Cybersicherheit kritischer Infrastrukturen

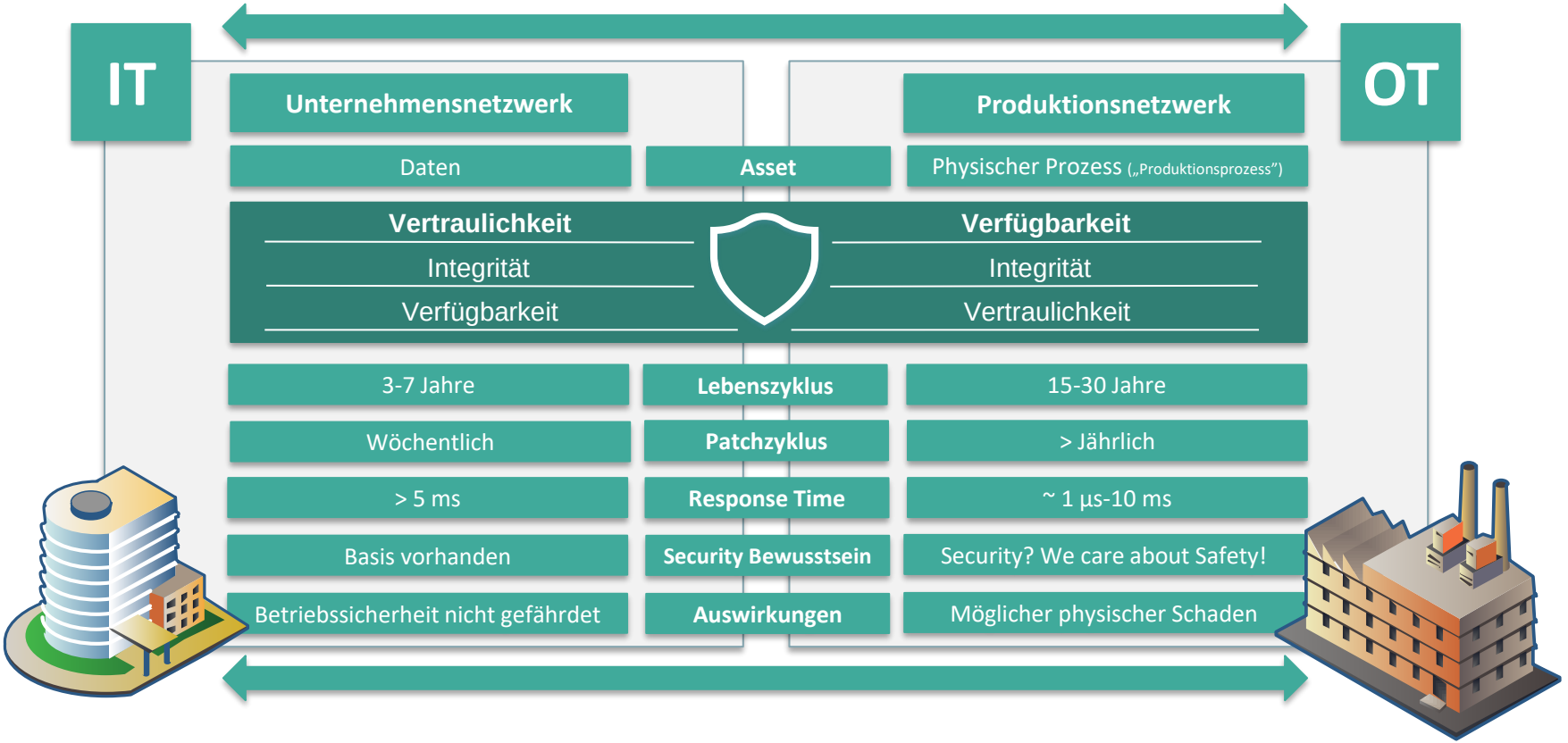
Risiken und Folgen von Angriffen auf das Stromnetz

Matthias Eckhart, Stefan Übermasser

EUROSOLAR AUSTRIA, 21.08.2025

Information Technology vs. Operational Technology

Ein Vergleich

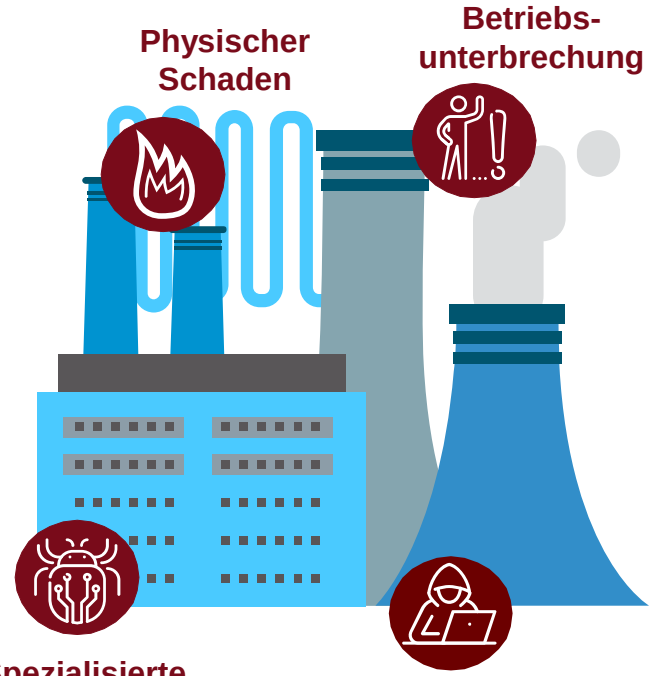


Zunehmende Bedrohung durch cyber-physische Angriffe

- Cyberangriffe auf industrielle Steuerungssysteme können die Sicherheit gefährden, Umwelt schädigen und industrielle Prozesse stören (z.B. Blackout)
- **Besonderheiten** von industriellen Steuerungssystemen erfordern spezielle Sicherheitsmaßnahmen:
  - Hohe Anforderungen bzgl. Verfügbarkeit & Performance
  - > 10 Jahre Lebensdauer der Komponenten
  - Proprietäre Technologien, oft inhärent unsicher
  - Begrenzte Systemressourcen für Sicherheitsmechanismen

Security by Design

Sicherheit darf kein nachträglicher Gedanke sein, sondern muss von Anfang an fest im Lebenszyklus verankert werden. Nur so lassen sich Schwachstellen frühzeitig vermeiden und robuste, resiliente Systeme schaffen. (Eckhart et al., 2019)



Industrie 4.0 treibt die digitale Transformation voran

…bringt jedoch auch eine Vielzahl neuer Angriffsvektoren mit sich

Robotik

- „Gold Plating“ birgt Sicherheitsrisiken
- Spoofing von Sensordaten (z.B. Kamera, LiDAR)
- Angriffe auf die Supply Chain (wenige Hersteller)

Big Data & Cloud

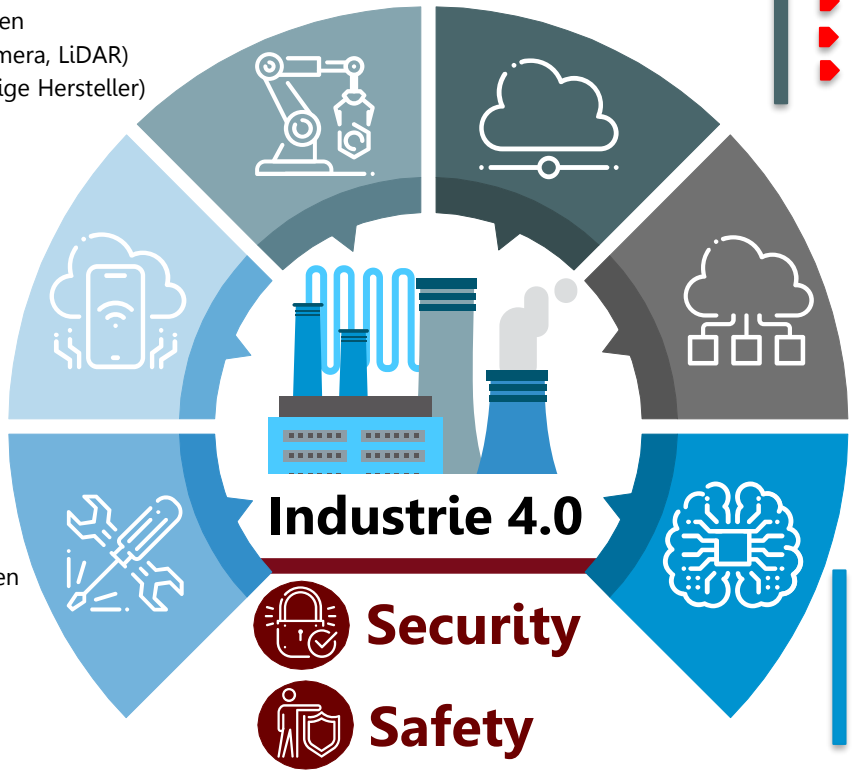
- Abhängigkeit von Drittanbietern
- Risiko des „Vendor Lock-in“
- Ausfallrisiko von Cloud-Dienstleistern

Konnektivität & IoT

- Vergrößert die Angriffsfläche
- IoT Geräte: Attraktive Angriffsziele
- Internetanbindung von Altsystemen

Edge Computing

- Unsicher durch begrenzte Ressourcen
- Inkonsistente Sicherheitskonzepte
- Komplexe Gerätelandschaft



Fernwartung

- Einschleusen manipulierter Updates
- Industriespionage mittels Telemetriedaten
- Sabotage durch direkten Fernzugriff

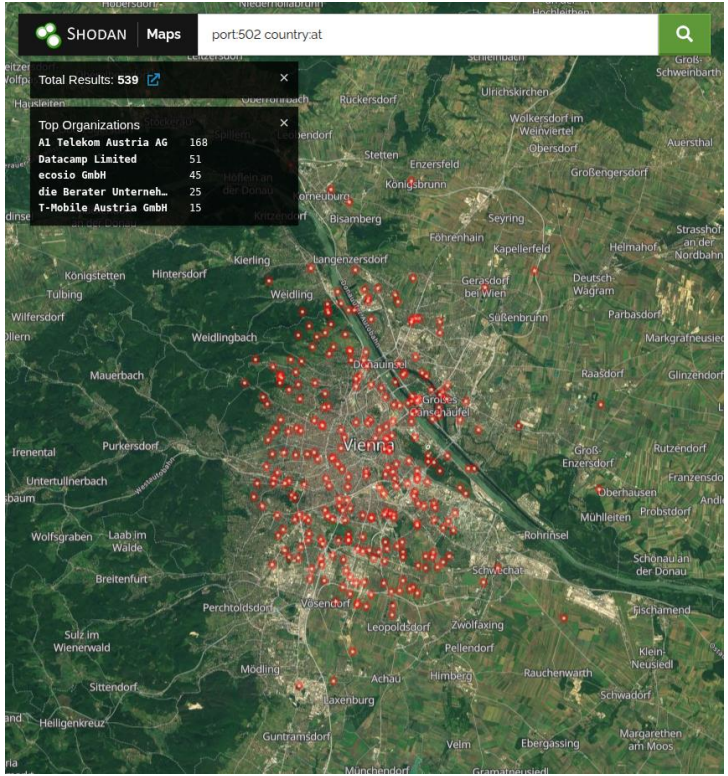
Künstliche Intelligenz

- Backdoors in den Trainingsdaten
- Datenleck durch LLMs (à la ChatGPT)
- Rückgewinnung sensibler Trainingsdaten

Industrielle Steuerungssysteme im öffentlichen Netz

Shodan.io, FOFA.info, …

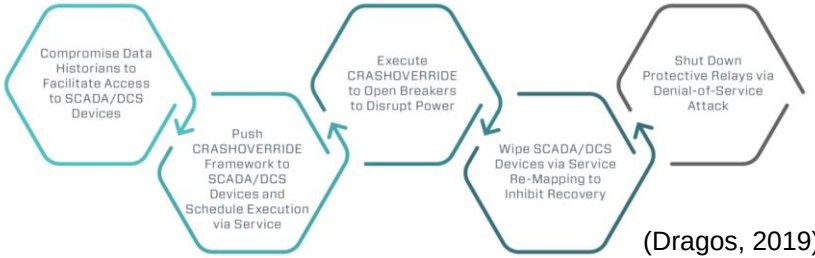
- Unterschiedliche Systeme leicht auffindbar:
  - Speicherprogrammierbare Steuerungen (u.a. von Kraftwerken)
  - Windräder, Photovoltaiksysteme
  - Ampelsteuerungen
  - Ladestationen für Elektrofahrzeuge
  - Kameras
- **Umfangreiche APIs**, die verschiedenste Abfragen unterstützen:
  - `port:502 country:AT`
  - `"authentication disabled" "RFB 003.008"`



CRASHOVERRIDE / Industroyer

Angriff auf das Ukrainische Stromnetz

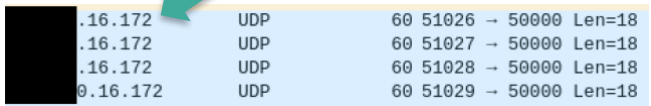
- Modulare Schadsoftware, gezielt für industrielle Steuerungssysteme in Stromnetzen entwickelt
- **Primärziel:** Längerfristiges Blackout (destruktiver Zweck im Vordergrund)
- **Einsatz:** Angriff auf Umspannwerke in Kiew am 17. Dezember 2016 (Entdeckung 2017)
- **Fähigkeiten:**
  - Nutzung von IEC 60870-5-101/-104-Modulen (potenziell einsetzbar gegen Betreiber in Europa, Nahost, Asien)
  - DoS-Angriff auf 4 Siemens SIPROTEC-Schutzrelais nach Öffnen der Leistungsschalter + Wiper-Angriff
- **Auswirkung:** Blackout in Teilen von Kiew (~1 h)



(Dragos, 2019)

Endianness Bug

(Dragos, 2019)



SIPROTEC-Schwachstelle:

- Auslösbar durch ein UDP:50000-Paket
- Versetzt System in Firmware-Update-Modus → Betrieb ohne Schutzfunktion
- Ausnützung der CVE-2015-5374 Schwachstelle schlug fehl

Sicherheitsrisiken von PV-Wechselrichter

Gefahren für das Stromnetz

Marktlage

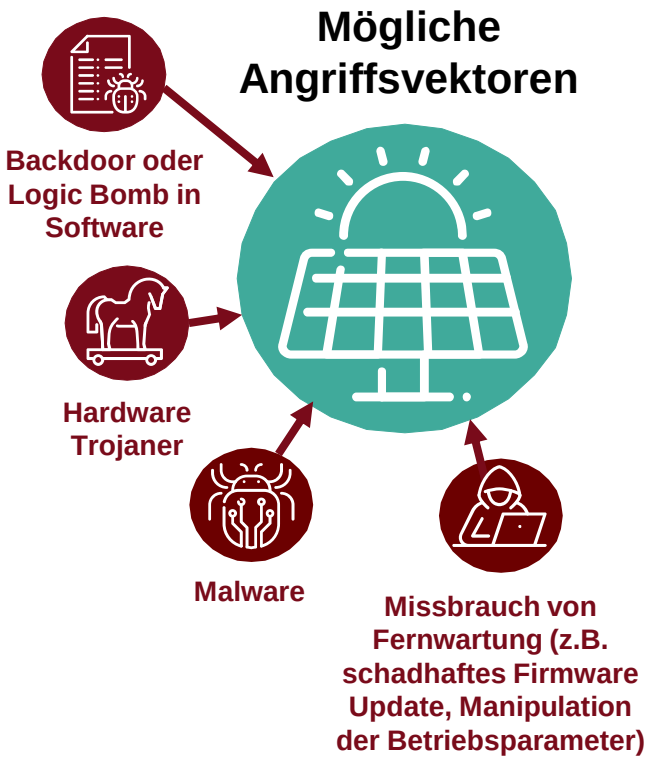
- Markt wird dominiert von Herstellern aus Nicht-EU-Ländern
- Starke Abhängigkeit von ausländischen Lieferketten

Potenzielle Bedrohung

- PV-Wechselrichter sind IoT-Geräte: Konnektivität und Cloud-Dienste als Einfallstor
- Gezielte Angriffe könnten großflächige Blackouts auslösen

Cyber-Risiken

- Hersteller-Seite: Staatliche Einflussnahme, Insider
- Lieferkette: Kompromittierte Komponenten
- Externe Angreifer



“Cyber Accumulation”

Kumulative Cyber Risiken

- **Diversität** in der Natur stärkt die Resilienz
- „Technologielandschaften“ sind jedoch zunehmend homogen
- Im Gegensatz zu Naturkatastrophen, sind Cyber-Risiken nicht geografisch gebunden
- Durch die **Homogenität** der Systeme sowie **Wechselwirkungen bzw. Abhängigkeiten** zwischen Schwachstellen, Diensten, und Unternehmen könnten sich Cybergefahren global rasch ausbreiten

Welche möglichen Gegenmaßnahmen gibt es?

1) “Nähe” (Proximity) als möglichen Indikator:
   - Logische Nähe: Gemeinsame Komponenten/Architekturen
   - Zeitliche Nähe: Mehrere Systeme können in kurzer Abfolge ausfallen
   - Kausale Nähe: Anfälligkeit von Systemen aufgrund starker Abhängigkeiten voneinander
2) Regulierungen

(Coburn et al., 2018)

Referenzen

(Coburn et al., 2018) Coburn, A. and Leverett, E. and Woo, G. “Solving Cyber Risk: Protecting Your Company and Society”. John Wiley & Sons, December 2018.

(Dragos, 2019) Dragos, Inc., “CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack”, Aug. 2019.

(Eckhart et al., 2019) Eckhart, M., Ekelhart, A., Lüder, A., Biffl, S., & Weippl, E. “Security development lifecycle for cyber-physical production systems” In IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society (Vol. 1, pp. 3004-3011). IEEE. October 2019.

(SolarPower Europe, 2025) SolarPower Europe, „Solutions for PV Cyber Risks to Grid Stability” 2025.

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

PV-POWERPLANT PORTFOLIO

Daten & Cybersecurity

PV SHARE OF INSTALLED POWER IN THE NATIONAL POWER PLANT PORTFOLIO

AUSTRIAN INSTITUTE OF TECHNOLOGY

Installed PV Power in Europe 2024:

~338 GW

Total installed power in Europe:

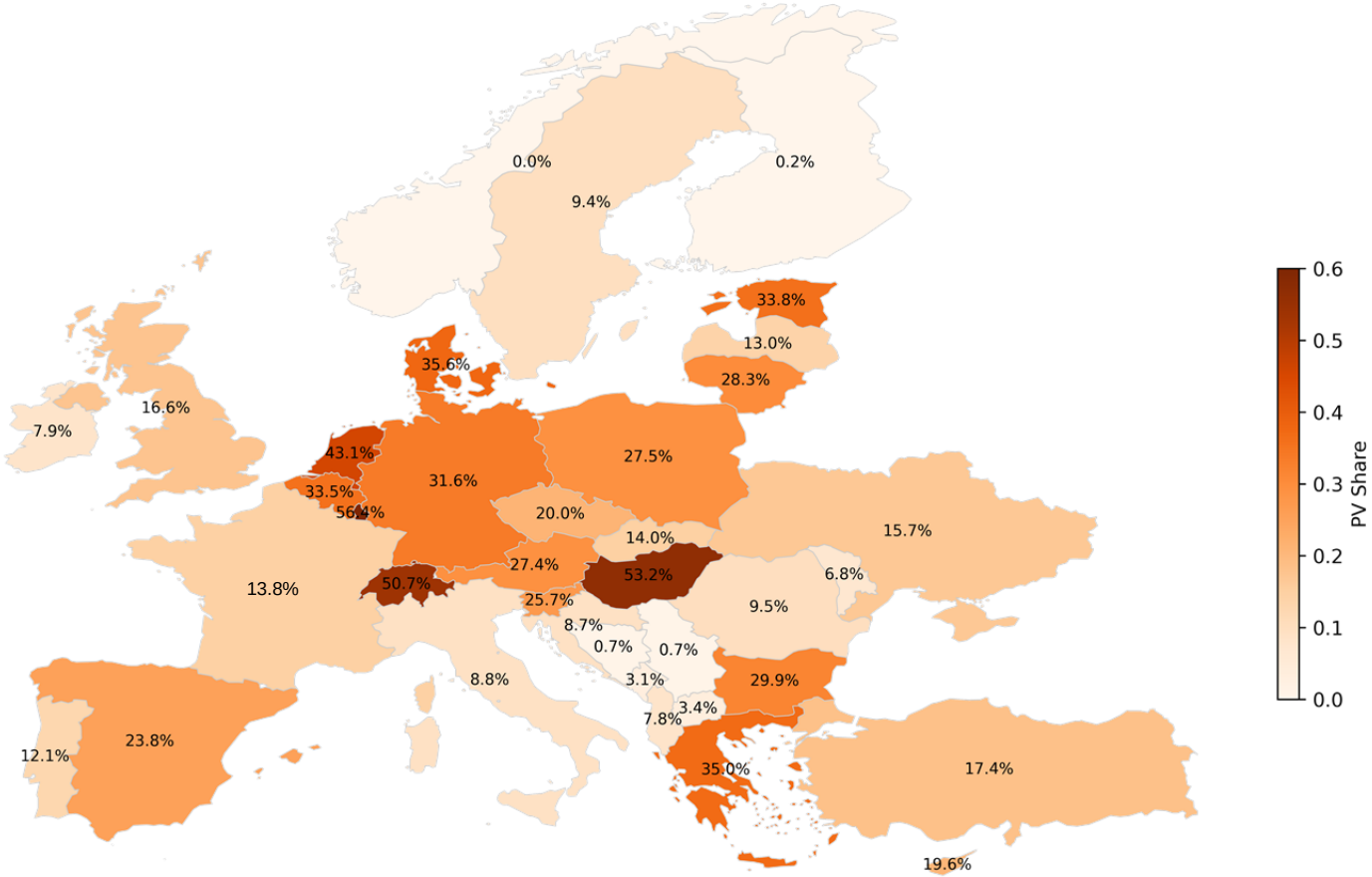
~1455 GW

Overall PV Share:

~23%

Overall renewables share:

~47%

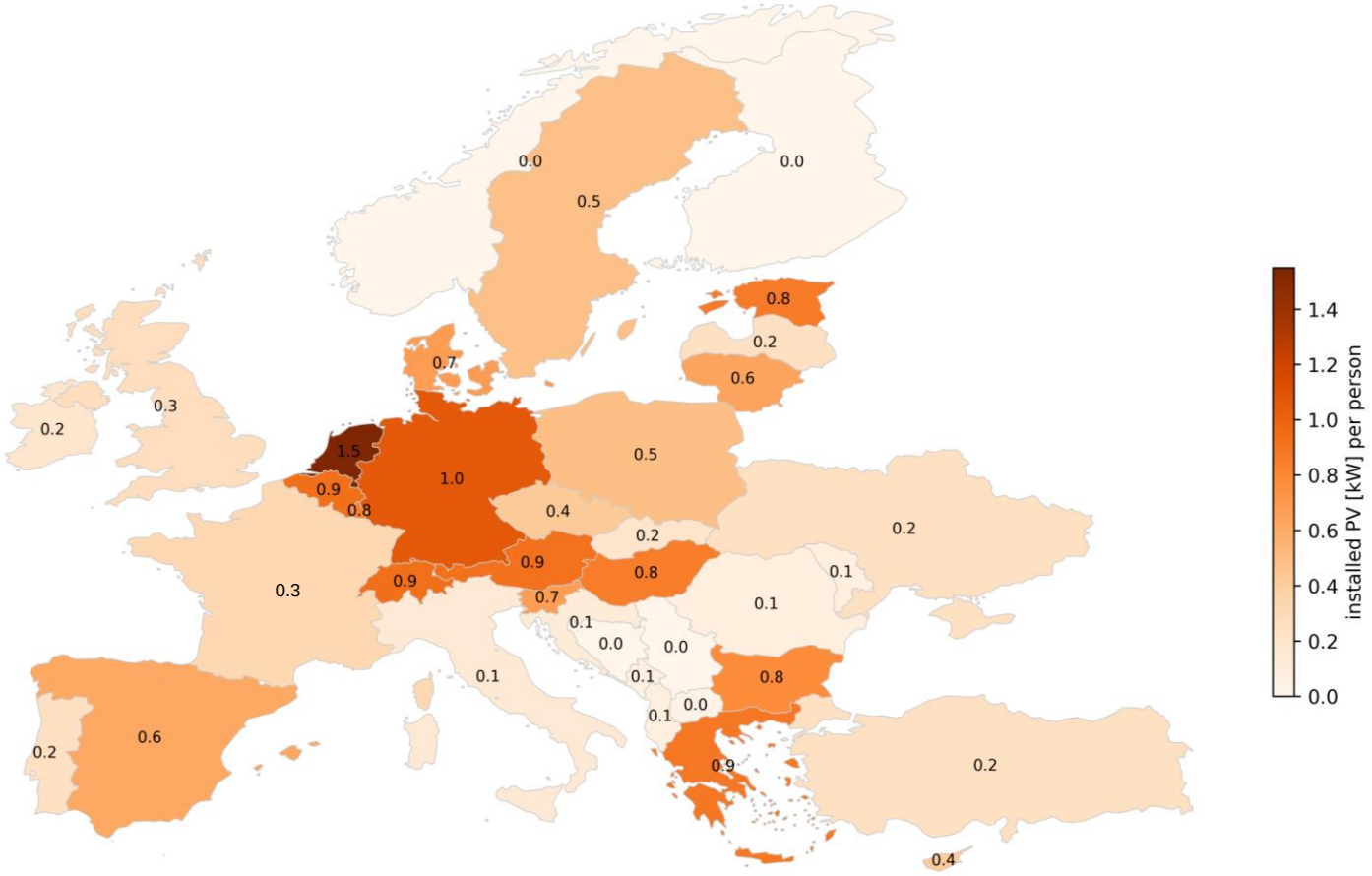


Source: ENTSO-E 2024

INSTALLED PV POWER PER PERSON IN EUROPEAN COUNTRIES

Installed PV Power per person in Europe 2024:

~0,44 kW



Source: ENTSO-E 2024

PV PORTFOLIO AUSTRIA

	Power [kW]	Number	Share [%]	Installed Power [MW]	Installed Power [%]
	≤ 0,8	1676	0,37%	1	0,0%
Typ-A	0,8 ≤ 250	444694	**99,13%**	5968	**78,2%**
Typ-B	250 ≤ 35000	2208	**0,49%**	1668	**21,8%**
Typ-C	35000 ≤ 50000	-	-	-	-
Typ-D	≥ 50000	-	-	-	-
TOTAL Sept. 2024		448578		7637	
TOTAL April 2025				8614	
TOTAL August 2025		537263		10143	

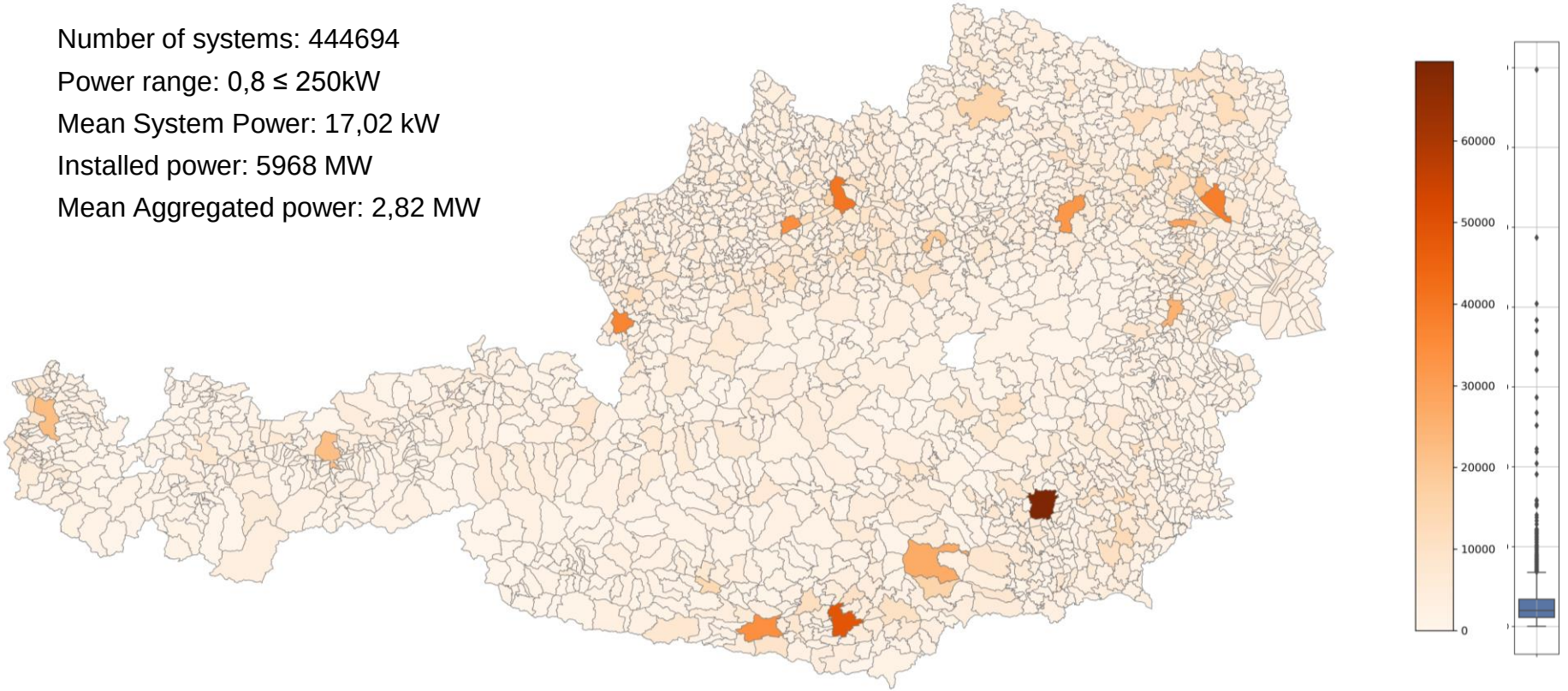
PV Target 2030: ~**10000** MW

PV Target 2040: ~**40000** MW

Source: E-Control Anlagenregister

TYPE-A: PV POWER PER DISTRICT

Number of systems: 444694
Power range: 0,8 ≤ 250kW
Mean System Power: 17,02 kW
Installed power: 5968 MW
Mean Aggregated power: 2,82 MW



Data set: 1.9.2024

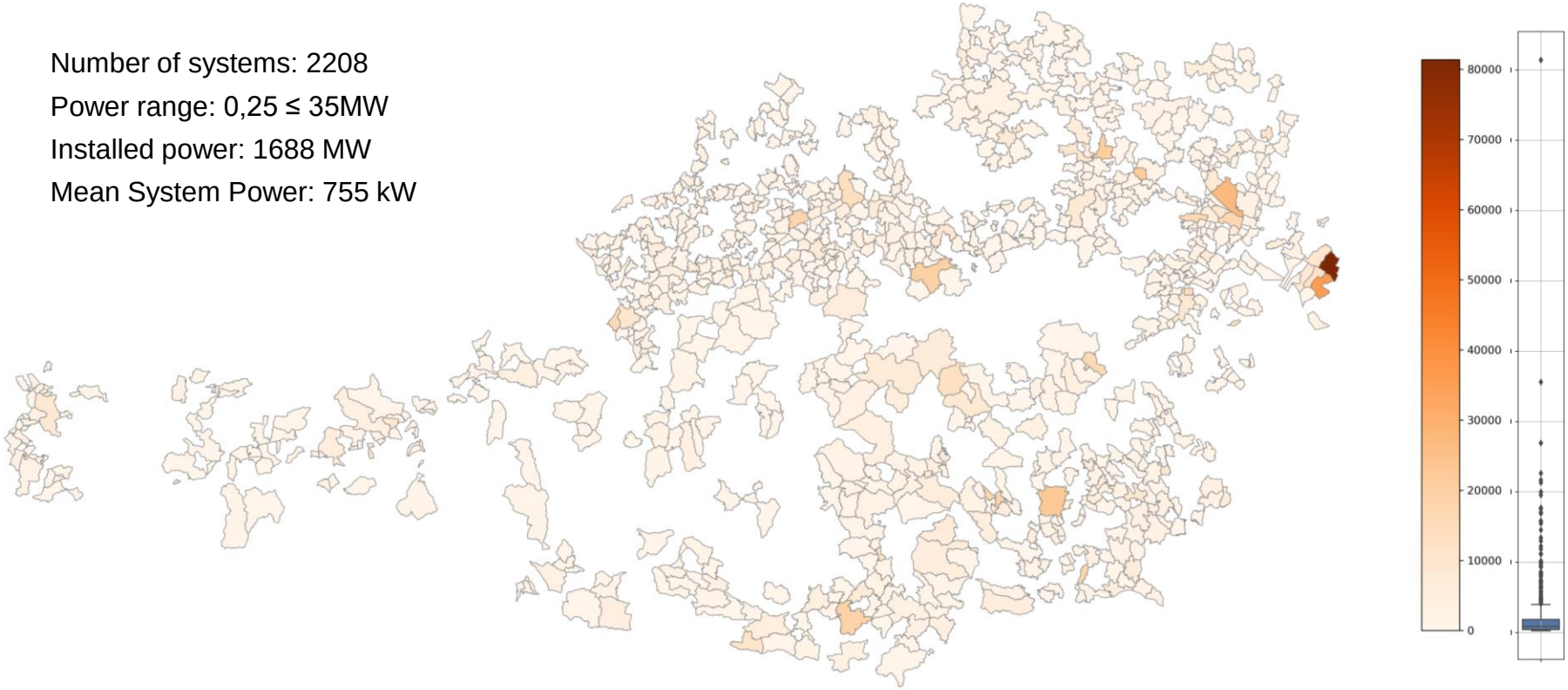
TYPE-B: PV POWER PER DISTRICT

Number of systems: 2208

Power range: 0,25 ≤ 35MW

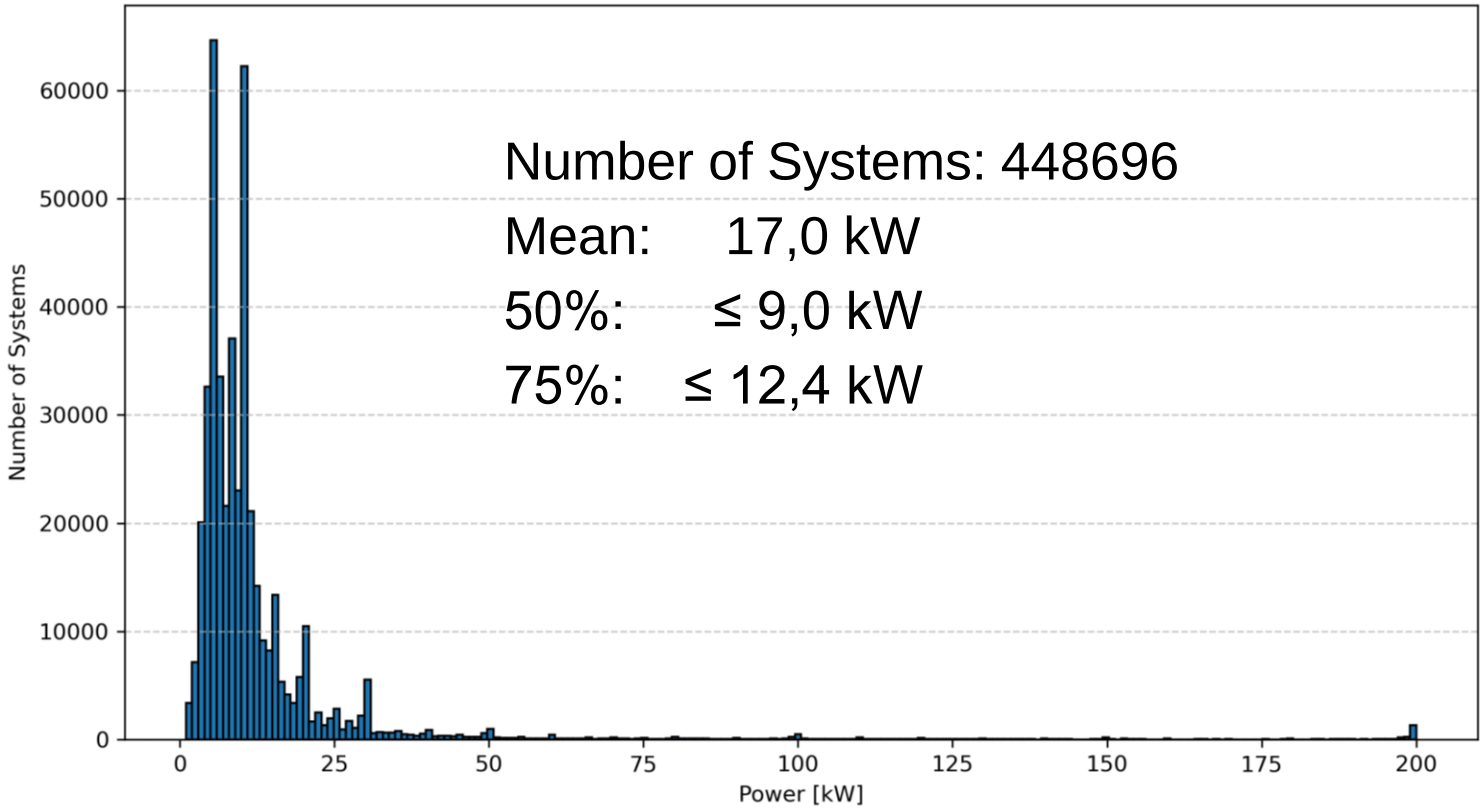
Installed power: 1688 MW

Mean System Power: 755 kW



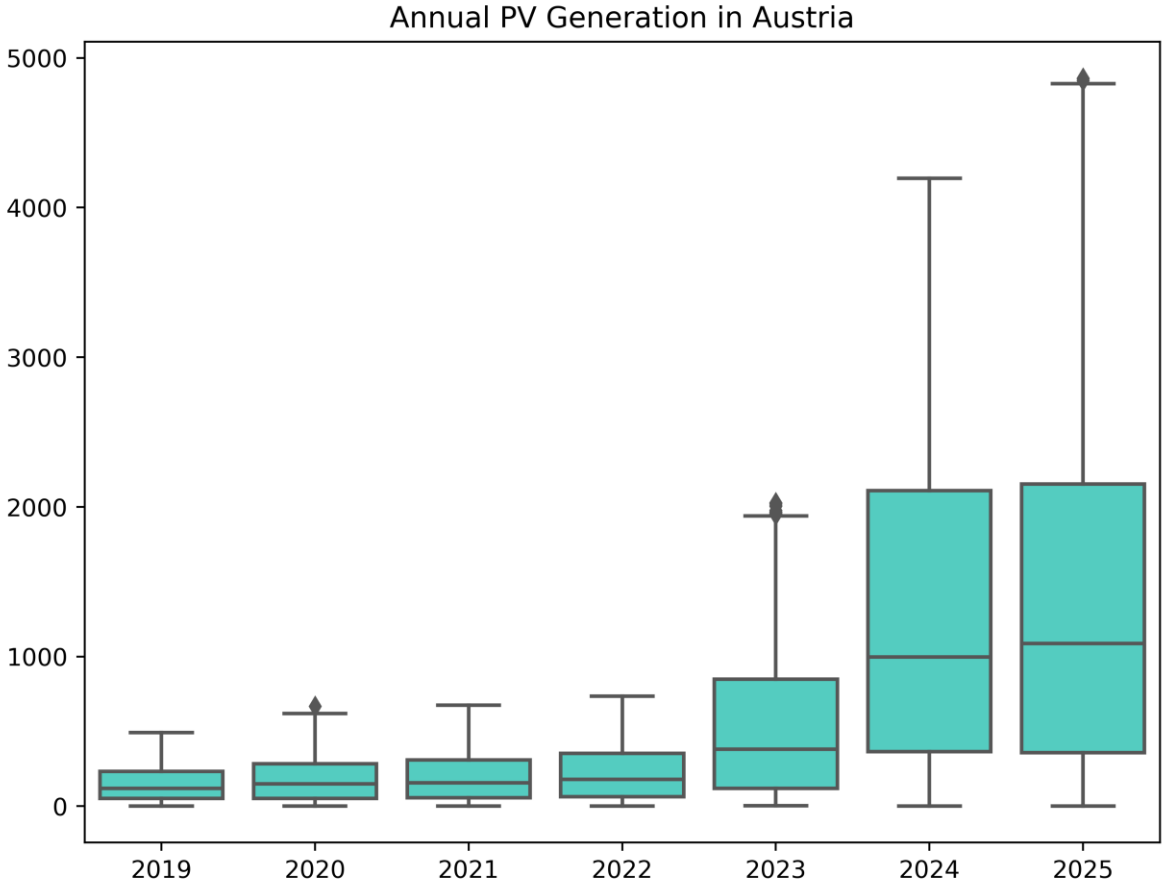
Data set: 1.9.2024

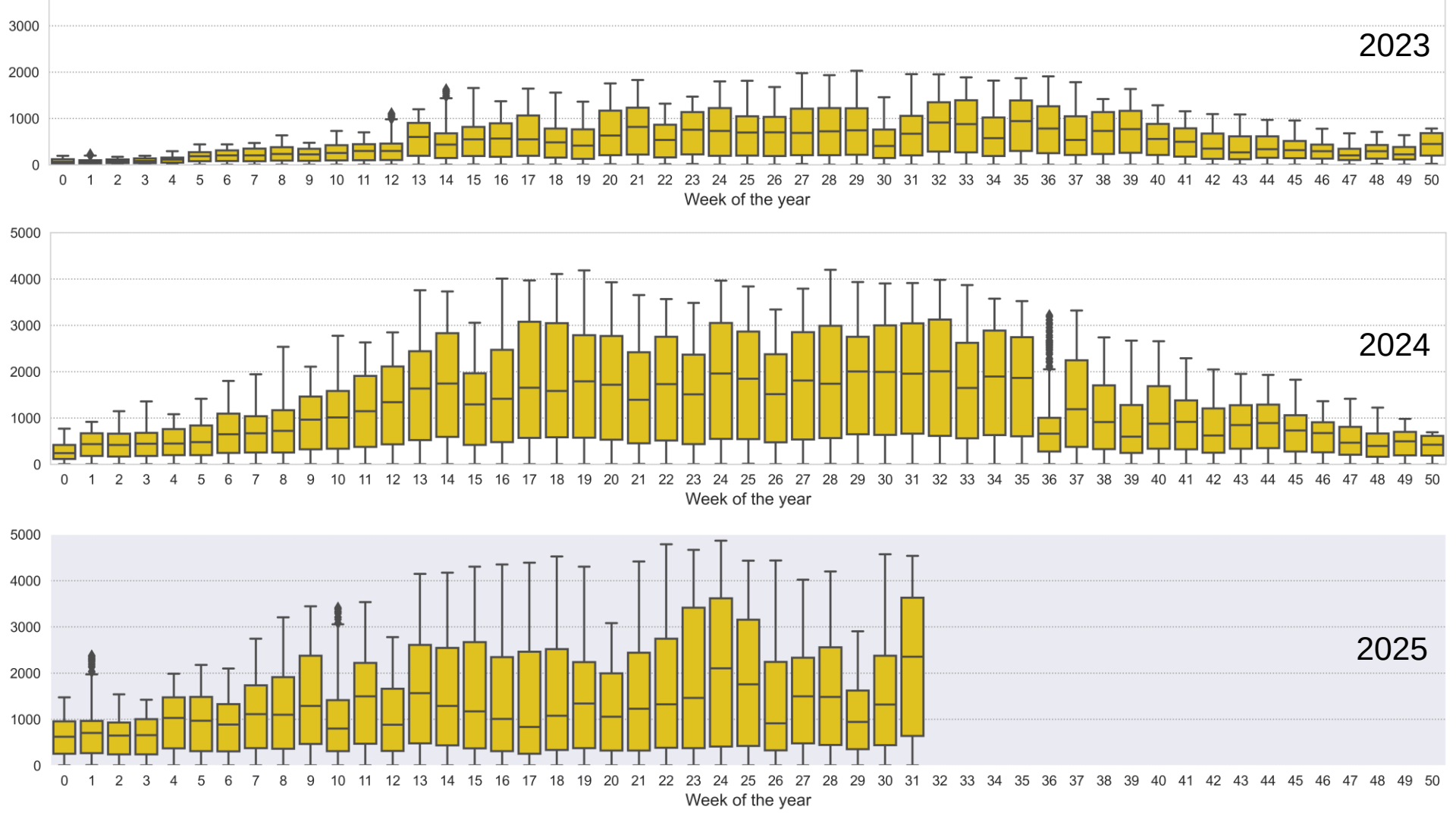
SYSTEM SIZE DISTRIBUTION OF PV IN AUSTRIA



Data set: 1.9.2024

PV GENERATION AUSTRIA




2023
2024
2025
Week of the year
Week of the year
Week of the year

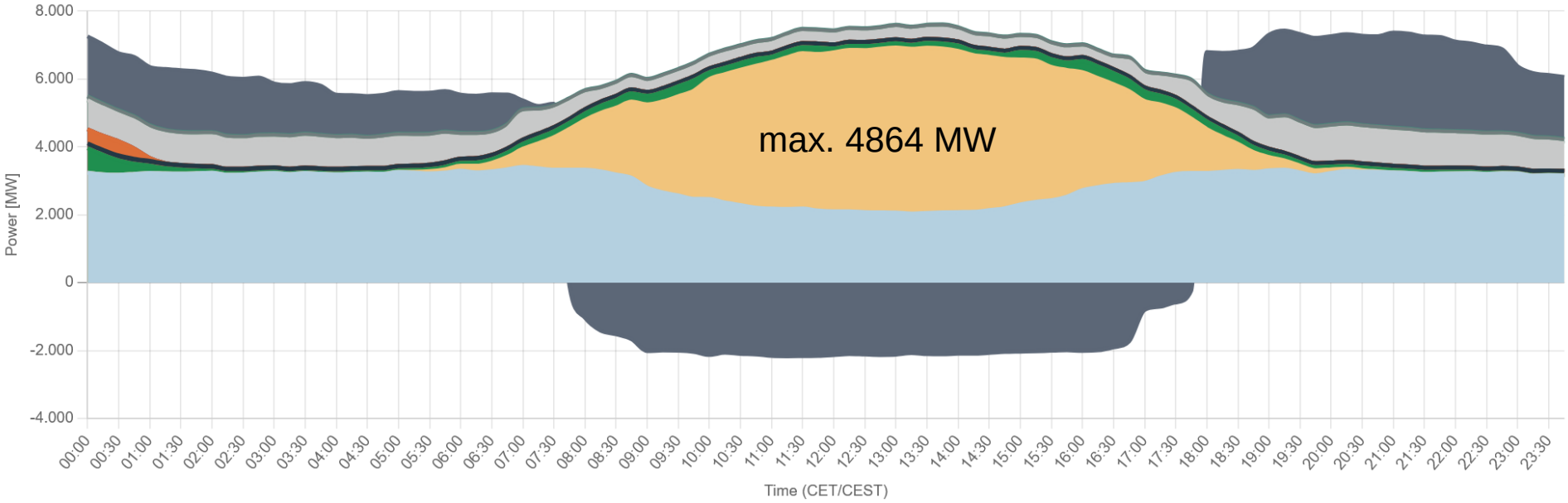
GENERATION PER PRODUCTION TYPE (21.06.2025)

Resolution: 15 Min.

Date: 21.6.2025

Hydro Run-of-river and poundage [MW] | Solar [MW] | Wind Onshore [MW] | Geothermal [MW] | Biomass [MW] | Fossil Gas [MW] | Fossil Coal [MW]

Fossil Oil [MW] | Hydro Water Reservoir [MW] | Other renewable [MW] | Waste [MW] | Other [MW] | Hydro Pumped Storage [MW]



Last Change: 03.07.202507:16 (Version 6)

(EU) Nr. 543/2013

Article 16.1.b Actual aggregated generation per type

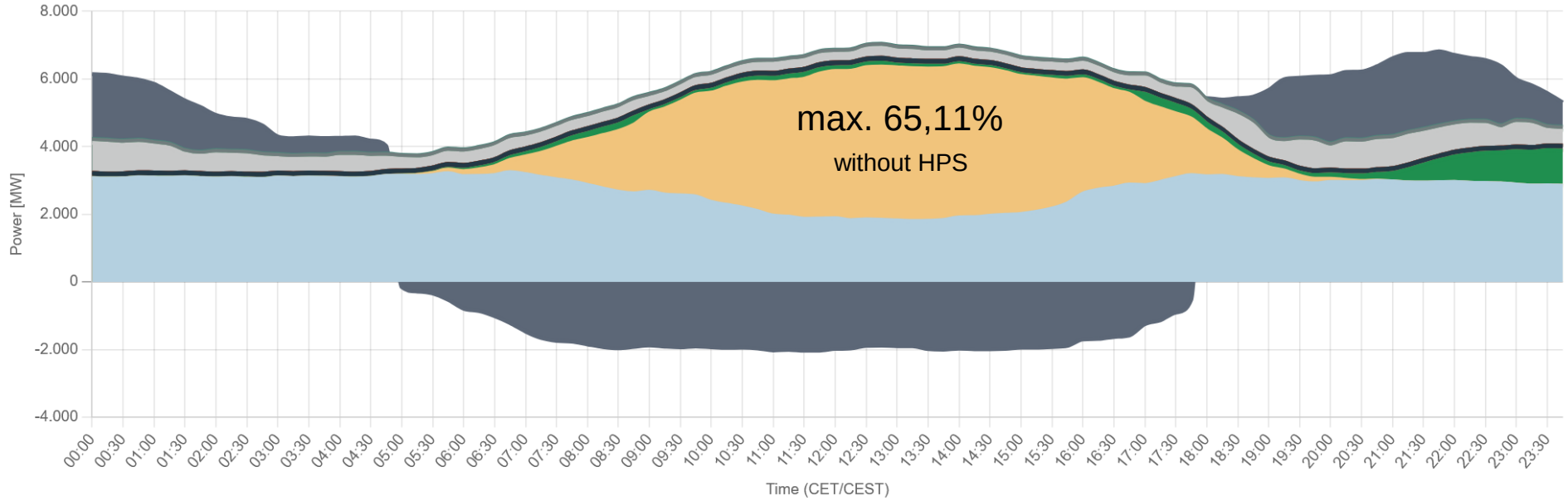
GENERATION PER PRODUCTION TYPE (22.06.2025)

Resolution: 15 Min.

Date: 22.6.2025

Hydro Run-of-river and poundage [MW] | Solar [MW] | Wind Onshore [MW] | Geothermal [MW] | Biomass [MW] | Fossil Gas [MW] | Fossil Coal [MW]

Fossil Oil [MW] | Hydro Water Reservoir [MW] | Other renewable [MW] | Waste [MW] | Other [MW] | Hydro Pumped Storage [MW]



Last Change: 03.07.202506:55 (Version 6)

(EU) Nr. 543/2013

Article 16.1.b Actual aggregated generation per type

IOT RESEARCH • WHITEPAPERS • 9 min read •

60 Hurts per Second – How We Got Access to Enough Solar Power to Run the United States

Ioan Alexandru MELNICIUC Alexandru LAZĂR George CABĂU Radu Alexandru BASARABA
August 07, 2024

The gigantic and unregulated power plants in the cloud

Aug 19 2024

Recently a Dutch hacker was able to take control of 4 million solar panel installations (FTM (Dutch), Euractiv, Victor Gevers). And this wasn't the first time something like this has happened either (PV Magazine).

News / Forschung & Technik /

IT-Sicherheitsforscher entdecken neue Sicherheitslücken in Wechselrichtern

27.03.2025 - 15:47

Forscher des IT-Sicherheitsunternehmens Forescout Technologies, Inc. haben 46 neue Schwachstellen bei drei der zehn weltweit führenden Hersteller von Solar-Wechselrichtern entdeckt: Sungrow, Growatt und SMA. Diese könnten die Netzstabilität gefährden, indem Angreifer die Kontrolle über die Wechselrichter übernehmen, teilte das Unternehmen mit. Die Ergebnisse sind in dem heute (27. März) veröffentlichten Bericht »SUN:DOWN – Destabilizing the Grid via Orchestrated Exploitation of Solar Power Systems« nachzulesen

SOLARANLAGEN UND DIE CLOUD

Entwickler befürchtet Kollaps europäischer Stromnetze

Moderne Solaranlagen sind häufig mit Clouddiensten der Hersteller verbunden. Ein Entwickler sieht darin eine große Gefahr für unsere Energieversorgung.

in Pocket speichern merken

20. August 2024, 12:45 Uhr, Marc Stöckel

Rogue communication devices found in Chinese solar power inverters

By Sarah Mcfarlane

May 14, 2025 6:55 PM GMT+2 · Updated May 15, 2025

Aa

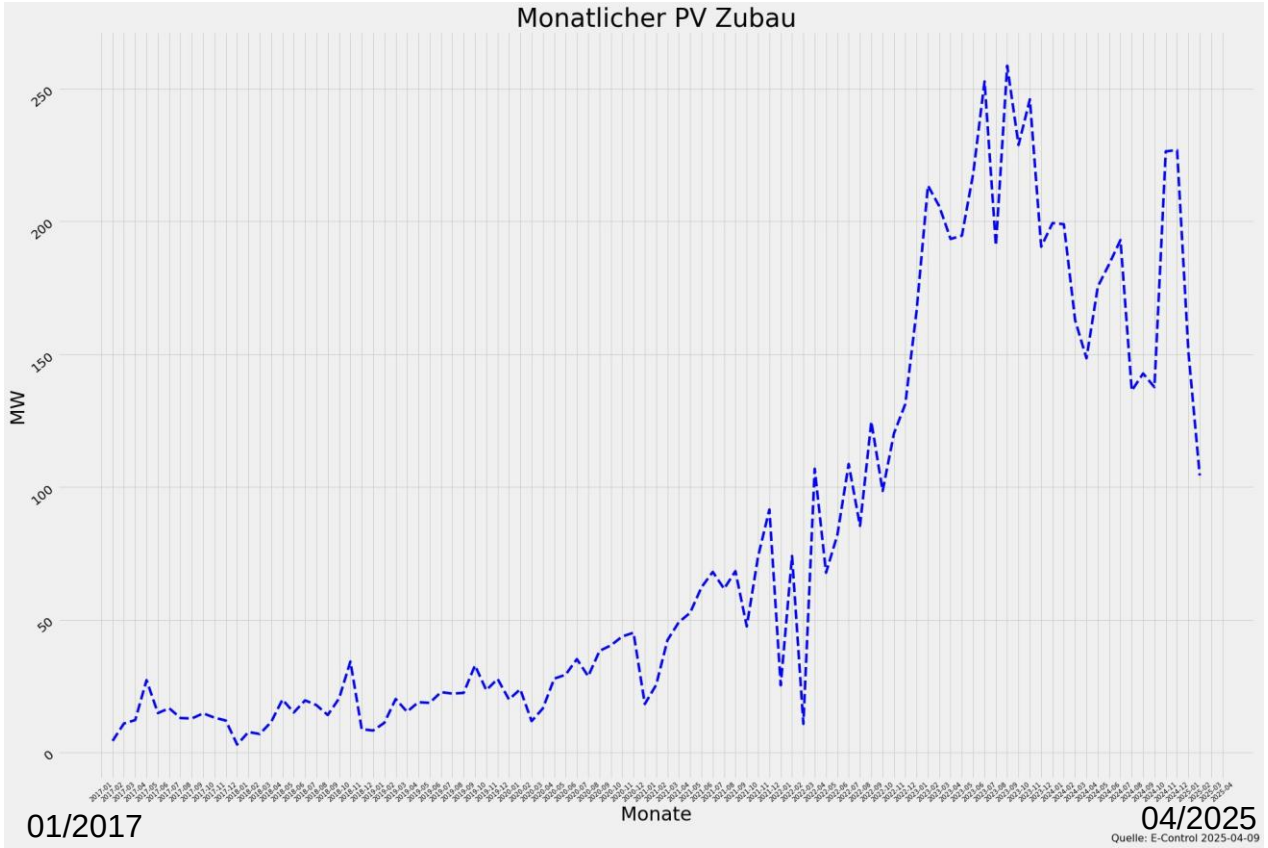
Netherlands increasing vigilance on solar inverter-related cybersecurity risks

The Dutch government said it remains vigilant on potential cybersecurity threats coming from solar inverters. It minimized, however, the risk of hidden hardware components in inverters and said these devices would be “easily detectable” by the Dutch authorities.

JULY 9, 2025 EMILIANO BELLINI

https://www.bitdefender.com/en-us/blog/labs/60-hurts-per-second-how-we-got-access-to-enough-solar-power-to-run-the-united-states
https://berthub.eu/articles/posts/the-gigantic-unregulated-power-plants-in-the-cloud/
https://www.golem.de/news/solaranlagen-und-die-cloud-entwickler-befuerchtet-kollaps-europaeischer-stromnetze-2408-188177.html
https://www.photon.info/news/it-sicherheitsforscher-entdecken-neue-sicherheitsluecken-in-wechselrichtern/
https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/
https://www.pv-magazine.com/2025/07/09/netherlands-increasing-vigilance-on-solar-inverter-related-cybersecurity-risks/

PV INVERTER MANUFCTURERS ORIGIN



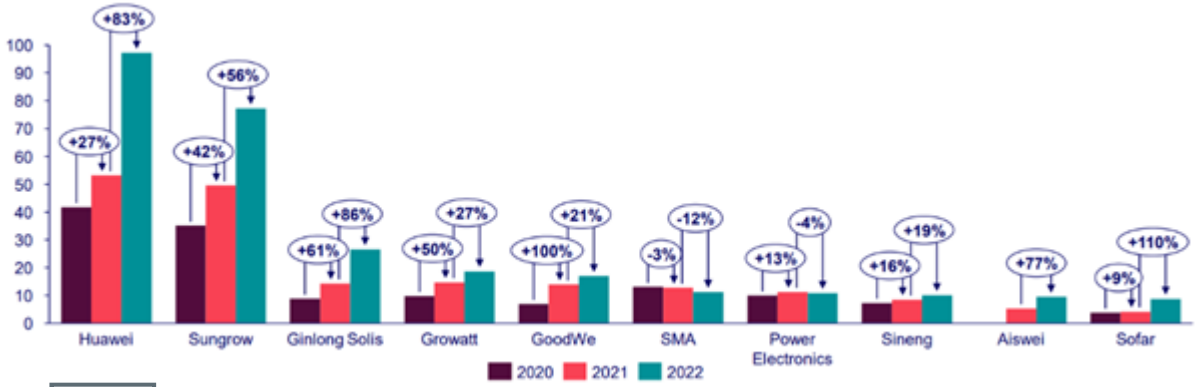
Quelle: https://www.solarpowereurope.org/advocacy/position-papers/inverters-explained

PV INVERTER MARKT DISTRIBUTION

86% of global market

50% of global market

MARKET SHARE AND PV POWER PLANT PORTFOLIO IMPLICATIONS



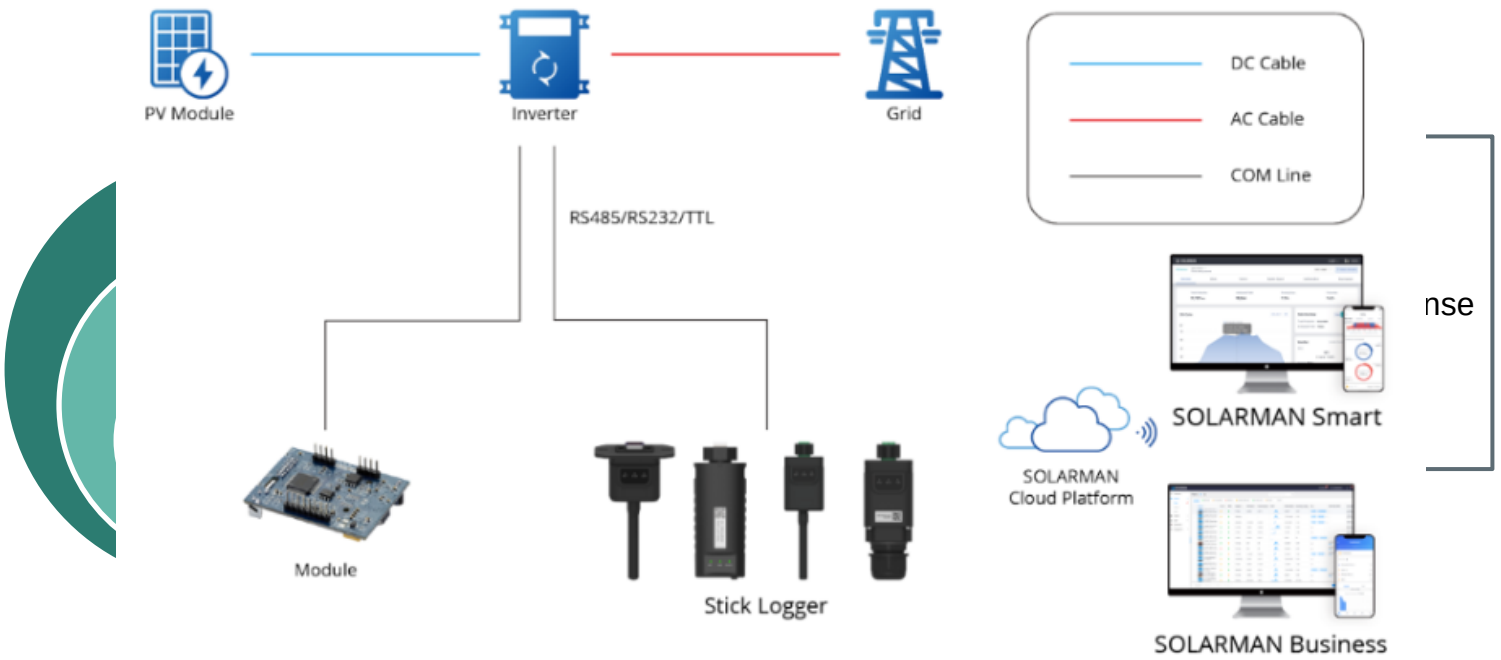
20%

EU	67,6 GW
AT	1,6 GW

N-1	1,5 GW
Primary Reserve	3 GW

„Critical Market Share“
0,44%
0,88 %

SECURITY LAYERS & ATTACK VECTOREN



RELEVANT GUIDELINES AND STANDARDS

Inverters:

- **2014/35/EU (LVD)** – Low Voltage Directive
- **2014/30/EU (EMC)** – Electromagnetic Compatibility Directive
- **2009/125/EC** – Ecodesign Directive
- **EU 2016/631 (NC RfG)** – Grid Connection Requirements
- **TOR** – Generators and grid

Cloud systems:

- **GDPR (2016/679)** – Data protection
- **NIS2 Directive (2022/2555/EU)** – IT security for critical infrastructures
- **Cyber Resilience Act (CRA)** – Cybersecurity throughout the lifecycle of digital products
- **ISO/IEC 27001** – Information security standard

POTENTIAL PATHWAYS FOR COUNTERMEASURES

- **Situation Analysis** & Risk Assessment
  - Record of all PV Inverters
- **Monitoring** & Detection
  - Device-, Network and Cloud monitoring
- Protection **Measures** & Critical Infrastructure Adjustment
  - Lower power limit for critical infrastructure
- **Cloud System** Requirements
  - Security by design
  - Bring systems under EU control/surveilance/legislation
- Incident **Response & Recovery**
  - Plan -> Simulate -> Test
- **Governance** & Compiance
  - Clarify responsibilities, conduct audits and reports

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

Matthias Eckhart
matthias.eckhart@ait.ac.at

Stefan Übermasser
stefan.uebermasser@ait.ac.at