Statement: "Ban on High-Risk Inverter Suppliers from EU Funding"

On April 23, 2026, the European Commission issued a policy to restrict EU funding for "high-risk inverter vendors". A "high-risk supplier" is any company that is owned or controlled by companies from a third country that is guilty of malicious acts in cyberspace against the EU or one of its member states. The decision explicitly names China, Russia, Iran and North Korea. The decision covers inverters for all renewable energy applications (e. g. photovoltaics) and explicitly electricity storage systems with their "Power Conversion Systems" (PCS).

Press clipping:

- "EU Commission wants to force Chinese inverters out of EU-funded projects", pv-magazine.de (23 April 2026)
- "European Commission Halts Subsidies for Chinese Inverters," Spiegel.de (23 April 2026)
- "Subsidies for Inverters from China Halted — Fears of a Blackout," Handelsblatt.com (23 April 2026)
- "ESMC Welcomes EU Commission Decision: Inverters from High-Risk Countries Excluded from EU Funding", ESMC.solar

1. General conditions & problems

The decision comes at a time of global uncertainties, military conflicts and armament with both conventional weapons and in cyberspace. It is in line with the regulatory framework of recent years, such as the Cyber Resilience Act (CRA), the NIS-2 Directive, the EU AI Act ("AI Regulation") and the Radio Equipment Directive (RED), as well as the discussions on "digital sovereignty".

The decision follows numerous discussions that FENECON has actively followed and supported as part of its work in associations. Implementation in other EU countries is already taking up these new and other expected requirements — in some cases going even further.

Energy is critical infrastructure — just like telecommunications, for example. Here, manufacturers have already been banned in the past or their hardware must be removed. The reality is that it is estimated that around 80% of the inverters[1] installed in Europe now come from China — and are often permanently compounded with Chinese cloud services. With more than 117 GWp of installed photovoltaic capacity[2] in Germany alone, this corresponds to an output of approx. 93 GW, i. e. more than 50 modern nuclear reactors with an output of approx. 1.6 GW.

1.1. Why PV, battery inverters and energy management systems are critical:

As with any security issue, there is no such thing as 100 % protection; gaps and "predetermined breaking points" can be hidden in any component. However, PV, battery inverters and energy management systems are key components because they combine three unfavorable properties at the same time:

Large quantities are deployed

Millions of identical devices → a successful attack scales massively.

They are controlling, not just measuring

They actively intervene in the electricity grid (power, reactive power, frequency support, charging/discharging).

They form a communication network

Cloud connection, remote maintenance, APIs, aggregators.

Cyberattacks via networked energy infrastructure systems are real. Example: "Coordinated cyberattacks on Polish energy infrastructure in December 2025"

- Article in German
- Article in English incl. detailed incident report

1.2. General risk analysis

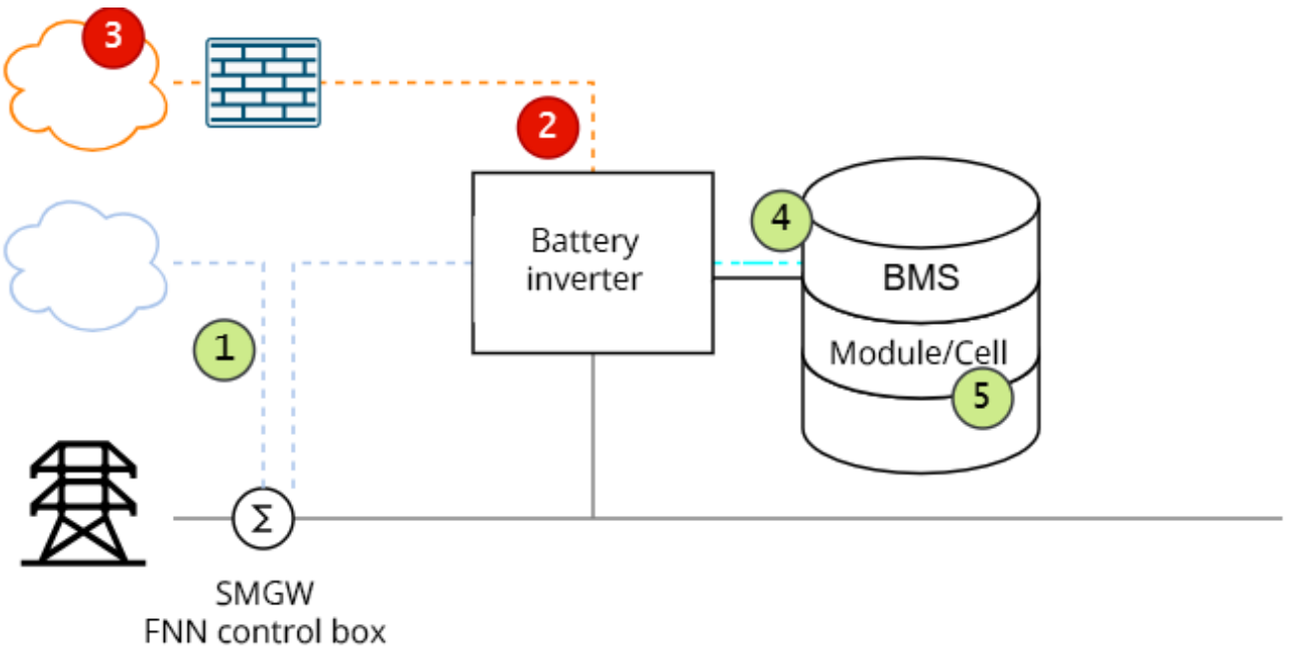

Abbildung 1. General risk analysis of energy storage systems

(1) BSI-compliant communication and control via market communication, metering point operators, smart meter gateway infrastructure and FNN control box:

- Risk: low

(2) Permanent, bidirectional internet connection to the manufacturer's cloud:

- For live monitoring, firmware updates, remote maintenance.
- Advanced optimizations (artificial intelligence, forecasting, timetable, etc.) from the cloud.
- Risk: high

(3) Manufacturer clouds are largely unregulated, without requirements such as KRITIS, ISO 27001, possibly NIS2, etc.

- These servers are often located in China or the USA or are subject to their sphere of influence (e. g. Amazon Web Services (AWS))
- Risk: high

(4) Internal communication between components, not cloud-connected:

- Risk: low

(5) Passive components such as battery cells/modules:

- Risk: low

2. FENECON "Cybersecurity by Design"

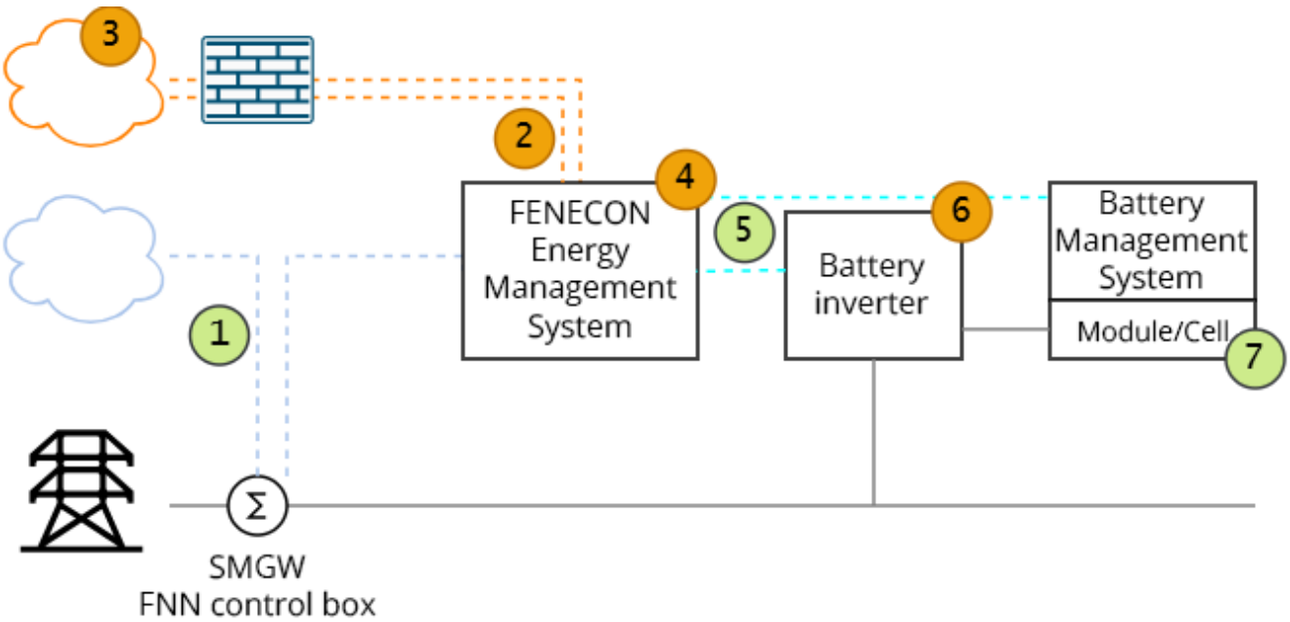

Abbildung 2. FENECON — Cybersecurity by Design

(1) Processing of critical grid commands (e. g.: dimming in accordance with §14a EnWG, curtailment, PV curtailment in accordance with §9 EEG) by the energy management system and forwarding to battery inverters or other controllable consumer equipment

- Risk: low

(2) Permanent, bidirectional internet connection to the FENECON cloud:

- For live monitoring, firmware updates (EMS, but also peripherals such as inverters and BMS), remote maintenance.
- Separate connections to third-party services (e. g. weather forecast, electricity prices from ENTSO-E, Tibber, etc.) enable individual firewall releases.
- Local AI models for forecasts and timetable optimization.
- Risk: medium

(3) FENECON cloud:

- in ISO-27001-certified data centers in Germany with a German data center operator; German jurisdiction
- Information security management system (ISMS) and reporting obligations in accordance with NIS2
- Risk: medium

(4) FEMS (FENECON Energy Management System):

- developed as open source software together with the "OpenEMS — Open Energy Management System" project in Germany; auditable.
- Permanent internet connection optional.

- Risk: medium

(5) Internal communication between non-cloud-connected components via physically separate networks:

- e.g. depending on the system, separate Ethernet LAN/VLAN or serial communication (RS485)
- Risk: low

(6) Internal components from third-party providers:

- Battery inverter from GoodWe (OEM with customized firmware) or Siemens/KACO, depending on the system
- Battery management system e. g. from Ampace/CATL
- Possible attack vector: infected firmware updates; risk reduced by disconnecting from the network or internet connection
- Risk: medium

(7) Battery cells from China. Passive components without permanent internet connection:

- Risk: low

2.1. How does FENECON deal with the topic of "cyber security in electrical energy storage and energy management"?

- Basic principle of "cyber security by design"
  - Reduction of cloud connections: No components other than FEMS are directly connected to the internet
  - Local AI optimization and algorithms: All functions are available as a fallback even without a (permanent) internet connection. In this case, there are limitations, e. g. for production forecasts based on the weather forecast and for exchange electricity tariffs. Variable high/low tariffs (e. g. "Octopus Go") can work completely offline.
  - Smart Meter Gateway (SMGW): The official, BSI-compliant (Federal Office for Information Security) way to control controllable consumer equipment ("SteuVE") is implemented via the SMGW with FNN control box. FEMS can already receive critical control commands (according to §14a EnWG) from the SMGW via relay contacts; we will present a deeper integration via EEBUS at EES 2026.
- Made in Germany
  - As a German company, we are subject to German liability law, German courts and German and European cybersecurity regulations (e. g. GDPR, NIS2, CRA)
  - In the event of a disaster, authorities have far-reaching access to companies — this reliability can only be practically implemented with German companies.
  - Buying from a German manufacturer like FENECON not only supports Germany as a business location with local added value, but also makes a direct contribution to internal and external safety and energy sovereignty.
- Open Source
  - The auditing of source code is an essential part of the verification test for operators of critical infrastructures (KRITIS) in accordance with Section 8a of the BSI Act (BSIG)
  - FENECON takes this one step further: by developing OpenEMS as the "open source operating system of the energy transition" together with a global community, we are committed to continuously improving the safety of the software used.
    i. Closed source means: "Trust us, we haven’t implemented anything harmful."
    ii. Open source means: Source code can be checked, security functions are transparent, security backdoors cannot be concealed
  - However, OpenEMS is not a monoculture, but is structured in such a way that different integrators can use it to build their own solutions. This leads to diversity in manufacturers, hardware and operating models and prevents the creation of a "single point of failure" or a central point of attack
  - "Is Open Source unsafe?"
    Security gaps do not arise from openness but through a lack of auditing.
- Simply spoken: The one who does not build the technology does not control it.
  - Inverters & EMS are not toasters. They are controllable network components and software-defined infrastructure.
  - If software, firmware, update servers are not subject to European laws:

→ No real control

- A market with 80 % dependency on imports of critical technologies is a risk, not a competition
- Monocultures are cheap when procured but expensive during crises
- "No German electricity grid must depend on foreign servers." Critical functions are to be implemented: locally, independent from cloud services, offline-capable (= "local control requirement")
- "What kind of energy supply gives us the capability to act in the event of a crisis?" Locally controllable, decentralized systems with: local protection logic, offline capability, clear liability

Stefan Feilmeier, Second Managing Director, 28/04/2026

[1] https://www.tagesschau.de/investigativ/monitor/solar-anlagen-sabotage-china-100.html, German

[2] https://www.energy-charts.info/downloads/Stromerzeugung_2025.pdf, Fraunhofer ISE: "Electricity production in Germany in 2025", German