IoT/OT Security Conference Cham

Into the Dark

Geopolitik
Angriffsgeografien
Branchenfokus

Stephan Gerling

kaspersky

Into the Dark

Geopolitik, Angriffsgeografien, Branchenfokus

Stephan Gerling

Senior Security Researcher
Kaspersky ICS-CERT

@ObiWan666

Windkraft

ERNEUERBARE ENERGIEN

Massive Störung der Satellitenverbindung: Enercon meldet fast 6000 betroffene Windanlagen

Der Störfall bei einem Satellitenanbieter weckt Sorgen vor einem Hackerangriff. Betroffen sind Anlagen mit einer Gesamtleistung von elf Gigawatt.

Larissa Holzki, Lars-Marten Nagel, Michael Verfürden, Kathrin Witsch

28.02.2022 • Update: 28.02.2022 - 17:09 Uhr • Kommentieren • 43 x

Bruch einer Hochspannungsleitung

Großer Stromausfall in niederländischer Provinz - Menschen sitzen in Zügen fest

rom ausgefallen. Weil
Straßen gesperrt und der

Stromausfall im zentralen Teil der Niederlande verursachte Rekordschäden an der Eisenbahninfrastruktur

3 September 2022 38

Solar Power Systems

TOTAL RESULTS

1,360,082

TOP COUNTRIES

United States	279,000
Japan	136,285
Germany	72,557
France	69,658

View Report Do

New Service: Keep tr

100.24.107.71

ec2-100-24-107-71.compute-1.amazonaws.com

Amazon Data Services NoVa

United States, Ashburn

cloud honeypot

54.219.202.104

ec2-54-219-202-104.us-west-1.compute.amazonaws.com

Amazon.com, Inc.

United States, San Jose

cloud honeypot

(shodan.hq query)

Wer suchet, der findet.

Power:	1004 W
Daily yield:	2.68 kWh
Total yield:	34.85 MWh

Language: English

Password:

Login

Der Klassiker

Potenza:	**0 W**
Rendimento giornaliero:	**0 Wh**
Rendimento totale:	**13,02 GWh**

Lingua: Italiano

Password:

Entra

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

Language: English

Password:

Login

#1 Problem – Hardcoded credentials

Developer D1 - 7116 2.00.07.R

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...

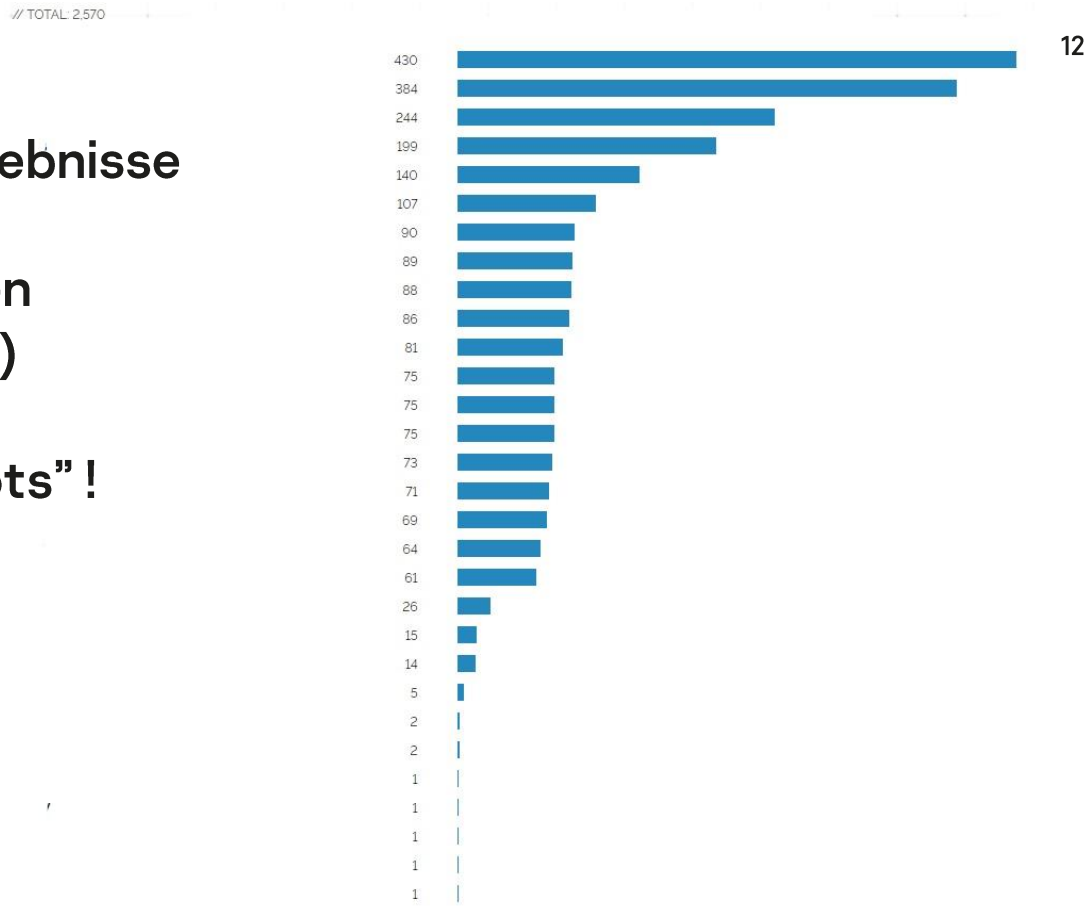
Etwas Magie auf die Ergebnisse

- Keine kleine PV Anlagen
  (1 kWP -30 kWP)

- Weg mit den “honeypots” !

+ nur die dicken Fische!
  (1 MW – 5 MW)

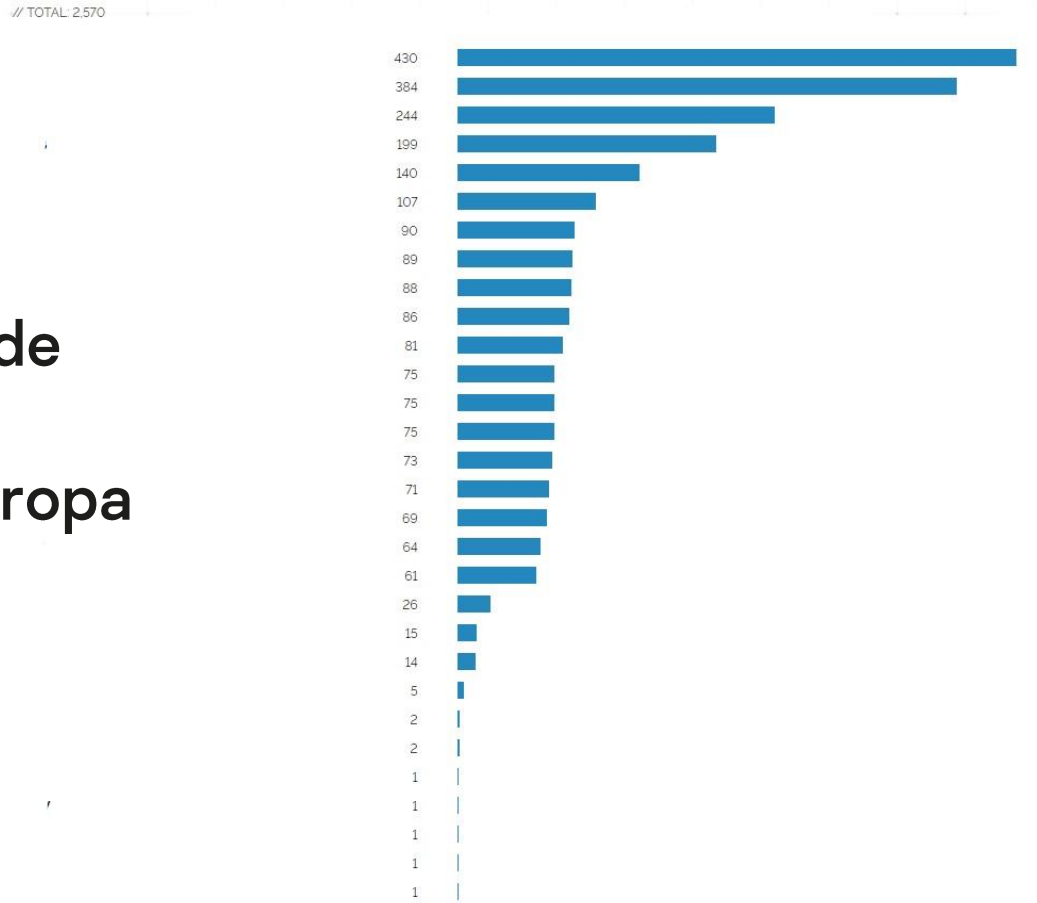
#total ~2570



~2570 Anlagen

~ 7200 MW worldwide

Ergebniss nur für Europa
~ 2800 MW



Positiv:

- Meldung der Sicherheitslücke an den Hersteller
- Patch wurde rasch bereitgestellt
- Zusätzlich Meldung an das BSI

Ergebniss:

Zahl der angreifbaren Anlagen geht immer weiter zurück.

Welche Auswirkung hätte es haben können?

Ein kleiner Blick in das Europäische Stromnetz

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

Netzfrequenz von 50 Hz als Regelbasis

Erzeuger :
Kraftwerke
Wind
Solar
Speicher
etc.

Verbraucher:
Industrie
Bewohner
Elektromobilität

etc.

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

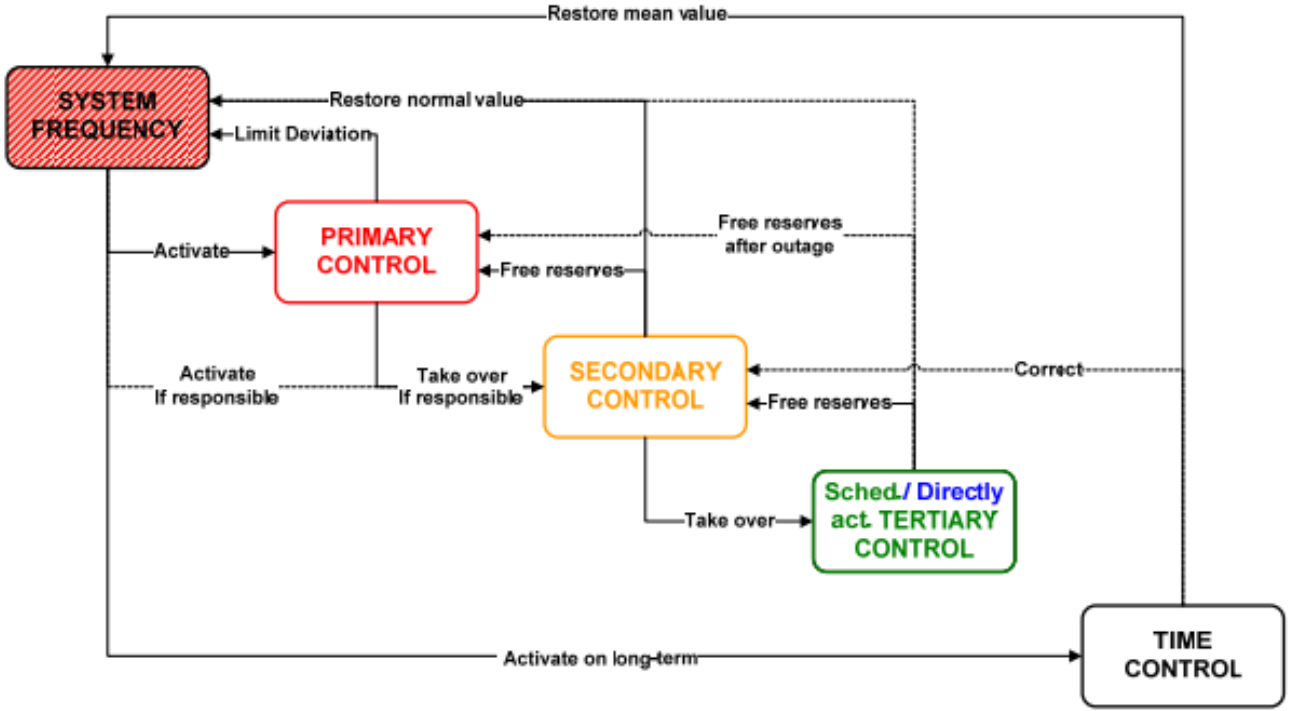


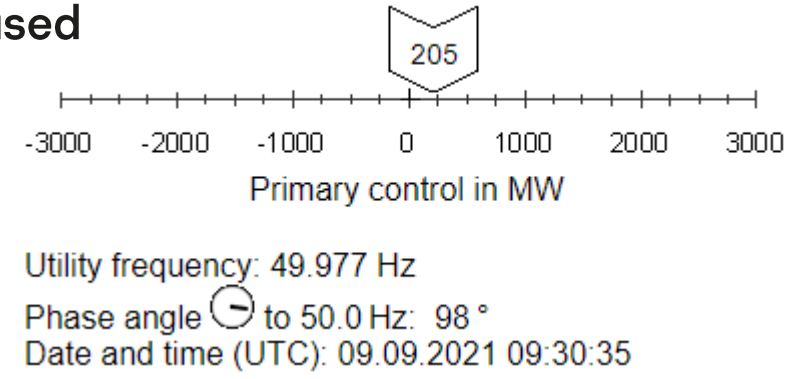
Figure 2: Control scheme and actions starting with the system frequency

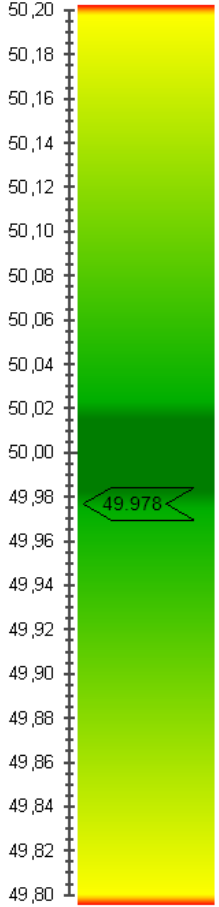
Picture: (https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/ce/oh/Policy1_final.pdf)

Primary stage control

deviation > +- 10mHz
- +- 3000MW control power

Primary stage control in range of +- 200mHz
50.2Hz = 3000MW fully dropped
49.8Hz = 3000MW fully used



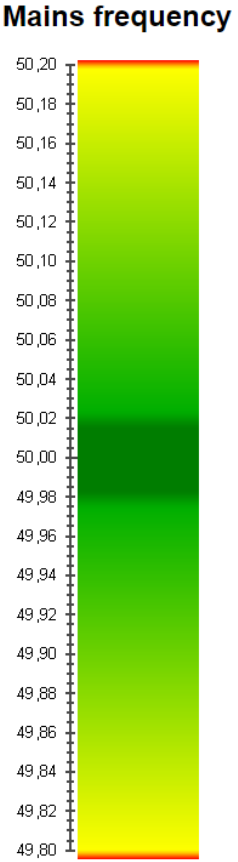


Picture source: (https://www.mainsfrequency.com/index.htm)

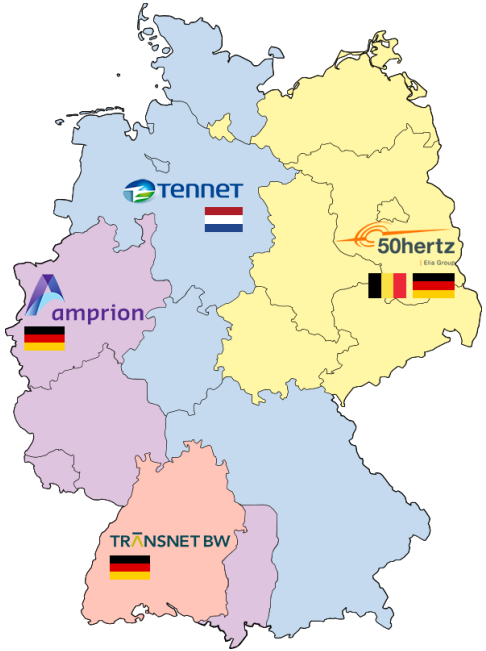
50 hertz

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



German Grid stabilization



In total:
7000MW +CP
5500MW -CP

+CP = reserve power and dropping loads
-CP = dropping renewable Energy

„Lastabwurf “

Wie funktioniert Lastabwurf “load shedding”

mittels “Rundsteuerempfänger”

- PLC (Power line communication)
- RF signals (TETRA, others)

Picture Source: (https://de.wikipedia.org/wiki/Rundsteuertechnik & https://de.wikipedia.org/wiki/Funkrundsteuertechnik)

Load shedding

- TETRA
- Funk „Langwelle“
- PLC

PLC – power line communication

- 110 – 2000 Hz Amplituden Moduliertes Signal
- Einkopplung in 10kV, 20kV or 35kV Umspannwerken auf allen 3 Phasen
- 80kVA – 200kVA, bis zu 2400kVA Leistung

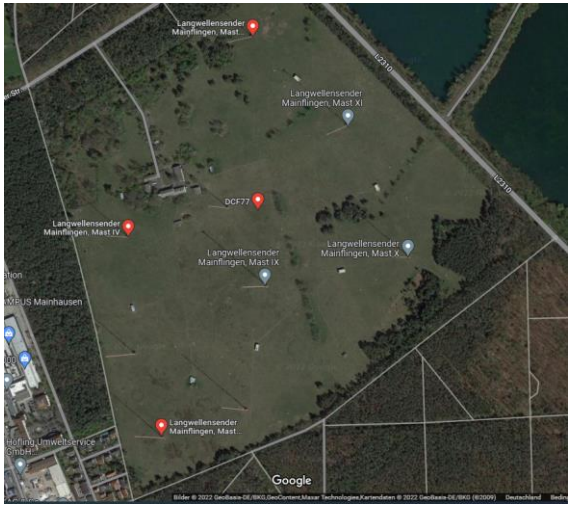
Pictures: Transmitter, serial coupling, receiver Picture source: (http://www.vlf.it/polard/rcf.html)

Beispiel Straßenbeleuchtung

Heligkeitsensoren senden ein Signal per IT an Rundsteuerzentrale in Mainflingen

Mainflingen sendet ein Funksignal auf 129.1kHz
Um das Licht ein/aus zu schalten

Mainflingen DCF77 station



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

Frequenzen in Deutschland “Rundsteuertechnik”

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

Und viele weitere

Funkfrequenzen in DE für “Rundsteuertechnik”

Ort	Netzbetreiber	Vers.- Gebiet	Best.	Freq. [Hz]	Einspeiseebene [kV]	Impulsraster	Bemerkung
Aachen	ASEAG Energie GmbH		⊖	383,3	P20,P10		
Aachen	Finanzamt Aachen, Camp Eschweiler		⊖	200	_0.4		
Aachen	Finanzamt Aachen, de Gete		⊖	1350	P0.4		
Aachen	Finanzamt Aachen, Lager Brand		⊖	600	_0.4		
Aachen	Stadtwerke Aachen AG (STAWAG)		⊕	750	P10	Decabit	
Aalen	Stadtwerke Aalen		⊗	228	P20	Ricontic s	
Achern/Baden	Süwag Energie AG	Überlandwerk Achern	⊗	216,7	S20	Ricontic b	
Achim b. Bremen	Stadtwerke Achim AG		⊖	383,3	P20	Ricontic b	
Ahaus	Stadtwerke Ahaus GmbH		⊖	316,7	P10		
Albstadt	Albstadtwerke		⊗	383,3	P20	Semagyr 50	
Albstadt	Elektrizitätswerk Ebingen Gebr. Haux GmbH & Co. KG		⊖	725	P20		
	Elektrizitätswerk Ebingen Gebr. Haux						

Source: https://rundsteuerung.de/frequenzen/deutschland.html

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

Tetra for load shedding

Frequencies to use

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 sicherer?

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)

TETRA Rundsteuertechnik Analyse

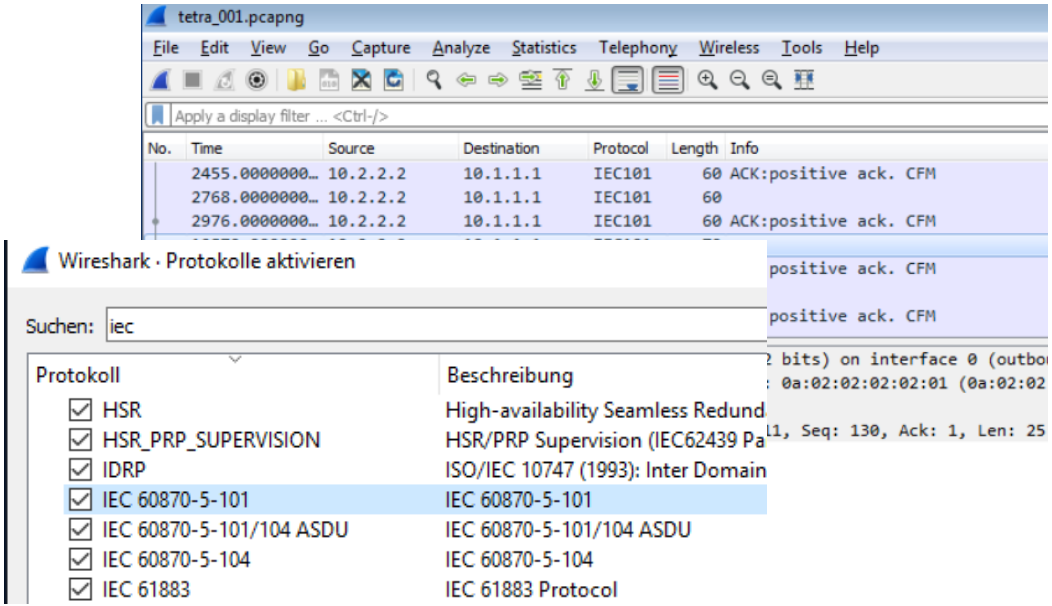
Frequenz (Oberband)	MCC	MNC	LA	Air-Interface-Encryption	End-to-End-Encryption	Daten
426.6625 MHz	262	207	10085	nein	nein	IEC 60870-5-101
426.7125 MHz	262	207	10081	nein	nein	IEC 60870-5-101
427.2375 MHz	262	207	10080	nein	nein	IEC 60870-5-101
426.8875 MHz	262	168	4	nein	nein	IEC 60870-5-101

Yes → digital
No → not encrypted

Übertragung der Signale Unverschlüsselt

```
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
```

Wireshark IEC 60870-5-101 Protocol Dissector



Selbstbau eines TETRA Senders/Empfängers?

software:

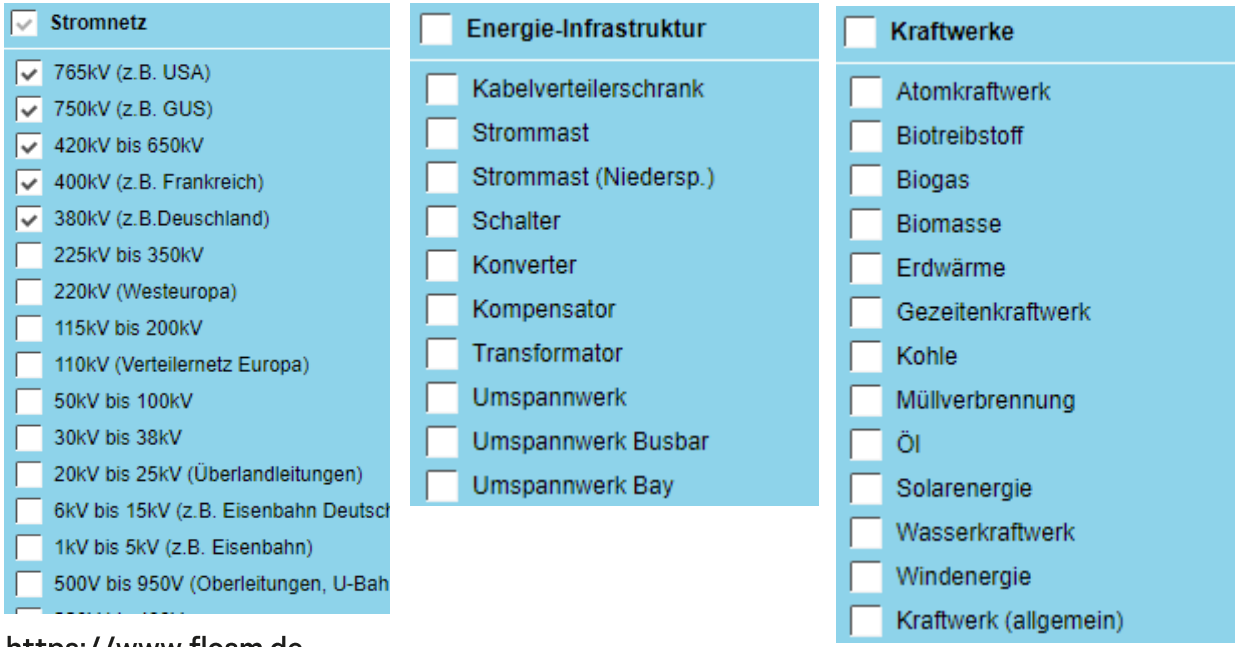
- https://github.com/osmocom/osmo-tetra

Hardware:

- SDR-Transceiver + amplifier < 300 €

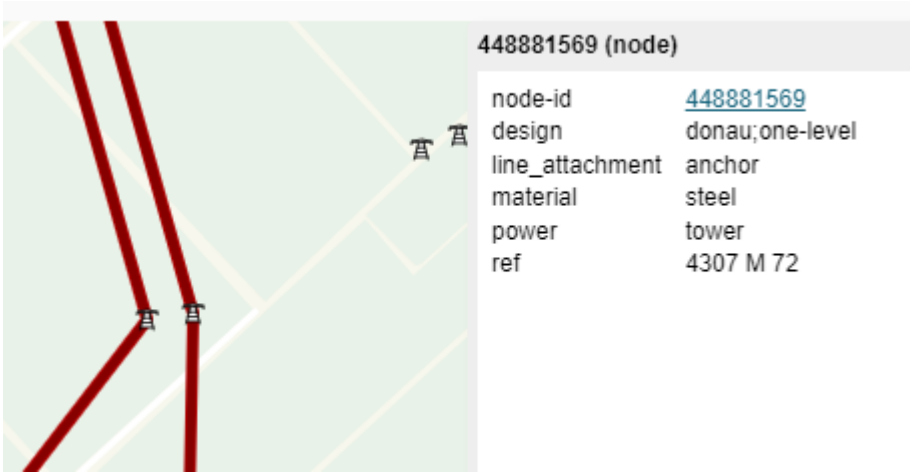
„criminal Energie“

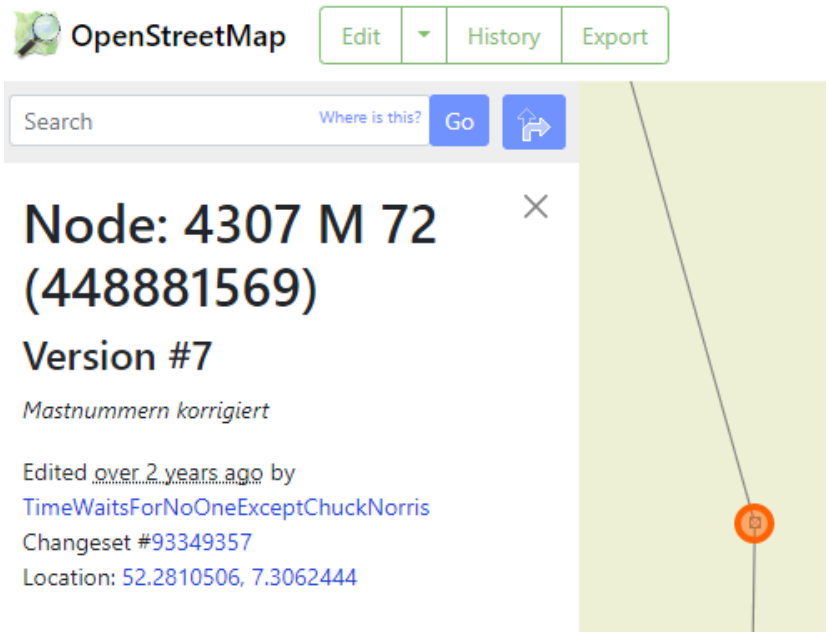
Ein weiteres Problem – Transparenz



https://www.flosm.de

Ein weiteres Problem – Transparenz





https://www.flosm.de

Was kann man tun?:

Grundfrage: Muss das “Device” Internet Access haben?

Für Remote Management und Diagnose Sichere Kommunikationskanäle aufbauen

Authentifizierung und Verschlüsselung der Übertragung

Herstellerangaben vor Implementierung “verifizieren” (Testbetrieb)

Öffentliche Dokumentationen überprüfen (zu viele Details)

Usw.

Vielen Dank!

Stephan Gerling

Senior Security Researcher
Kaspersky ICS-CERT

@obiwan666

kaspersky