NISDUC Conference

Interdependencies between Energy and Telecoms Sector

Ludovic Rigaux
Energy Security Officer
SPF Economie – DG Energie- Haute Surveillance du Marché et Infrastructures Critiques

19th May 2026

1. Regulatory and legal framework

NIS2 and CER: Interplay and Synergies

A holistic approach to critical infrastructure protection in Belgium.

NIS2: Cyber Pillar

Security of network and information systems: risk management, incident reporting and supply-chain controls.

DIGITAL RESILIENCE

CER: Physical Pillar

Physical and operational resilience measures to prevent service disruptions.

OPERATIONAL CONTINUITY

Streamlined Compliance in Belgium

Belgian law aligns CER-designated critical entities with NIS2 essential status to reduce duplication and enable unified oversight.

CER

European Program of Critical Entities Protection (EPCIP)	→	***Critical Entities Resilience* (CER)**
Critical infrastructures	→	Critical Entities
Single point of failure	→	Essential Services
Human made threats	→	All hazard approach
Protection	→	**Resilience** : prevention, monitoring, detection, mitigation, containment, recovery, crisis communication

Network Code on Cybersecurity (NCCS)

Sector-specific standards for the European electricity grid.

Purpose & Scope

The NCCS supports a high, common level of cybersecurity for cross-border electricity flows in Europe, addressing the unique challenges of the energy transition.

- **Operational Focus:** Targets the cybersecurity of cross-border electricity flows and related market processes.
- **IT/OT Integration:** Addresses the convergence of Information Technology and Operational Technology in smart grids.
- **Risk Assessments:** Establishes a recurrent process for cybersecurity risk assessments in the electricity sector.

Relationship with NIS2

The NCCS acts as a "lex specialis" to the NIS2 Directive, providing more granular, sector-specific requirements for electricity operators.

While NIS2 sets the horizontal baseline, NCCS ensures that the technical specificities of the power grid are addressed at the EU level.

Harmonized cross-border security standards.

2. Technical framework Energy-Telecoms interactions

Energy - Electromagnetism

$$\Delta E_c = \sum W(\vec{F})$$

E = V x I x t

$$E = h\nu$$

Operational Interdependencies

The Inextricable Link Between Energy Supply and Telecommunication Services

Telecom's Reliance on Energy

- **Continuous Power:** Essential for base stations, data centers, and core network equipment.
- **Cooling Systems:** High-density server environments require constant energy for thermal management.
- **Backup Limitations:** Batteries and generators provide only temporary resilience during outages.

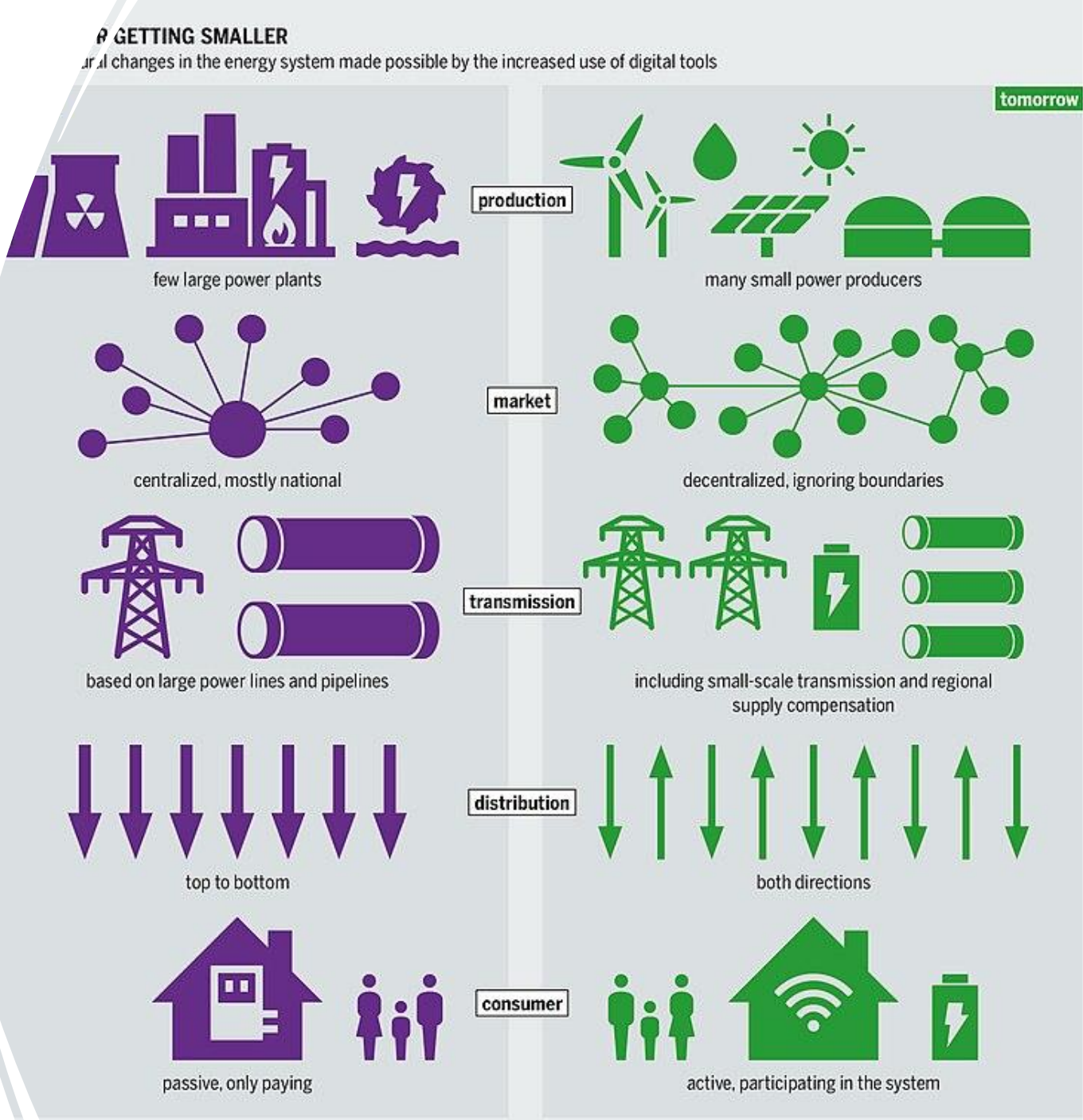
Energy's Reliance on Telecom

- **Smart Grids:** Real-time data exchange for balancing supply and demand across the network.
- **SCADA Systems:** Remote monitoring and control of substations and generation plants.
- **Incident Response:** Critical communication channels for field technicians and emergency coordination.

Cascading Effects: A disruption in one sector can rapidly impact the other, leading to widespread systemic failures. Integrated risk assessments under NIS2 and CER are vital to mitigate these cross-sectoral vulnerabilities.

Energy transition: paradigm shift

- Decentralized
- Interconnected
- Digitalized (5G, IoT, smart homes, VPP, aggregators, data clouds, …)
- New vectors (SAFs, H2, ethanol, …)
- Storage
- Ultra dynamic loads and supply
- Ultra dynamic prices
- …



Spain Portugal Blackout Incident

- Instabilities (complex system)
- Default protections
- Lack of reactive power and inertia

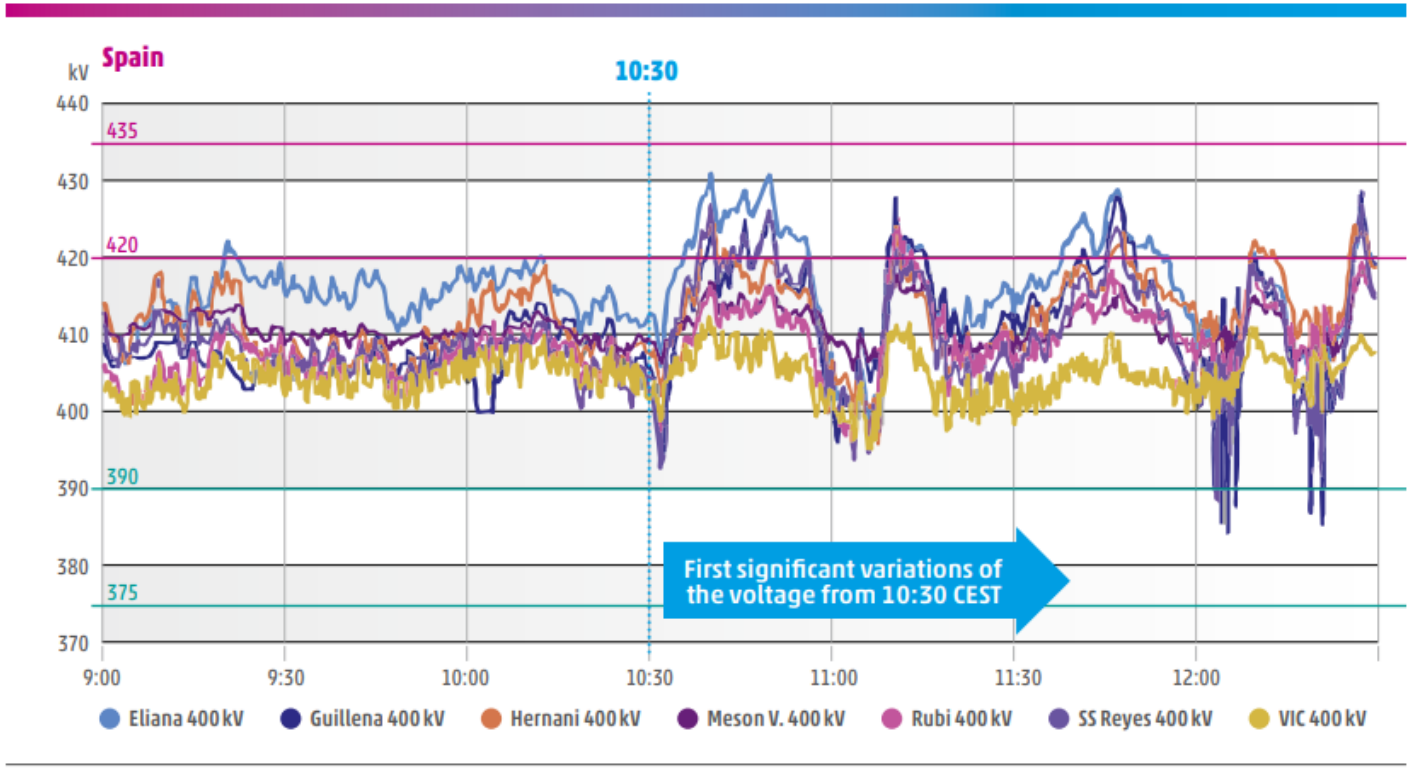


Figure 1-2: Voltage evolution in the main 400 kV transmission substations (pilot nodes) in Spain

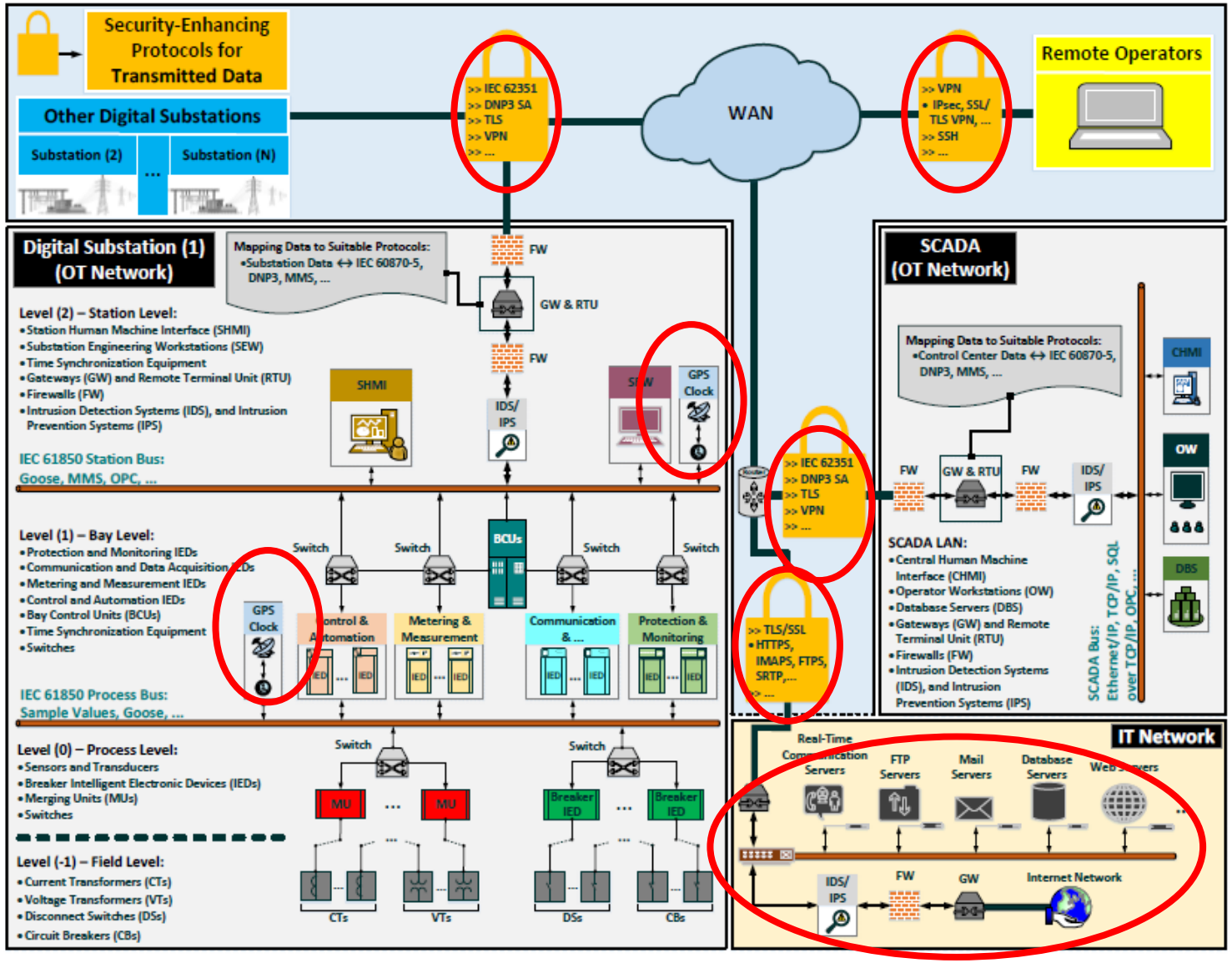


Figure 3.18: Integrated IT-OT Communication Network Model for Power Grids.

GPS & Synchronization

Open Access Review

Time Synchronization Techniques in the Modern Smart Grid: A Comprehensive Survey

by Yu Liu [1], Biao Sun [1,*], Yuru Wu [1], Yongxin Zhang [1], Jiahui Yang [1], Wen Wang [1], Naga Lakshmi Thotakura [1], Qian Liu [1] and Yilu Liu [1,2,*]

[1] Department of Electrical Engineering & Computer Science, Tickle College of Engineering, The University of Tennessee at Knoxville, Knoxville, TN 37996, USA

[2] Oak Ridge National Laboratory, Oak Ridge, TN 37831, USA

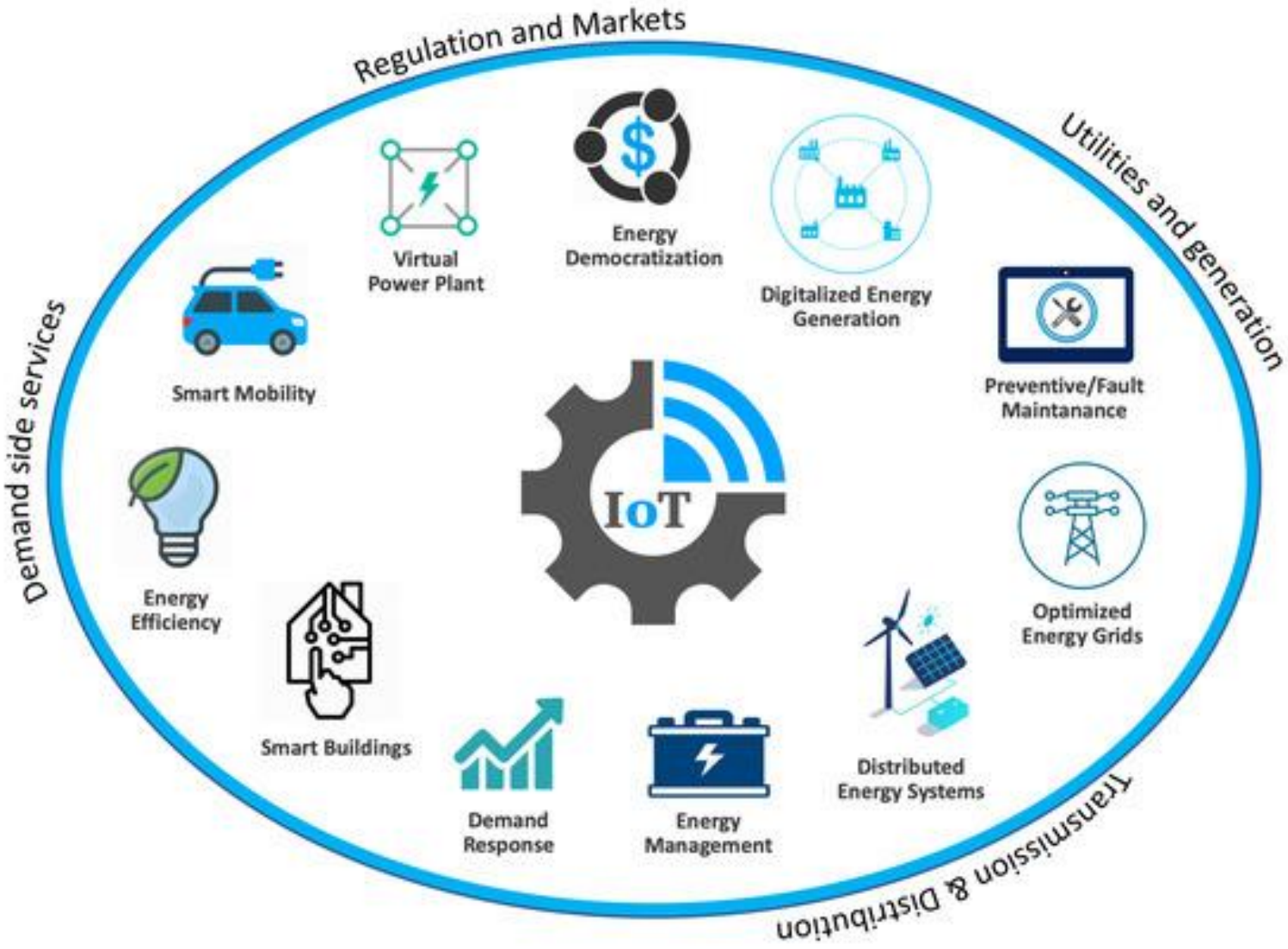
[*] Authors to whom correspondence should be addressed.

Energies **2025**, *18*(5), 1163; **https://doi.org/10.3390/en18051163**

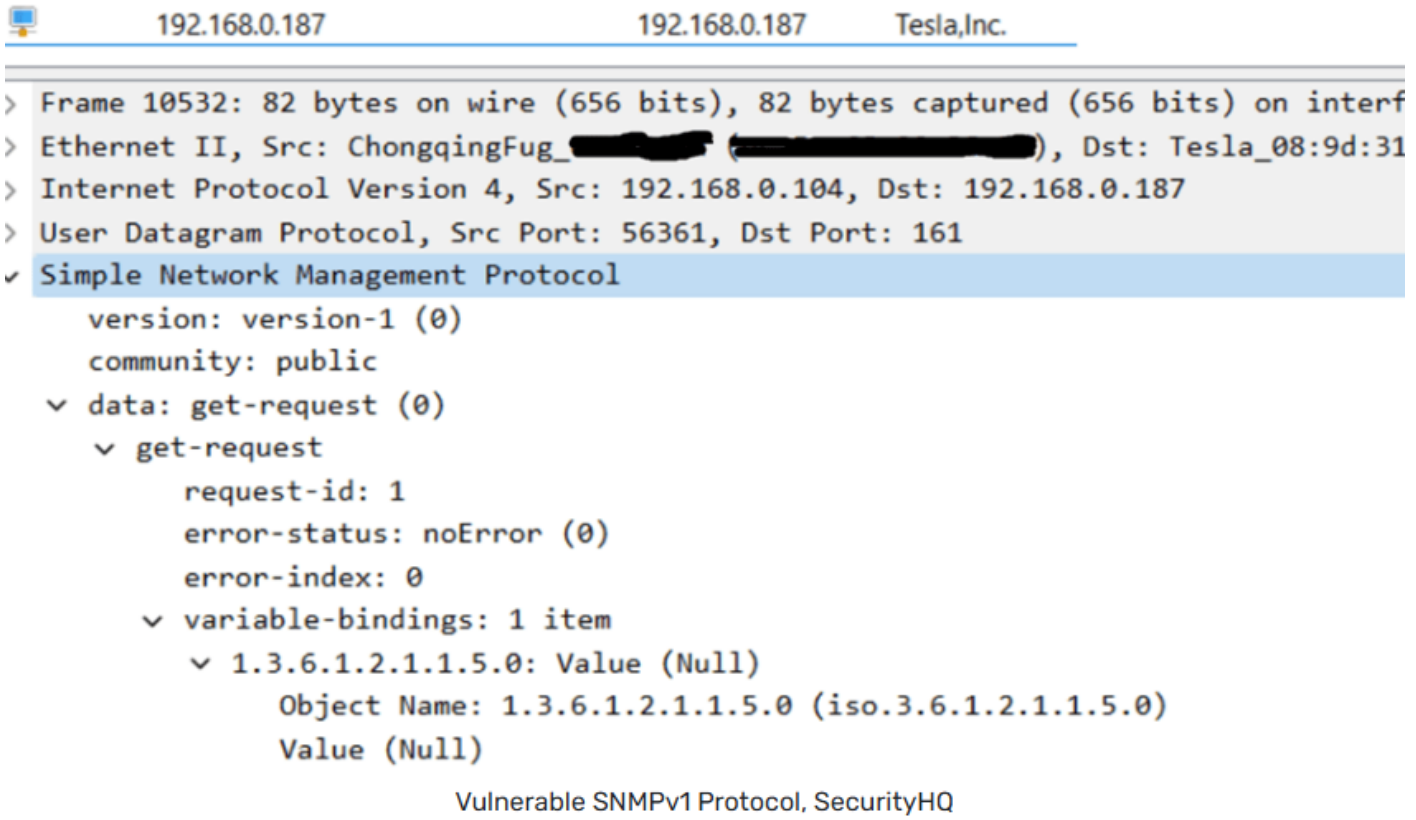
Submission received: 6 January 2025 / Revised: 20 February 2025 / Accepted: 24 February 2025 / Published: 27 February 2025

(This article belongs to the Special Issue **Energy, Electrical and Power Engineering: 3rd Edition**)

Energy : IoT


Regulation and Markets
Utilities and generation
Transmission & Distribution
Demand side services
Virtual Power Plant
Energy Democratization
Digitalized Energy Generation
Smart Mobility
Preventive/Fault Maintanance
IoT
Energy Efficiency
Optimized Energy Grids
Smart Buildings
Distributed Energy Systems
Demand Response
Energy Management

Energy : EV chargers

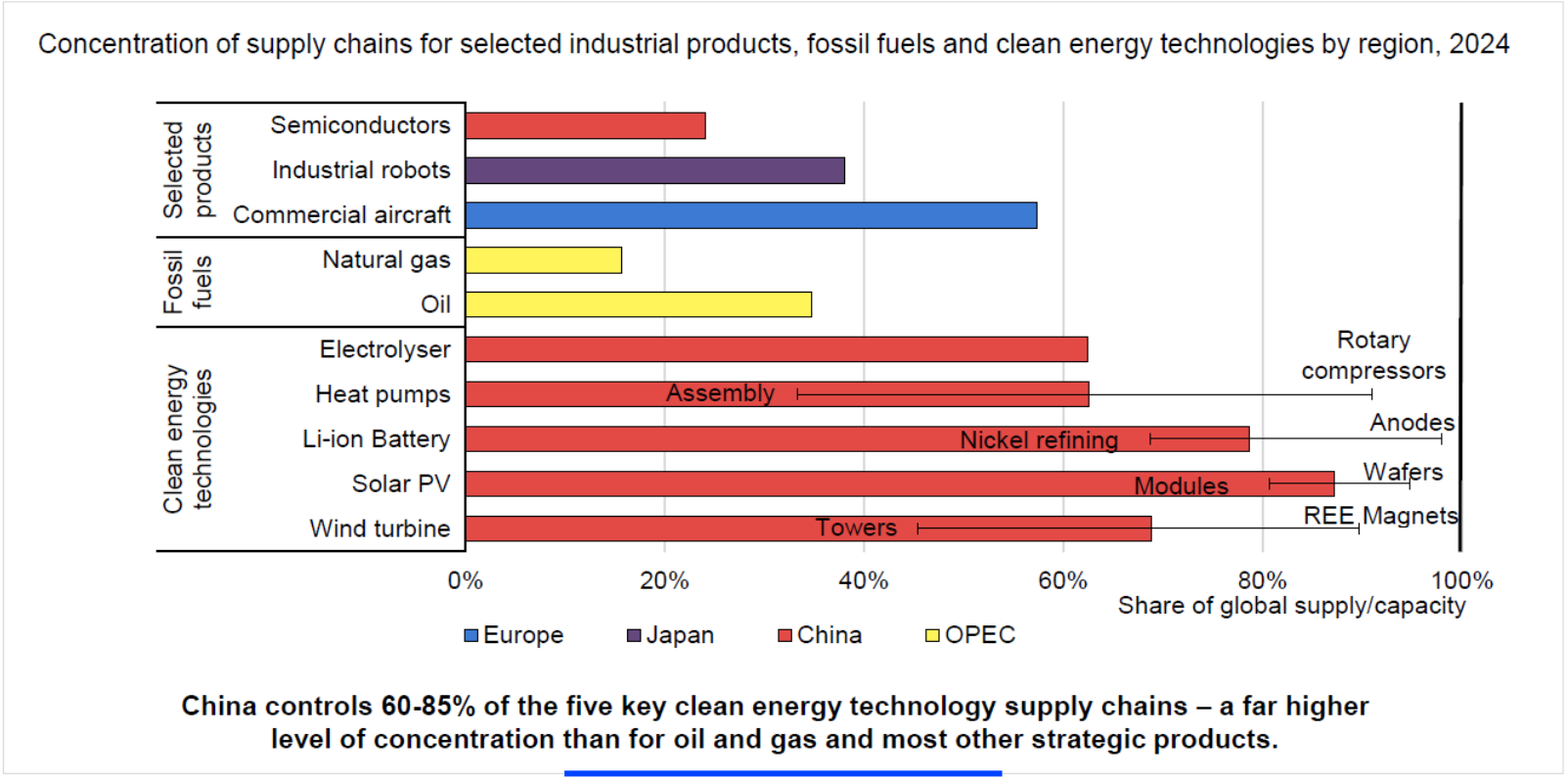


M. Bahrami and L. Wehenkel, "Coordinated EV Charging Attacks to Cause Transmission Line Overloads," *2024 9th International Youth Conference on Energy (IYCE)*, Colmar, France, 2024, pp. 1-6, doi: 10.1109/IYCE60333.2024.10634957.

Energy : renewables

Supply Chain

Energy technologies are significantly concentrated in China



Energy : renewables

- Solar inverters : fully scalable attacks on ~20% of the PVs
- Goerke et al. 2024 : 3,9% sufficient to lead to blackout

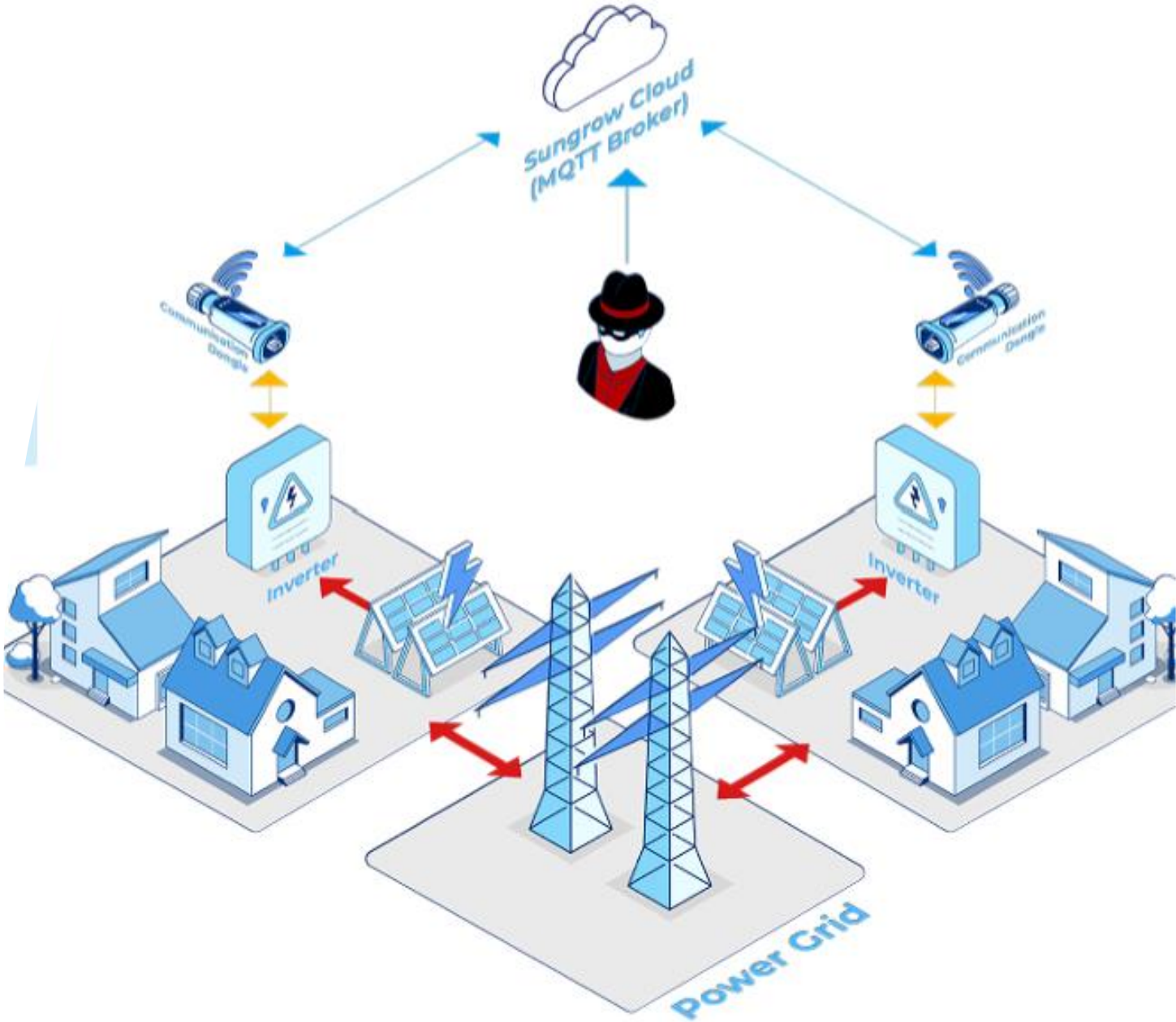
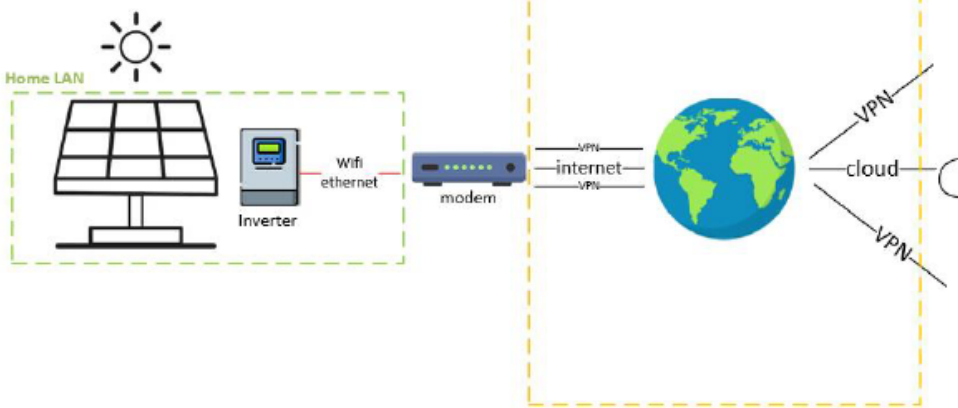
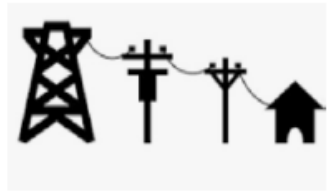


Figure 7 – Taking control of Sungrow inverters

Who Ensures Secure Access to Rooftop PV?



Installer \ TPO



Utility / balancing authority

White Label Device Sellers

OEM

Cloud API
E.g. EV Chargers, EMS, Heat Pump

Virtual Power Plant

Others
Ex: Physical access, Multi-Stakeholder Trust Vendor, 3rd party monitoring services, customer, internet (if IP visible)

Energy : smart metering

E.DSO Technology and Knowledge Sharing Committee Cybersecurity Task Force. Smart-Metering Task Force Position Paper

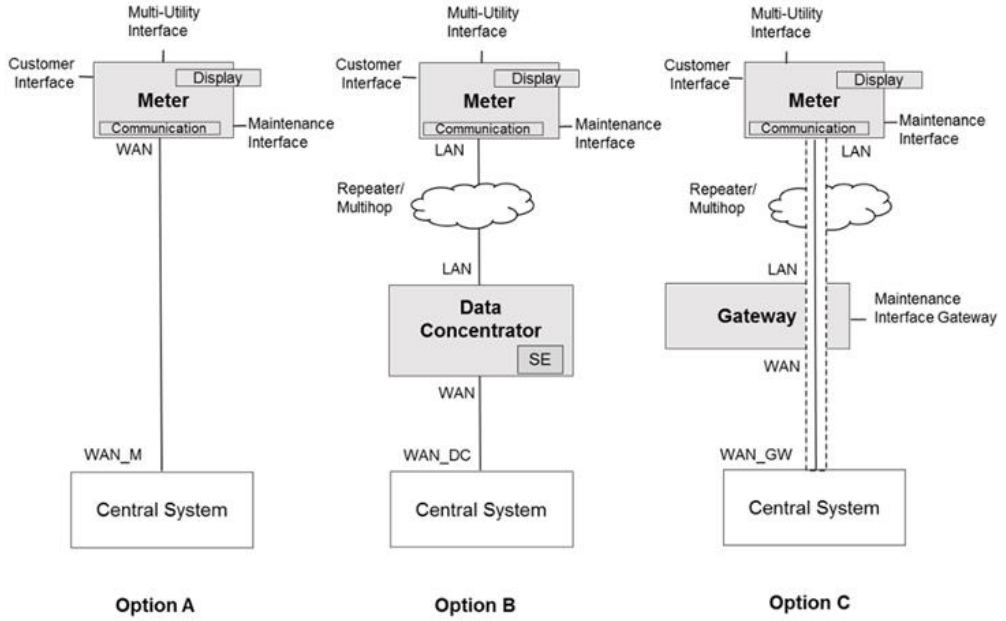
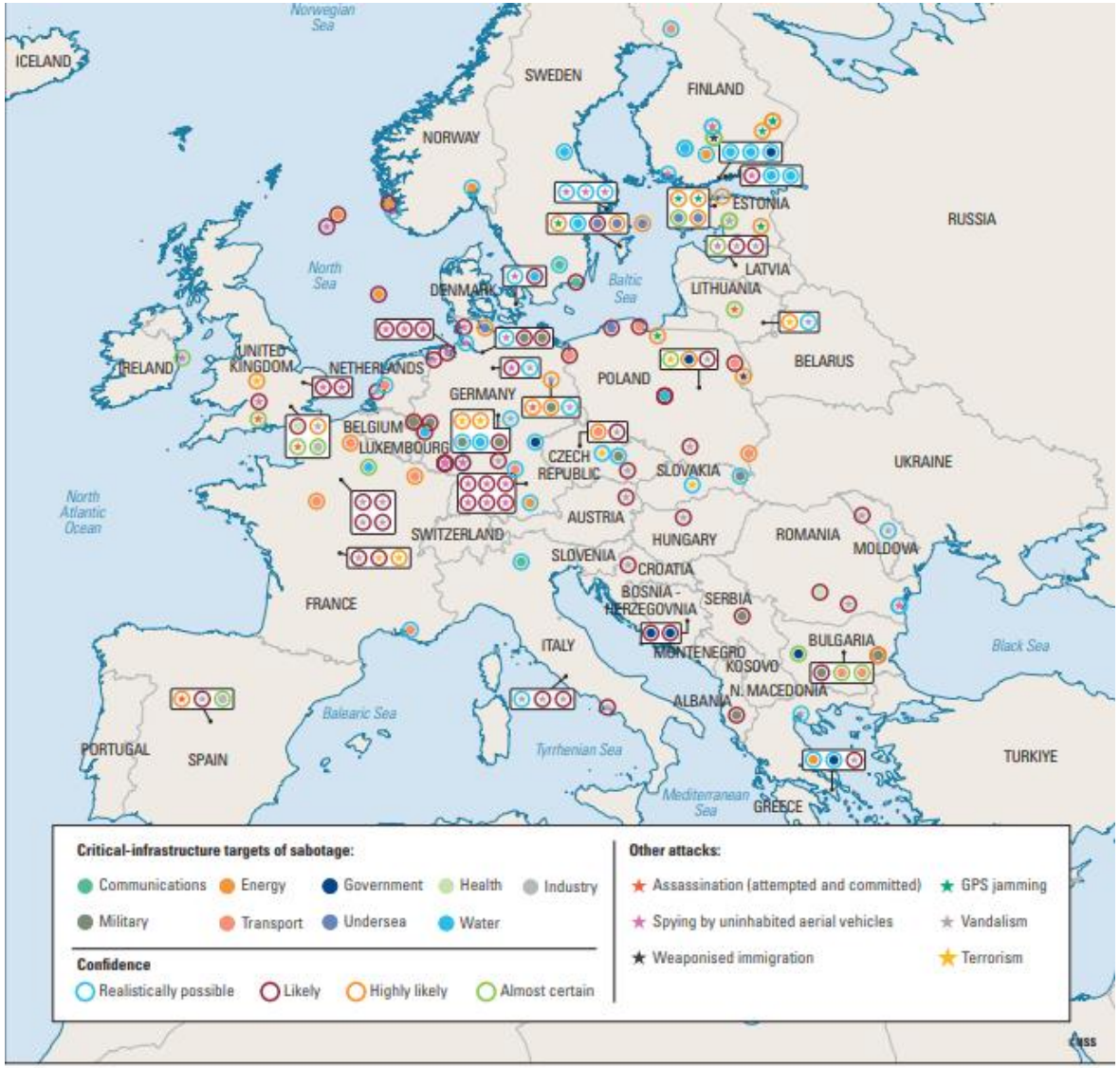


Figure 1 Smart Meter architecture possibilities

Energy: diversity, complexity

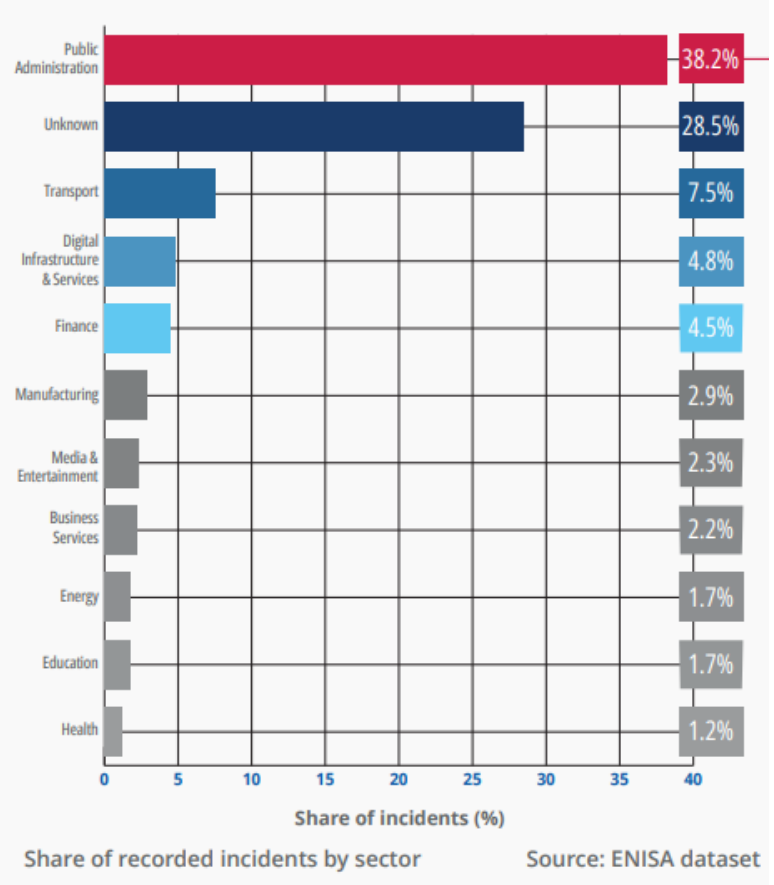
Tendances 2025 Hybrid warfare

(IISS Oct 2025, The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure)

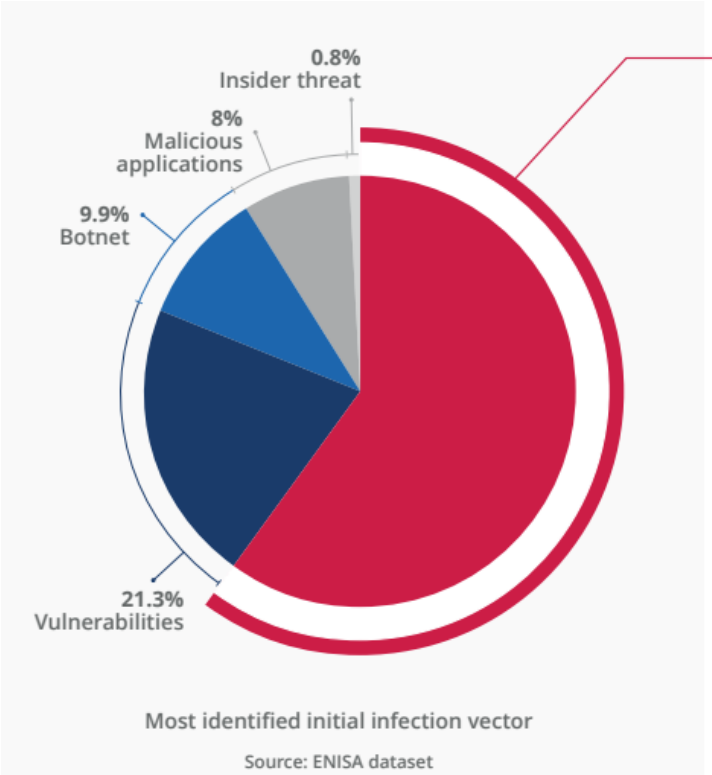


Note: Energy and communications categories exclude Russian efforts to sabotage undersea cables and pipelines; these actions are counted in the undersea category.

Tendances 2025 Cyber (ENISA)



Share of recorded incidents by sector Source: ENISA dataset



Most identified initial infection vector

Source: ENISA dataset

60%
Phishing

Phishing was the dominant intrusion vector, accounting for approx. 60% of cases, including malspam, vishing, and malvertising. Vulnerability exploitation represented 21.3% of initial access vectors, with 68% leading to malware deployment as a follow-up activity.

Mobile devices and Internet- exposed services and devices, particularly Operational Technology (OT) systems remain high value targets across all types of threats.

State-aligned intrusion sets and cybercriminal operators increasingly leverage AI for productivity and optimisation of their malicious activities.

Ukraine Power Grid – December 2015 Cyberattack SCADA

First publicly confirmed cyberattack causing a power outage.

230,000 customers lost power for several hours.

Attack Chain

1. Spear-phishing emails delivered BlackEnergy malware.

2. Attackers stole operator credentials.

3. Remote access into SCADA/ICS networks.

4. Operators' HMIs used to open breakers remotely.

5. KillDisk malware disrupted recovery efforts.

6. Telephone DoS flooded customer support lines.

Colonial Pipeline – May 2021
Cyberattack on billing system

CRITICAL INFRASTRUCTURE ATTACK

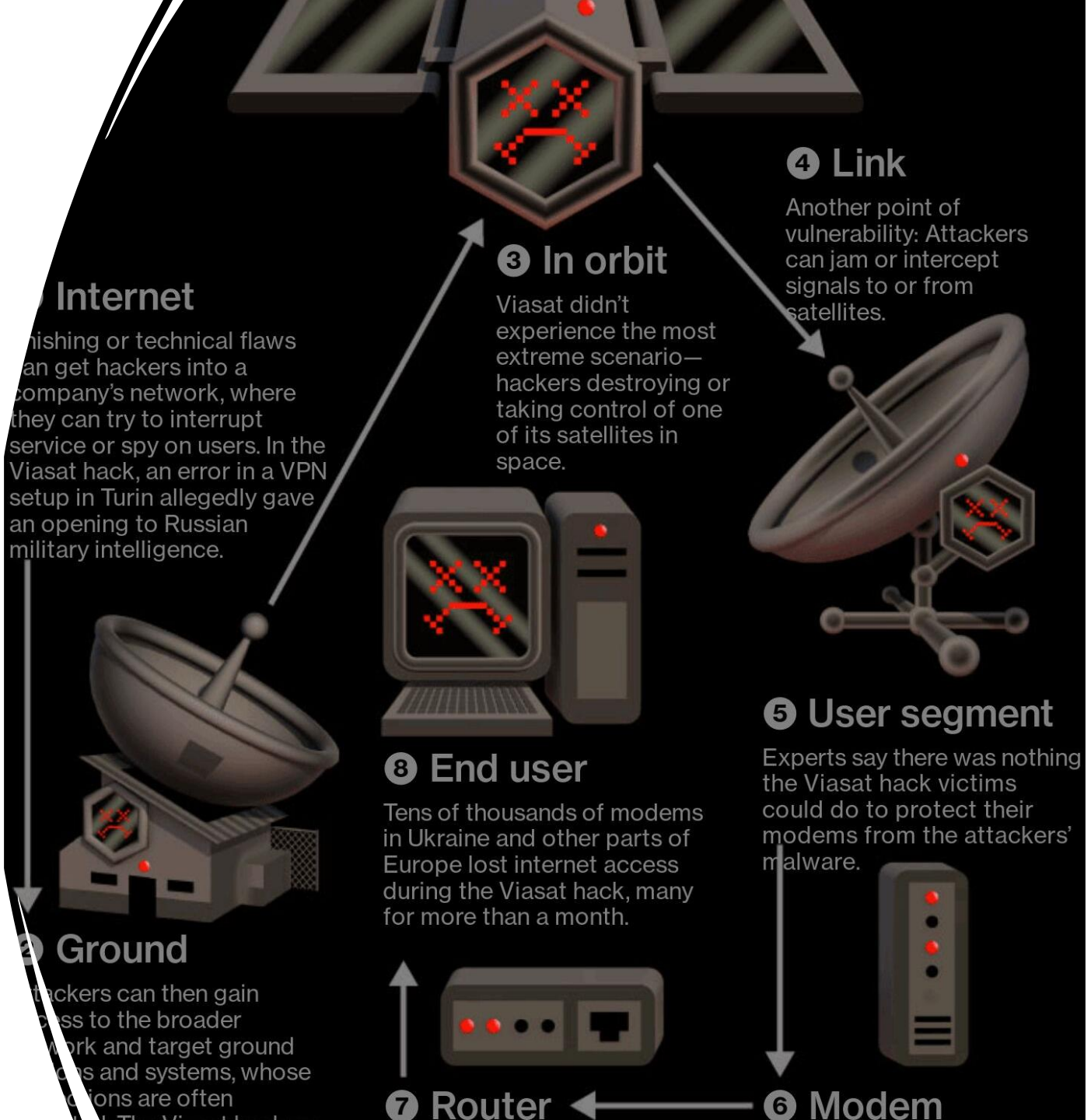
Colonial Pipeline Ransomware Incident

May 7–12, 2021 · DarkSide ransomware group · United States

ansom paid 4.4M bitcoin	Recovered by DOJ $2.3M ~64 bitcoin	Data stolen ~100 GB In under 2 hours	Shutdown durat 6 days May 7–12
uel affected 45% ast Coast supply	Pipeline length 5,500 mi Houston to New York		

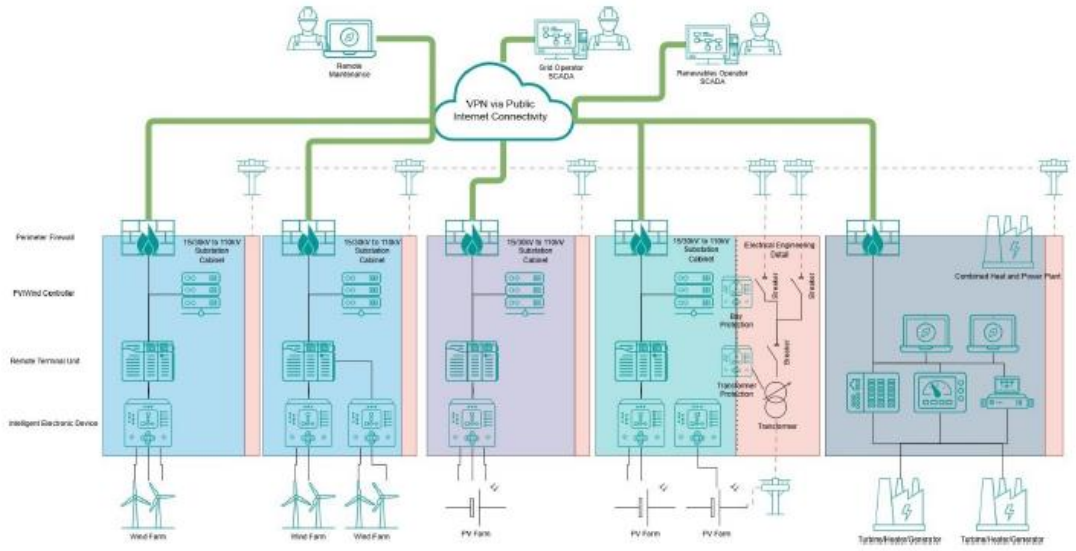
ViaSat K-SAT Cyberattack February 2022

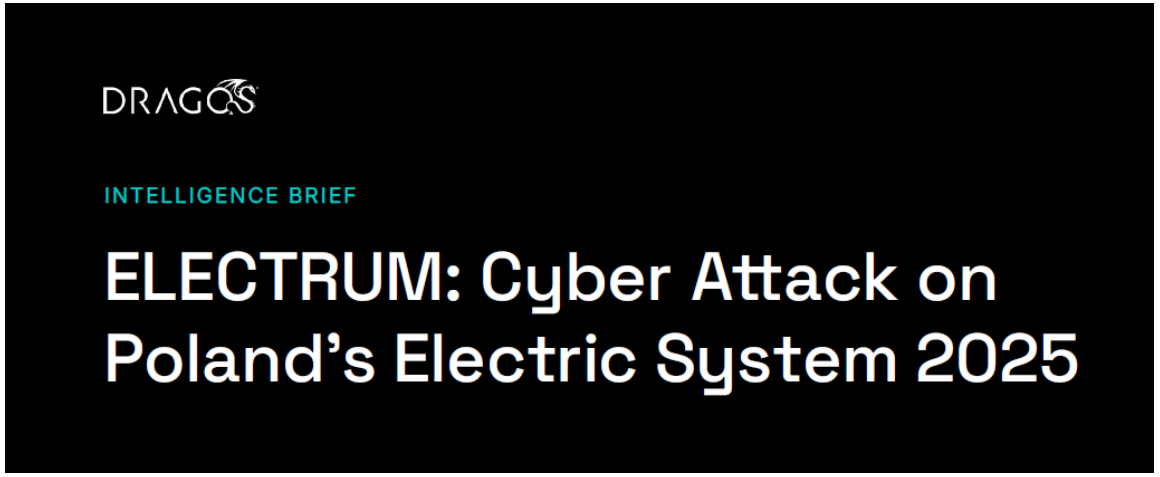
- Cause : misconfigured VPN at the Eutelsat. “AcidRain” wiper clean the flash memory of the routers
- Actors : GRU (attributed)
- Consequences : disconnection of remote monitoring for 5,800 Enercon wind turbines in Germany (11 GW)



Coordinated Cyber Attack on DERs December 2025

- Cause: Exposed RTUs from exploited vulnerabilities
- Actors : Electrum Group, responsible of attacks on UKR energy sites in 2015-16 and Feb 2022
- Consequences : 12 sites affected, of 100 MW each (1,2 GW in total, 5% of Poland’s consumption), likely the double. No blackout due to reserves and interconnection.





Challenges and Opportunities in Resilience

Navigating complexities and leveraging collaboration for a resilient future.

Key Challenges

Technological Evolution

Rapid integration of IoT and smart grid technologies increases the attack surface.

Sophisticated Threats

Rise in state-sponsored actors and advanced persistent threats (APTs) targeting infrastructure.

Regulatory Complexity

Harmonizing diverse requirements across CER, NIS2, and sector-specific codes.

Strategic Opportunities

Cross-Sectoral Synergy

Improved information sharing between energy and telecom operators.

Security Innovation

Development of AI-driven threat detection and resilient communication protocols.

Standardization

Establishing common EU-wide standards for operational security and risk assessment.

Public-Private Partnerships: Engaging industry stakeholders is essential for developing practical, effective, and innovative security measures.

Switching paradigm from Rationnal Market behaviour to Weaponized market Behaviour: RU in UKR, Ormuz crisis, …

Thank you for your attention

Many thanks to IBPT

For more informations:

Ludovic.Rigaux@economie.fgov.be

economie

FOD Economie, K.M.O., Middenstand en Energie

• Load shedding plan electricity

- NISDUC – 20 may 2026

Overview

- When to use load shedding
- Automatic load shedding
- Manual load shedding
- Consequences of load shedding

When to use load shedding

Automatic load shedding

Manual load shedding

Consequences

Context: Causes of a Crisis

Electricity grid

Production and demand (load) in equilibrity

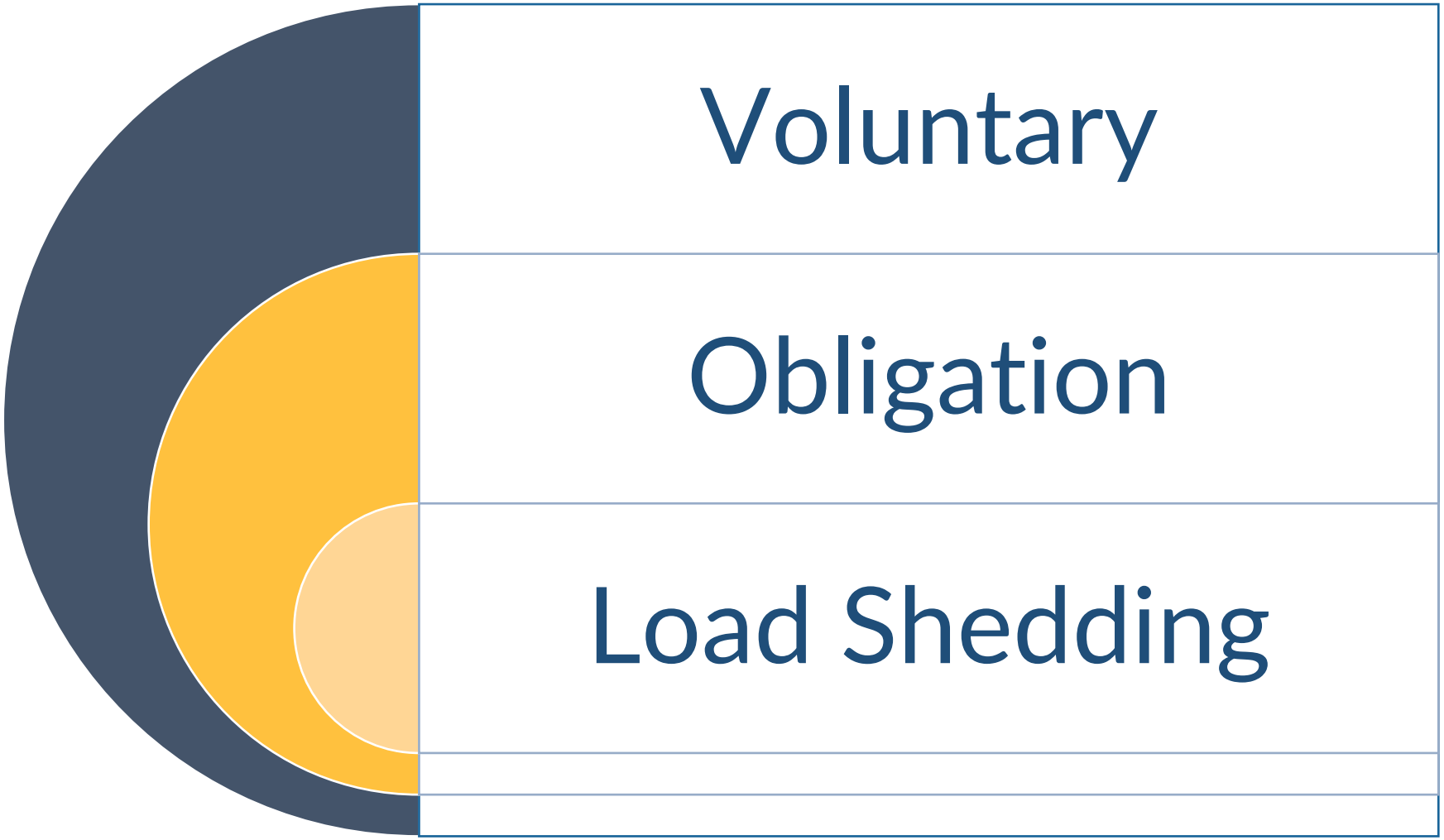
Grid frequency 50Hz

Inequilibrity between production & demand triggers crisis

Two types of crisis:
Sudden phenomena <> Scarcity

Low probability on transmission system

Potential measures



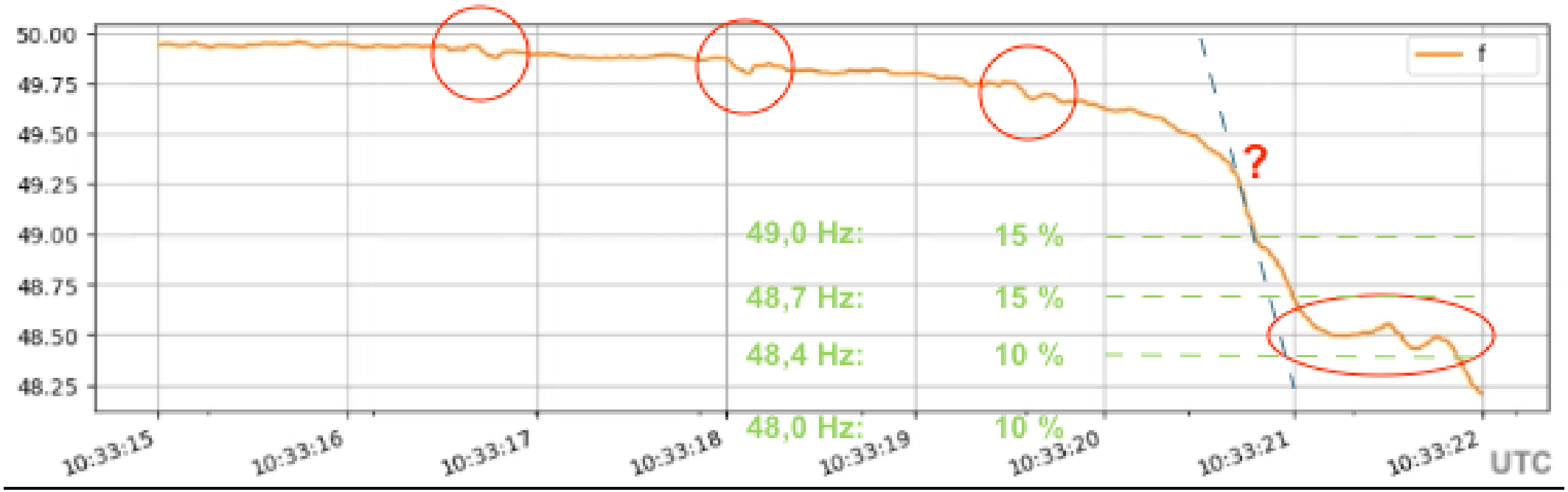
When to use load shedding

Automatic load shedding

Manual load shedding

Consequences

Automatic Load Shedding Plan



No human intervention

Loss of load to stabilize frequency

1 to 8 Section(s) of the load shedding plan activated

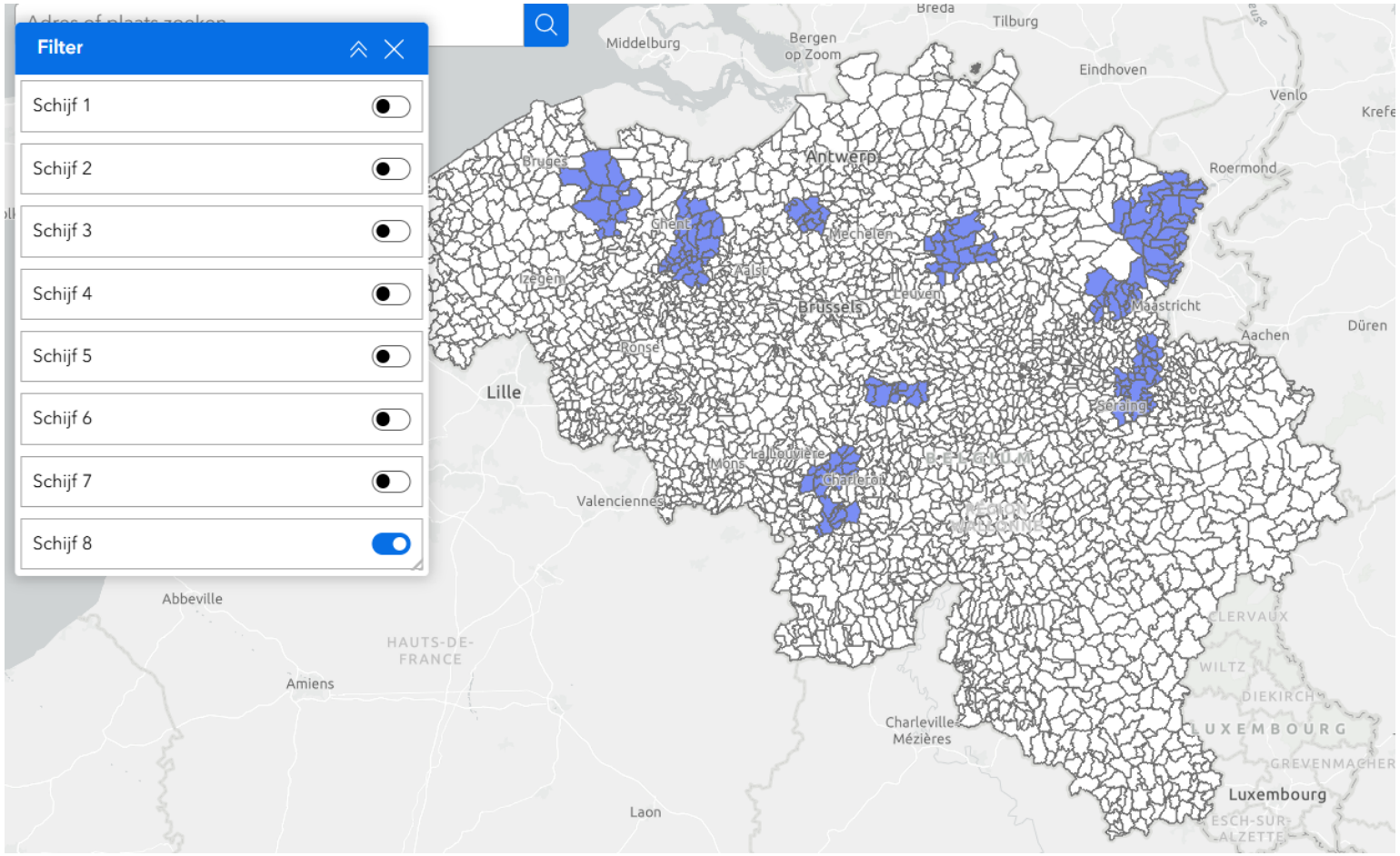
When to use load shedding

Automatic load shedding

Manual load shedding

Consequences

Manual loadshedding



Human intervention

Non-contiguous zones

8 sections representing 420-640 MW (rotation)

Limited timeframe

Proposal of Elia, decision by federal minister of Energy

Manual load shedding

Included: Rural areas (exclusing HPSGUs)

Excluded: large cities, airports, harbors, *industries

When to use load shedding

Automatic load shedding

Manual load shedding

Consequences

Impact activation manual load shedding

Local consequences – depending on the number of sections activated

Fixed telephone & data interrupted

Mobile telephone & data potentially available

Electric equipment & lighting unavailable

No charging of batteries

*No production with solar panels**

*No use of home batteries**

No use of natural gas

Petrol stations unavailable

Loss of water pressure

Thank you