




India Smart Grid Forum

RESEARCH REPORT ON
SECURITY CONCERNS IN
SOLAR INVERTERS IN INDIA
MAY 2025



Malware and Kill Switches in Solar Inverters - Call for Immediate Action

India is pursuing an ambitious renewable energy (RE) program with the target of 500 GW by 2030; and has already installed 235 GW of non-fossil based generation resources and out of which 105 GW is solar. In 2024, Government of India (GoI) launched the PM-Surya Ghar: Muft Bijli Yojana aiming to install rooftop solar (RTS) on 10 million households, with a cumulative capacity of 30 GW. The increasing penetration of small RTS systems on distribution feeders has led to reverse power flow challenges. During peak solar generation hours, local demand often remains low as most houses are locked, causing power to flow back onto the grid. Presently, there are about 1.8 million RTS systems connected to the grid with a cumulative capacity of 16.5 GW; and another 14 million households have expressed interest to install RTS under the PM Surya Ghar Yojana. It is estimated that over 80% of the inverters deployed for connection of RTS systems with the grid are made by Chinese companies.

 India Total PV Inverter Market Share (% of Shipped MW _{ac})		
Ranking	Company	Market Share
1	Sungrow*	36%
2	Sineng	17%
3	Fimer*	17%
4	TBEA	11%
5	Ginlong Solis	4%
6	Sofar	4%
7	Growatt	3%
8	Hypontech	3%
9	Kehua	2%
10	All Others	3%
2023 PV Inverter Shipments (MW_{ac})		21,959

Source: Woodmac, 2024

Appendix-A presents the shipments of major inverter OEMs in India since 2015.

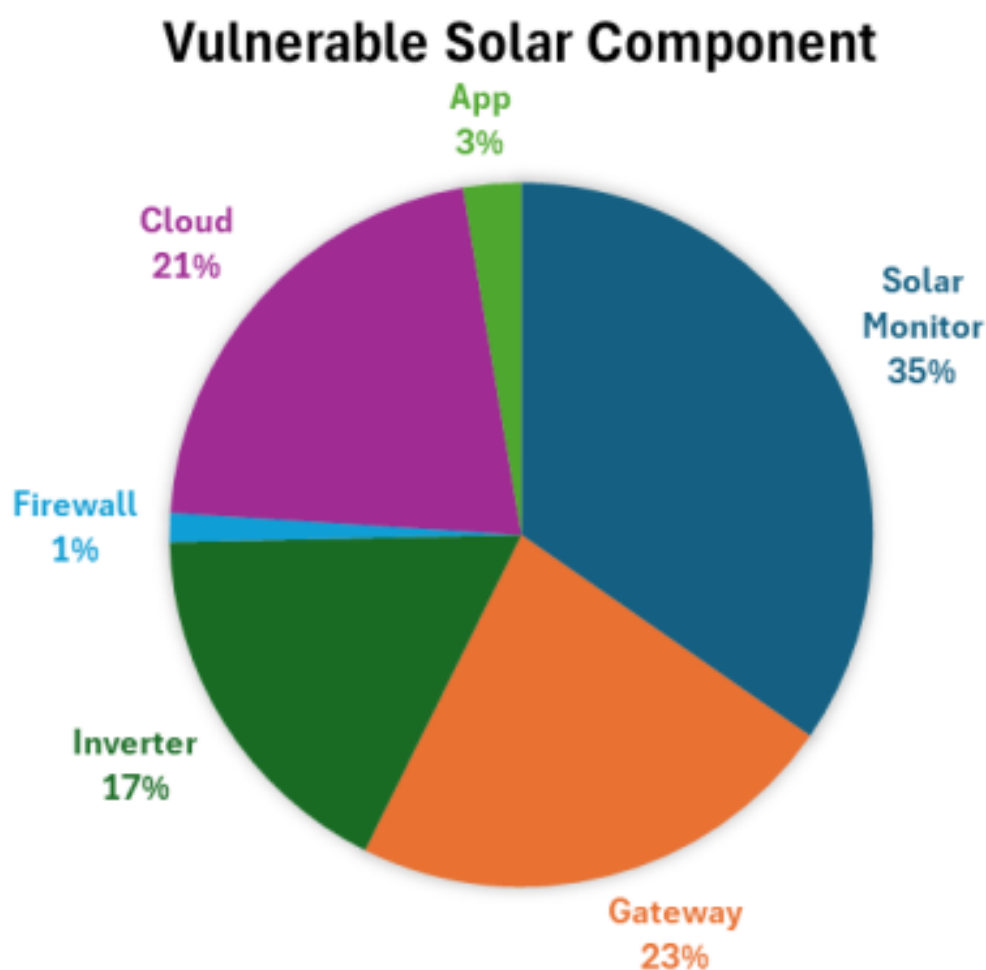
Recently engineers in American solar farms have found “**rogue communication devices**” in Chinese made components which raised severe fears that China might have the power to manipulate supplies or physically impact grids across the US, UK, Europe, India and other countries. Unauthorised communication devices were discovered inside some solar inverters. The devices, not mentioned in product documentation, were found by US experts who stripped the equipment connected to grids to check for security issues. Using these devices the actors behind these devices could skirt firewalls and switch-off inverters remotely, or change their settings to destabilize power grids, damage energy infrastructure and trigger widespread blackouts across the country. Some utilities, including Florida's

largest power supplier Florida Power and Light Company, are attempting to ban the use of Chinese inverters by sourcing equipment from elsewhere.

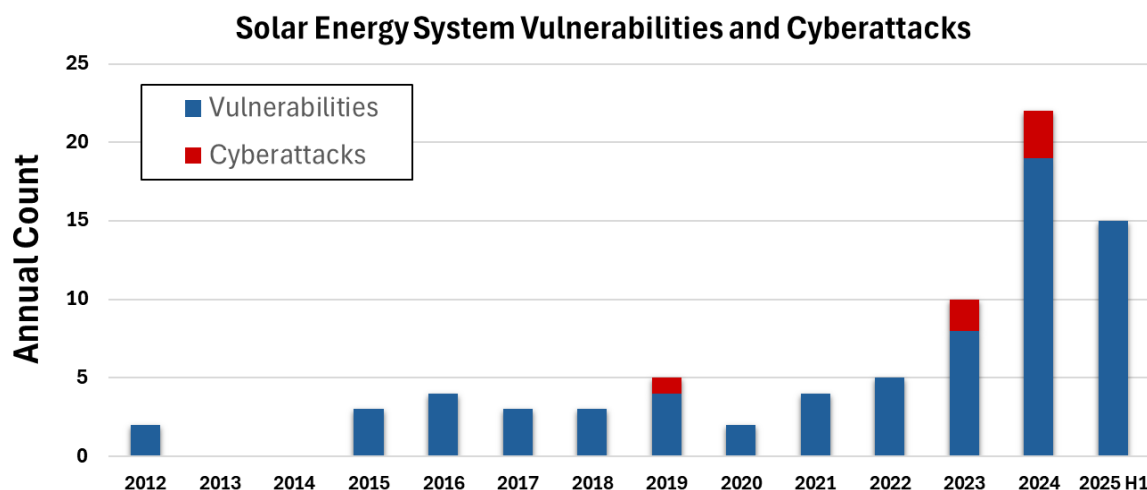
Recently Engineers in Denmark has detected “kill-switches” in Chinese solar PV systems (<https://m.economictimes.com/news/international/us/after-kill-switches-in-chinese-solar-panels-in-u-s-denmark-finds-suspicious-parts-in-east-asian-circuit-boards/articleshow/121381403.cms>). The head of the lobby group SolarPower Europe, Walburga Hemetsberger, called for a detailed investigation and described the discovery as extremely alarming. Experts have warned more forcefully in recent years about the security threat posed by China's monopoly on the supply of numerous types of renewable energy components in Europe, including batteries, turbines, and inverters that provide grid stability. This has amplified the risk of Europe’s energy sovereignty due to the unregulated and remote-control capabilities of solar inverters from high-risk, non-European manufacturers most notably from China.

Solar Component Vulnerabilities

DER Security Corp, USA has found 129 unique Common Vulnerabilities and Exposures (CVEs) and other issues identified in solar PV systems and the cloud software. As shown in Figure below, most issues were related to solar monitoring systems and gateways, with cloud infrastructure and inverters also



having a sizable share of the vulnerabilities. From a risk perspective, cloud vulnerabilities would likely lead to more significant impacts because they allow attackers.



Source: DER Security Corp, USA

In their May 2025 report, DER Security Corp has catalogued vulnerabilities in solar based Distributed Energy Resource (DER) systems. According to the disclosures, these vulnerabilities exposed approximately ~45% of the world-wide solar generation (>1 TW) to cyber exploitation¹.

Some of the biggest vulnerabilities identified include:

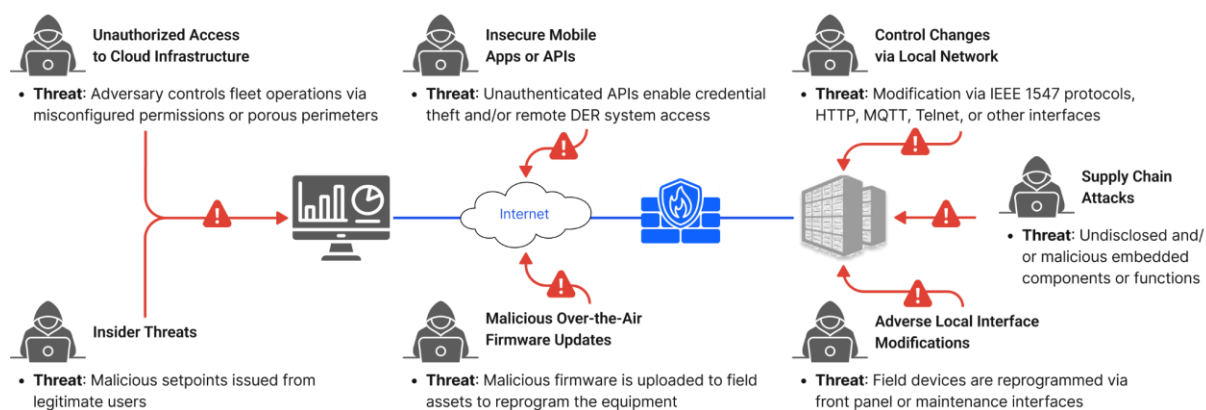
- Vangelis Stykas’s recent cloud platform compromise demonstrations purportedly allowed him to gain access to a staggering 740 GW of solar generation and perform firmware updates on many of these generation devices.
- In the SUN:DOWN report from Forescout, exploit chains were presented to control or disconnect over 1 TW of solar capacity.
- Sébastien (a.k.a. veganmosfet) has demonstrated the ability to gain unauthorized access to four different inverter types, modify the firmware of these devices, and arbitrarily control transistor switching operations.
- In May 2019, a utility in the western United States reported to the US Department of Energy (DOE) that they had been compromised by a denial-of-service cyberattack that targeted the company’s firewall. This attack broke the connection between the utility’s wind and solar power generation installations. The impacted generation totalled 500 MW including 106.3 MW PV project in California and 80 MW wind power plant in Wyoming. This is the first-of-its-kind attack to hit a renewable energy provider and disconnecting a U.S. electric grid operator from its power generation stations.

Based on these findings, common threat vectors can be represented. The image below highlights these paths in solar energy infrastructure, exposing hidden components in Chinese-made inverters like insecure Solar Monitoring Wi-Fi Dongles which could be exploited to remotely disable solar assets

¹ <https://dersec.io/reports/DERSec-Solar-Vulnerability-Summary-v2.0-Final.pdf>

or destabilize entire power grids. With over 80% of inverters in countries like India and a significant share in the U.S. supplied by Chinese firms, this creates a systemic risk to national energy security. This calls for urgent policy action, enhanced cybersecurity standards, and localized data governance for distributed energy resources (DERs).

Distributed Energy Cybersecurity Threats



Source: DER Security Corp, USA

Coupling the findings from these researchers, it is not difficult to imagine attacks in which 100s of GWs of solar generation are simultaneously disconnected, sub-synchronous power oscillations are injected, power quality is intentionally degraded with high harmonic distortion, or all power stage switches are closed to short the DER phases and trip protection equipment. Worse, given increasing deployment of residential and light commercial battery and hybrid generation systems, additional attack scenarios are plausible outside of typical solar energy generation windows by leveraging bidirectional power flows to exceed distribution or transmission line ratings or overload transformer capacities. Because modern solar inverters are a combination of computing devices and power conversion equipment, large-scale impacts on the grid are possible if (a) vendor, operator, or aggregator of the cloud systems is compromised or (b) valid firmware updates are issued that disable equipment. Negative impacts can be realized with traditional cloud breaches or when attackers gain a foothold on fielded equipment and pivot upstream. Fred Bret-Mounet demonstrated this attack vector by accessing hundreds of customer devices by compromising and escalating privileges on a Tigo Energy gateway that was connected to a virtual private network.

DER Security Corp has discovered close to 50 new vulnerabilities affecting Sungrow, Growatt, and SMA inverters; and demonstrated a complete exploit chain that allows attackers to control a fleet of power inverters remotely, thus enabling a coordinated attack against power grids.

Scenario in India and Call for Immediate Action

As indicated, about 80% of the 1.8 million RTS units are connected with the grid through inverters of Chinese make. Most people with RTS systems in India use mobile apps to monitor their solar generation. This is made feasible by installing a communication device in the inverter (Cellular SIM or broadband internet). In all such cases the inverter communicates the real-time generation data with the OEM's server in China from where it is transferred to the customer's mobile app. This is a real

danger to the grid which must be stopped immediately. Most inverter OEMs in India (including Indian companies) currently outsource their monitoring systems to one or two third-party providers such as “Solarman²” (also discussed in DERSec’s reporting). As a result, a disproportionate share of solar telemetry and in some cases, command and control access is now concentrated outside the country, with very little transparency. This creates an unregulated data monopoly embedded across OEM brands, even when the hardware itself is domestically certified. If the inverter is connected to the OEM’s server in China, they can control the inverter functions and can switch-on or switch-off or make it malfunction anytime. If millions of RTS systems with several GWs are switched off, the entire Indian grid can collapse. The Government of India (GoI) should take immediate actions to mitigate the situation.

The solution to this vulnerability is to mandate all new RTS (and other DERs such as BESS, EVSE etc.) connections to have inverters with data loggers that will communicate with a server in India which could be managed by a GoI entity. There can be one mobile app or multiple apps (which are interoperable) that could transmit the solar generation data from the inverter to the GoI managed server. To address this structural risk, it may be timely for the CEA to define a national interoperable data architecture for DER telemetry, aligned with the emerging unified energy interface (UEI) and DER Device communication standards for IEEE 1547-2018 such as IEEE 2030.5, SunSpec Modbus or DNP3 to ensure secure, domestically governed data flows across all future deployments. This solution can be immediately implemented for all future DER connections with the grid while existing inverters may be modified/replaced within the next few years.

Smart Inverters

Smart inverters equipped with a communication module will play a pivotal role in modernizing distributed energy systems by enabling two-way communication between rooftop solar systems and the electricity grid. Unlike traditional inverters, smart inverters can autonomously adjust voltage and frequency, ride through disturbances, and provide grid support services such as voltage regulation and frequency response. Based on ISGF recommendation, the Bureau of Indian Standards (BIS) has adopted the IEEE 1547 – 2018 standards as IS 18968 -2025 which sets out the technical requirements for interconnection and interoperability of DERs with the grid. This standard ensures that smart inverters installed in India meet international benchmarks for safety, performance, and communication protocols. To enable real-time monitoring and control, smart inverters must support communication protocols like IEC 61850, IEC 60870-5-104, or Modbus, depending on the specific application and utility requirements.

Smart inverters form the operational backbone of a digitalized energy ecosystem offering the following critical functionalities:

- **Reactive Power Support:** They can inject or absorb reactive power to regulate grid voltage locally.
- **Voltage and Frequency Ride-Through:** They continue to operate during voltage/frequency disturbances, thus supporting grid stability.

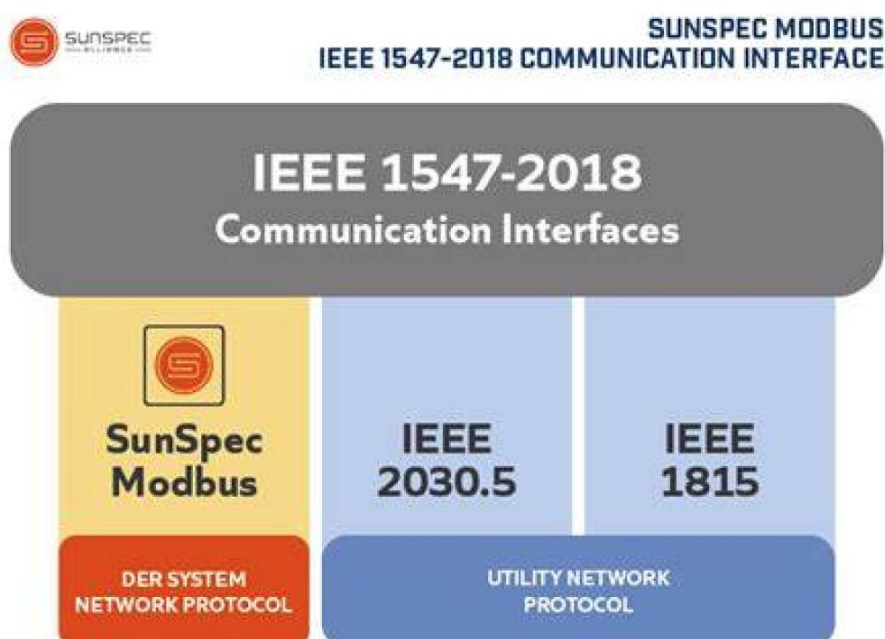
² Solarman is a Chinese company offering solar monitoring solution including the communication dongle at very cheap price (~\$14 per dongle for 25 years, though warranty is only for one year). It is believed that over 90% of solar inverters in India have monitoring solution from Solarman which is a huge risk to the Indian power system

- **Two-Way Communication:** These inverters are equipped with communication modules that allow real-time, bidirectional data flow with utilities and grid operators.
- **Remote Monitoring and Control:** Operators can send commands and receive status updates through secure interfaces.

Smart inverters can be fully autonomous, but they often require that inverters be connected to the local electric power system, via communication network, to produce appropriate responses for grid support based on varying conditions. The progression of smart inverter technologies and uptake enables a more dynamic and responsive grid including DERs, but it can also elevate the potential for cyberattacks through communications connectivity. The most common attack vector is through monitoring and control solutions. Solar inverters often use default passwords and lack physical tamper detection, which make them vulnerable for unauthorized access to the system. Spectre and Meltdown chip vulnerabilities enable attackers to seize passwords and other sensitive information. Additional vulnerabilities, such as remote code execution, stem from unpatched software and connecting solar systems to public facing networks.

To test and validate functionalities and compliance, ISGF has procured an 8 kW 3-phase smart inverter and delivered it to Underwriters Laboratories (UL) in Bangalore for testing against the IS 18968-2025 standard. This exercise is a critical step in ensuring that certified devices deployed in India meet the required specifications for grid interoperability and safety.

Communication interfaces for smart inverters per IEEE 1547 – 2018 is depicted below:



Conclusion

Currently, inverters which are predominantly produced in China are used throughout the world to connect solar panels and wind turbines to electricity grids. They are also found in batteries, heat pumps and electric vehicle chargers. Inverters are built to allow remote access for updates and maintenance. For larger systems, the utility companies install firewalls to prevent direct

communication back to OEMs in China, but this isn't the case for rooftop PV systems. As exposed by the DER Security Corp report, even systems with firewalls were vulnerable, especially in cases where rooftop systems owners are using the inverter OEM's mobile apps to monitor the solar generation.

ISGF recommends that the GoI may take immediate action to address this issue and mandate all inverters may be connected with data loggers that will communicate only to servers located within India, managed by Ministry of New and Renewable Energy (MNRE), CEA or any other government agencies.

From the cyber security perspectives, the following key measures are also necessary:

- Trusted Vendor policy for the power sector needs to be finalised on similar lines as that of the telecom sector. Although a trusted vendor does not guarantee a trusted product, it makes the vendor responsible for sanitising the product
- There must be a mechanism to track software bill of materials (SBOM) and supply chain contamination for critical assets installed in the power sector. It also needs to check hardware trojans which may be maliciously implanted in any critical asset
- During mandatory OT audit, the audit firms should be asked to do vulnerability assessment, log analysis and traffic analysis going in and out of the premises of the asset owner

APPENDIX -A

Shipments of Solar Inverters by major OEMS in India since 2015

SI No	Company	Solar Inverter Market Share in %								
		2015	2016	2017	2018	2019	2020	2021	2022	2023
1	Sungrow	-	-	2	6	15	25	24	28	36
2	Sineng	-	-	-	-	11	8	11	19	17
3	Fimer	-	-	-	-	12	17	12	14	17
4	TBEA	-	-	-	-	9	11	-	-	11
5	Ginlong Soils	-	-	-	-	3	2	3	8	4
6	Sofar	-	-	-	-	5	4	4	6	4
7	Growatt	-	-	-	-	4	3	3	5	3
8	Hypontech	-	-	-	-	-	-	-	-	3
9	Kehua	-	-	-	-	-	6	7	11	2
10	Huawei	3	7	10	15	20	20	20	3	-
11	GoodWe	-	-	-	-	2	3	5	3	-
12	TMEIC	22	19	16	10	13	-	11	2	-
13	Hitachi	5	5	5	3	3	-	-	-	-
14	Omron	13	12	13	15	-	-	-	-	-
15	Panasonic	7	7	8	11	-	-	-	-	-
16	Delta Energy Stystems	-	5	9	10	-	-	-	-	-
17	SMA	2	9	8	7	-	-	-	-	-
18	Tabuchi Electric	13	9	7	6	-	-	-	-	-
19	KACONew Energy	-	-	-	5	-	-	-	-	-
20	ABB	3	2	2	3	-	-	-	-	-
21	Fuji Electric	7	5	3	3	-	-	-	-	-
22	Nissan Electric	5	4	3	2	-	-	-	-	-
23	Shindengen	3	-	2	-	-	-	-	-	-
24	Daihen	4	3	-	-	-	-	-	-	-
25	Schnieder Electric	-	2	-	-	-	-	-	-	-
26	All Others	12	11	11	5	4	2	1	1	3
PV Inverter Shipments (MW_{AC})		9126	7509	6751	6092	9246	13083	16513	12355	21959

Source: Woodmac, 2024

Head Quarters and Manufacturing Locations of Inverter OEMs

Sl No	Company	HQ & Country	Manufacturing Location(s)
1	Sungrow	China	China
2	Sineng	China	China
3	Fimer	Italy	Italy, India
4	TBEA	China	China
5	Ginlong (Solis)	China	China
6	Sofar	China	China
7	Growatt	China	China
8	Hypontech	China	China
9	Kehua	China	China
10	Huawei	China	China, Vietnam
11	GoodWe	China	China
12	TMEIC	Japan/India JV	India, Japan
13	Hitachi	Japan	Japan, SE Asia
14	Omron	Japan	Japan, SE Asia
15	Panasonic	Japan	Japan, Malaysia
16	Delta Energy Systems	Taiwan	Taiwan, China, Thailand
17	SMA	Germany	Germany, China (JV)
18	Tabuchi Electric	Japan	Japan
19	KACO (post-Huawei)	Germany	China (under Huawei)
20	ABB	Switzerland	Italy, India, China (historical)
21	Fuji Electric	Japan	Japan
22	Nissan Electric	Japan	Japan
23	Shindengen	Japan	Japan

India Smart Grid Forum

CBIP Building, Malcha Marg, New Delhi

Website: www.indiasmartgrid.org | **Email:** contactus@indiasmartgrid.org | **Phone:** 011 4103 0398



@IndiaSmartGridForum

ISGF Research Report On Security Concern in Solar Inverters in India