

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

Die EU-Kommission hat am 23. April 2026 eine Policy zur Beschränkung von EU-Fördermitteln für "High-Risk Inverter Vendors" erlassen. Unter "High-Risk Supplier" fällt dabei jedes Unternehmen, das sich im Besitz von oder unter der Kontrolle von Unternehmen aus einem Drittland befindet, das sich im Cyberspace böswilliger Handlungen gegen die EU oder einen ihrer Mitgliedstaaten schuldig gemacht hat. Der Beschluss benennt dabei explizit die Länder China, Russland, Iran und Nordkorea. Der Beschluss umfasst Wechselrichter aller Erneuerbare-Energie-Anwendungen (z. B. Photovoltaik) und explizit Stromspeichersysteme mit ihren "Power Conversion Systems" (PCS).

Presse-Clipping:

- "EU-Kommission will chinesische Wechselrichter aus EU-geförderten Projekten drängen", [pv-magazine.de](#)
- "EU-Kommission stoppt Förderung von chinesischen Wechselrichtern", [Spiegel.de](#)
- "Förderung für Wechselrichter aus China gestoppt — Angst vor Blackout", [Handelsblatt.com](#)
- "ESMC Welcomes EU Commission Decision: Inverters from High-Risk Countries Excluded from EU Funding", [ESMC.solar](#)

1. Rahmenbedingungen & Problemstellungen

Der Beschluss fällt in eine Zeit globaler Unsicherheiten, militärischer Auseinandersetzungen und Aufrüstung sowohl mit konventionellen Waffen als auch im Cyberspace. Er reiht sich ein in die Regulatorik der letzten Jahre, wie dem Cyber Resilience Act (CRA), die NIS-2-Richtlinie, dem EU AI Act ("KI-Verordnung") und der Radio Equipment Directive (RED), sowie den Diskussionen zu "Digitaler Souveränität".

Der konkrete Beschluss folgt auf zahlreiche Diskussionen, die FENECON im Rahmen seiner Verbandsarbeit aktiv verfolgt und begleitet hat. Die Umsetzungen in anderen EU-Ländern greifen diese neuen und weiteren erwarteten Vorgaben bereits — teils auch weitergehend — auf.

Energie ist kritische Infrastruktur — genau wie z. B. Telekommunikation. Dort wurden bereits in der Vergangenheit Hersteller verboten bzw. müssen aktiv rückgebaut werden. Die Realität ist, dass Schätzungen zufolge ca. 80 % der in Europa verbauten Wechselrichter^[1] mittlerweile aus China kommen — und häufig dauerhaft mit chinesischen Cloud-Services verbunden sind. Bei mehr als 117 GWp installierter Photovoltaik-Leistung^[2] allein in Deutschland, entspricht das einer Leistung von ca. 93 GW also mehr als 50 modernen Atomreaktoren mit ca. 1,6 GW Leistung.

1.1. Warum gerade PV-, Batterie-Wechselrichter und Energiemanagementsysteme kritisch sind:

Wie bei jedem Sicherheitsthema, gibt es auch keine 100-%ige Sicherheit; Sicherheitslücken und "Sollbruchstellen" können in jedem beliebigen Bauteil versteckt werden. PV-, Batterie-Wechselrichter und Energiemanagementsysteme sind aber Schlüsselkomponenten, weil sie drei ungünstige Eigenschaften gleichzeitig vereinen:

Sie sind massenhaft im Feld

Millionen identischer Geräte → ein erfolgreicher Angriff skaliert massiv.

Sie sind steuernd, nicht nur messend

Sie greifen aktiv ins Stromnetz ein (Leistung, Blindleistung, Frequenzstützung, Laden/Entladen).

Sie sind vernetzt

Cloud-Anbindung, Fernwartung, APIs, Aggregatoren.

Cyberangriffe über vernetzte Energieinfrastruktur-Systeme sind real. Beispiel: "Koordinierte Cyberangriffe auf polnische Energieinfrastruktur im Dezember 2025"

- [Artikel auf Deutsch](#) 
- [Artikel auf Englisch inkl. detailliertem Incident Report](#) 

1.2. Allgemeine Risikoanalyse

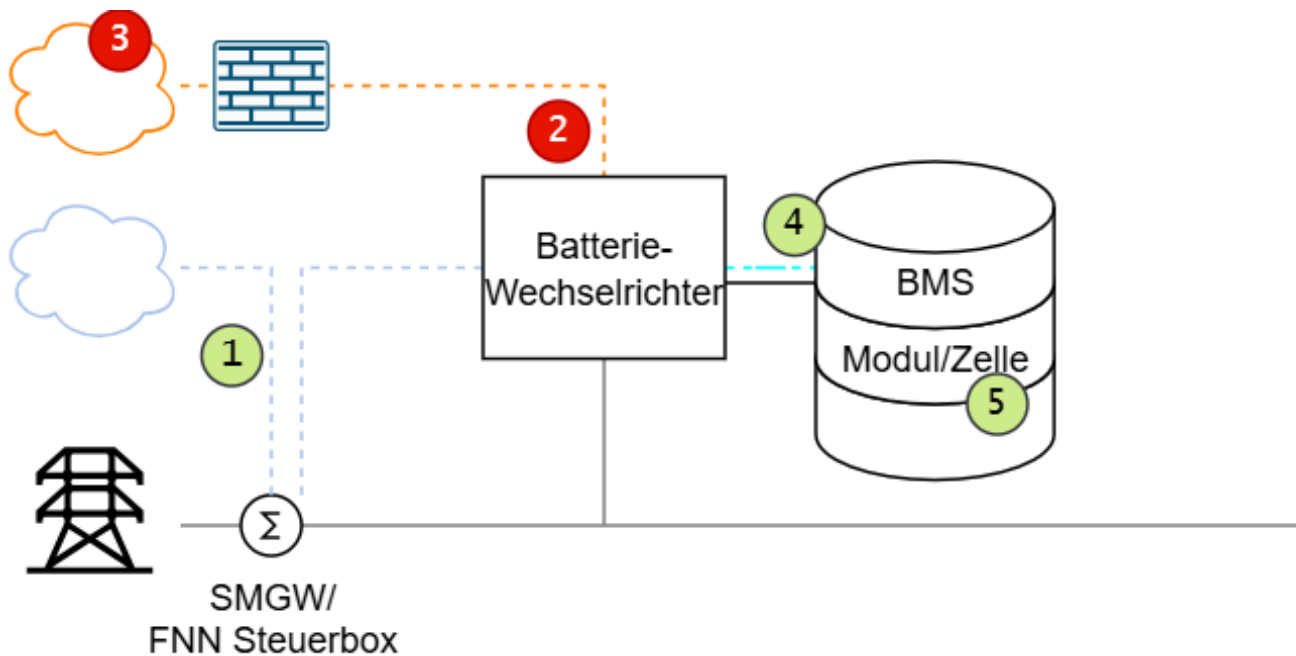


Abbildung 1. Allgemeine Risikoanalyse von Energiespeichersystemen

(1) BSI-konforme Kommunikation und Steuerung über Marktkommunikation, Messstellenbetreiber, Smart-Meter-Gateway-Infrastruktur und FNN Steuerbox:

- Risiko: **gering**

(2) Dauerhafte, bidirektionale Internetverbindung zur Hersteller-Cloud:

- Für Live-Monitoring, Firmware-Updates, Fernwartung.
- Erweiterte Optimierungen (Künstliche Intelligenz, Prognose, Fahrplan, etc.) aus der Cloud.
- Risiko: **hoch**

(3) Hersteller-Clouds sind weitgehend unreguliert, ohne Anforderungen wie KRITIS, ISO 27001, ggf. NIS2, etc.

- Diese Server stehen häufig in China oder USA oder unterliegen deren Einflussbereich (z. B. Amazon Web Services (AWS))
- Risiko: **hoch**

(4) Interne Kommunikation zwischen Komponenten, nicht Cloud-Connected:

- Risiko: **gering**

(5) Passive Komponenten wie Batteriezellen/-module:

- Risiko: **gering**

2. FENECON "Cybersicherheit by Design"

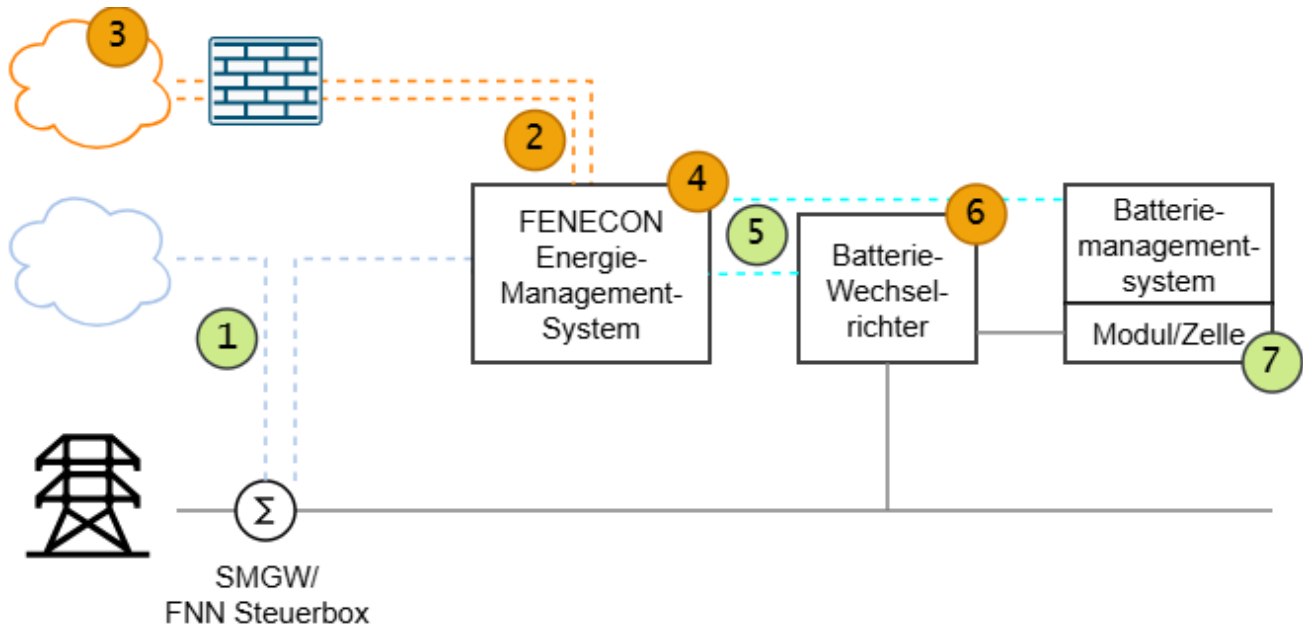


Abbildung 2. FENECON — Cybersicherheit by Design

(1) Verarbeitung kritischer Netzbefehle (z. B.: Dimmung nach §14a EnWG, Abregelung, PV-Abregelung nach §9 EEG) durch das Energiemanagement und Weitergabe an Batteriewechselrichter bzw. weitere SteuVE

- Risiko: **gering**

(2) Dauerhafte, bidirektionale Internetverbindung zur FENECON-Cloud:

- Für Live-Monitoring, Firmware-Updates (EMS, aber auch Peripherie wie Wechselrichter und BMS), Fernwartung.
- Separate Verbindungen zu Services von Dritt-Anbietern (z. B. Wetterprognose, Strompreise von ENTSO-E, Tibber, etc.) ermöglichen individuelle Firewall-Freigaben.
- Lokale KI-Modelle für Prognosen und Fahrplan-Optimierung.
- Risiko: **mittel**

(3) FENECON-Cloud:

- in ISO 27001-zertifizierten Rechenzentren in Deutschland mit deutschem Rechenzentrumsbetreiber; deutsche Gerichtsbarkeit
- Informationssicherheitsmanagementsystem (ISMS) und Meldepflichten nach NIS2
- Risiko: **mittel**

(4) FEMS (FENECON Energiemanagementsystem):

- als Open-Source-Software gemeinsam mit dem Projekt "OpenEMS — Open Energy Management System" in Deutschland entwickelt und auditierbar.
- Dauerhafte Internetverbindung optional.

- Risiko: **mittel**

(5) Interne Kommunikation zwischen nicht Cloud-Connected-Komponenten über physisch getrennte Netzwerke:

- z. B. je nach System separates Ethernet LAN/VLAN oder serielle Kommunikation (RS485)
- Risiko: **gering**

(6) Interne Komponenten von Drittanbietern:

- Batteriewechselrichter je nach System von GoodWe (OEM mit angepasster Firmware) oder Siemens/KACO
- Batteriemanagementsystem z. B. von Ampace/CATL
- Möglicher Angriffsvektor: infizierte Firmware-Updates; Risiko reduziert durch Trennung vom Netzwerk bzw. der Internetverbindung
- Risiko: **mittel**

(7) Batteriezellen aus China. Passive Komponenten ohne dauerhafte Internetverbindung:

- Risiko: **gering**

2.1. Wie geht FENECON mit dem Thema "Cybersicherheit in Stromspeichern und Energiemanagement" um?

- Grundprinzip "Cybersicherheit by Design"
 - Reduzierung der Cloud-Anbindungen: keine Komponenten außer FEMS sind direkt mit dem Internet verbunden
 - Lokale KI-Optimierung und Algorithmen: Alle Funktionen sind als Fallback grundsätzlich auch ohne (dauerhafte) Internet-Verbindung verfügbar. Einschränkungen ergeben sich in diesem Fall z. B. bei Erzeugungsprognosen basierend auf der Wettervorhersage und bei Börsenstromtarifen. Variable HT/NT-Tarife (wie z. B. "Octopus Go") können vollständig offline arbeiten.
 - Smart-Meter-Gateway (SMGW): Der offizielle, BSI-konforme (Bundesamt für Sicherheit in der Informationstechnik) Weg zur Steuerung von SteuVE (Steuerbare Verbrauchseinrichtungen) ist über das SMGW mit FNN-Steuerbox umgesetzt. FEMS kann bereits über Relaiskontakte kritische Steuerbefehle (nach §14a EnWG) vom SMGW entgegennehmen; eine tiefere Integration via EEBUS werden wir auf der EES 2026 vorstellen.
- Made in Germany
 - Als deutsches Unternehmen unterliegen wir dem deutschen Haftungsrecht, deutschen Gerichten und den deutschen und europäischen Verordnungen zur Cybersicherheit (z. B. DSGVO, NIS2, CRA)
 - In einem Katastrophenfall haben Behörden weitreichende Zugriffsmöglichkeiten auf Unternehmen — diese Verlässlichkeit ist nur bei deutschen Unternehmen praktisch umsetzbar.
 - Wer bei einem deutschen Hersteller wie FENECON kauft, unterstützt somit nicht nur den Wirtschaftsstandort Deutschland mit lokaler Wertschöpfung, sondern leistet einen direkten Beitrag zur inneren und äußeren Sicherheit und Energiesouveränität.
- Open-Source
 - Die Auditierung von Quellcode (Source Code Audit) ist ein wesentlicher Bestandteil der Nachweisprüfung für Betreiber Kritischer Infrastrukturen (KRITIS) nach § 8a des BSI-Gesetzes (BSIG)
 - FENECON geht hier einen Schritt weiter: indem wir — gemeinsam mit einer weltweiten Community — OpenEMS als das "Open-Source Betriebssystem der Energiewende" entwickeln, setzen wir uns maßgeblich für kontinuierliche Verbesserung der Sicherheit der eingesetzten Software ein.
 - i. Closed Source heißt: "Vertraut uns, wir haben nichts eingebaut."
 - ii. Open Source heißt: Quellcode ist prüfbar, Sicherheitsfunktionen sind nachvollziehbar, Backdoors sind nicht versteckbar
 - OpenEMS ist aber keine Monokultur, sondern so aufgebaut, dass verschiedene Integratoren daraus eigene Lösungen bauen können. Das führt zu Vielfalt bei Herstellern, Hardware und Betriebsmodellen und verhindert die Schaffung eines "Single-Point-of-Failure" bzw. eines zentralen Angriffspunkts
 - "Ist Open Source nicht unsicher?"
Sicherheitslücken entstehen nicht durch Offenheit, sondern durch fehlende Prüfung.
- Plakativ formuliert: Wer die Technik nicht baut, kontrolliert sie auch nicht
 - Wechselrichter & EMS sind keine Toaster, sondern steuerbare Netzkomponenten & software-definierte Infrastruktur

- Wenn Software, Firmware, Update-Server nicht unter europäischem Recht stehen:
→ keine echte Kontrolle
- Ein Markt mit 80 % Importabhängigkeit bei kritischer Technik ist kein Wettbewerb, sondern ein Risiko
- Monokulturen sind: billig im Einkauf — teuer im Krisenfall
- "Kein deutsches Stromnetz darf von einem ausländischen Server abhängen." kritische Funktionen müssen: lokal, cloud-unabhängig, offline-fähig sein (= "Local-Control-Pflicht")
- "Welche Energieversorgung macht uns im Krisenfall handlungsfähig?" lokal kontrollierbare, dezentrale Systeme mit: lokaler Schutzlogik, Offline-Fähigkeit, klarer Haftung

Stefan Feilmeier, Stv. Geschäftsführer, 28.04.2026

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

[2] https://www.energy-charts.info/downloads/Stromerzeugung_2025.pdf, Fraunhofer ISE: "Stromerzeugung in Deutschland im Jahr 2025" 