Energiewende

Herausforderung für die Cybersicherheit

Stephan Gerling

Senior Security Researcher
im ICS CERT

kaspersky

Aktuelle Cyberrisiken für erneuerbare Energie

Windkraft

Windkraft

- Ausbau Infrastruktur
- Einspeisemanagement

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.

Lanssa Holdin, 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

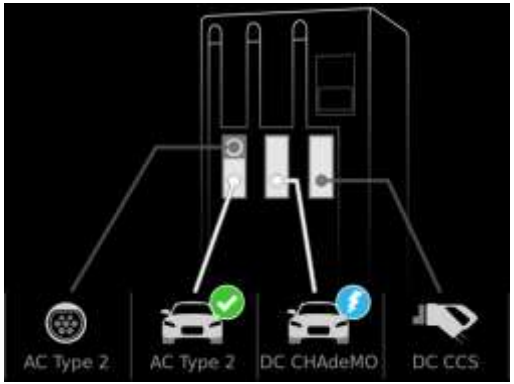
3 September 2022 38

Elektromobilität

- Ladesäulen Infrastruktur
- Lastmanagement
- Abrechnungssysteme

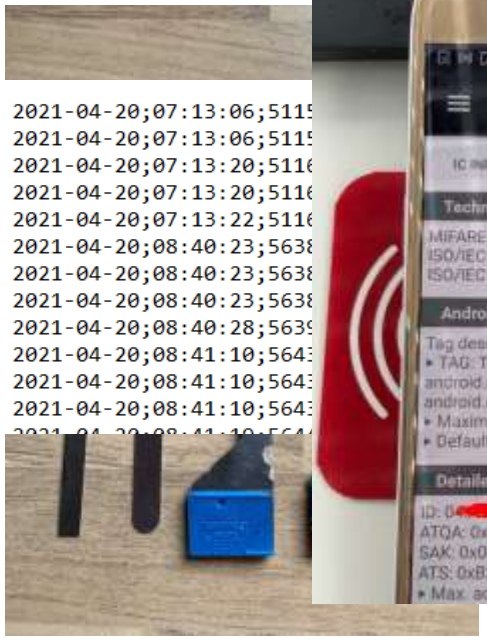
“Laden muß so einfach werden wie Tanken”

- Massiver Ausbau der Ladesäulen Infrastruktur nötig



Cybersicherheit der Ladesäule selbst ist oft ein Problem

- Unzu



Problem:
Kommunikation zwischen der Ladesäule und dem Betreiber erfolgt unverschlüsselt

Version 2.0.1 (März 2020) enthält erste Security Implementierungen

Version 1.6 wird immer noch als mindest Standard gefordert

Kein Zwang zur Umrüstung bestehender Anlagen

Solarenergie

- Speichersysteme
- Wechselrichter
- Monitoring / remote Management
- Einspeisemanagement

Speichersysteme

- Oft unzureichend geschützt
- Standard Passwörter
- Remote Management
- Unverschlüsselte Protokolle

Solar Wechselrichter

- Oft unzureichend geschützt
- Standard Passwörter
- „Hardcoded“ Passwörter
- Remote Management
- Unverschlüsselte Protokolle

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)

Der Klassiker

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

Verwundbare Systeme Online

[redacted]

result from last year

TOTAL RESULTS

21,724

TOP COUNTRIES

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

More...

[redacted]

result from today

TOTAL RESULTS

16,721

TOP COUNTRIES

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

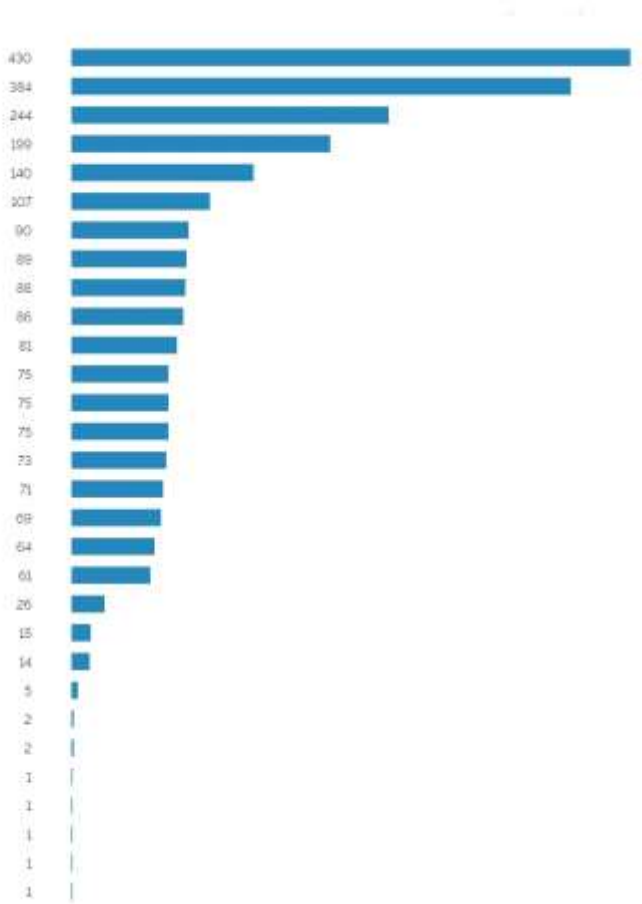
More...

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

~ 7200 MW Weltweit
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?

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

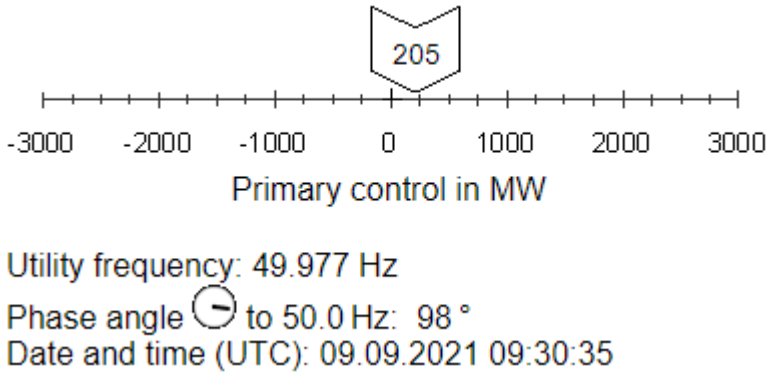
etc.

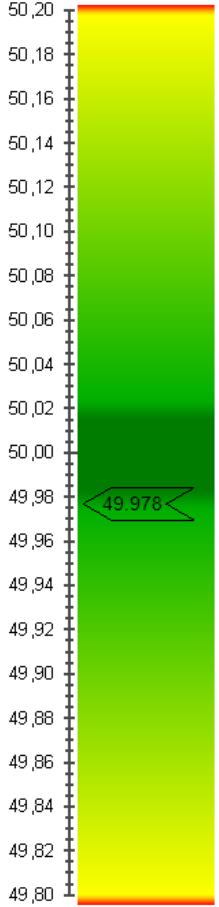
Picture: (https://www.swissgrid.ch/de/home/operation/regulation/grid-stability.html)

Primär Regelenergie

3 Giga Watt Regelenergie
Varianz > +- 10mHz

Im Bereich von +- 200mHz
>50.2Hz = 3 Giga Watt komplett vom Netz
<49.8Hz = komplett Einspeisung der 3 Giga Watt



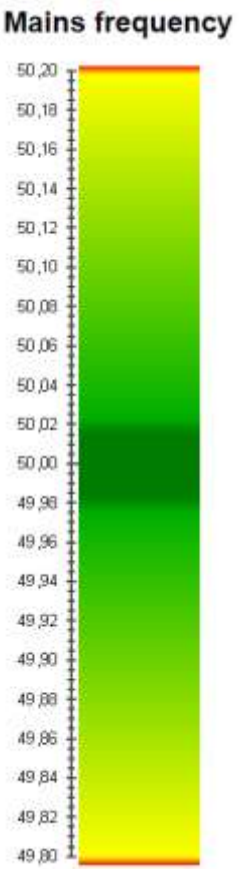


Picture source: (https://www.mainsfrequency.com/index.htm)

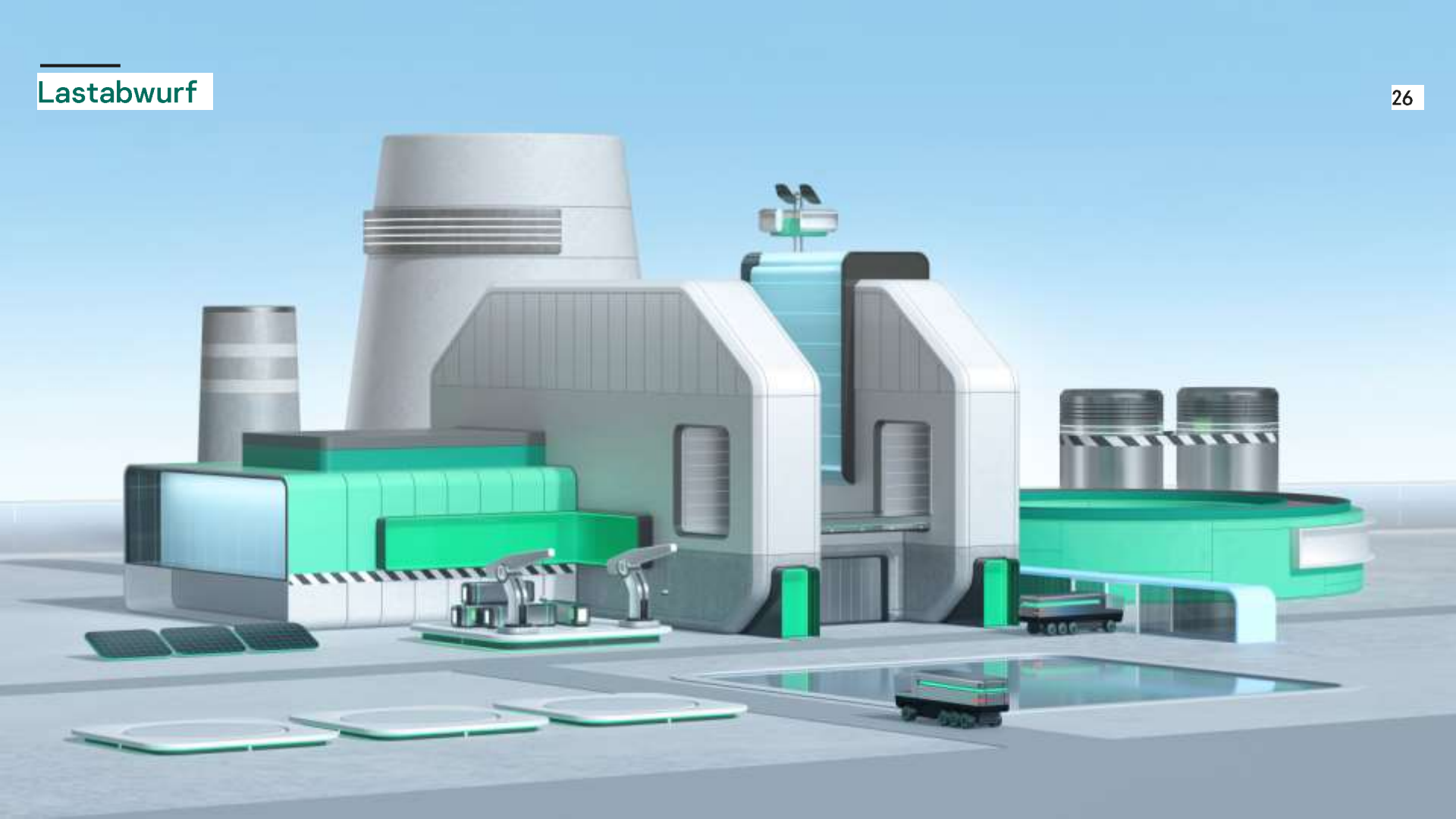
50 hertz

Netzfrequenz level

Frequenz	Aktion	Last	Aktivierung
51,5 Hz	Alle erneuerbaren Energien vom Netz	100%	Automatisch
50,2 Hz	Einspeiseregelung erneuerbare Energien		Automatisch
50,1 Hz	keine Maßnahmen		
50,0 Hz	Baseline		
49,9 Hz	keine Maßnahmen		
49,8 Hz	aktivieren der Standby Energie		Manuel/ Automatisch
49,2 Hz	Aktivierung Pumpspeicher usw.		Automatisch
49,0 Hz	Lastabwurf LEVEL 1 , 10-15 %	ca. 12,5 %	Automatisch
48,8 Hz	Lastabwurf LEVEL 2, 10-15 %	ca. 25,0 %	Automatisch
48,6 Hz	Lastabwurf LEVEL 3, 10-15 %	ca. 37,5 %	Automatisch
48,4 Hz	Lastabwurf LEVEL 4, 10-15 %	ca. 50,0 %	Automatisch
47,5 Hz	alle Stromerzeugungsanlagen vom Netz		Automatisch



Lastabwurf



Temporäre Reduzierung des Strombezugs

RNG Rheinische NETZGesellschaft

Über einen Schaltkontakt eines Rundsteuerempfängers dürfen maximal 30 Ladeschütze oder Hilfsrelais geschaltet werden, deren Spulen-Nennleistung maximal je 7 VA betragen darf. Wird diese Anzahl überschritten, sind die Maßnahmen mit dem NB abzustimmen.

Wärmepumpen

- Wärmepumpen in monovalent (Raumwärmebedarf wird allein durch die Wärmepumpe gedeckt ggf. inkl. der integrierten elektrischen Zusatzheizung) oder bivalent-parallel (zu einer nichtelektrischen Raumheizung) betriebenen Anlagen **(Standard).**
  - Die Elektrizitätsversorgung der Wärmepumpen kann bis zu sechs Stunden täglich, dabei nicht länger als zwei Stunden zusammenhängend unterbrochen werden.
- Wärmepumpen in bivalent-alternativ betriebenen Anlagen (Raumwärmebedarf wird während der Unterbrechungszeiten durch eine nichtelektrische Raumheizung gedeckt)
  - Die Elektrizitätsversorgung der Wärmepumpen kann bis zu 960 Stunden je Jahr unterbrochen werden.

Während der Unterbrechungszeiten darf der Raumwärmebedarf nur durch eine nicht-elektrische Raumheizung gedeckt werden. Die aktuellen Unterbrechungszeiten erhalten Sie auf Anfrage.

Bundesnetzagentur: Netzbetreiber sollen Strombezug von Wärmepumpen und Ladestationen drosseln können

Bei der Behörde läuft zurzeit ein Festlegungsverfahren zur Integration von steuerbaren Verbrauchseinrichtungen und steuerbaren Netzanschlüssen nach Paragraf 14a Energiewirtschaftsgesetz. Dem Eckpunktepapier zufolge sollen Verteilnetzbetreiber ab 2024 die Möglichkeit bekommen, bei Wärmepumpen und Kälteanlagen, Ladeeinrichtungen und Batteriespeichern steuernd einzugreifen, um Stromausfälle wegen Überlastungen örtlicher Leitungen zu vermeiden. Konsultationsbeiträge zu dem Festlegungsverfahren sind noch bis zum 27. Januar möglich.

18. JANUAR 2023 PETRA HANNEN

https://web.cdn.rheinenergie.com/cms/media/documents/marktpartner/Technische_Anschlussbedingungen_fuer_den_Anschluss_an_das_Niederspannungsnetz_RNG-min.pdf

https://www.pv-magazine.de/2023/01/18/bundesnetzagentur-netzbetreiber-sollen-strombezug-von-waermepumpen-und-ladestationen-drosseln-koennen/

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)

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

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

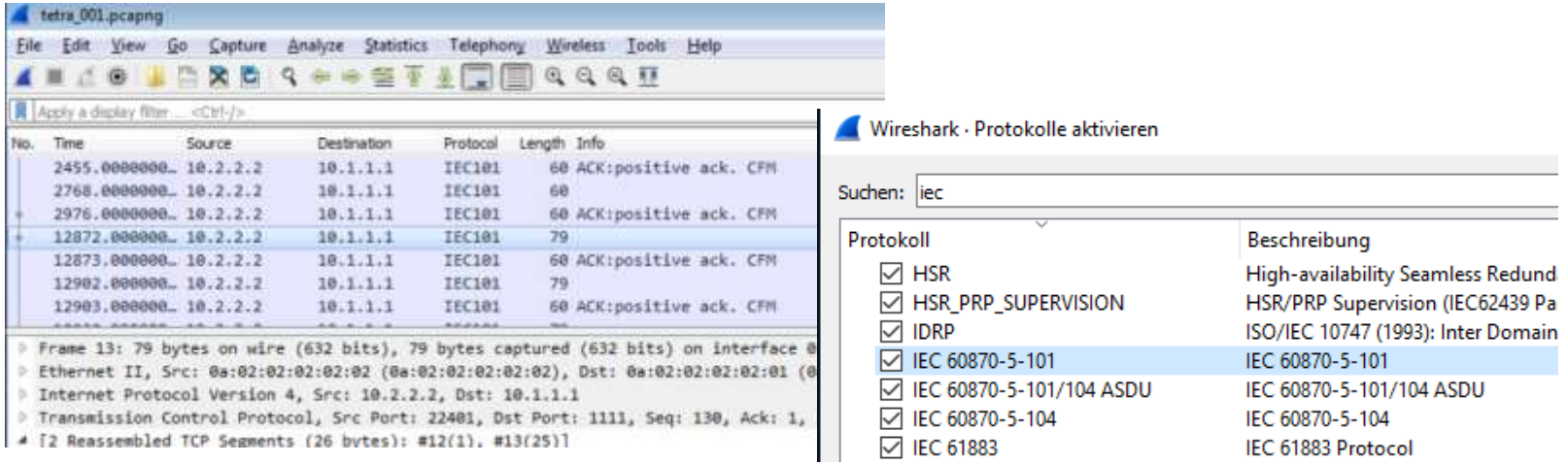
Frequenz (Oberband)	MCC	MNC	LA	Air-Interface-Encryption	End-to-End-Encryption	Daten
426.6625 MHz	262	207	10085	nein	nein	IEC 60870-5-101
426.7125 MHz	262	207	10081	nein	nein	IEC 60870-5-101
427.2375 MHz	262	207	10080	nein	nein	IEC 60870-5-101
426.8875 MHz	262	168	4	nein	nein	IEC 60870-5-101

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“

Was kann man tun?:

Grundfrage: Muss das “Device” Internet Access haben?

Sichere Kommunikationskanäle für Fernwartungund Diagnose

Authentifizierung und Verschlüsselung der Übertragung

Pflicht zum Update / Upgrade bei Sicherheitslücken

kaspersky