

# Southern Europe PV Inverter Avoidance

Are non-European solar inverters a threat to Europe's Energy Autonomy?

The European Solar Manufacturing Council (ESMC) has issued a stark warning, highlighting a critical threat to Europe's energy autonomy stemming from the unregulated remote access capabilities of PV inverters produced by non-European, high-risk manufacturers--particularly those from China. A recent study by DNV substantiates these concerns.

Should ESMC restrict remote control of solar inverters sourced from 'high-risk non-European manufacturers'?

The European Solar Manufacturing Council (ESMC) has urged EU member states to restrict remote control capabilities of solar inverters sourced from "high-risk non-European manufacturers," primarily targeting Chinese firms, over alleged cybersecurity vulnerabilities linked to grid integration and software updates.

What are the cybersecurity challenges of PV installations in Europe?

A report by the European solar association SolarPower Europe highlights the cybersecurity challenges of PV installations in the European Union. A main concern are the vulnerabilities of connected inverters and data management via cloud services outside of Europe. From pv magazine France

Are Chinese inverters a threat to Europe's remote infrastructure?

ESMC Secretary-General Christoph Podewils warned that Chinese-made inverters, which account for 70% of new European installations in 2023 (with Huawei and Sungrow as dominant suppliers), now power over 200 GW of capacity--equivalent to "more than 200 nuclear plants"--stripping the continent of "critical remote infrastructure oversight."

Is software-enabled remote access to solar inverters a threat?

A recent study by DNV substantiates these concerns. As solar power becomes increasingly integral to Europe's clean energy goals and energy security, a major vulnerability looms: software-enabled remote access to PV inverters--the essential control units of solar power systems.

Could Chinese inverters shut down Europe's grid?

It is one of six Chinese vendors that collectively control over 219 GW. Given that Spain's grid collapsed after a 2.2 GW drop, these vendors could remotely shut down Europe's grid. Reports of rogue communication devices in Chinese inverters, allowing them to bypass firewalls, further highlight the need for action.

Web: <https://edukacja-aktywna.pl>

