



Sicherheit für die Energiewende

Fronius International, Philipp RECHBERGER, 17.11.2025 Information Class: Public



Fronius

Österreichisches Familienunternehmen seit 1945

37 internationale Tochtergesellschaften



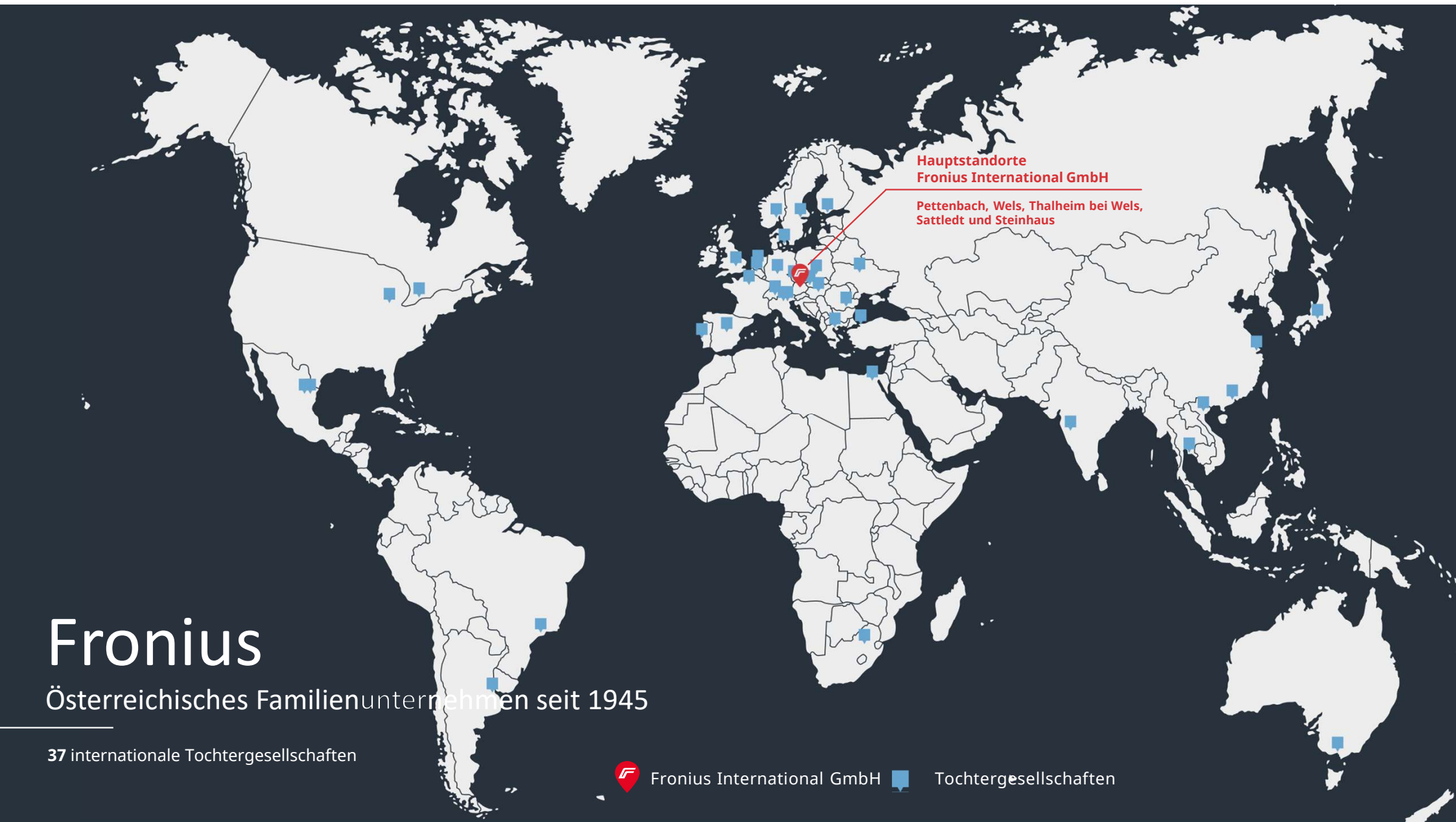
Fronius International GmbH



Tochtergesellschaften

Hauptstandorte
Fronius International GmbH

Pettenbach, Wels, Thalheim bei Wels,
Sattledt und Steinhaus





Solar & Energy

- Pionier im Bereich Erneuerbare Energie
- Vision „24 Stunden Sonne“

- Nachhaltige Ladelösungen
- Charge & Connect - Digitale Vernetzung der Ladetechnik

Wir forschen, entwickeln und produzieren selbst und schaffen Lösungen, die neue Perspektiven eröffnen: Egal, ob es um effizienten Solarstrom geht, um smarte Wege Batterien zu laden oder um die perfekte Schweißnaht.

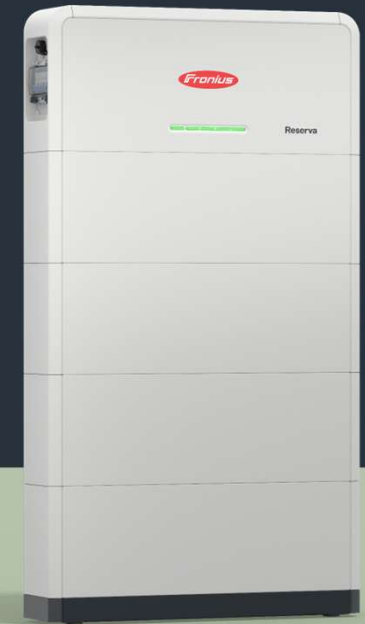
Heute für morgen:

Wir haben viel erreicht.

Mehr als **38 TWh**
erzeugte Energiemenge
jährlich

Mehr als **38 GW**
installierte Leistung

Rund **4 Mio.**
installierte Wechselrichter
weltweit



Energiesicherheit hat viele verschiedene Aspekte

CYBERSECURITY

DATENSICHERHEIT /
DATENSOUVERÄNITÄT /
„DATA RESIDENCY“

ENERGIE- SICHERHEIT

FERNSTEUERBARKEIT
DER KRITISCHEN
INFRASTRUKTUR

ETC.

IMPORTABHÄNGIGKEIT /
TECHNOLOGISCHE
SOUVERÄNITÄT

PHYSISCHER SCHUTZ DER
KRITISCHEN INFRASTRUKTUR
SICHERHEIT



Funktionen PV Wechselrichter



a) DC/AC-Wandlung, Einspeisung & **Netzstützung** ($P(U)$, $Q(U)$,...)



b) Lastmanagement

All-in-One Systeme
mit langfristiger Erweiterbarkeit und
Upgradefähigkeit (20 Jahre!)
vielfunktionalitäten,...)



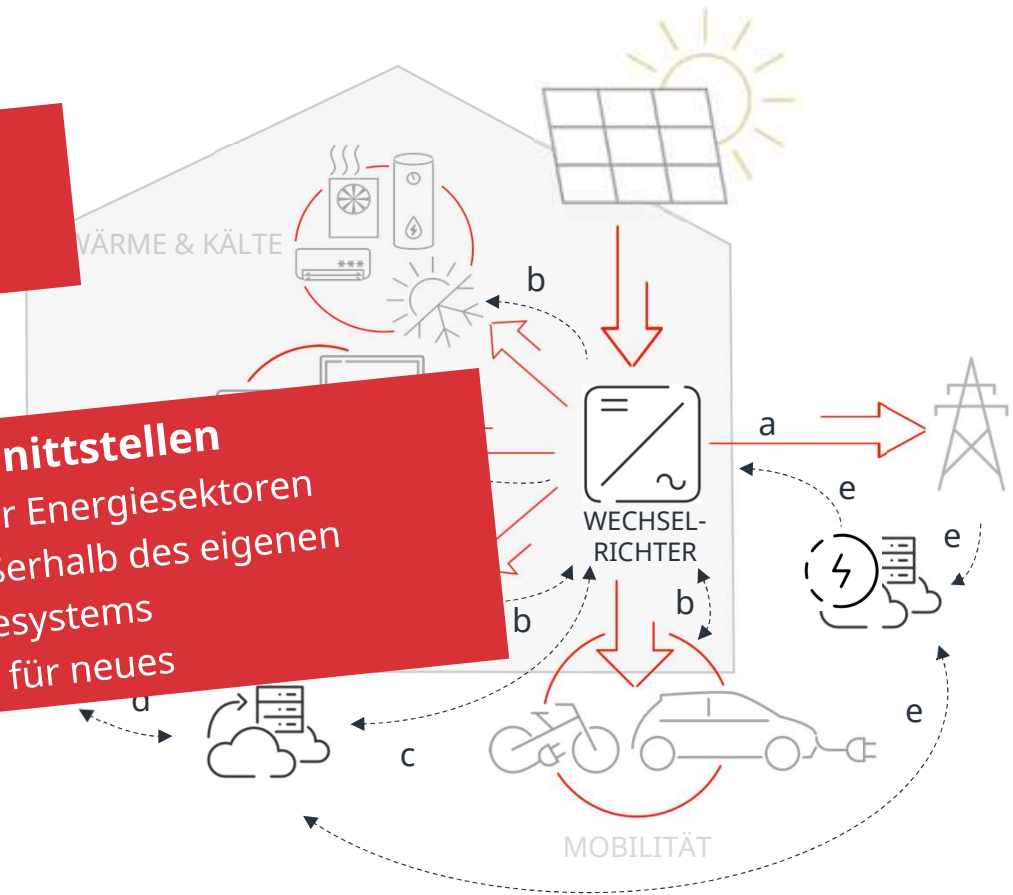
c) Messung zahlreicher Parameter
Datenmanagement



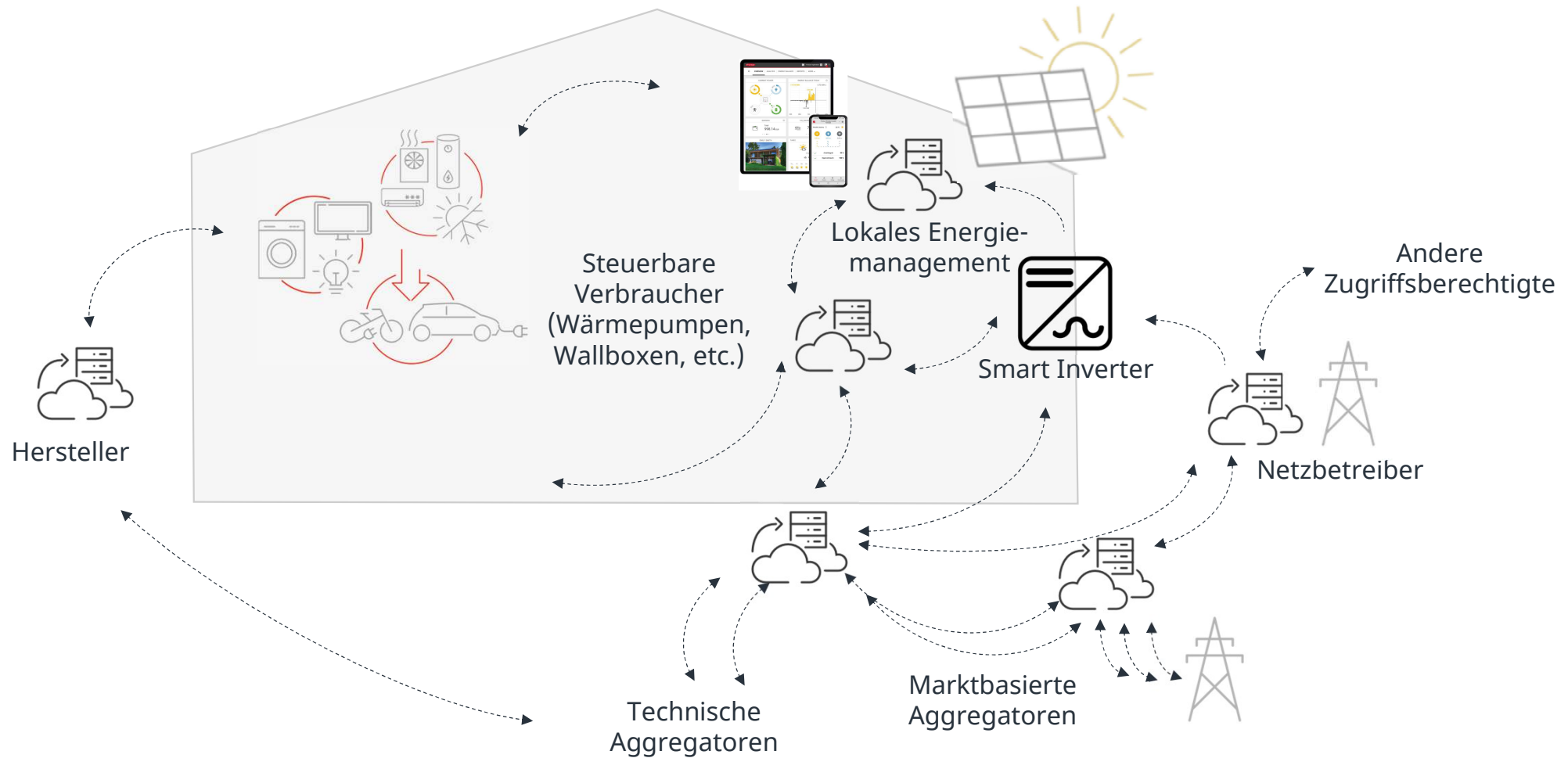
d) **Visualisierung**



e) Bereitstellung von **Flexibilitäten**
 („Demand Response“, VPP,...)



Rollen und Verantwortlichkeiten



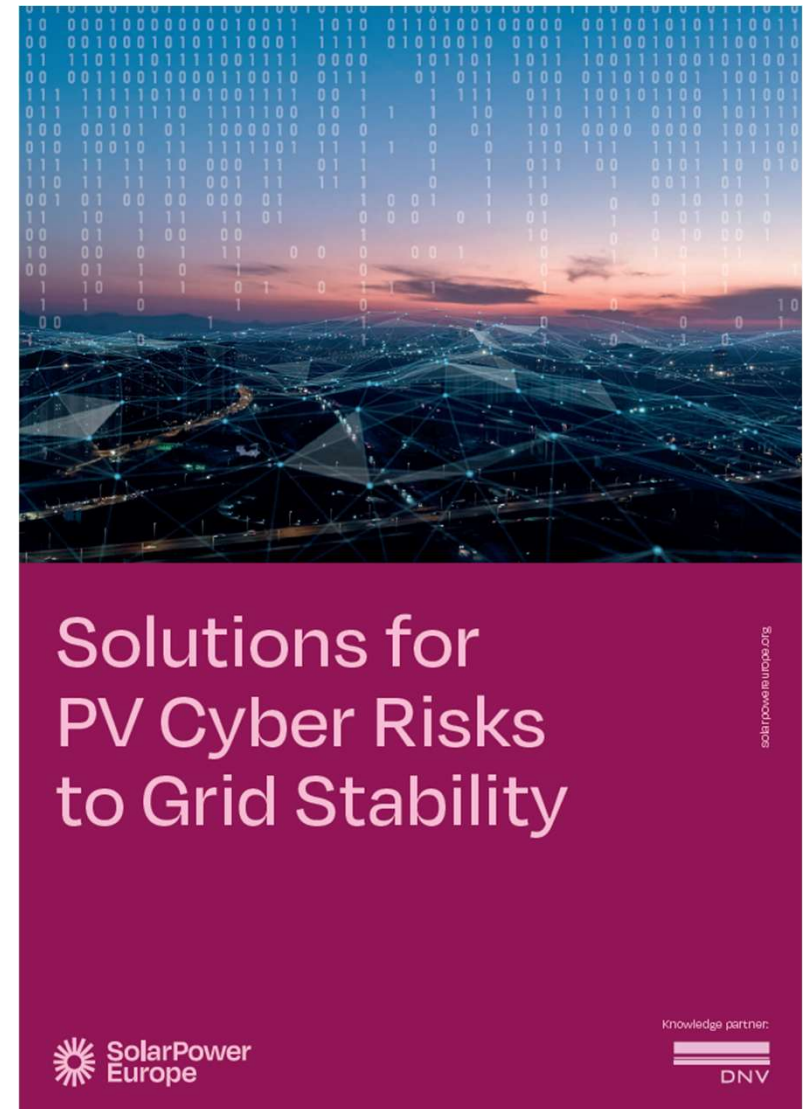
DNV-Studie

„...in Zusammenarbeit mit einem der vielen großen chinesischen Hersteller ist der Aufwand für einen groß angelegten Cyberangriff gering. ...

*In der Telekommunikationsbranche wurde im Zuge des Ausbaus der 5G-Infrastruktur in vielen Mitgliedstaaten Technologie von Anbietern verboten, die als „hochriskant“ gelten. Grundlage hierfür sind die Risikobewertungskriterien der von der Europäischen Kommission entwickelten 5G-Toolbox. Konkret umfasste dies das Verbot von 5G-Geräten [...]. **Zukünftig muss die Europäische Kommission entscheiden, ob das Konzept einer solchen Toolbox auf andere für die kritische Infrastruktur Europas relevante Technologien wie Wechselrichter ausgeweitet wird.** (S. 33)“*

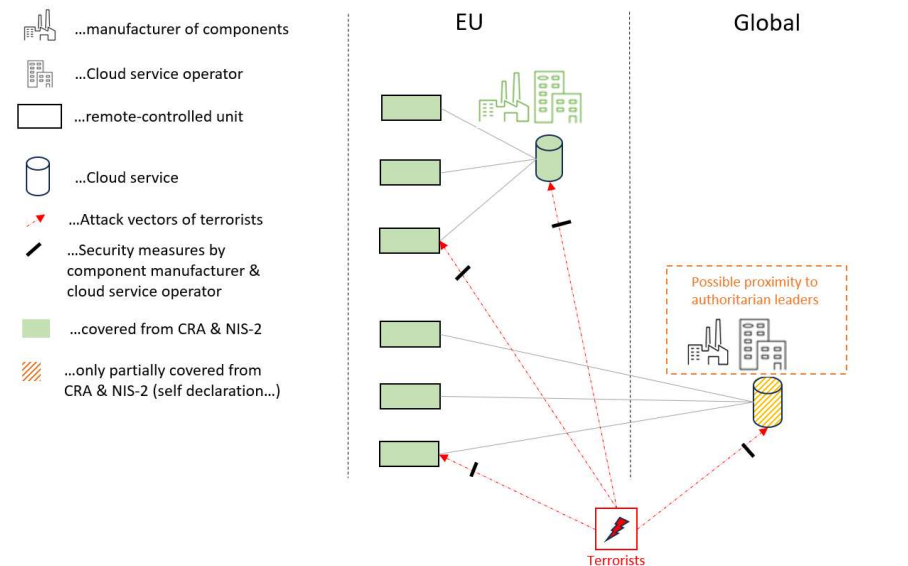
Quelle:

https://api.solarpowereurope.org/uploads/SPE_2025_Solutions_for_PV_Cyber_Risks_to_Grid_Stability_032dc2ae5a.pdf?updated_at=2025-04-29T07:11:32.315Z



Cybersicherheit

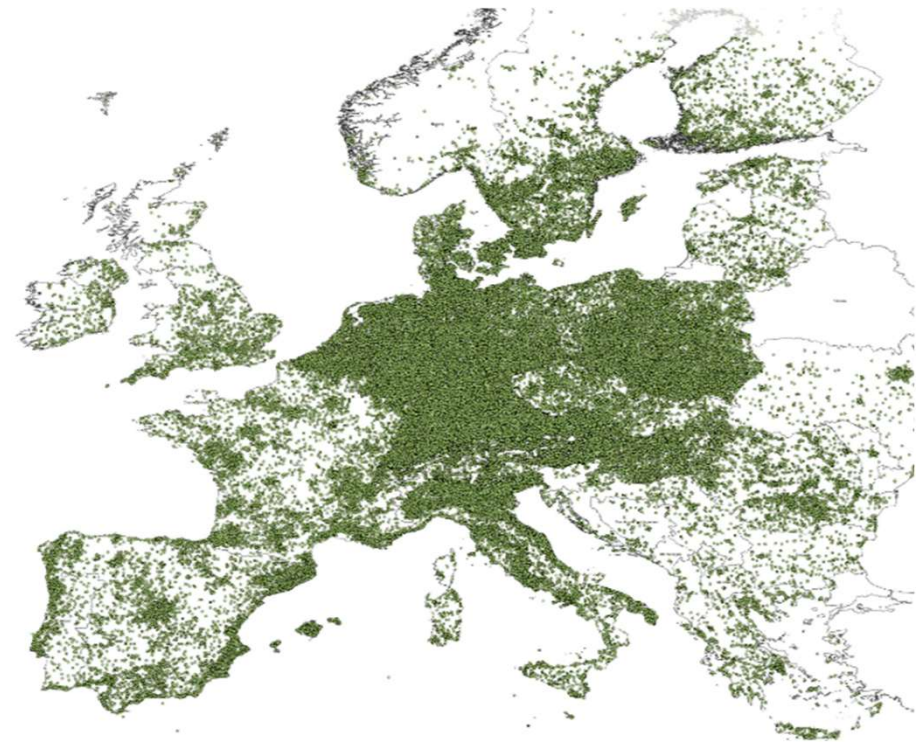
- Schutz von Produkten (und im Hintergrund Unternehmen und Dienstleistungen) vor Angriffen von Hackern, Terroristen usw. geschützt sind.
- Die Anforderungen an die Cybersicherheit sind in der EU bereits hoch. Laufend werden neue Gesetze und Vorschriften erlassen bzw. verschärft (CRA, NIS2,...).
 - Kontrolle und Haftung der Hersteller ist essentiell! Bei nicht in der EU ansässigen Unternehmen ist dies oft kaum möglich.
 - Von nicht in Europa ansässigen Herstellern sollte zumindest der selbe Standard nachweisbar gefordert werden (Beispiel NIS2...), wie von europäischen Herstellern.



Die Möglichkeiten der “Fernsteuerung” über ggf. bewusst manipulierte Softwareupdates wird meist nicht als Teil von Cybersecurity verstanden, bzw. könnten vorhandene Gesetze und Vorschriften dies nicht verhindern.

Fernsteuerbarkeit

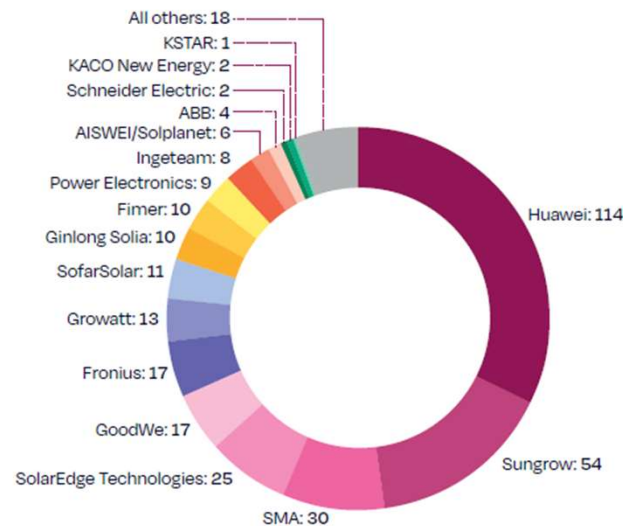
- Millionen von PV-Anlagen leisten heute schon einen wichtigen Beitrag zur europäischen Stromversorgung. Ihre Bedeutung wird weiter zunehmen und Wechselrichter werden damit zunehmend Teil der kritischen Infrastruktur.
- Alle modernen Wechselrichter verfügen über die Möglichkeit einer Online-Verbindung worüber **Software-Updates** und Steuerbefehle durchgeführt werden können.
- Hersteller sind damit für das Verhalten der PV-Anlagen mitverantwortlich und können diese aus der Ferne abschalten und bspw. kritisches Verhalten auslösen.
- Die Hoheit über die Fernsteuerung von Millionen Einheiten und damit indirekt dem Stromnetz geht damit einher.



Übersicht von PV-Systemen mit Fronius Wechselrichtern mit Online-Verbindung

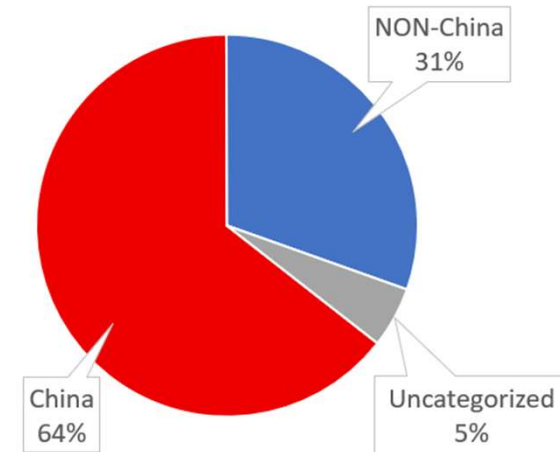
Versteckte Abhängigkeit

- Europa verfügt über **350 GW installierte Photovoltaik-Leistung** (Stand 2023)
- **219 GW** oder 64 % der europäischen Photovoltaik-Leistung **nutzen Wechselrichter chinesischer Unternehmen (114 GW von einem einzelnen Hersteller!)**
- Manipulation großer Leistungen stellt ein Sicherheitsrisiko für die Stromversorgung dar:
 - **0,05 – 0,1 GW** → Lokaler Blackout im Verteilnetz
 - **> 1 GW** → Regionaler Blackout im Übertragungsnetz
 - **2 – 4 GW** → Überregionaler Blackout im Übertragungsnetz



PV Inverter shipments to Europe over 2015-2023 in GW_{ac} (total 350 GW_{ac})

Quelle: DNV, S. 40

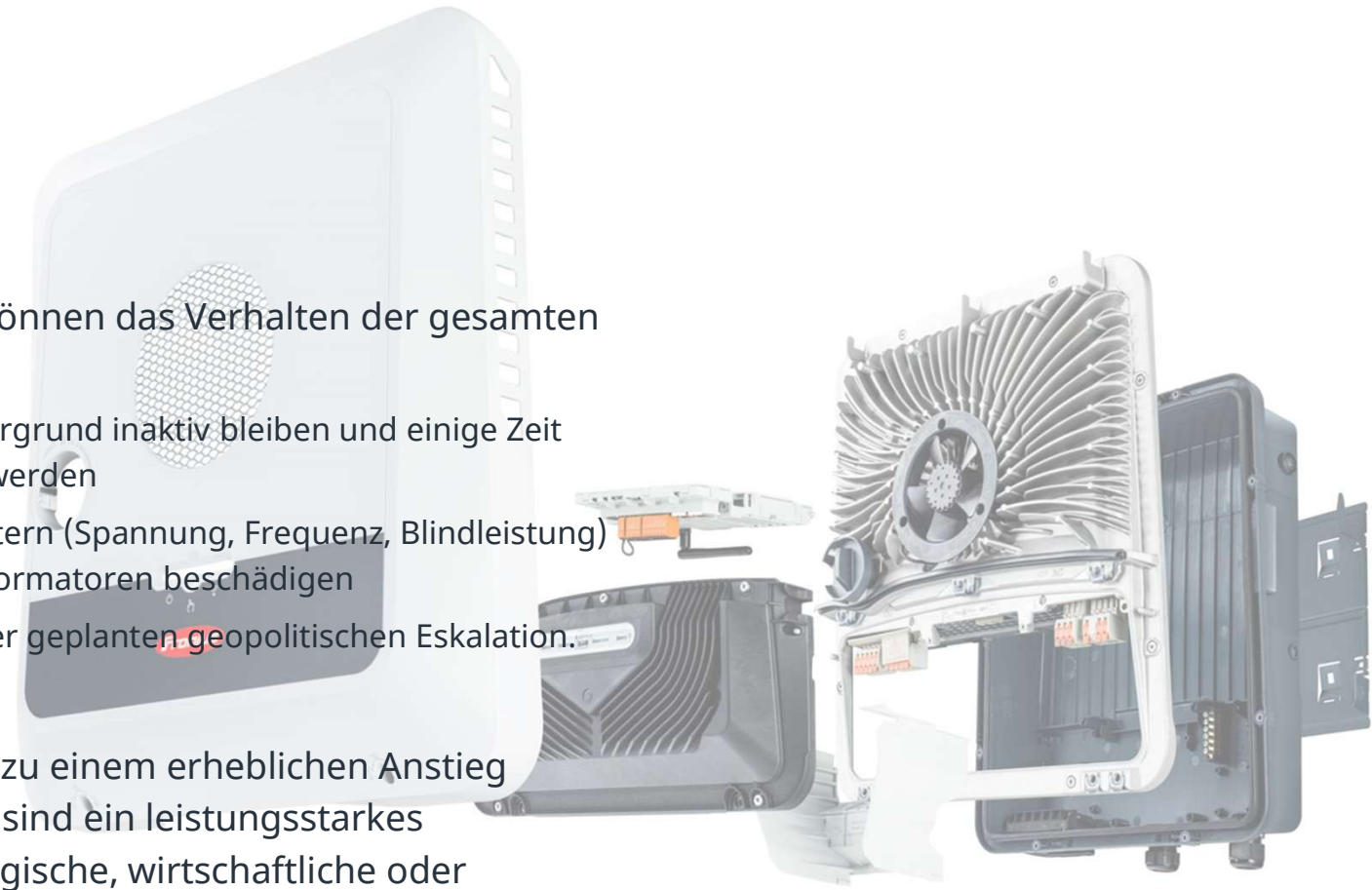


PV Inverter Shipments to Europe over 2015-2023, grouped by country of origin

Eigene Darstellung, basierend auf DNV, S. 40

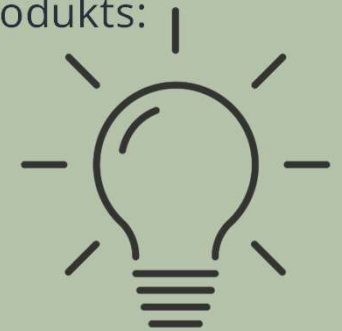
Risiken

- **Sabotage Risiko:** Firmware-Updates können das Verhalten der gesamten installierten PV-Flotte verändern.
 - Bösertige Funktionen können im Hintergrund inaktiv bleiben und einige Zeit nach dem Update aktiviert/ausgelöst werden
 - Böswilliges Verhalten von Wechselrichtern (Spannung, Frequenz, Blindleistung) kann wichtige Infrastruktur wie Transformatoren beschädigen
 - Beispielsweise in Abstimmung mit einer geplanten geopolitischen Eskalation.
- **Spionage Risiko:** Digitalisierung führt zu einem erheblichen Anstieg sensibler Betriebsdaten. Energiedaten sind ein leistungsstarkes Informationsinstrument, das für strategische, wirtschaftliche oder militärische Zwecke genutzt werden kann.
 - Hochauflösendes Bild des Energiesystems
 - Standort und das Verhalten sensibler Anlagen: Strategisch wichtige Netzknoten, Große industrielle Verbraucher, Militäranlagen...



Sinnvolle Vorkehrungen

- Hoher Fokus auf Produktsicherheit beginnt bereits vor der Entwicklung eines neuen Produkts:
 - **security by design**
 - **security by default**
- Regelmäßige Audits und Zertifizierungen auf **Produkt- und Unternehmensebene**
 - Bspw. **Radio Equipment Directive**, ETSI EN 303 645, UL 2941, CRA, etc.
 - **ISO 27001** (für Menschen, Prozesse und Technologie)
 - **NIS 2** (relevant nur für große europäische Hersteller)
 - **Cyber Resilience Act**
- Datenstandorte: ausschließliche **Nutzung europäischer Server und Clouds** zur Datensicherheit
 - **Remote Control** nur innerhalb Europas
 - Datenschutz und -trennung: **Kundendaten und Systemdaten** werden **getrennt gespeichert**, um Cyberangriffe zu vermeiden
- Bewusstseinsbildung und **Sensibilisierung für Cyberkriminalität**



Empfehlungen



- (1) Erkennen von **Parallelen in Bezug auf die Bewertung von Risikopotenzialen im Telekommunikationssektor** und Nutzung der dafür entwickelten Instrumente:
- Einführung einer „**EU toolbox for inverter security**“ (in Anlehnung an die „EU toolbox for 5G security“)
 - Durchführung einer Risikoanalyse von Unternehmen (Herstellern, Aggregatoren,...) und ergreifen von entsprechenden Maßnahmen.



- (2) Die europäische Gesetzgebung zur Cybersicherheit sollte **Anbieter von Dienstleistungen und Technologien aus Nicht-EU-Ländern** (z. B. Komponentenhersteller, Betreiber von Cloud-Diensten usw.) mindestens **genauso zur Verantwortung ziehen wie europäische Anbieter!**



- (3) **Datensouveränität:** Europa sollte einen Ansatz anwenden, der lokalen/europäischen Souveränität bei der Speicherung, Nutzung und Weitergabe **relevanter Energiedaten** Vorrang einräumen! (wie bspw. in den USA, Australien und sogar China)



- (4) **"Energiesicherheit und heimische Wertschöpfung: Eine starke Verbindung"**
- Europa ist technologisch bei Wechselrichtern an der Spitze und hat noch große (und auch ungenutzte) Fertigungskapazitäten. Wir sollten diese Stärken nutzen!
 - **Einsatz von Produkten und Technologien mit hoher europäischer Wertschöpfungstiefe!**
 - Dies verringert die Abhängigkeiten von China, steigern die Energiesicherheit, Souveränität, Resilienz, schafft technologische Innovationen und Arbeitsplätze!



Philipp RECHBERGER
rechberger.philipp@fronius.com
+43 664 88635266

Fronius International
Solar & Energy
System Integration and Energy Solutions

Froniusplatz 1
4600 Wels
Austria

All information is without guarantee in spite of careful editing –
liability excluded.

Intellectual property and copyright: all rights reserved.
Copyright law and other laws protecting intellectual property
apply to the content of this presentation and the documentation
enclosed (including texts, pictures, graphics, animations etc.)
unless expressly indicated otherwise. It is not permitted to use,
copy or alter the content of this presentation for private or
commercial purposes without explicit consent of Fronius.