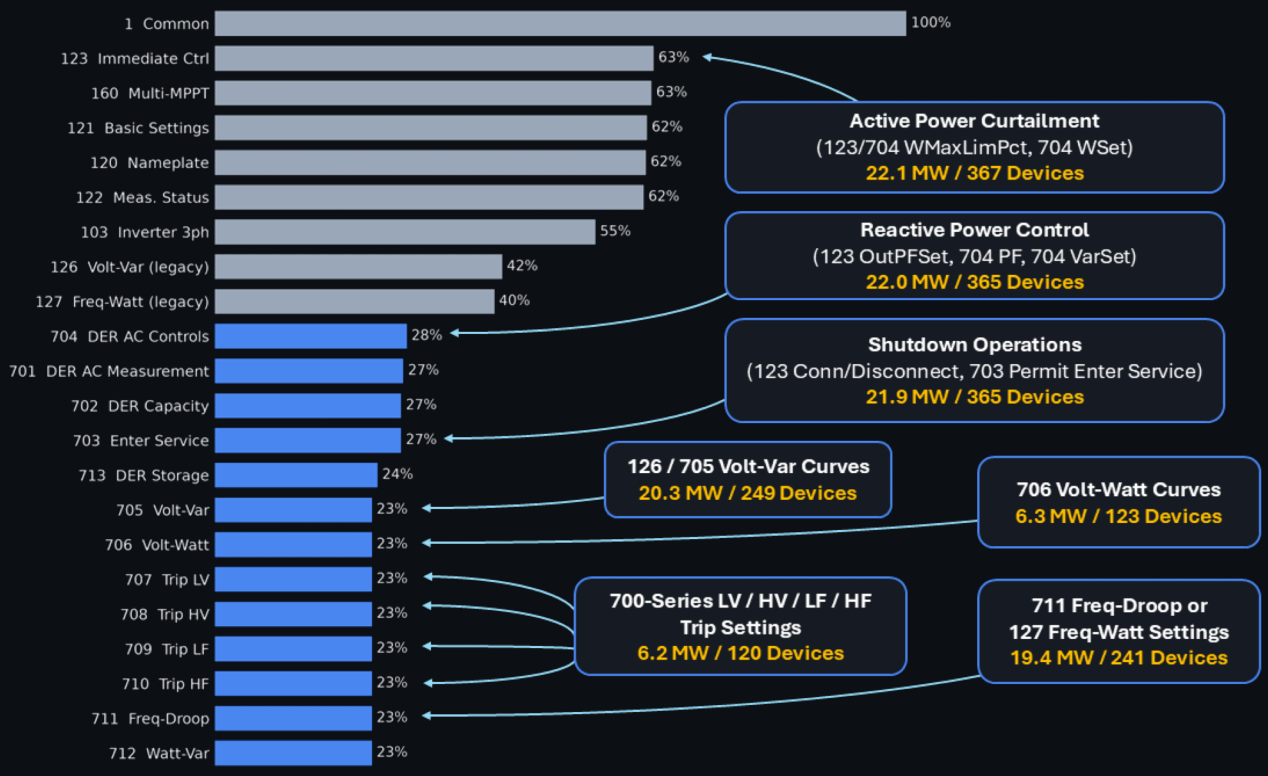
We discovered grid-interactive inverters and batteries (DER) alongside revenue / AC meters. Only the DER share carries writable grid-control functions.

Network Owners

Devices sit overwhelmingly on consumer / small-business ISP networks (Verizon, Deutsche Telekom, Telia, A1). These are primarily residential and C&I solar, not utility plants.

SunSpec Models Implemented

The share of identified devices exposing each SunSpec model is shown below, with the IEEE 1547-2018 DER control models (701–714) highlighted; the SunSpec Common Model (Model 1) is universal by definition. What is most worrisome is that 22.1 MW of nameplate generation/ storage includes writable grid-control functions over unauthenticated Modbus on the public internet. The Modbus protocol does not include an authentication mechanism, so Modbus servers should never be publicly exposed. Devices are reachable only because a site-side network configuration exposed them, such as a forwarded port, NAT rule, or an internet-exposed datalogger/gateway.



What an Attacker Could Write

- Curtail or zero active power (WMaxLimPct or WSet = 0) across the fleet at once
- Force disconnection or disable enter-service permissions, synchronizing de-energization
- Rewrite low/high voltage/frequency trip or ride-through settings so protection mis-operates
- Modify volt-var / volt-watt / freq-watt curves to destabilize the grid
- Command reactive power using power factor, VarSet, etc. to stress the local feeder

22.1 MW
writable active-power control

20.3 MW
autonomous volt-var control

6.2 MW
writable trip settings

Responsible Research

All probing was read-only; no device was altered.
Owners can request exclusion at security@dersec.io.

DER Security · security@dersec.io

From Exposed Controls to Grid Impact

The writable capacity is small against any bulk grid; there is little risk of widespread outages from these devices on the internet. Instead the bigger risk is that the grid-support functions are abused to cause localized impacts to the distribution system through active and reactive power manipulation. The impacts could be much more significant if any of these devices are part of microgrid installations, where malicious PV or battery energy storage setpoints could easily cause complete blackout of the site when operating in island mode.

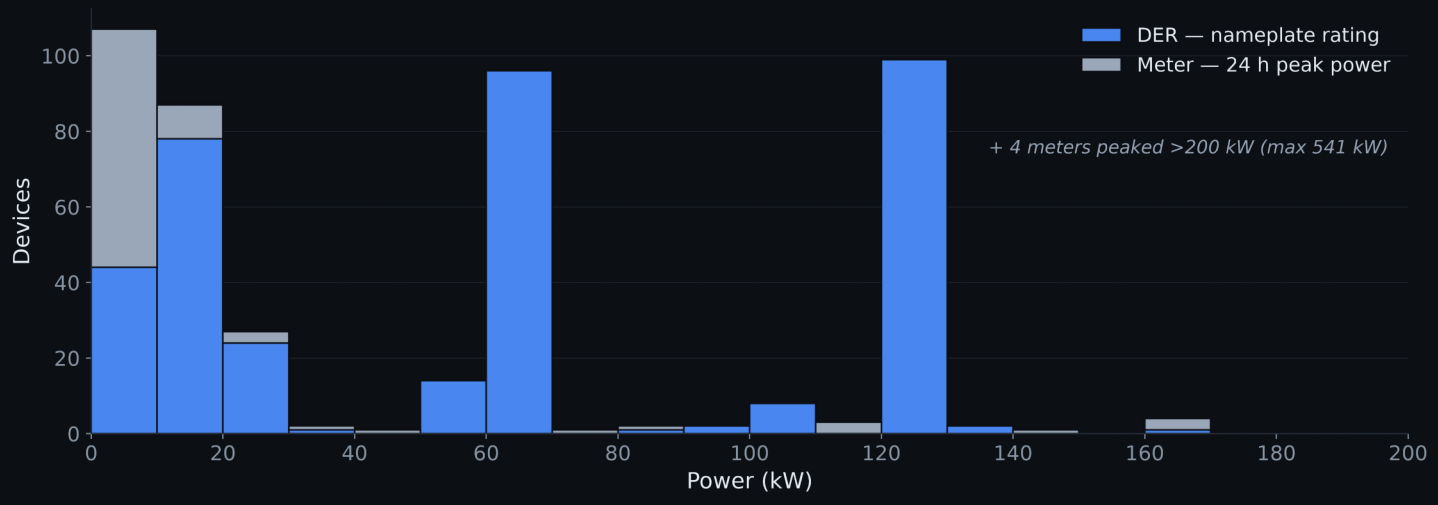
South Korea carries the largest controllable share, about 18.5 MW across 204 CPS and Hyundai inverters at 95 sites, which represents multi-inverter installations using a single feeder point of interconnection. At that concentration, the danger is not bulk power operations but coordinated misuse of the controls to impact the feeder. Simulations from Sandia National Laboratories quantified the effect: inverting an inverter's volt-var curve drove a 12 kV feeder to ~1.12 p.u. (134 V on a 120 V base), past ANSI C84.1 limits. Such excursions may damage equipment or trip protective relays, and under high PV penetration the resulting mass disconnection could deepen the disturbance.

Beyond any single-site impact, the exposed fleet is itself a resource for adversaries: an internet-reachable DER is a live cyber range on which to learn how these devices behave and to build and validate power-manipulation payloads — tradecraft that transfers to a later intrusion against a larger, better-defended power network. Insecure energy network access gained through compromised credentials or insecure remote access systems would expose more DER devices to manipulation.

Korea's comparatively isolated 60 Hz grid with a 98.8 GW peak summer load that has incorporated ~34 GW of installed PV make feeder overvoltage, protection mis-coordination, and even bulk system impacts a concern if a large enough fleet of PV systems could be maliciously controlled. To counter this, the Sandia study recommends defenses, including bounding each control with engineered parameter limits and segmenting DER control networks off the public internet, which are covered below.

DER Fleet by Nameplate Size

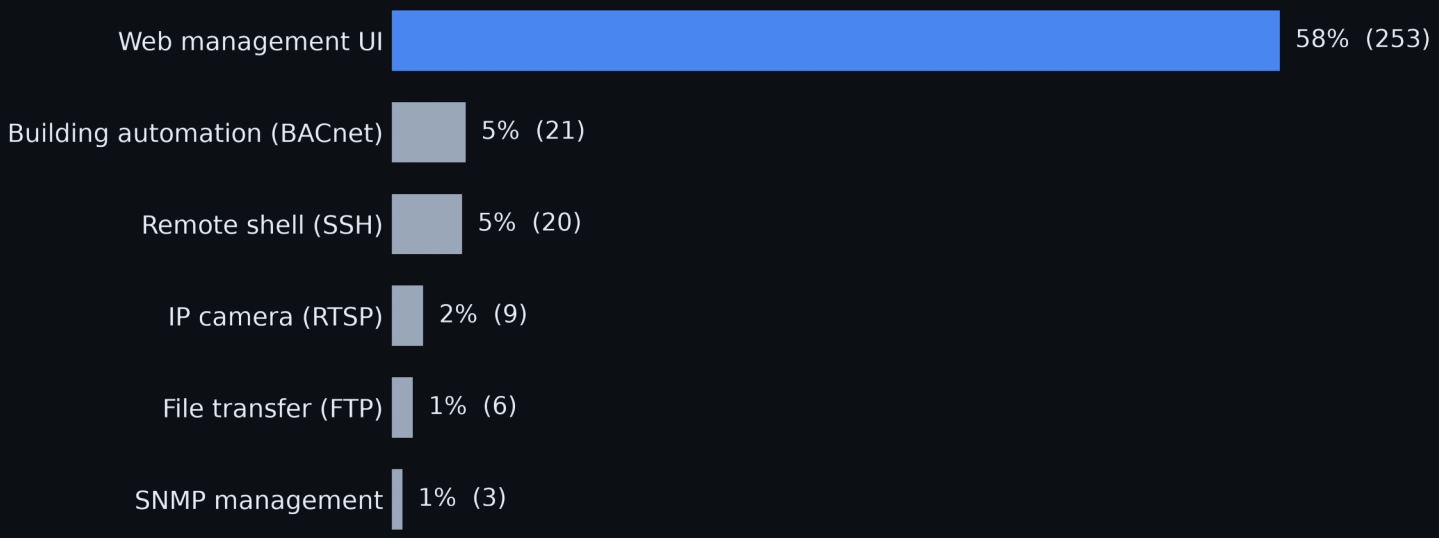
DER nameplate ratings with the metered fleet's 24-hour peak power (sampled every 15 seconds) overlaid in gray are shown below. The fleet is overwhelmingly small residential / light-C&I systems. The largest single DER found, a 1 MW central inverter at a U.S. solar-plus-storage site, carried its operational data in a vendor-proprietary SunSpec model rather than the standard control models, so its controllability over this interface could not be determined.



† *Data was collected in two 24-hour runs separated by less than a week. Each run included 8 daylight zones to ensure the equipment was powered. The 2nd 24-hour scan surfaced 82 additional sites carrying ~9 MW of further writable-control capacity, while 76 previously-seen sites had gone offline. This indicates that a single snapshot understates the true exposure. The numbers shown in this paper represent the accumulated values across the two passes. If an adversary timed their attack, they could manipulate more than 10 MW instantaneously.*

Beyond Modbus: The Wider Attack Surface

Modbus/502 is rarely the only door. Across the internet-exposed fleet, most devices also answer on other ports — web management consoles, building-automation, even remote shells and cameras — sharply widening what an attacker can reach. These data were collected using Shodan IP lookups.



64%
expose a service beyond Modbus

58%
expose a web management UI

123
identifiable vendor device UIs

Whose Web UI Is It?

Of 253 web-exposed hosts, 123 present an identifiable vendor management page, most without a login requirement. The common pages were: 44 Fronius, 22 Obvius AcquiSuite datalogger, 16 SMA, 13 Sungrow, 11 AccuEnergy, and 4 KACO.

Some exposed endpoints were Ethernet-to-Serial gateways, which are sold by some inverter vendors to remotely access multiple SunSpec Modbus RTU devices. 86 endpoints fronted multiple inverters this way (up to 22 on one bus), so a single exposed IP exposed control over an entire group of inverter devices.

Closing the Door

Five steps to take DER assets off the open internet and keep them controllable only by trusted parties.

1 Take the Device Off the Public Internet

The simplest fix: if a DER, gateway, or meter does not need inbound internet access, remove its public exposure entirely. Close any inbound port-forward or NAT rule that publishes port 502.

2 Audit for Unintended Exposure

Exposure is often unintentional: Even a local-only device can be published to the internet by an upstream datalogger, gateway, or router. Periodically scan your own public IPs to identify remote access services.

3 Allowlist Only the IPs that Need Access

Where remote access is genuinely required (an aggregator, O&M vendor, or DERMS), use a VPN or restrict port 502 at the site firewall to a small allowlist of known source IPs and default-deny all other inbound Modbus.

4 Adopt Secure SunSpec (Modbus over TLS)

Migrate from cleartext Modbus to the SunSpec Alliance's secure transport, authenticated, encrypted Modbus over TLS , so set-points cannot be read or written by unauthenticated parties.

5 Monitor Assets with Cyber-Physical IDS

Deploy the DERSec Sentry cyber-physical Intrusion Detection System to observe every interaction with the DER assets, baseline normal control traffic, and alert on malicious or unexpected operations against the equipment.

Coordinated Disclosure

We reported the findings to the national CERTs, CISA and KrCERT/CC, so asset owners could be notified.

Of the SunSpec devices, the 68 sites on U.S. networks identified in the first census pass were prioritized for disclosure. They included a multi-megawatt utility-scale solar-plus-storage plant, government and public-sector facilities (including transportation, corrections, and court operations), and commercial sites — most reached through internet-exposed dataloggers and unauthenticated Modbus.

We provided CISA a per-site report sufficient for rapid owner notification. All findings came from passive, read-only discovery: no device was accessed beyond what it already published. No control actions were taken.

A parallel disclosure covering the 59 South Korean sites in that census was filed with KrCERT/CC, the Korea Internet & Security Agency. Owner outreach proceeds through each agency's coordination channels.

The U.S. utility whose jurisdiction included the 1 MW inverter was notified of the exposure, and the product vendors listed in this report were provided with advance copies of these findings. Several rightfully noted that the insecure configurations are outside of their control. For example, Fronius noted that their devices are securely configured by default and that their documentation explicitly warns against the risks of internet exposure. Any insecure state is the result of active and explicit user misconfiguration.

About DER Security

DER Security Corp (DERSec) builds a cyber-physical anomaly-detection system that protects distributed energy resources at the device, local-network, and cloud levels — correlating an asset's electrical behavior with its network control signals so insider threats, network-based intrusions, and malicious DER updates are detected and mitigated in real time.

This brief is a companion to DER Security's Solar Energy Cybersecurity Vulnerability Summary, which catalogs 88 disclosed solar/DER vulnerabilities and six publicly reported attacks — collectively exposing more than 1 TW of solar generation to remote control. Where that report surveys the disclosed vulnerability landscape, this census measures what is exposed and controllable on the open internet today.

We work with manufacturers, integrators, and operators to take DER devices off the open internet and keep them controllable only by trusted parties.

Learn more: dersec.io

Further reading

- → **Solar Energy Cybersecurity Vulnerability Summary (DER Security, 2025)**
- → **Power system effects and mitigation recommendations for DER cyberattacks (IET, 2019)**