Cyberrisiken im Stromnetz

Energiewende und neue Risiken

Linz, 3.10.2023

Stephan Gerling

Senior Security Researcher
Kaspersky ICS-CERT

@ObiWan666

Kaspersky ICS CERT: key facts

Established in 2016

The first ICS CERT created by a commercial organization

CVE Numbering Authority (CNA)

Who we are

A global project by Kaspersky to coordinate the efforts of industrial automation system vendors and industrial facility owners and operators.

More than 30 experts in ICS threat and vulnerability research, incident response and security analysis

Membership

ISO

ITU

IEC

Industry IoT Consortium

GLOBALPLATFORM

what is renewable/green energy?

Renewable energy - is energy derived from natural sources that are replenished at a higher rate than they are consumed. Sunlight and wind, for example, are such sources that are constantly being replenished. Renewable energy sources are plentiful and all around us.

Solar

Wind

Geothermal

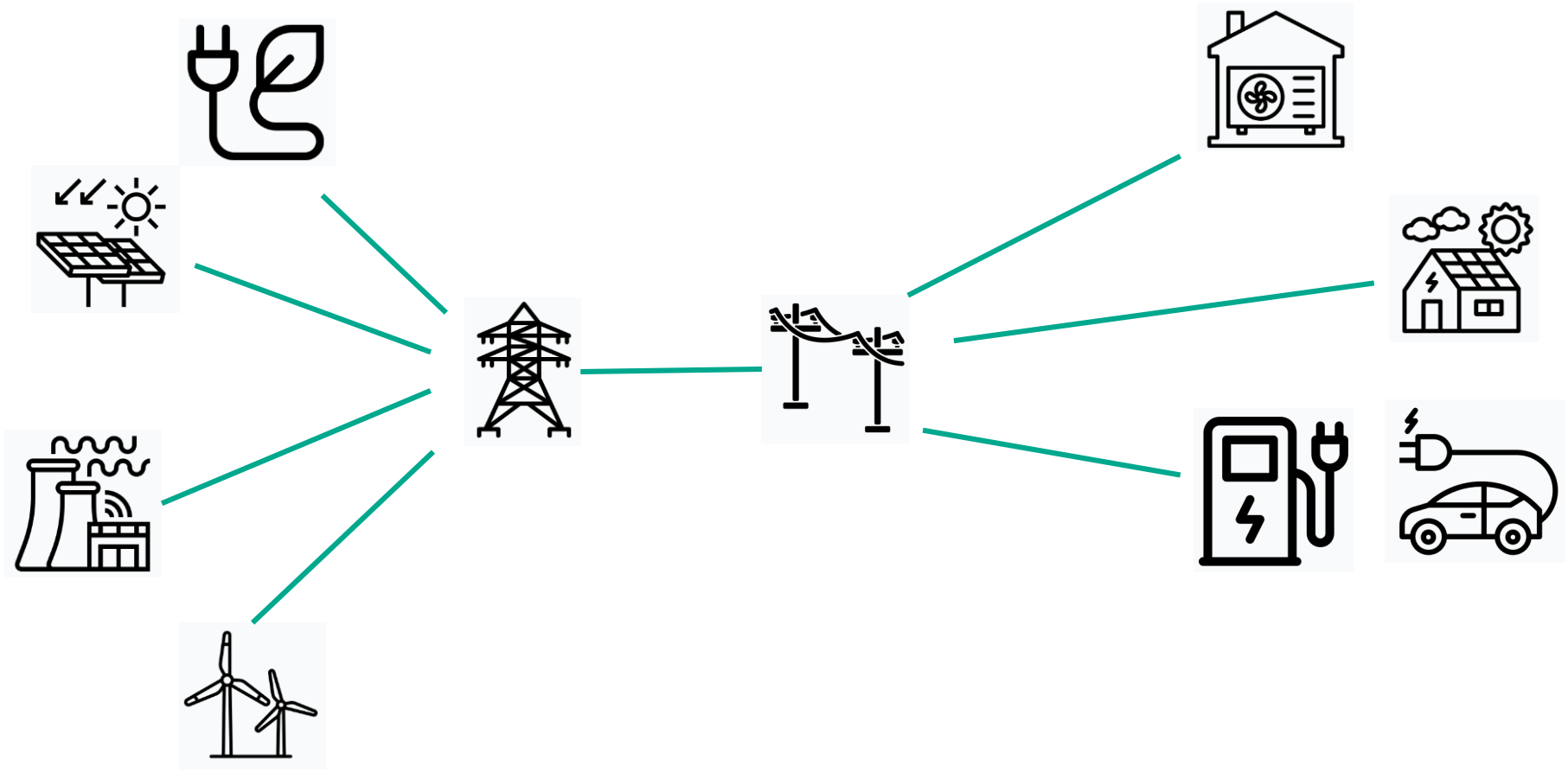
Hydropower

Ocean

Bioenergy

1. Code Security and misconfiguration
2. Unsecured API´s
3. SCADA Systems
4. Automation
5. Remote Control
6. Physical location/security
7. Network or Data traffic
8. Internet connectivity
9. Old infrastructure
10. Missing regulations

Everything is connected



Grid frequency is used as base metric

Production side:
Power plants
Wind
Solar
etc.

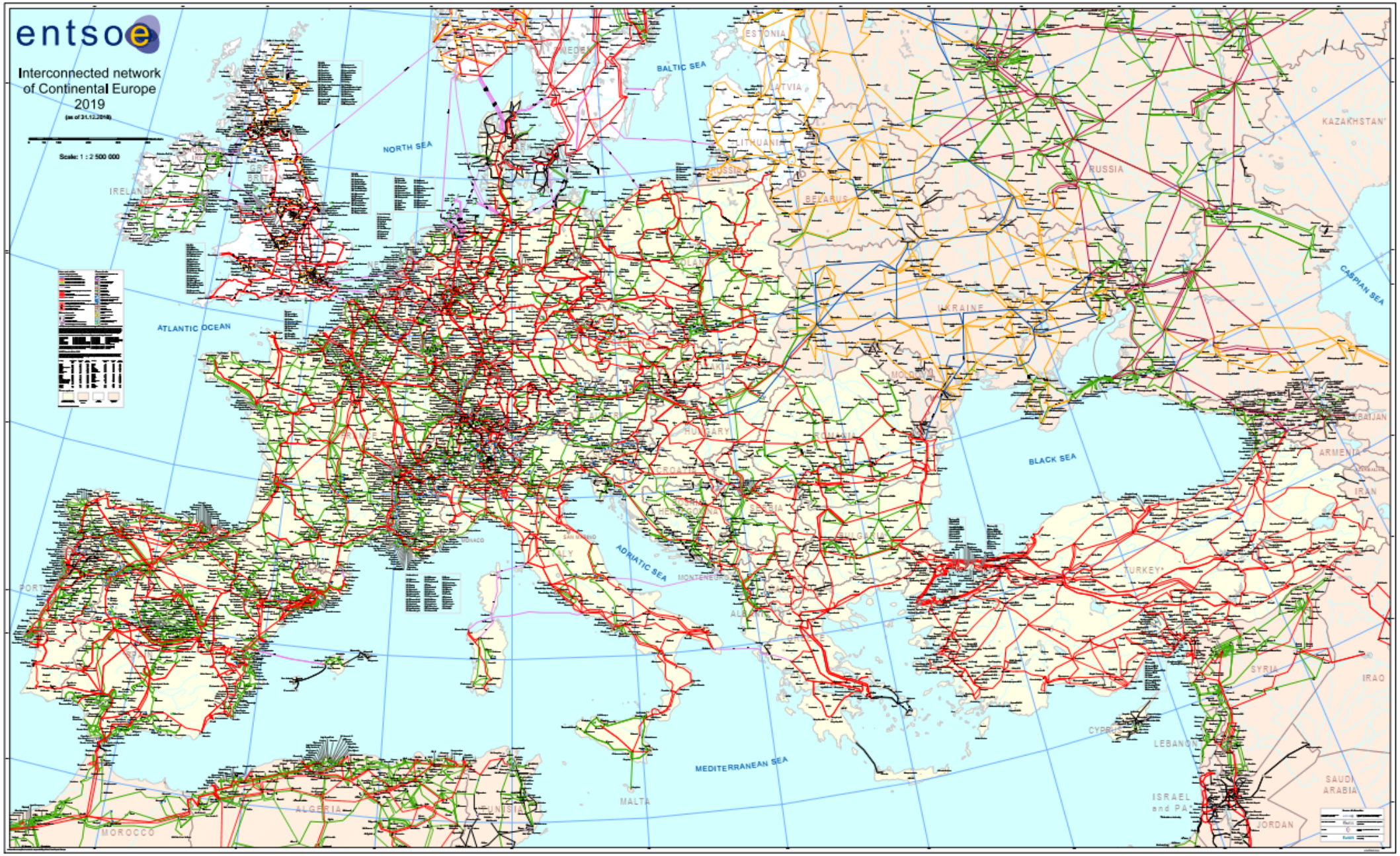
consumption side:
industry
houses
EV
etc.

Picture: (https://www.swissgrid.ch/de/home/operation/regulation/grid-stability.html)

But how is the Grid working?

A quick view

The Grid



Interconnected Network of continental Europe (entso-e) https://www.entsoe.eu/data/map/downloads/

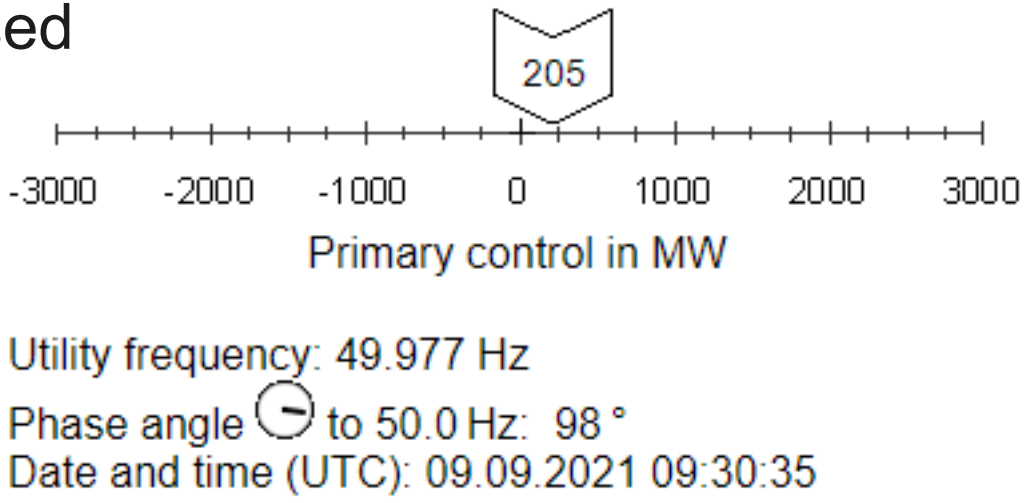
50 hertz

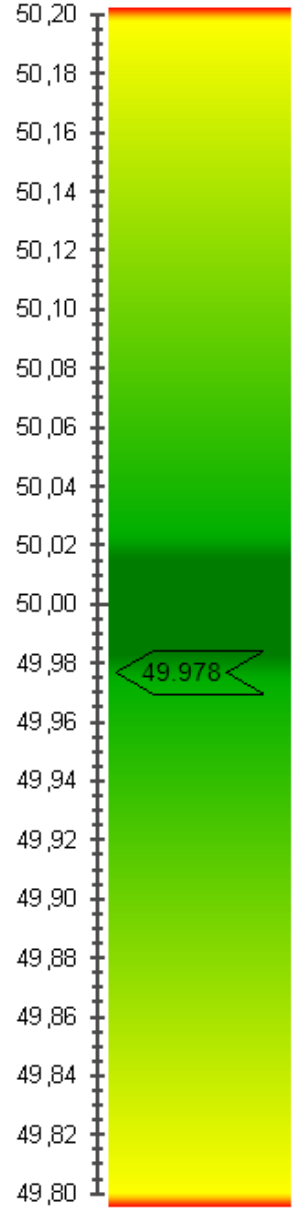
Primary stage control

3000MW control power +-

Primary stage control in range of +- 200mHz

50.2Hz = 3000MW fully dropped
49.8Hz = 3000MW fully used





Picture source: (https://www.mainsfrequency.com/index.htm)

grid frequency levels

Frequency	Action	load sum	activation
51,5 Hz	all renewable energy disconnected from grid	100%	automatic
50,2 Hz	starting of demand side management of renewable energy		automatic
50,1 Hz	no action		
50,0 Hz	Baseline		
49,9 Hz	no action		
49,8 Hz	immediately activating +control power & load shedding of pumps (t<10s)		manual/automatic
49,2 Hz	direct load shedding of storage pumps		automatic
49,0 Hz	load shedding LEVEL 1 , 10-15 %	ca. 12,5 %	automatic
48,8 Hz	load shedding LEVEL 2, 10-15 %	ca. 25,0 %	automatic
48,6 Hz	load shedding LEVEL 3, 10-15 %	ca. 37,5 %	automatic
48,4 Hz	load shedding LEVEL 4, 10-15 %	ca. 50,0 %	automatic
47,5 Hz	disconnecting power plants from grid		automatic

„load shedding“
&
Cyber risk

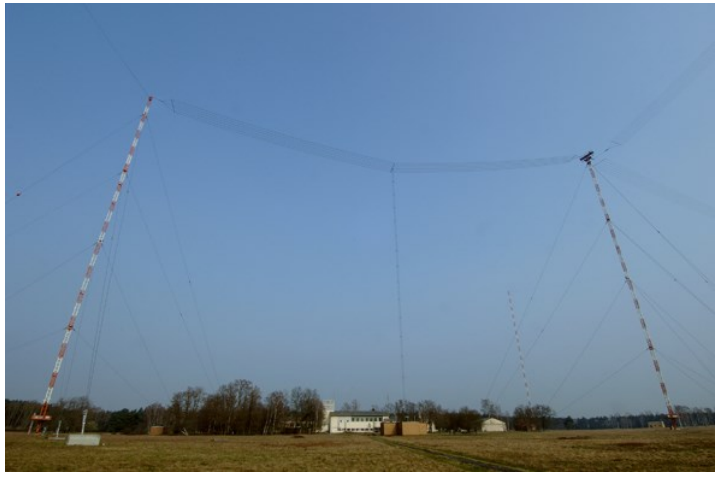
Communication via:

- TETRA
- Radio signal
- **P**ower**l**ine **c**ommunication

No encryption in protocol

Only 3 Radio stations for entire Europe

- Mainflingen, 129,1kHz (DCF49) 100kW
- Burg, 139kHz (DCF39) 50kW
- Lakihegy 135,6kHz (HGA22) 100kW



https://www.ptb.de/cms/en/ptb/fachabteilungen/abt4/fb-44/ag-442/dissemination-of-legal-time/dcf77/localizacion-del-transmisor.html
https://www.google.de/maps/search/mainflingen+sendeanlage/@50.0162799,9.0079328,1486m/data=!3m1!1e3

Is TETRA secure?

TETRA MANAGED SERVICES AGREEMENT FOR xxx xxxx GMBH

xxx relies on its _____ IP network, not only for critical communications but also for grid automation and remote meter reading.

It is therefore essential, that its communications platform is always 100 per cent operational, efficient, reliable and secure.

xxx knew it could trust xxxxxxxx Solutions' TETRA network

(source: hxxps://www.somevendor.com/xxxxxxxxxxx.pdf)

Build your own RF receiver

Antenna: Just one meter of copper wire on balcony

Receiver: RTL-SDR (DVB-T) ~20 €
(https://www.rtl-sdr.com/buy-rtl-sdr-dvb-t-dongles/)

Computer Laptop works, RaspberryPi possible

Software: Linux Mint
TETRA live Monitor
https://github.com/sq5bpf/telive

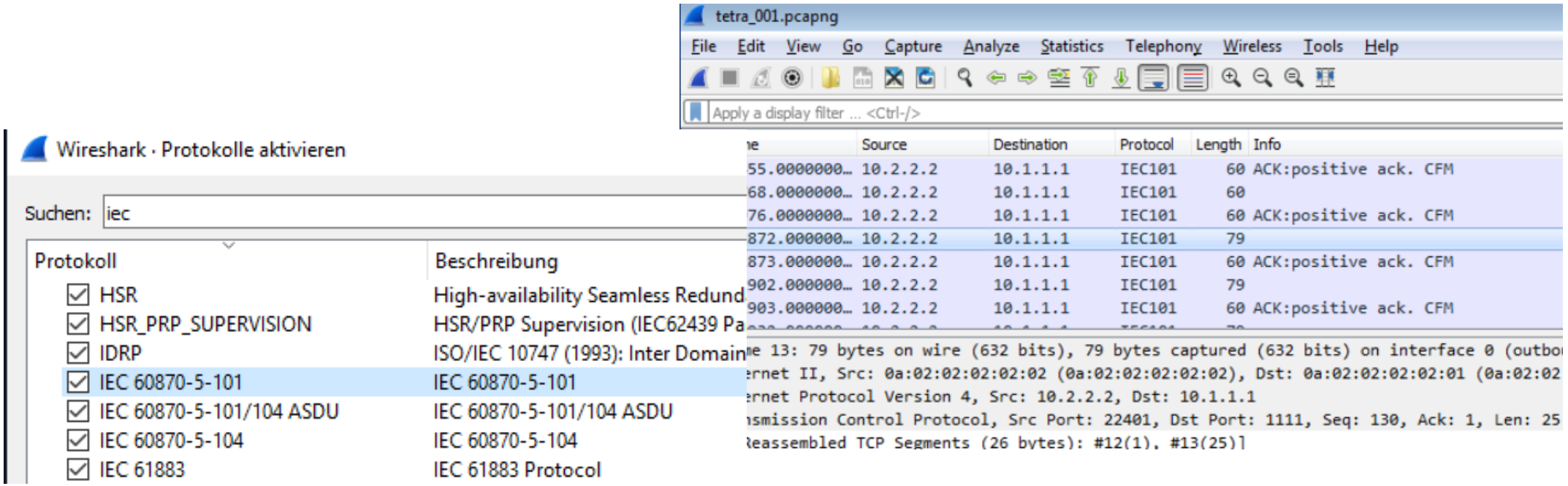
or OSMO-Tetra
https://github.com/osmocom/osmo-tetra

And capture a couple of days

Control frames are send unencrypted

```
20181221 15:43:26 FUNC:SDSDEC [CPTI:1 CalledSSI:9600005 CallingSSI:9600000 CallingEXT:0  UserData4: len:128 protoid:C0
(Teltronic) SDS-TL:[ MsgType:SDS-TRANSFER MSG_REF:164 TO_GROUP:1] DATA:[$H1080E6016716]] RX:1
20181221 15:43:26 FUNC:D-SDS DATA SSI:09600005 IDX:000 IDT:1 ENCR:0 RX:1
```

use wireshark IEC 60870-5-101 Protocol Dissector



Tetra for load shedding

Frequenz (Oberband)	MCC	MNC	LA	Air-Interface-Encryption	End-to-End-Encryption	Daten
426.6625 MHz	262	207	10085	nein	nein	IEC 60870-5-101
426.7125 MHz	262	207	10081	nein	nein	IEC 60870-5-101
427.2375 MHz	262	207	10080	nein	nein	IEC 60870-5-101
426.8875 MHz	262	168	4	nein	nein	IEC 60870-5-101

Digital, but not encrypted !

What´s needed to control the grid in some areas?

software: same as for capturing

Hardware:

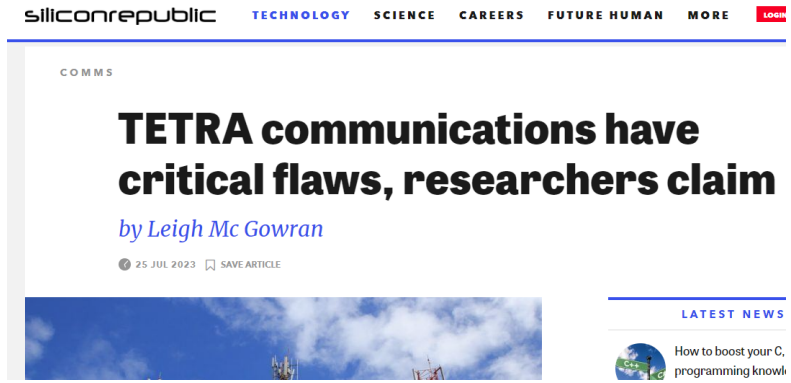
- SDR-Transceiver + amplifier < 300 €

„criminal Energie“

Tetra backdoor

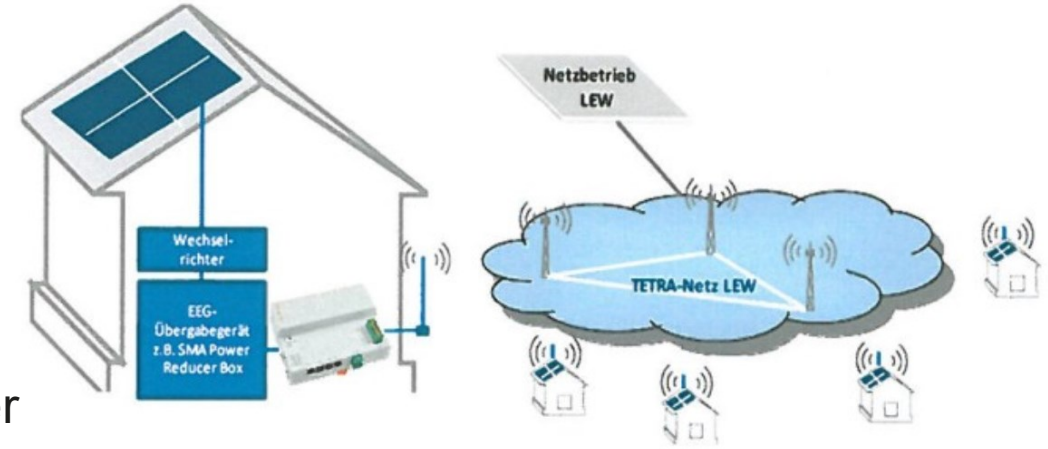
TETRA:BURST

- collection of five vulnerabilities
- two of which are deemed critical,
- affecting the Terrestrial Trunked Radio (TETRA) standard



used by

- ~~law enforcement~~
- ~~Military~~
- critical infrastructure
- industrial asset owners in the power, oil & gas, water and transport sectors and beyond.



https://tetraburst.com/

- RF signals not protected
- Outdated Protocol used
- Mostly no encryption on protocols
- Broken protocols
- 3 RF stations for entire europe

Wind Energy

Wind energy

COMMODITIES NEWS FEBRUARY 28, 2022 / 5:49 PM / UPDATED A YEAR AGO

UPDATE 2-Satellite outage knocks out thousands of Enercon's wind turbines

By Reuters Staff 3 MIN READ

* Remote control of 5,800 wind turbines knocked out

https://www.reuters.com/article/ukraine-crisis-cyber-enercon-idAFL8N2V36NR

Satellite cyber attack paralyzes 11GW of German wind turbines

The communication channels affected are also used by photovoltaic systems.

MARCH 1, 2022 MARIAN WILLUHN

GRIDS & INTEGRATION TECHNOLOGY UTILITY SCALE PV GERMANY

In the event of a communication breakdown, solar and wind power plants automatically switch to a kind of "autopilot."

Image: Matthias Böckel/Pixabay

https://www.pv-magazine.com/2022/03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/

24.Febr 2022

- KA-Sat communication Satellite System belonging to ViaSat was hacked

- Collateral damage to around 5800 wind Turbines using KA-Sat for Internet access

19.Apr 2022
Over 95 per cent of WECs (**W**ind **e**nergy **c**onverters) back online

“A key challenge prevailing at the moment is the backup communication link that is missing from many wind farms”

https://www.enercon.de/en/news/news-detail/cc_news/show/News/over-95-per-cent-of-wecs-back-online-following-disruption-to-satellite-communication/

- SPOF – no backup connection
- RF signals not protected
- Protocols with no security used

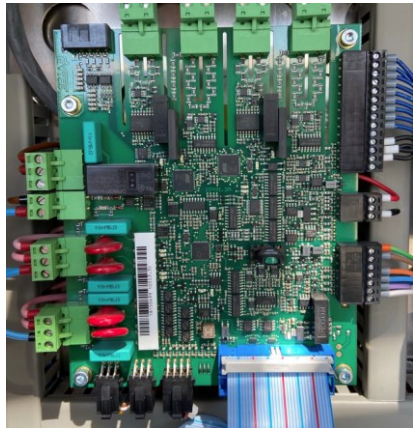
EV charging

Electrical vehicle charging

“charging must be as easy as refueling”

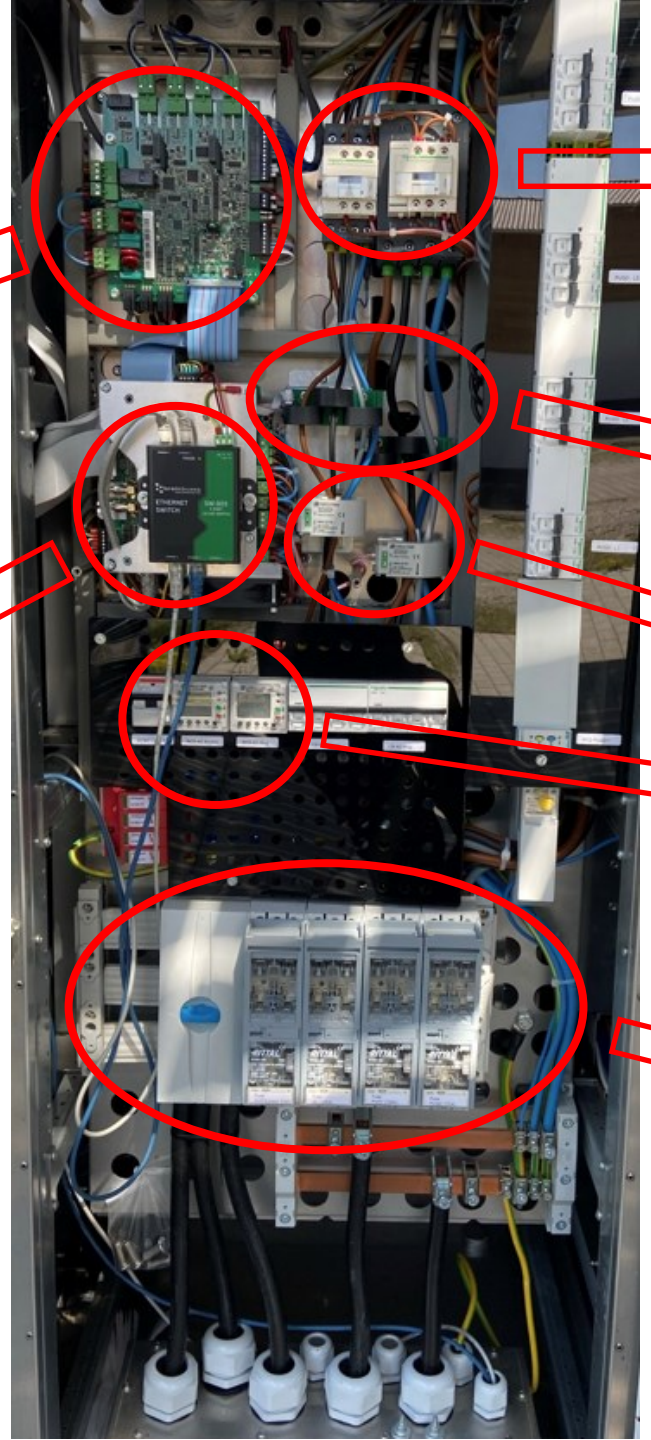
- massive build of infrastructure needed
- Electrical grid need improvement
- Various Payment systems in place
- Each CP needs Internet access

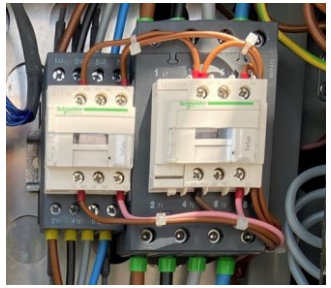
Inside a charging station



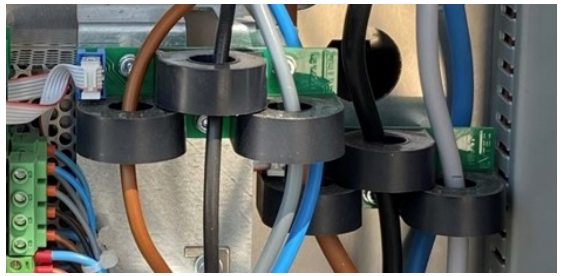
Control electronic

Embedded System & Network

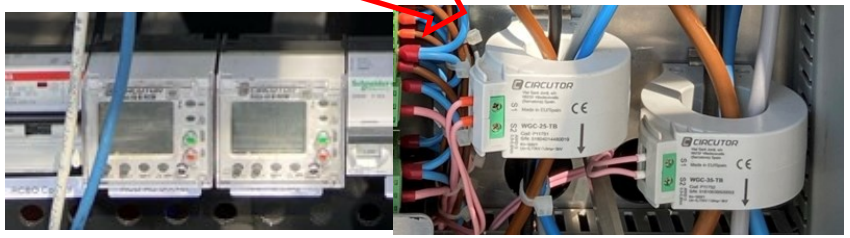




Relais for power connector



Smart Meter



RCD/RCM

Circuit protection (fuses)

Charging point cybersecurity

- Payment cards still insecure
- Easy to clone (for example with flipper zero)
- Wrong implementation of security measures
- No “security by design”
- Missing backend encryption
- And many other

An interesting one: reboot charging station and disconnect cars

Lets see some samples

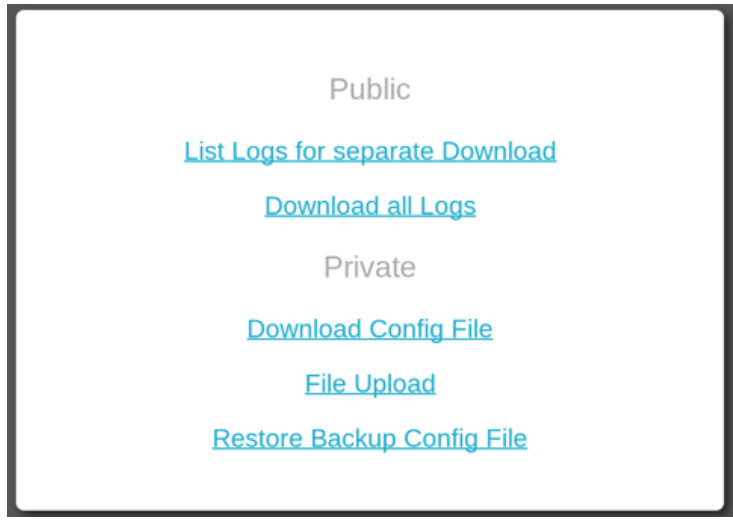
Cyber Security of charging points

Selfmade Lockpick Set

open the lock

nothing protected

access to all Data



Cyber Security of charging points


```
2021-04-20;07:13:06;51152.471;Plug1: AuthPlug Plug1, scanned RFID 13[redacted] / 4A[redacted]80  -> idTag accepted, Transaction State: running
2021-04-20;07:13:06;51152.582;Plug1:   Start charge
2021-04-20;07:13:20;51166.387;Plug1:   SOC Start 56%
2021-04-20;07:13:20;51166.388;Plug1:   Nissan Leaf MY18 (40 kWh) and later, Bidirectional
2021-04-20;07:13:22;51168.384;Plug1:   Enter charge mode
2021-04-20;08:40:23;56388.882;Plug1:   Charge Finished by END_EV_CHARGE_MAXIMUM_LEVEL
2021-04-20;08:40:23;56388.882;Plug1:   Charge SUCCEED, Duration: 87.0min, Energy 16.79kWh
2021-04-20;08:40:23;56388.982;Plug1:   SOC End 100%
2021-04-20;08:40:28;56394.384;Plug1:   Charge power summary, Power Max:                                .9C, Start: 11.5C
2021-04-20;08:41:10;56435.877;-------- begin Linux reboot process ------
2021-04-20;08:41:10;56435.941;!!!!!!!! stop all Transactions !!!!!!!!
2021-04-20;08:41:10;56435.957;End Transaction {'displayName': 'DC CHAdeM                              'energy': 16787.0, 'idTag': 131
```

Copy the charging card UID to an NFC device

Check with Android

Flipper one also works fine!

Whats wrong with the TCP/IP Stack?

Sending a crafted

IP packets

to chrash

communication between CP and backend mostly unencrypted

Latest Version 2.0.1 (March 2020) with first Security Implementations

But, Version 1.6 still minimum required Standard to implement

No need to upgrade existing Charging Stations

- Unsecure Protocols still standard
- Security by design is missing
- Outdated Protocol used
- Physical security needs improvement
- Wrong security configuration

Solar Power System

Power:	**0 W**
Daily yield:	**1497.7 kWh**
Total yield:	**5199.85 MWh**

Language: English

Password:

Login

What is wrong here?

Power:	**0 W**
Daily yield:	**1497.7 kWh**
Total yield:	**5199.85 MWh**

Language: English

Password:

Login

Try to logon with the hardcoded credential succeeded

Developer D1 - 7116 2.00.07.R

And switch off Power production

CWE-259: use of hardcoded Passwords

Description:
The product contains a hard-coded password, which it uses for its own inbound authentication or for outbound communication to external components.

Common consequence:
If hard-coded passwords are used, it is almost certain that malicious users will gain access through the account in question.

Likelihood of Exploit: high

Online solar systems

result from last year

TOTAL RESULTS

21,724

TOP COUNTRIES

Portugal	7,719
Germany	4,657
Greece	2,436
France	883
Belgium	768

More...

result from today

TOTAL RESULTS

16,721

TOP COUNTRIES

Portugal	4,740
Germany	3,666
Greece	2,185
France	696
United States	677

More...

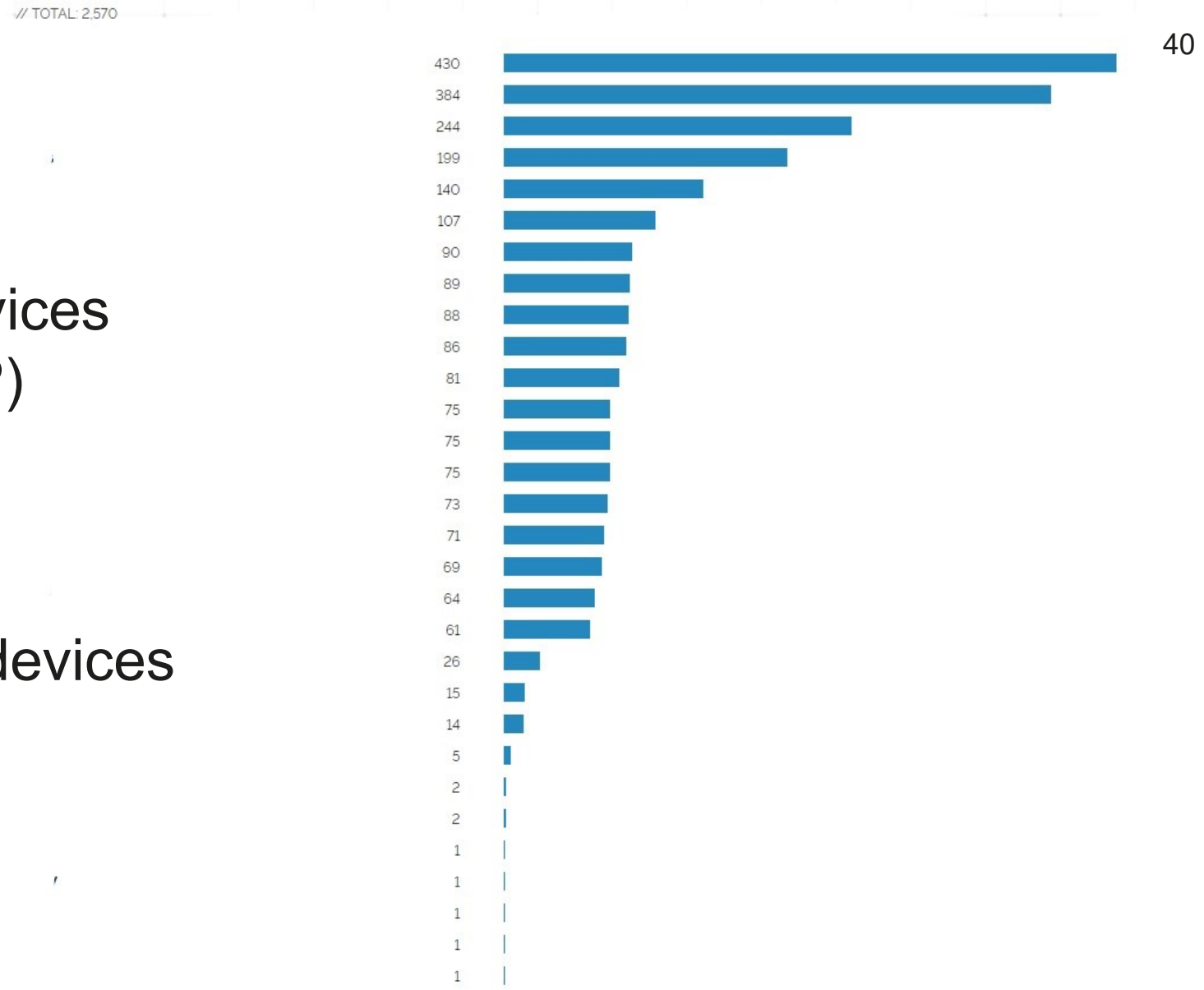
Do some Shodan foo….

Remove home Solar devices
(1 kWP -30 kWP)

Remove honeypots !

Include only vulnerable devices
(1 MW – 5 MW)

#total ~2570

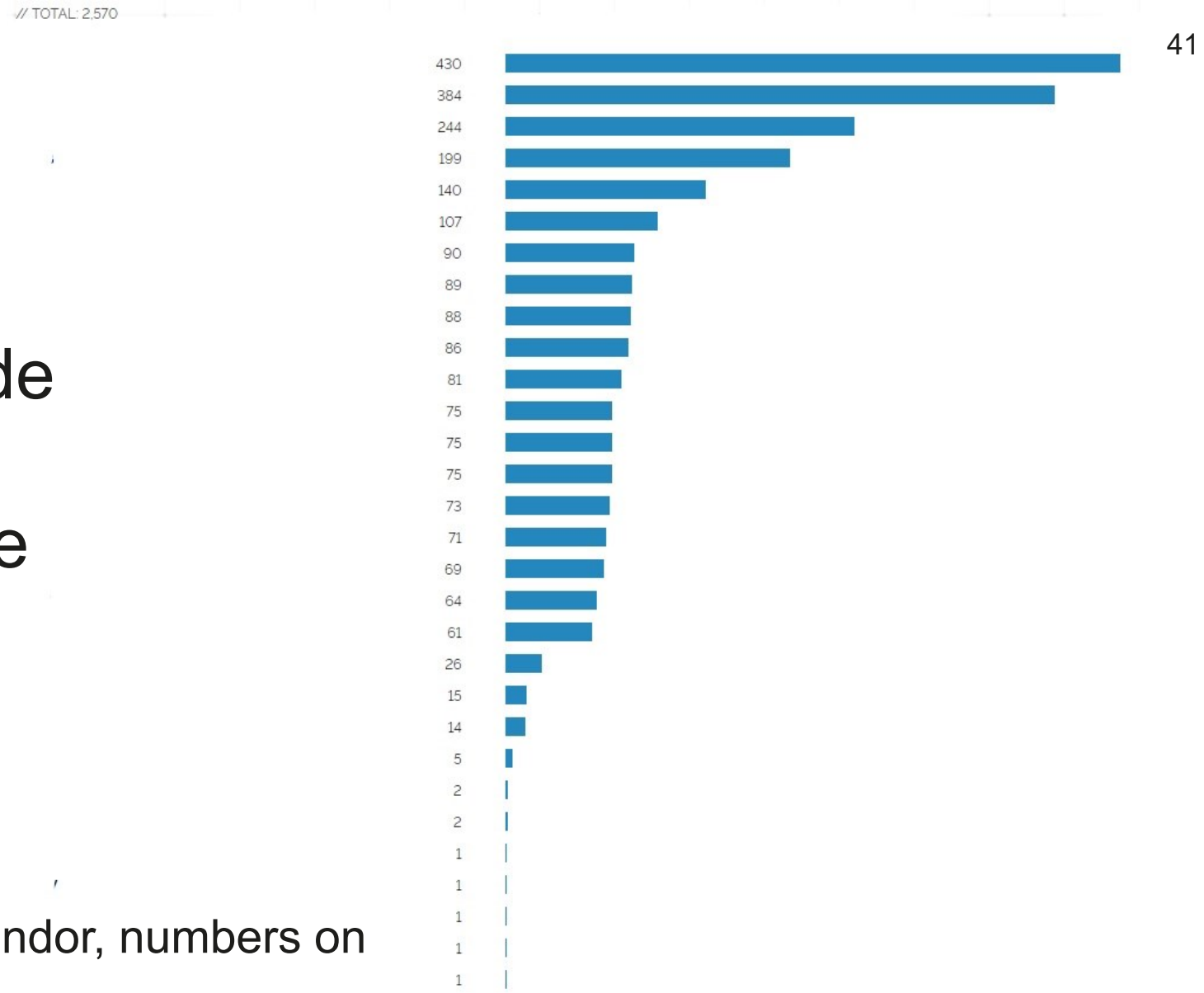


~2570 devices

~ 7200 MW worldwide

Filter out only Europe
~ 2800 MW

Interesting fact:
some time after reporting to Vendor, numbers on Shodan massively decreased



Germany has 7000MW reserve (+CP)

destabilization with ~2800MW now possible

= not enough to directly force a blackout

But what,

if combined all together?

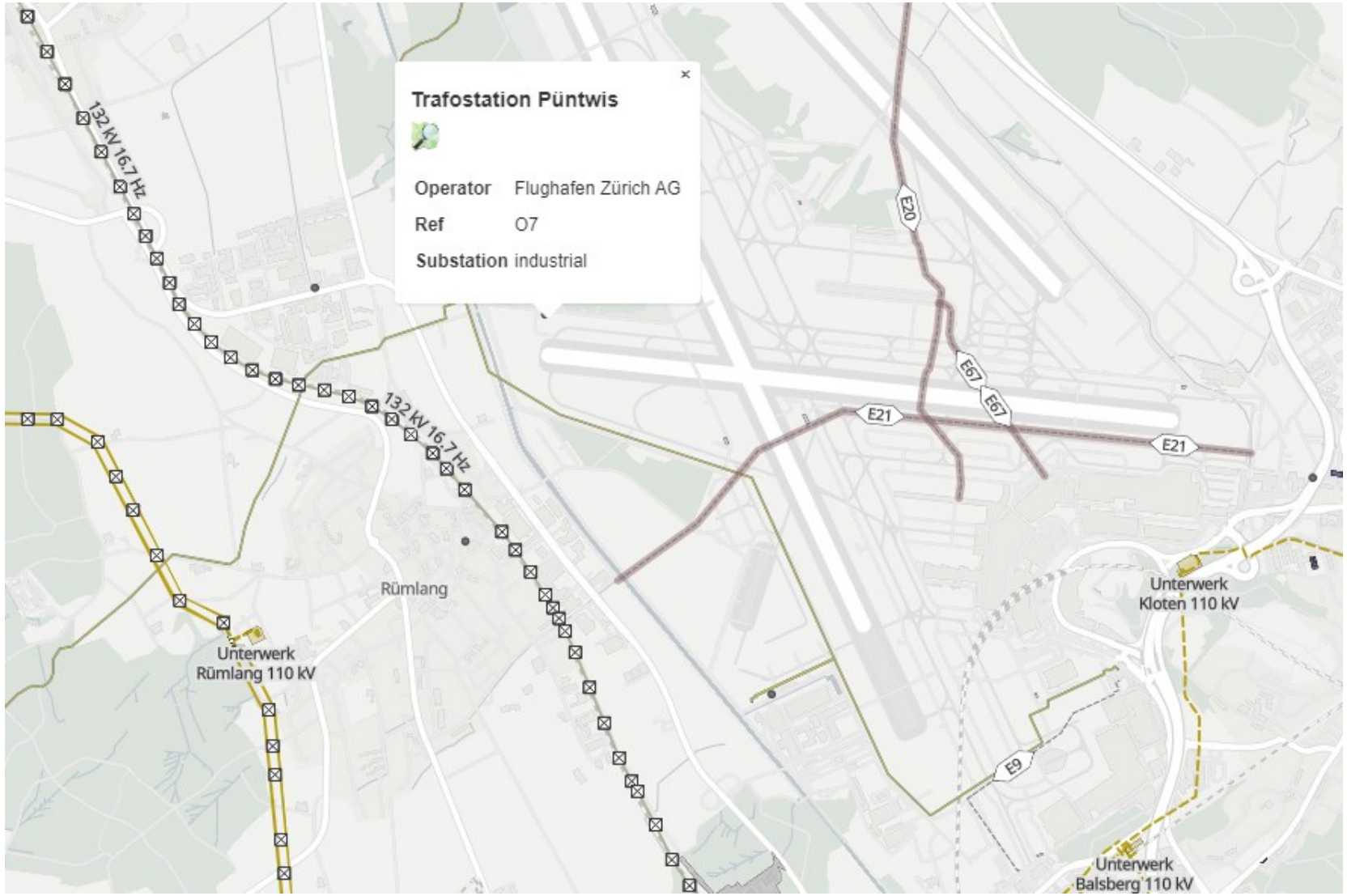
- Load shedding issues
- Solar power inverter
- Wind energy converter
- Home solar power inverter

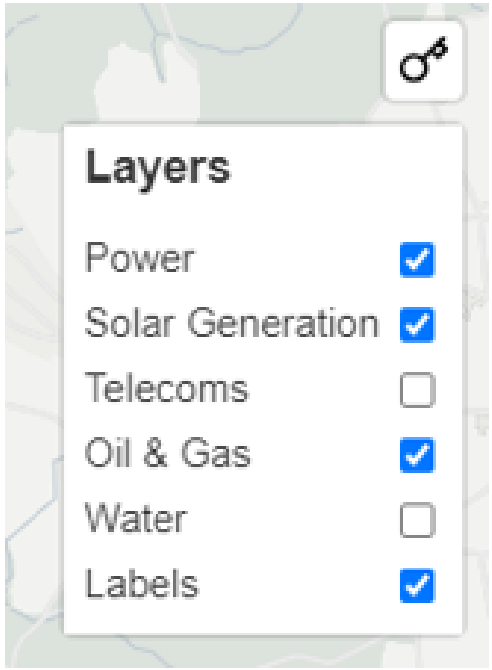
- Code security and wrong configuration
- Security by design is missing
- Outdated Protocol used
- Proprietary radio signals used
- RF not protected

kaspersky

OSINT

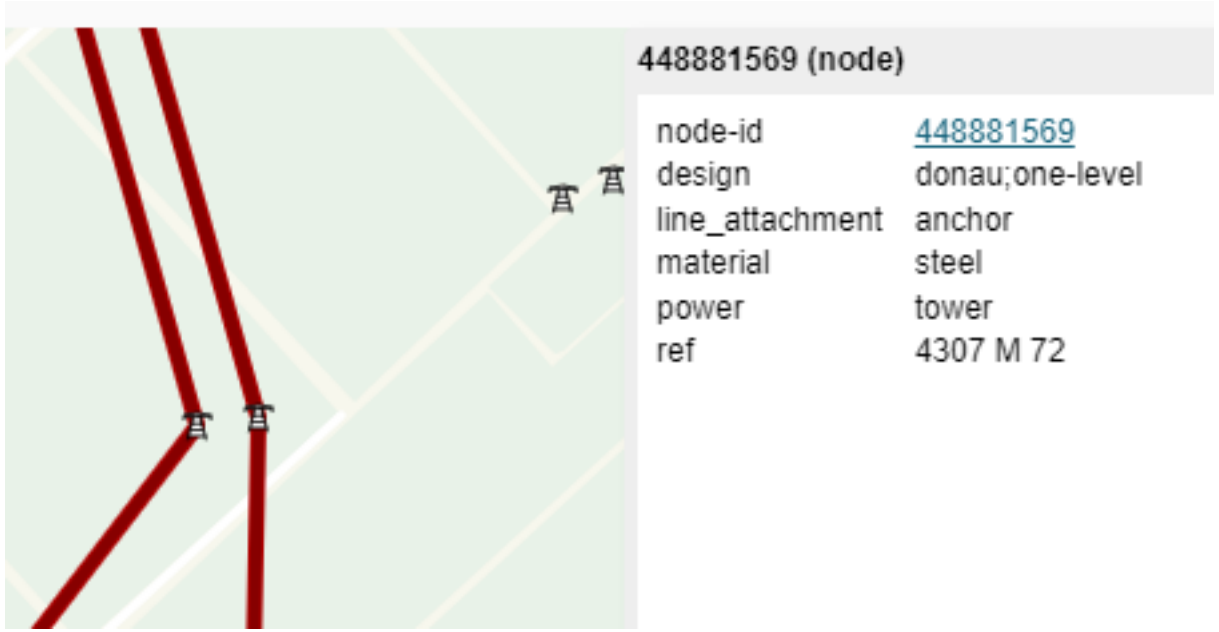
OSINT – Open Source Intelligence

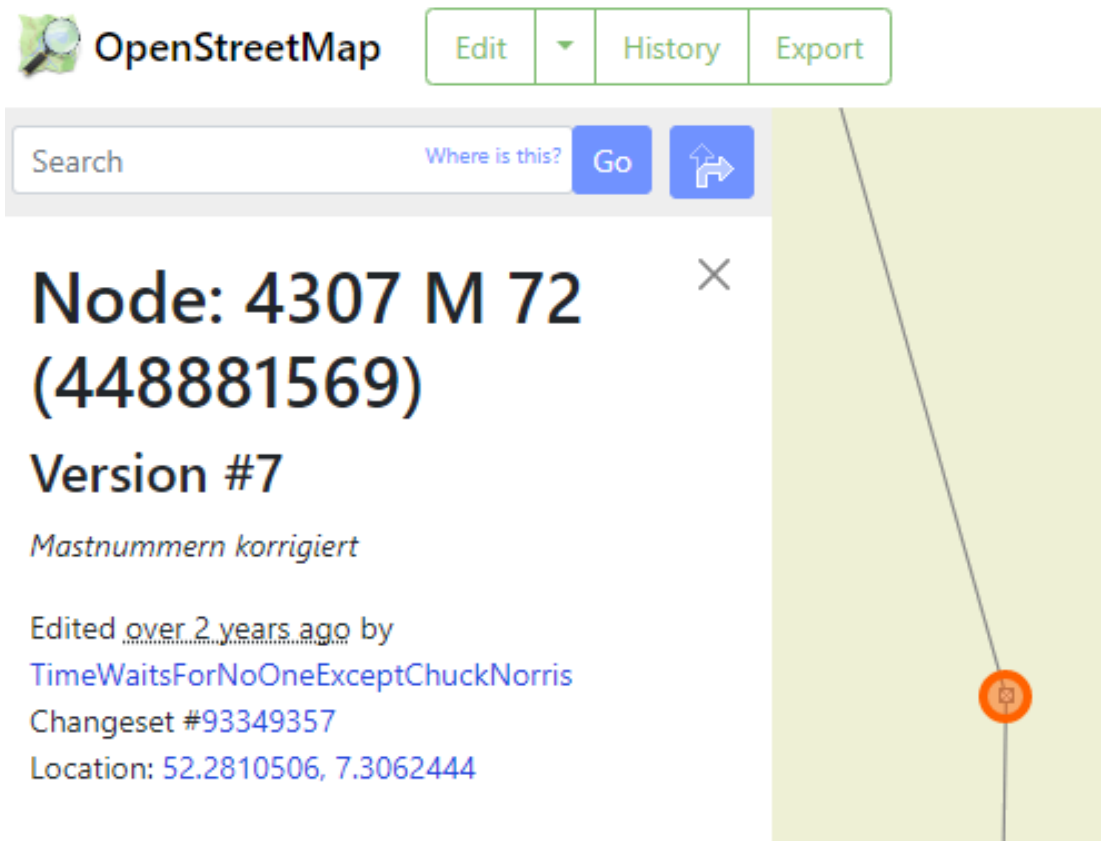




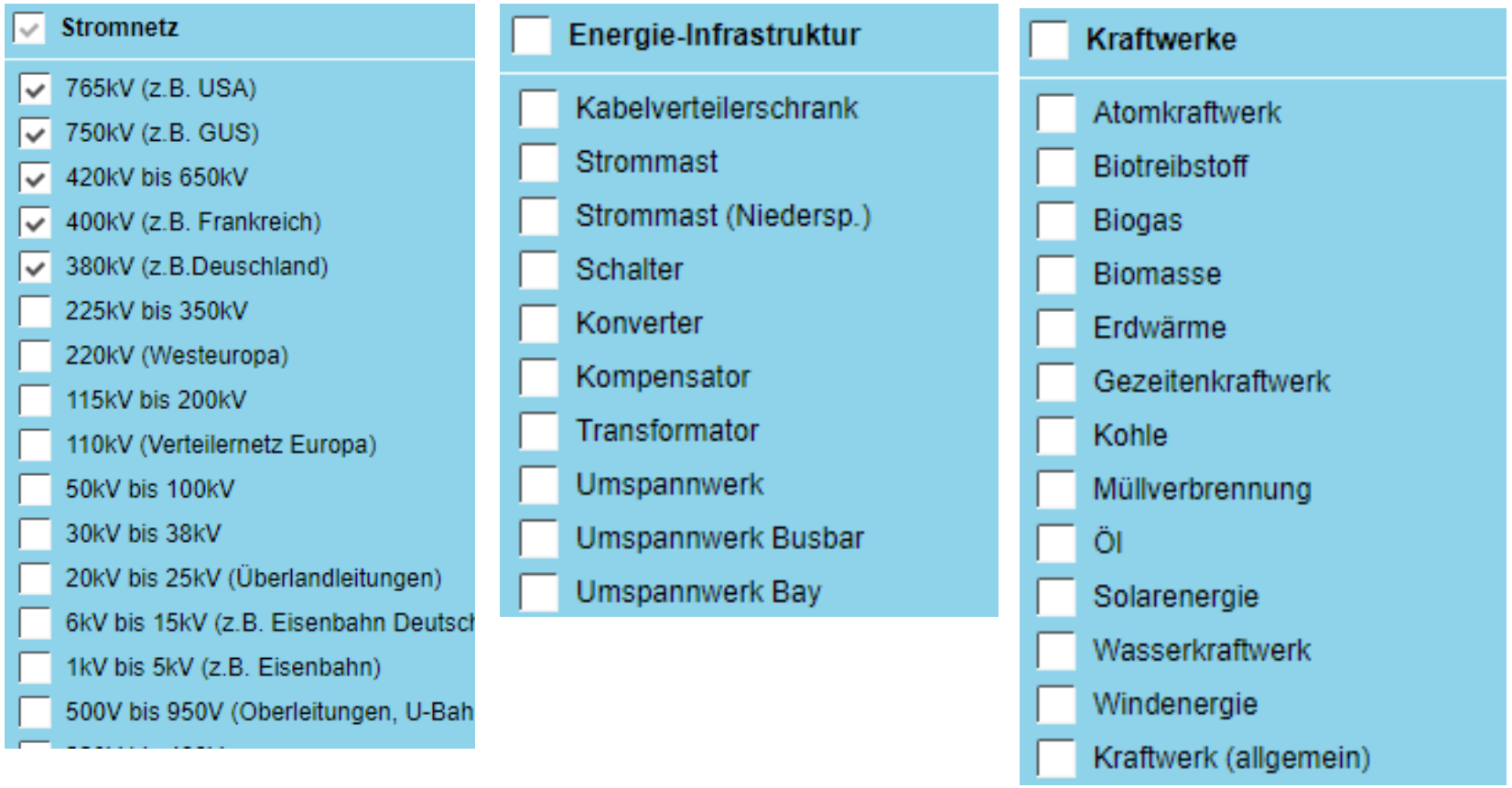
https://openinframap.org/

Wenn Transparenz zum Problem wird





https://www.flosm.de


Stromnetz
765kV (z.B. USA)
750kV (z.B. GUS)
420kV bis 650kV
400kV (z.B. Frankreich)
380kV (z.B.Deuschland)
225kV bis 350kV
220kV (Westeuropa)
115kV bis 200kV
110kV (Verteilernetz Europa)
50kV bis 100kV
30kV bis 38kV
20kV bis 25kV (Überlandleitungen)
6kV bis 15kV (z.B. Eisenbahn Deutsch
1kV bis 5kV (z.B. Eisenbahn)
500V bis 950V (Oberleitungen, U-Bah
Energie-Infrastruktur
Kabelverteilerschrank
Strommast
Strommast (Niedersp.)
Schalter
Konverter
Kompensator
Transformator
Umspannwerk
Umspannwerk Busbar
Umspannwerk Bay
Kraftwerke
Atomkraftwerk
Biotreibstoff
Biogas
Biomasse
Erdwärme
Gezeitenkraftwerk
Kohle
Müllverbrennung
Öl
Solarenergie
Wasserkraftwerk
Windenergie
Kraftwerk (allgemein)

We have seen samples of:

1. Code Security and misconfiguration
2. SCADA Systems
3. Remote Control
4. Physical location/security
5. Network or Data traffic
6. Internet connectivity

What to do?

Defense-in-depth strategy

Products does not protect you 100%.

threat intelligence together with products, tailored TI.

IT/OT security strategy

Train OT specialist on IT security and vice versa

Implement OT Security solutions like KICS for Networks

Thank you!

Stephan Gerling

Senior Security Researcher
Kaspersky ICS-CERT

@obiwan666

kaspersky