

Press Release 2025-04-30

Restrict Remote Access of PV Inverters from High-Risk Vendors

The European Solar Manufacturing Council (ESMC) today issued a clear and urgent warning: Europe's energy sovereignty is at serious risk due to the unregulated and remote control capabilities of PV inverters from high-risk, non-European manufacturers – most notably from China. Study by DNV provides the evidence.

Brussels, 30 April 2025 - While photovoltaics (PV) play an increasingly central role in Europe's clean energy transition and energy independence, a hidden vulnerability threatens this progress: the software-based remote access to inverters, the critical "brains" of any PV system.

"Today, over 200 GW of European PV capacity is already linked to inverters manufactured in China – the equivalent of more than 200 nuclear power plants," said **Christoph Podewils**, the ESMC Secretary General. "This means Europe has effectively surrendered remote control of a vast portion of its electricity infrastructure."

The risk is not theoretical. Modern inverters are required to be connected to the internet to fulfill essential grid functions or to participate in the power market. However, these connections also allow for software updates – meaning any manufacturer can alter the performance of these devices remotely. This introduces significant cybersecurity threats, including the potential for deliberate interference or mass shutdowns. A recent DNV report, commissioned by SolarPower Europe, reinforces this concern and warns of the real possibility of cascading blackouts caused by malicious or coordinated inverter manipulation.

Further concerns include:

- **70% of all inverters installed in 2023 came from Chinese vendors**, mainly Huawei and SunGrow.
- These two companies alone already control **remote access to 168 GW of PV capacity in Europe** (DNV Report, p. 40).
- By 2030, this figure is projected to exceed 400 GW – comparable to the output of 150–200 nuclear power plants.
- **One of these vendors is already banned from the 5G sector** in many countries and is currently under investigation in Belgium for bribery and corruption.

In light of these findings, the ESMC calls for the immediate development of an EU "Inverter Security Toolbox", modeled after the successful 5G Security Toolbox. This would involve:

- A comprehensive risk assessment of inverter manufacturers.
- A requirement that high-risk vendors must not be permitted to maintain an online connection to European electricity systems.
- Consideration of outright bans for such vendors from connecting to the grid.
- A replication of Lithuania's proactive legislation - banning inverters from China - across all EU Member States – ensuring security measures apply to PV systems of all sizes.

“Europe must act now to prevent a future energy crisis that would rival the gas dependency on Russia,” said Podewils. “We support the European Commission’s upcoming assessment of cybersecurity risks in the solar value chain and are ready to contribute our expertise.”

About ESMC

The European Solar Manufacturing Council (ESMC) promotes solar manufacturing Made in Europe, the creation of a political environment to support industrial manufacturing and research while maintaining it at the top level globally. It promotes the development and investment in solar technology along the whole value chain (i.e. materials, wafer, modules, inverters and other electronic components) to assist high level system integration as well as production of equipment in Europe.

The ESMC represents around 70 companies and research organisations from all parts of the value chain. It is an international non-profit organisation registered under Belgian law.

Media Contact

Christoph Podewils, Secretary General ESMC
podewils@esmc.solar
+49 177 8741214