

ITSA 2022

Energiewende

Herausforderung für die Cybersicherheit

Stephan Gerling

kaspersky



Energiewende

Herausforderung für die Cybersicherheit



Stephan Gerling

Senior Security Researcher
Kaspersky ICS-CERT

@ObiWan666

Aktuelle Cyber Risiken für Erneuerbare Energie

Hack gegen Satellitennetzwerk

Angriff auf "Ka-Sat 9A"

4. April 2022, 13:30 Uhr | Leszeit: 3 min



Steckt Cyberangriff dahinter?

Steuerung von Tausenden Windräd

28.03.2022, 18:38 Uhr



Windräder von Enercon. Wegen des Hackerangriffs gegen ein Satellitennetzwerk waren 5800 der Anlagen des Unternehmens in Deutschland offline. (Foto: Jan Wotjak/dpa)



Nach Cyberangriff: Störung bei Windkraft-Fernwartung behoben

Stand: 29.04.2022 17:48 Uhr

Die betroffenen Anlagen laufen zwar, können aber nicht mehr aus der Ferne gesteuert werden.
(Foto: picture alliance/dpa/dpa-Zentralbild)

Kurzschluss in Hochspannungsnetz legt Windpark lahm.

NOS Nieuws Sport Uitzendingen



NOS Nieuws - Vrijdag 2 september, 16:27 - Aangepast vrijdag 2 september, 21:06

**Grote stroomstoring Flevoland na brand,
noodvoorzieningen werkten niet**

zeewolde_online @zeewolde_online Sep 4
#Windpark Zeewolde tijdelijk #stilgevallen door stroomstoring
omroepflevoland.nl/nieuws/30... via #zeewolde_online



Windpark Zeewolde tijdelijk stilgevallen door stroomstoring
De helft van de windmolens van Windpark Zeewolde staat momenteel nog stil, als gevolg van de stroomstoring in de provincie van vrijdag. Volgens Sjoerd Sieburgh Sjoerdsma, directeur van het windpark,...

omroepflevoland.nl

Solarkraftwerke

Tausende Online zu finden

query

Online Solarkraftwerke

(shodan.hq query)

TOTAL RESULTS

21,724

TOP COUNTRIES



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

[More...](#)

Verwundbare Systeme online

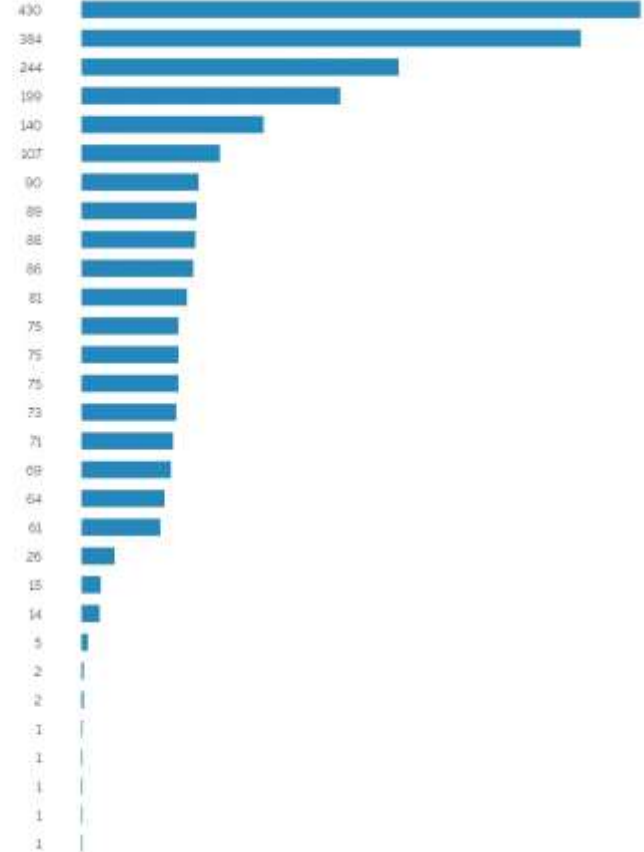
~2570 Solarkraftwerke

~ Weltweit 7200 MW

Davon in Europa:

~ 2800 MW

Nach Meldung und Patching sank die Zahl
Von 930 auf 760 **Geräte** Online

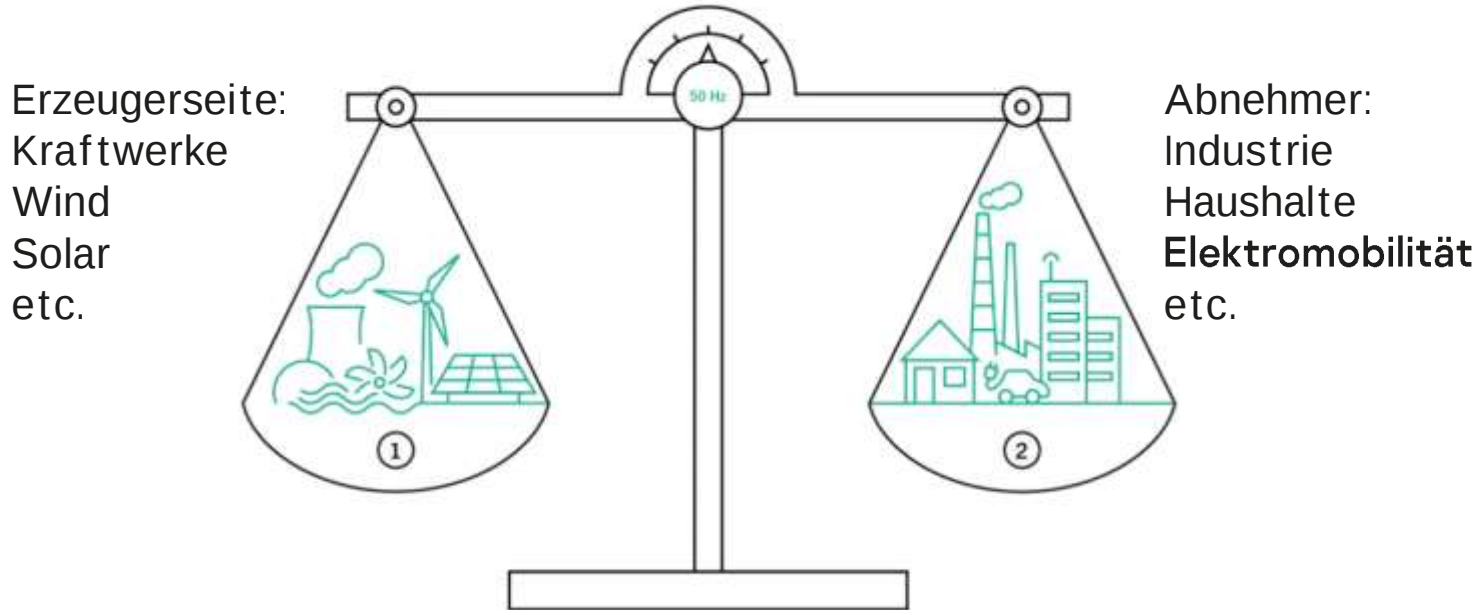


The Grid



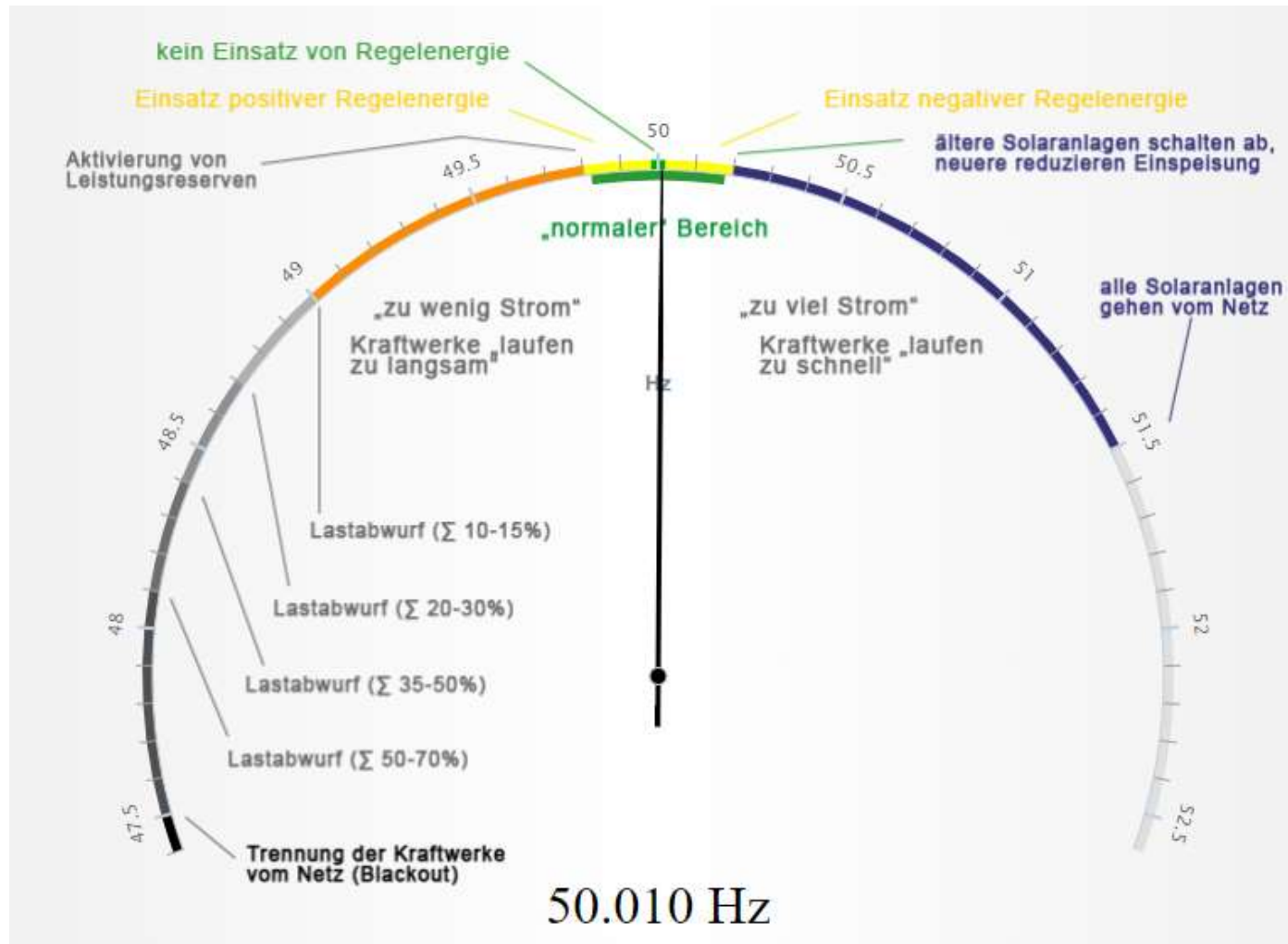
Interconnected Network of continental Europe (entso-e) <https://www.entsoe.eu/data/map/downloads/>

50 Hertz ist die Basis für die Netzstabilität



50 hertz

12



<https://www.netzfrequenz.info/aktuelle-netzfrequenz-full>

„Lastabwurf“ „Regelenergie“

Was? Wie?

Wie funktionieren

- Einspeiseregulierung
- Lastabwurf

Rundsteuertechnik

- PLC (Power line communication)
- Funk (TETRA, Langwelle,)



Regelleistung in Deutschland ~ 7000MW

~2800MW Leistung mit Cyber Risiko

Nicht genug **für** ein Blackout,

aber....

Einspeiseregulierung

Funk:

- TETRA
- Langwelle



Stromnetz:

- aufmoduliertes Signal



Powerline communication (PLC)

- 110Hz – 2000 Hz Amplituden Moduliertes Signal
- Typischerweise in 10kV, 20kV oder 35kV Netz
- Leistung: 80kVA – 200kVA, bis hin zu 2400kVA



Pictures: Transmitter, serial coupling, receiver Picture source: (<http://www.vlf.it/polard/rcf.html>)

Rundsteuersignal via Funk

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

Example: Semagyr Protocoll DIN 43861 part 3 & 4

- Start 68h
- L lenght User data
- L number of replies
- Start replies 68h
- secuencenum (07-F7h + 10h-Increment each sequence)
- rcpt address 1.Byte
- rcpt address 2.Byte
- User data 2-15 Bytes
- * functional and Adressbyte
- * max. 5 Byte functional specs
- * single or group addressing and relais info
- checksum
- Stop 16h

Lastabwurf mittels Tetra

Frequenzbereiche

2.1 Frequenzbereich 410 – 420 MHz / 420 - 430 MHz

Frequenzteilbereiche:	410,00 – 420,00 MHz	420,00 – 430,00 MHz
Bandbreite Teilband:	10,0 MHz	10,0 MHz
Frequenzgruppe:	Unterband	Oberband
Betriebsart	Duplex	
Maximal zulässige äquivalente Strahlungsleistung:	Mobile Funkstellen 6 W ERP (12,5-kHz-Systeme) 12 W ERP (25-kHz-Systeme) 12 W ERP (50-kHz-Systeme)	Ortsfeste Funkstellen 100 W ERP (12,5-kHz-Systeme) 200 W ERP (25-kHz-Systeme) 200 W ERP (50-kHz-Systeme)
Kanalbandbreite	12,5 kHz / 25 kHz / 50 kHz	
Kanalabstand:	12,5 kHz / 25 kHz / 50 kHz	

Source: (https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/Verwaltungsvorschriften/VV_B%C3%BCFu.pdf?__blob=publicationFile&v=4)

Ist TETRA Funk Sicher?

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: <https://www.somevendor.com/xxxxxxxxxxxxx.pdf>)

DIY TETRA Empfänger bauen

Antenne: Etwas Kupferkabel auf dem Balkon

Empfänger: RTL-SDR (DVB-T) ~20 €

(<https://www.rtl-sdr.com/buy-rtl-sdr-dvb-t-dongles/>)

Computer: Laptop, Raspberry Pi geht auch

Software: Linux Mint

TETRA live Monitor <https://github.com/sq5bpf/telive>

Und nun ein paar Tage Daten über Funk sammeln und auswerten



Lastregelung über TETRA Funk

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

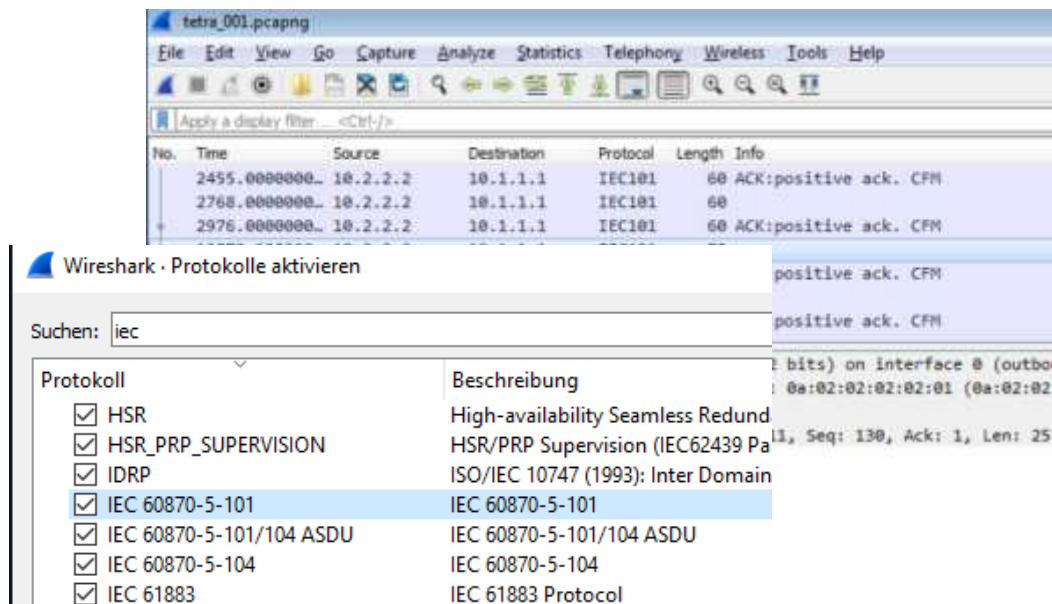
Digital? → Ja

Verschlüsselte Übertragung? → Nein!

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



DIY Rundsteuersender

Software:

- <https://github.com/osmocom/osmo-tetra>

Hardware:

- SDR- Sender/Empfänger (~ 300 €)



Weitere Infos

Halle 7, Stand 7-311!



Stephan Gerling

Senior Security Researcher
Kaspersky ICS-CERT

@obiwan666

kaspersky