



Positive Security

BlinkenCity

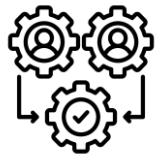
Radio-controlling street lamps and power plants

Fabian Bräunlein & Luca Melette | 28.12.2024

Disclaimer



Educational Purpose Only. The content of this presentation is intended solely for informational and educational purposes and to warn of the risks associated with the presented security vulnerabilities.



Responsible Disclosure. Any vulnerabilities discovered were reported to the appropriate parties through responsible disclosure practices.



Audience Responsibility. We do not encourage, support, or endorse the abuse of any vulnerabilities discussed. Attendees are responsible for ensuring that their actions comply with all legal and ethical standards. The presenters are not liable for any misuse of the information shared.

Let the research begin: once upon a time, we found an open street lamp in Berlin...



Having a peek inside



We found a **radio-controlled switch** for the street light!



Funkrundsteuerung is a nation-wide system able to control devices with longwave radio



Who delivers the control signal?

Through internet research we found that Funkrundsteuerempfänger are **managed by energy supply companies through a single company named EFR**, controlling devices in multiple EU countries.

How are they controlled?

Control messages (telegrams) are sent via **high power** (100kW) and **low frequency** transmitters, covering a good part of central Europe.

Two rather obscure low bitrate protocols are used:

- Versacom (DIN 43861-301/401)
- Semagyr-TOP (DIN 43861-302/402)

EFR broadcasting stations, covering parts of Europe



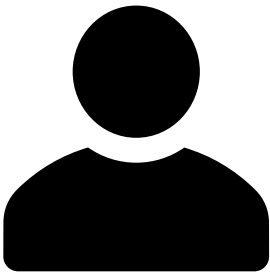
https://www.ptb.de/cms/fileadmin/internet/_processed_/csm_Empfangskarte_Langwellenfunk_616767aa0d.jpg

Devices are in: AT, CZ, DE, HU, SK

EFR longwave transmitters provide a one-way channel between energy suppliers and devices



Energy supplier (EVU)



Around 300 companies

EFR web app or desktop client



<https://efr-portal.de>

Broadcast tower



<https://efr-smart-control.de>

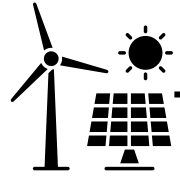
Radio ripple control receiver (Funkrundsteuerempfänger/FRE)



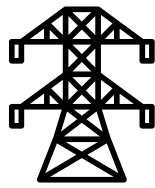
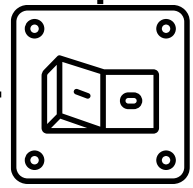
Can run programs

Up to 6 output signals

Controlled device (source or load)



Power regulator



Power grid

Besides street lights, the EFR ecosystem is applied to a variety of use cases



Power plant steering

- Solar
- Wind
- Biogas
- Geothermic
- Hydro generators



<https://commons.wikimedia.org/wiki/File:SolarPowerPlantSerpajpg>

Tariff switching

- Day tariff
- Night tariff



https://commons.wikimedia.org/wiki/File:Economy_7_Meter_and_Teleswitcher.JPG

Weather forecasts

- Weather stations
- Predictive heating and concrete core cooling



https://www.sigidwiki.com/images/a/ab/EFR_Metering_Billing_CIS_America.pdf

Load management

- Night storage heating
- Heat pumps
- Wall boxes



https://commons.wikimedia.org/wiki/File:Car2Go_Charging_Station_Stuttgart_2013_01.jpg

Custom devices

- For example:
- Food cooling systems



**EFR für Bäcker, Metzger
und für Gaststätten**

Time source

- Regular time and date
- Precise time



„EFR-Zeit“ ist jetzt auch gesetzliche Zeit
Drei Langwellensender der Europäischen Funk-Rundsteuerung GmbH liefern ihre Zeitsignale jetzt mit aufwendiger PTB-Prüfung

<https://www.ptb.de/cms/en/gateways/ptb-for-the-public/news/single-news.html>

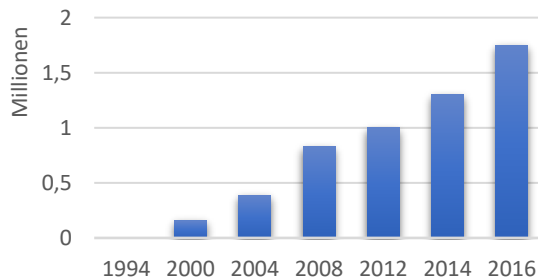
An attacker controlling power sources and loads could cause power grid instabilities



Device adoption growth



Devices



Source: efr.de

Meaningful power at stake



EFR lists several GigaWatts of both controlled power loads and power sources.

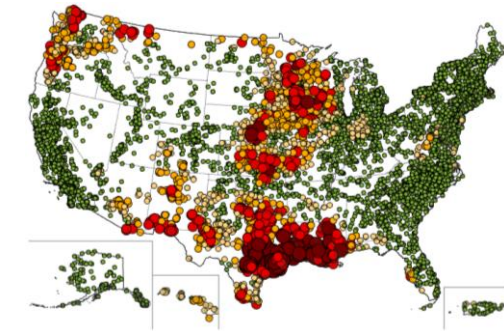
Example figures from 2009:

Customer	MW Controlled	Comment
e-on edis	2,100 MW	Wind Generation
e-on Avacon	600 MW	Wind Generation
WEMAG AG	25 MW	Wind Generation
energiequelle	230 MW	Wind Generation
e-on Bayern	2,500 MW	Heating Systems
berlin.de	20 MW	Street Lighting
All Companies	500,000 households	Tariff Switching
envia NSG	900 MW	Wind Generation, Solar & Biogas systems

Blackout risks



Major blackouts happened in the US, and there are reports of growing instabilities in the EU grid



Following the current worldwide political tensions and cyber attack strategies, **how likely can this ecosystem be abused to cause a power outage?**

But before things get too serious... let's combine this information with some creativity



Project Blinkenlights

By turning on and off lights programmatically, buildings become art exhibitions



Haus des Lehrers, Berlin 2001



Bibliothèque nationale de France/Arcade, Paris 2002



City Hall, Toronto 2008

We just got an idea!

What if Berlin becomes a giant screen? That would be... **BlinkenCity!**

Illustrative

Parody

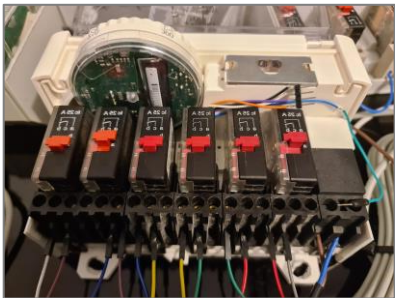


Back to our investigation, radio transmissions can be observed with a real device or an SDR

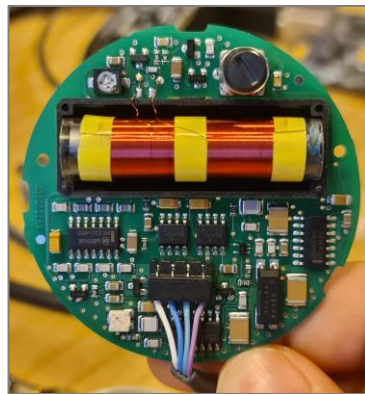


Option A: Use a real receiver

1. Buy a receiver



3. Tap the data lines, while the device is operating

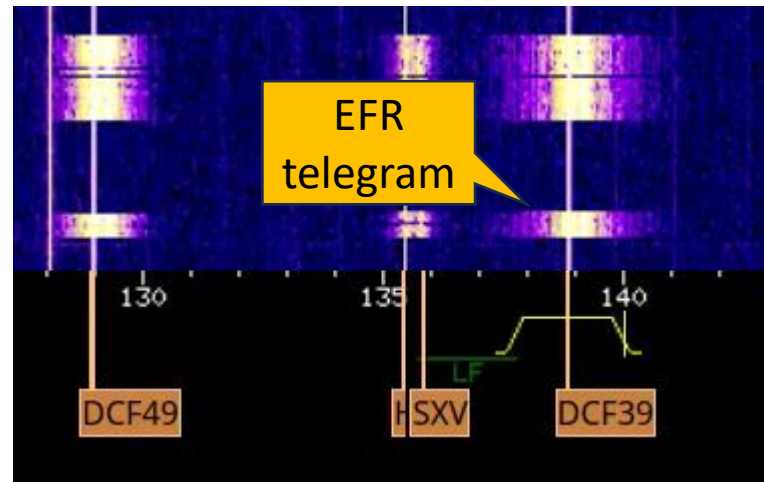


2. Open the device enclosure

Option B: An online SDR receiver

Find an SDR station near Germany:

- <http://www.websdr.org>
- <http://kiwisdr.com/public>



Use the EFR-FSK demod extension

Option C: Your own SDR



LF antenna

+



SDR with LF coverage

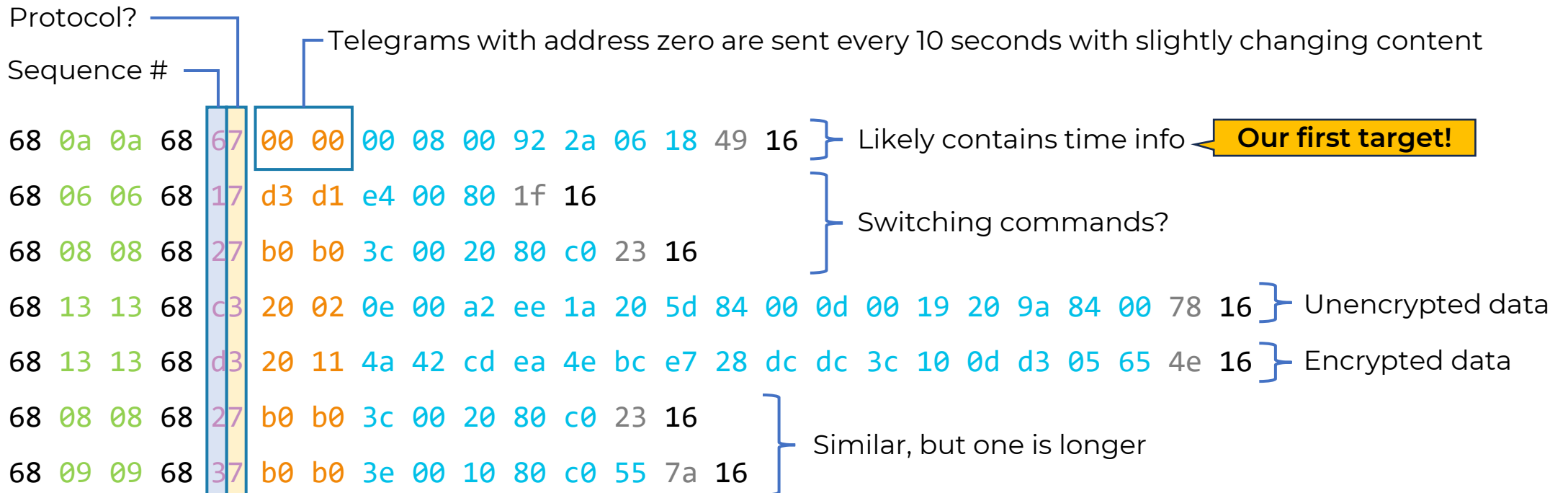
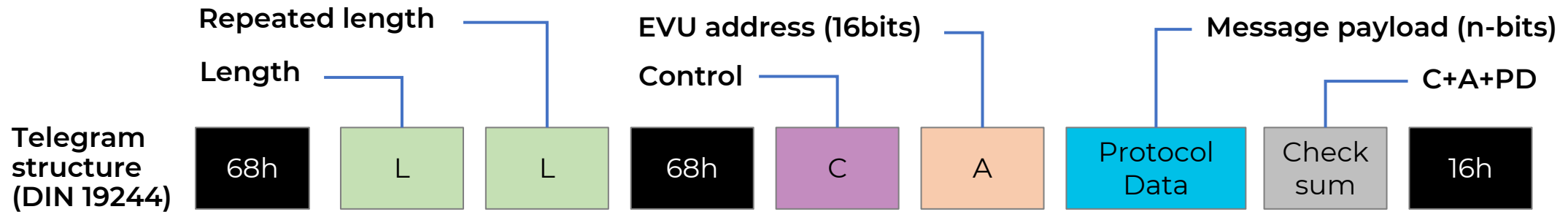
+

Custom code

Signal demodulation[1]: FSK-LSB with 170 Hz shift, 200 baud, 8E1 serial coding

[1] https://www.sigidwiki.com/images/a/ab/EFR_Metering_Billing_CIS_America.pdf
<https://www.bremerfunkfreunde.de/images/bilder/sdr/megaloop1.jpg>
https://www.rtl-sdr.com/wp-content/uploads/2016/08/RTLSDR_Front.jpg

Telegrams share a common header & trailer, but inner contents follow different standards



The first decoded telegram carries date and time information, and is read by all receivers



Decoding a time synchronization message

Special EVU value, indicating a message for all receivers

2024-11-30 11:47:22
2024-11-30 11:47:42
2024-11-30 11:48:22

68 0a 0a 68 57 00 00 00 80 2f 0b de 0b 18 12 16
68 0a 0a 68 77 00 00 00 d0 2f 0b de 0b 18 82 16
68 0a 0a 68 b7 00 00 00 80 30 0b de 0b 18 73 16

20sec later
1min later

Second (High 6 bits): 22
Minute: 48
Daylight saving (High bit): No
Hour (Low 7 bits): 11
Year: 24 (in the same century)
Month: 11
Weekday (High 3 bits): Sat (6)
Day (Low 5 bits): 30

KiwiSDR already has a decoder for this, look inside: https://github.com/jks-prv/Beagle_SDR_GPS

Attack 1: Time machine

Telegrams with spoofed date/time trigger programmed functions

Time is sent in plaintext, **without any integrity or replay protection...**

What happens if a device receives a telegram with a **timestamp in the past or in the future?**

Device time is updated, and time-based functions are triggered!

So, there is a way to control lights (probably not power plants), but **only all at once**



Reviving the job of a “lamplighter”

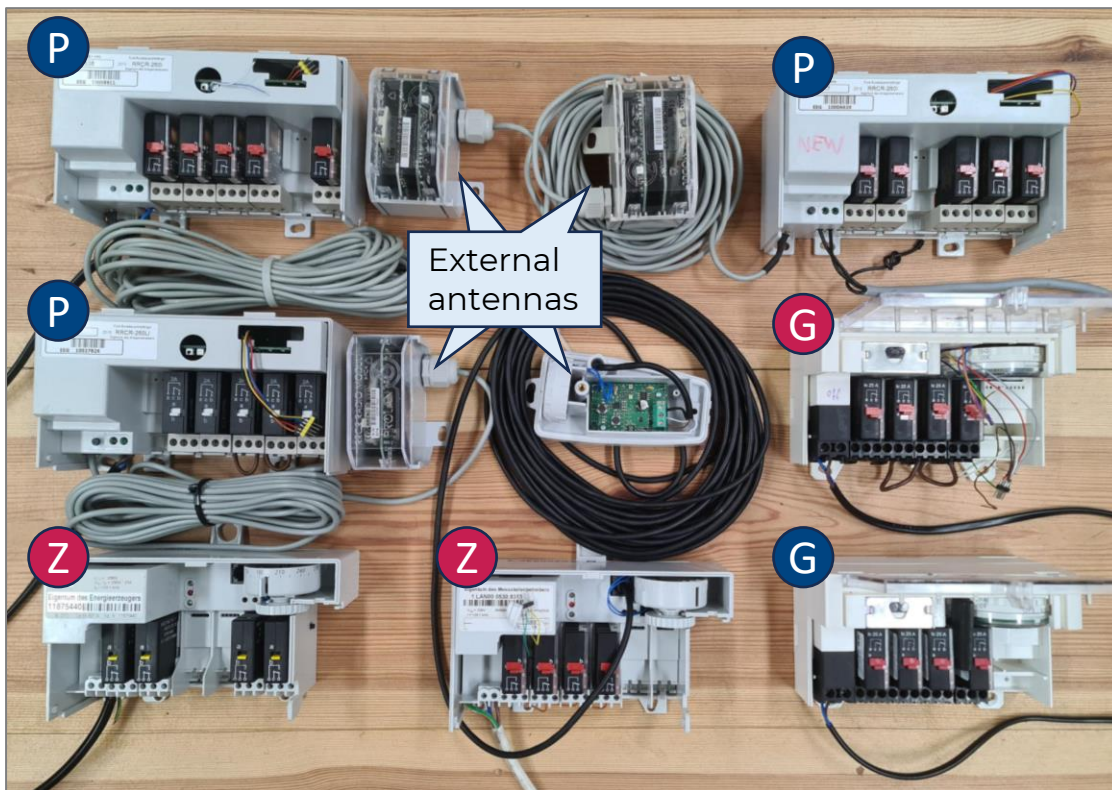


Lamplighters
Spotted at work

We built our own EFR replica lab to test various telegrams on different receivers

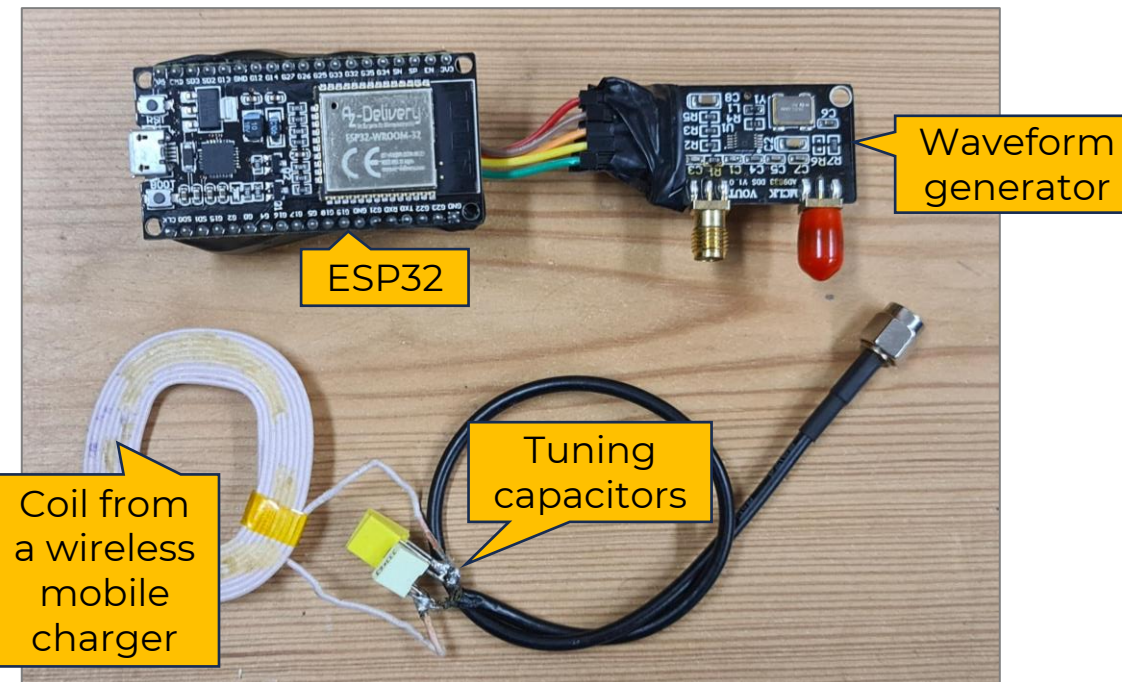


We acquired several used receivers from eBay



P = Prolan, G = Landis+Gyr, Z = Langmatz ■ Versacom ■ Semagyr

We created a near-field EFR emulator



Now we are ready to play with remote commands, but we still need to find out how to craft one 😊

Long wave systems have been designed as a cheaper alternative to ripple control over wire



Before we deep dive into the bits, let's understand how this technology came around

Year 1900 - Ripple Control

- Allows to remotely switch tariffs in electricity counters by adding tones ("ripple") over the 50 Hz main wave of electricity lines
- Multiple devices could be controlled by slowly sending a few bits
- Each country and vendor developed their own proprietary systems

Year 1990 - Radio Ripple Control

- Two of these protocols have been ported to radio waves, creating a cheaper alternative to powerline
- Later, some protocol extensions have been defined to cover new use cases



The following standards describe the used protocols

DIN 43861 „Rundsteuerempfänger“ besteht aus:

- Teil 1: „für Einbau in Lichtmaste; Hauptmaße“
- Teil 2: „Hauptmaße“
- Teil 3: „Übertragungsprotokolle“
- Teil 301: „Übertragungsprotokolle Typ A“
- Teil 302: „Übertragungsprotokolle Typ B“

Can be bought at DIN website

Funkrundsteuerempfänger

- Teil 4: „Übertragungsprotokolle“
- Teil 401: „Übertragungsprotokolle Typ A“ 
- Teil 402: „Übertragungsprotokolle Typ B“ 

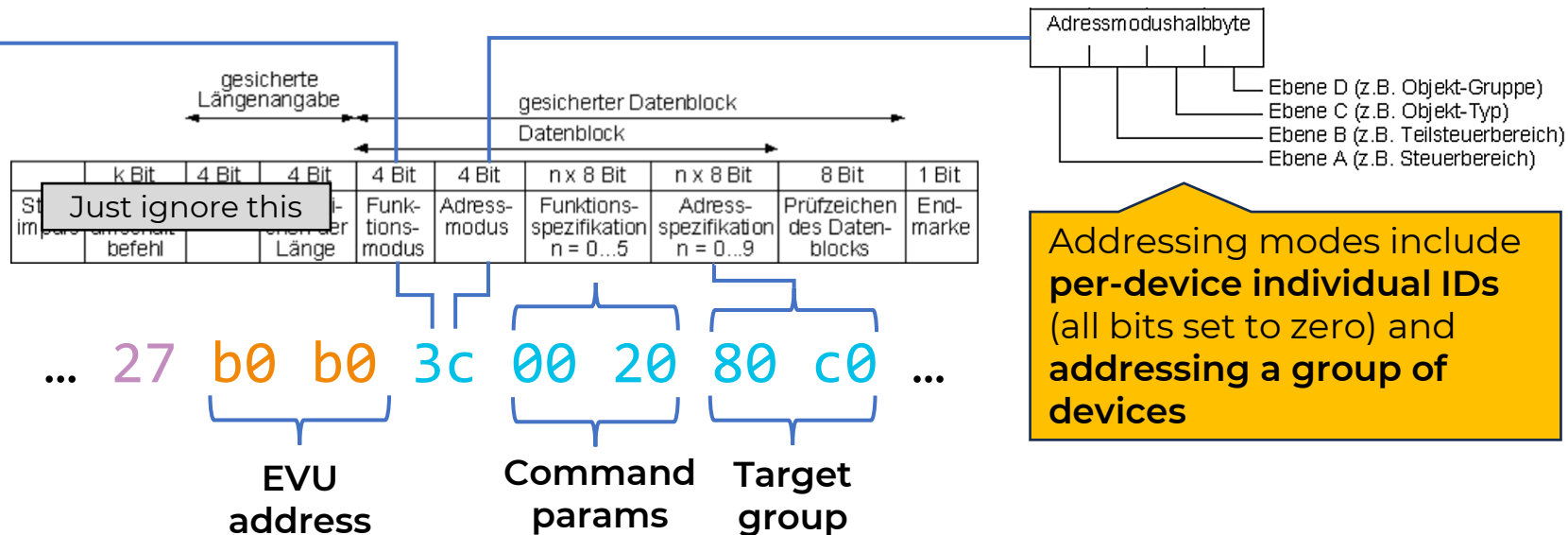
Can be bought by calling VDE

V Telegrams seem to follow the standard, but addressing schemes need to be investigated



Decoding a Versacom (DIN 43861-401) telegram

Code	Funktion
0000	Kalenderzuordnung
0001	Parametrierung der Schaltprogramme
0010	Weitere Funktionen
0011	Schaltprogrammwahl
0100	Zeitsynchronisation
0101	Schaltbefehl AUS
0110	Schaltbefehl EIN
0111	Herstellerspezifische Funktionen
1000	Wischerbefehl
1001	Schaltzyklusart 1
1010	Schaltzyklusart 2
1011	Rücksetzen der Zählerregister
1100	Deaktivierung des Empfängers
1101	Prüfbefehl
1110	Aktivierung des Empfängers
1111	Schaltbefehl AUS und Schaltprogrammssperrung



Commands: remote (de)activation of the device, programming of switching cycles, program selection, **manual switch on/off**, vendor-specific features

Great, but how can we address our device?

Addressing schemes are hierarchical: not all groups need to be specified at once



Group addressing in use

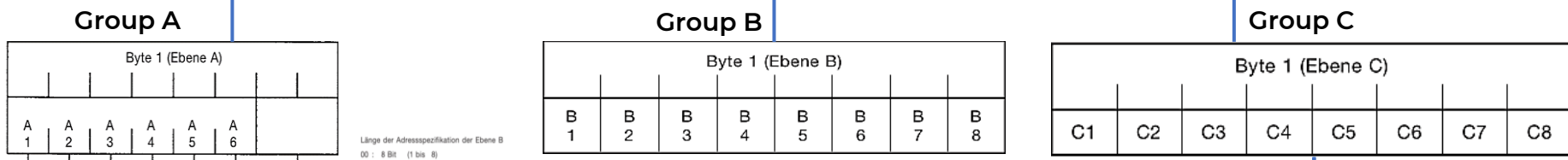
A+B

68 08 08 68 27 b0 b0 3c 00 20 80 c0 23 16

A+B+C (subset of A+B)

68 09 09 68 37 b0 b0 3e 00 10 80 c0 55 7a 16

Command argument

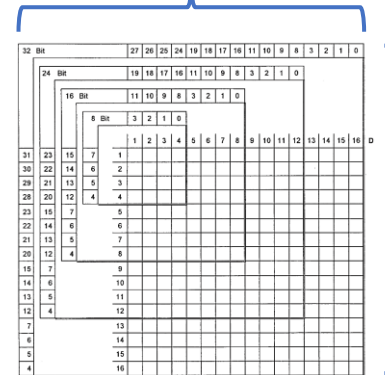


Länge der Adressspezifikation der Ebene B
 00 : 8 Bit (1 bis 8)
 01 : 16 Bit (1 bis 16)
 10 : 24 Bit (1 bis 24)
 11 : 32 Bit (1 bis 32)

Steuerbereich 6
 Steuerbereich 5
 Steuerbereich 4
 Steuerbereich 3
 Steuerbereich 2
 Steuerbereich 1

A device programmed as A=2/B=4/C=3/D=1 will **also be selected by:**

- A=2/B=4/C=3 only
- A=2/B=4 only
- A=2 only



Group D (not used in these telegrams)

Publicly available PDFs disclose the relation between address bits and power plants



Searching the internet we found documents that **describe the device addressing and use cases**

Classification of power plants by type and size

Nomenklatur

Eindeutige Kennzeichnung der Parametrierung: X_Y_Z (z. B. 2_III_45134)

X Energieart (im Beispiel: Energieart 2 Deponiegas)
 Y Leistungsklasse (im Beispiel: Leistungsklasse III <500kW)
 Z Postleitzahl (im Beispiel: Postleitzahl 45134 Essen)

Leistungsklassengrenzen/Energieart

Alle Angaben in kW

Leistungs-klasse	Energieart					
	1	2	3	4	5	6
	Windenergie	Deponiegas Grubengas Klärgas Biomasse	Wasserkraft	Solare Strahlungs- energie (PV)	BHKW-/IKW- Anlagen mit konventionellen Energieträgern (z.B. Erdgas, Öl), KWK-gefördert	Geothermie
I	≥ 10.000	≥ 2.000	≥ 1.000	≥ 500	≥ 1.000	≥ 5.000
II	≥ 1.000 und < 10.000	≥ 500 und < 2.000	≥ 500 und < 1.000	≥ 100 und < 500	≥ 100 und < 1.000	≥ 500 und < 5.000
III	< 1.000	< 500	< 500	< 100	< 100	< 500

Mapping of address bits to relay#, device type & location

Adressierungsebene A

Unterscheidung der Energiearten:

A1 Windenergie
A2 Deponiegas, Grubengas, Klärgas, Biomasse
A3 Wasserkraft
A4 Solare Strahlungsenergie (PV)

Adressierungsebene B

Unterscheidung der Relais und Leistungsklassen:

B1 Relais 1, Leistungsklasse I
B2 Relais 2, Leistungsklasse I
B3 Relais 3, Leistungsklasse I
B4 Relais 4, Leistungsklasse I
B9 Relais 1, Leistungsklasse II
B10 Relais 2, Leistungsklasse II
B11 Relais 3, Leistungsklasse II
B12 Relais 4, Leistungsklasse II
B17 Relais 1, Leistungsklasse III
B18 Relais 2, Leistungsklasse III
B19 Relais 3, Leistungsklasse III
B20 Relais 4, Leistungsklasse III

Adressierungsebene C + D

C \ D	German postcode												
	1	2	3	4	5	6	7	8					
1	45897	45881	45883	45884	45886	45888	45889	45891	45892	45894	45896	45897	45899
2	46236	46238	46240	46242	46244								
3	45964	45966	45968										

EVU values for different zones and energy providers

Anwenderadresse

Netzgebiet Nord - BOB1 Region A und B
 Netzgebiet Süd - BFB1 Region A und B
 Netzgebiet Süd - BFB2 Region C und D

Anwenderadresse ELE
 BFB9

Association between relay# and power reduction

100% keine Reduzierung (K1)
60% Reduzierung auf maximal 60% der Leistung (K2)
30% Reduzierung auf maximal 30% der Leistung (K3)
0% Reduzierung auf 0% der Leistung – keine Einspeisung möglich (K4)

Aside of understanding group addresses, we could enumerate a large number of EVUs



EVU and group addressing information can be found in FRE installation manuals (online PDFs)

Netzgebiet Nord – B0B1 EVU address

Adressierungsebenen C und D (Matrix)
 Unterscheidung der Einspeiseorte durch die Postleitzahl der EEG/KWK-Anlage.

Region A

D \ C	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	32139		32312	32339	32361	32361	32369		32609		33775	33790		33824	33829	
2	48477	48496			49074	49076	49078	49080	49082	49084	49086	49088	49090			
3	49124	49134	49143	49152	49163	49170	49176	49179	49186	49191	49196		49201	49205	49214	49219
4	49324	49326	49328		49356		49401	49406	49419	49434	49439	49448	49453	49457	49459	
5	49477	49479		49492	49497		49504	49509	49525	49536	49545	49549	49565	49577		
6	49584	49586	49593	49594	49596	49597	49599		49610	49626	49635	49637	49638			
7	44532	44534	44536				45711	45721	45731	45739		45768	45770	45772		
8	46282	46284	46286		46325	46342	46348	46354	46359		46414					
9	48143	48145	48147	48149	48151	48153	48155	48157	48159	48161	48163	48165	48167			
10	48249		48301	48308	48317	48329	48341	48366		48432		48527	48565	48599	48607	
11	48612	48619	48624	48629	48653	48683	48691			48703	48712	48720	48727	48734	48739	
12	59192				59348	59368	59379	59387	59394	59399						
13	48268	48282	48291		48356	48369		48429	48431	48455	48465	48480	48485	48488		
14	48493	48499		48529	48531				49716	49733	49740	49744	49767			
15	49808	49809	49811		49824	49828	49832	49835	49838	49843	49844	49846	49847	49849		
16				27232	27245	27246	27248	27249	27251	27252	27254	27257	27259			

EVU addresses in received telegrams

1235	b1a1	b3bc
a1a1	b1a2	b4a0
a1a3	b1b0	b4b1
a1a7	b1b1	b4b2
a1ab	b1b3	b4b4
a1ad	b1b5	b4b5
a3a2	b1b6	b4c0
a3a3	b1b8	b4d0
a9a9	b1c2	b5a1
ac01	b2a1	b5b5
ac02	b2a2	...
b040	b2b2	eaea
b0a3	b2b8	ec10
b0b0	b3b4	ece1
b0b1	b3b8	ece5
b1a0	b3b9	ede1

A more extensive list of EVUs leaked from EFR portal APIs

```

"43947":{
  "zrspeicher":{
    "anzahlSP":16,
    "lastUpdateFromZR":"Dec 13,
    "funkelegramme":{
      "g":{
        "infoteil":"","
        "prio":0,
        "status":-1,
        "anforderungsArt":0,
        "wdh":false,
        "platzNr":9,
        "wochentag":0,
        "tgID":0,
        "sendDate":0,
        "periodTgID":0,
        "sendTime":0
      }
    }
  }
}
    
```

EVU address

This leak has been fixed

This sounds quite useful, let's see if we can identify the right one for us!

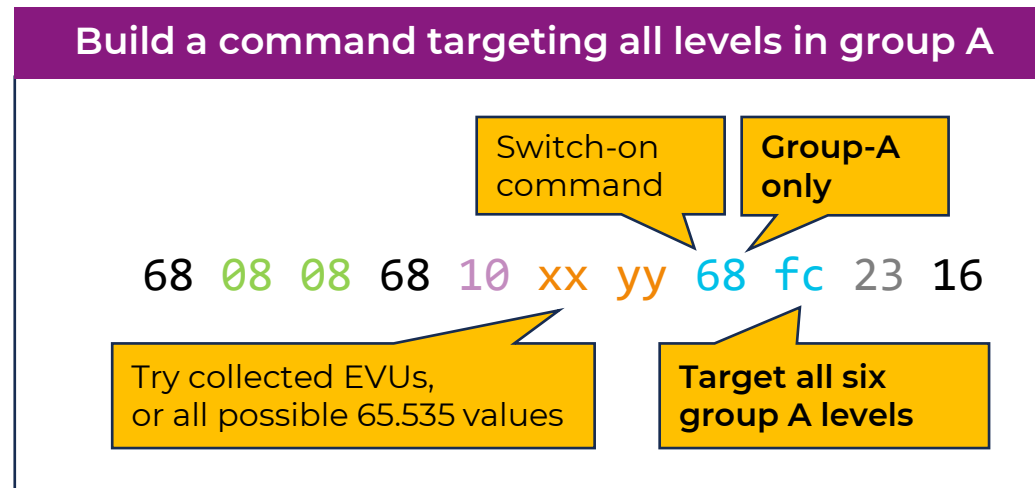
Attack 2: Device EVU recovery

Group A addressing can be abused to brute-force the actual EVU of a device



Based on the fact that group levels are hierarchical, a telegram **using group-A only** can select **all devices** belonging to the specified EVU

Choose a command that should **produce a measurable action**



Send telegrams iterating over EVU IDs, until device reacts

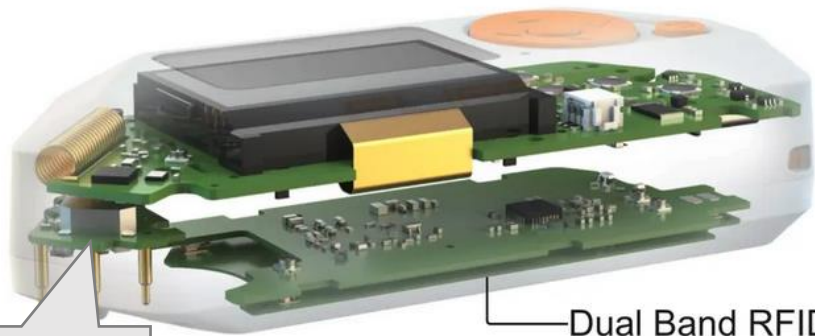
This attack can be used to disconnect real photovoltaic systems from the grid



Wait... just with a Flipper Zero?



Flipper Zero is a flexible tool that can be programmed to speak various radio protocols, including 125 kHz RFID



Allows selection and configuration of payloads

Dual Band RFID antenna

Infrared port could also be useful (more on that later)

RFID reading mode can be misused to send FSK modulated signals, also at 139 kHz with a reach up to ~1m

<https://docs.flipper.net/rfid>

With a custom app, it can **send EFR telegrams** that are correctly received by nearby devices

DCF Sender

Send Message

Send RAW

Bruteforce

Select message type

Timestamp

Versacom

Semagyr

Message

OFF >

EVU (quick)

EVU (full)

Individual ID

<< Send >>

Hours

<

14

>

Minutes

<

30

>

Seconds

<

35

>

Brute EVU (fast)...@ Pause

12 FF

A3 A4

#6: E3 E7 (q)

E4 A1

B5 B5

StreetLight-B-Gone

Illustrative

Parody



S Moving to the second telegram standard, we could not easily map it to any message



Following the **Semagyr** standard, we tried to identify the correct radio messages

Documents indicate that payload is split across telegrams

Fragments include a sequence, header, CRC and padding:

Start

	k Bit	4 Bit	4 Bit	4 Bit	n-(12+k) Bit
Start-impuls	Typ-B-Adresse	LN=1	Funktion	CRC1	Parameter

Impulsfolge 1

Middle

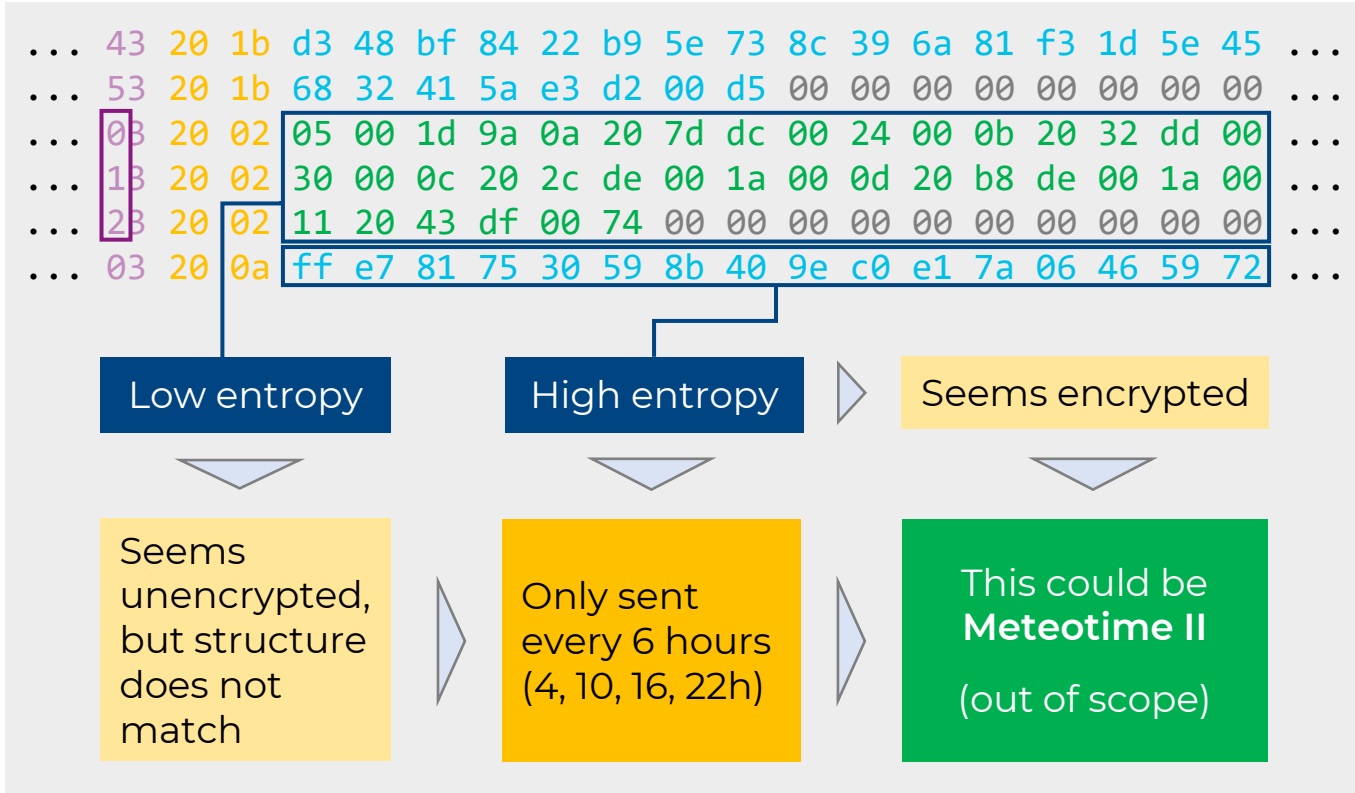
	k Bit	4 Bit	n-(4+k) Bit		
Start-impuls	Typ-B-Adresse	LN=2	Parameter		

Impulsfolge 2

End

	k Bit	4 Bit	x Bit	8 Bit	1 Bit	
Start-impuls	Typ-B-Adresse	LN=m	Parameter	CRC2	End-marke	leer

Impulsfolge m



So we assume Semagyr payloads must be somewhere else, but where?

To understand how telegrams are handled, we started looking at low level details



Among all the devices we acquired, we found only **two designs, using pretty obsolete CPUs**

Langmatz
and
Landis+Gyr
devices



- NXP/Motorola 68HC08
- SPI flash 95128
- Optional I2C RTC
- ULN2003 relay drivers
- Infrared serial port

This CPU implements certain security features to block code readout, but the **external flash is easy to dump**. Desolder it and use an Arduino or Raspberry PI to read it.

Prolan
devices



- Microchip PIC18F46xx
- ULN2003 relay drivers
- Infrared serial port

Code protection of this chip family is **known to be broken**, potentially allowing full firmware dumps. The difficulty depends on the actual security fuse configurations.

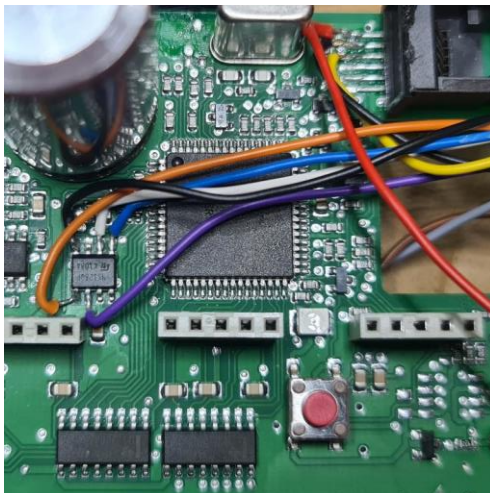
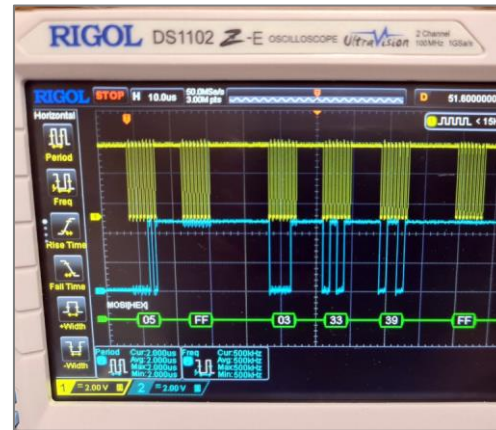
Tracing communication on specific PCB lines enhanced further our device understanding



By monitoring a selection of CPU and flash pins, we could **derive some key information**

The standard HW reversing procedure

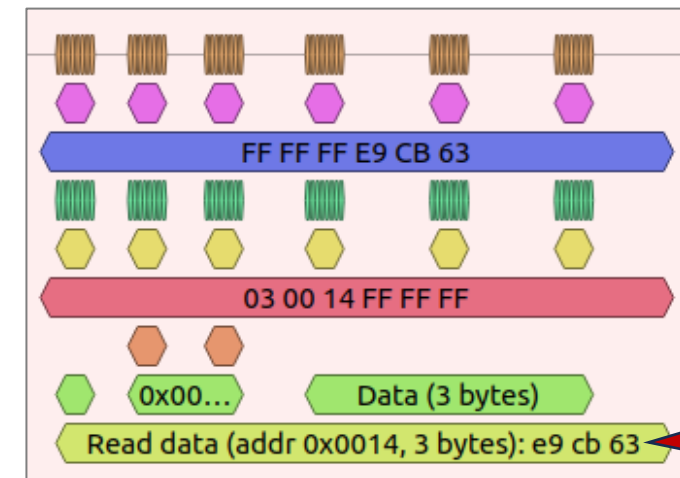
1. Measure voltages at multiple points
2. Check signals with an oscilloscope
3. Connect all lines to a logic analyzer
4. Let the device run, interact with it
5. Attempt to decode captured bits to known protocols (SPI, I2C, serial)



+



=



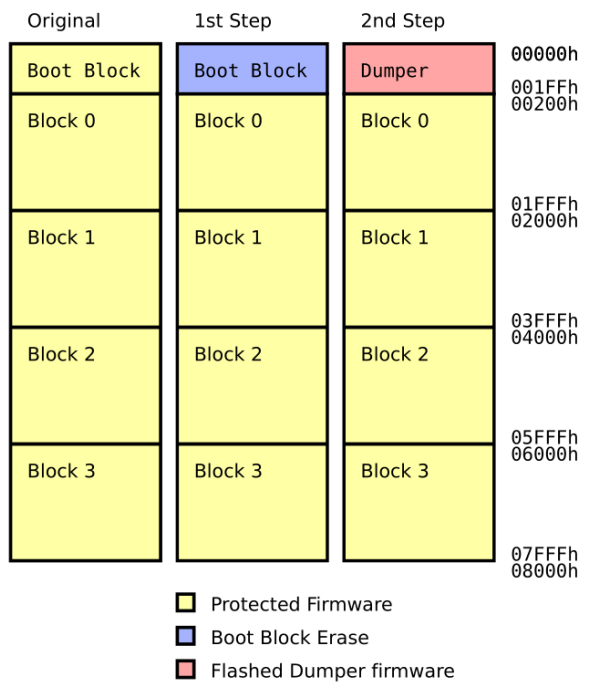
This is our device ID!

In addition to passive device observation, getting access to the firmware can be a useful resource



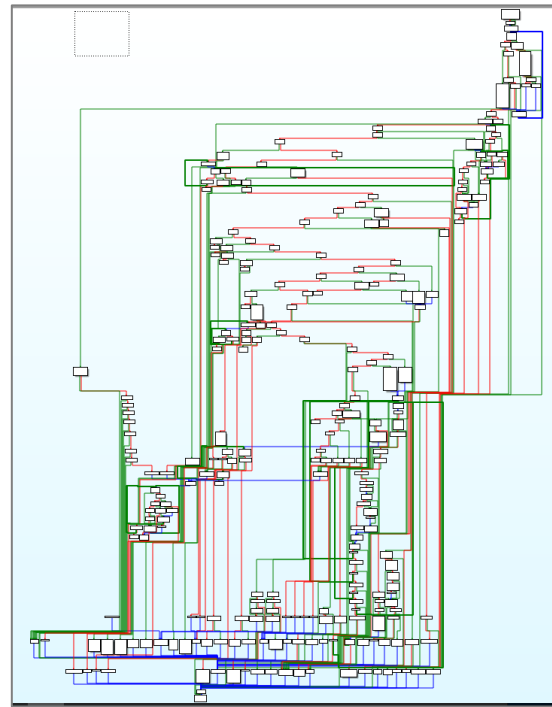
Flash memory dump

By bypassing CRP[1], the whole chip can be read from the boot block



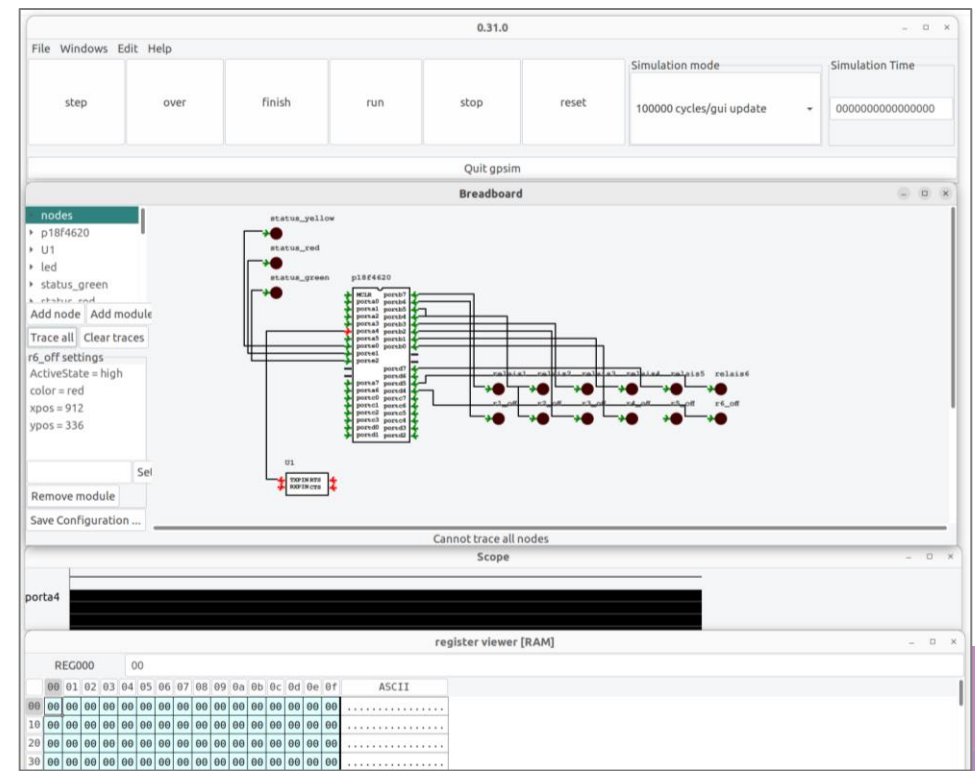
Manual code analysis

Understanding the code can be more challenging than expected



Chip and peripheral emulation

Another way would be to emulate the device to debug it, but it is also not trivial



This path requires time and resources, is there a better alternative?

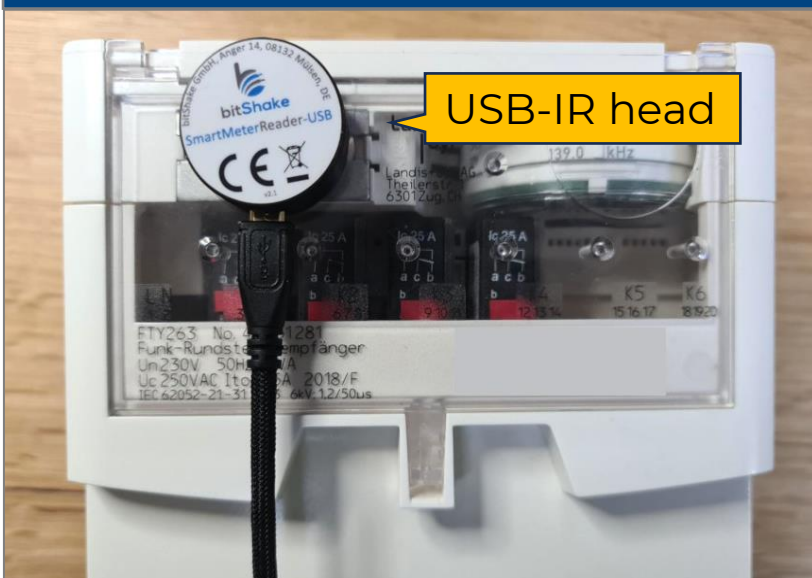
[1] <https://www.meriac.com/dl/HID-iCLASS-security.pdf>

What about that infrared port? All devices have it, so it must be important



All receivers are equipped with an infrared port to “parametrize” the device before use

Connecting to the infrared port



Choosing the protocol

FRE documentation suggests **IEC 62056-21**

- but no reply using open source tools

Internet search reveals some tool names:

ToolIC and **RPT01**

- but not available for download at vendor website

Trying random things

Sending various strings

based on the IEC spec

- at all possible serial speed and parity configurations

Got some **single bytes back** at 9600bps

- seemingly indicating an error condition

Without the right tools, it's hard to communicate to our devices over IR ☹️

S Searching the internet, we eventually found the RPT01 parametrization software



We can now read some parts of the device configuration, that includes unique IDs

RPT01 configuration files include lists of addresses and commands with nice comments that explain their scope

Empfänger-Test X

Looks like a device ID

Another device ID

Daten

Identifikation: FC28.B726

ROM-Nr.: 6

Geräteadresse: 2'951'281

Anzahl SPU's: 42

Empfänger-Uhr

(HH.MM): 22:28

(TT.MM.JJ): 15.09.24

Natürlicher Wochentag: So

Time is synced

Switching schedule

Rundsteuer-Wochentage

	15/09	16/09	17/09	18/09	19/09	20/09	21/09	22/09
Mo	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Di	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mi	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fr	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sa	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
So	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
S1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
S2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Teilprogramm-Kombination

	15/09	16/09	17/09	18/09	19/09	20/09	21/09	22/09
T0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
T1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
T2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
T3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Schliessen

Codierte Befehle - ██████████ Straßenbeleuchtung LANG

Name	DK	EIN	AUS	Adresse	Kommentar
H2RM	9	17	18	01-02 --+-----+	München Halbnacht 2
H2RR	9	17	18	01-03 --+-----+	Ostbayern Halbnacht 2
H2RW	9	17	18	01-06 --+-----+	Würzburg Halbnacht 2
H3RB	10	19	20	01-05 --+-----+	Bayreuth Halbnacht 3
H3RM	10	19	20	01-02 --+-----+	München Halbnacht 3
H3RR	10	19	20	01-03 --+-----+	Ostbayern Halbnacht 3
H3RW	10	19	20	01-06 --+-----+	Würzburg Halbnacht 3
H4RB	11	21	22	01-05 --+-----+	
H4RM	11	21	22	01-02 --+-----+	
H4RR	11	21	22	01-03 --+-----+	Ostbayern Halbnacht 4 Du...
H4RW	11	21	22	01-06 --+-----+	Würzburg Halbnacht 4 Du...
SBRB(L)	7	13	14	01-05 --+-----+	Bayreuth Ganznacht
SBRM(L)	7	13	14	01-02 --+-----+	München Ganznacht
SBRRN(L)	7	13	14	01-04 --+-----+	Schwandorf Ganznacht
SBRRS(L)	7	13	14	01-03 --+-----+	Eggenfelden Ganznacht
SBRW(L)	7	13	14	01-06 --+-----+	Würzburg Ganznacht
TSTR	7	13	14	01-01 --+-----+	Tarif Straßenbeleuchtung

But what are these numbers?

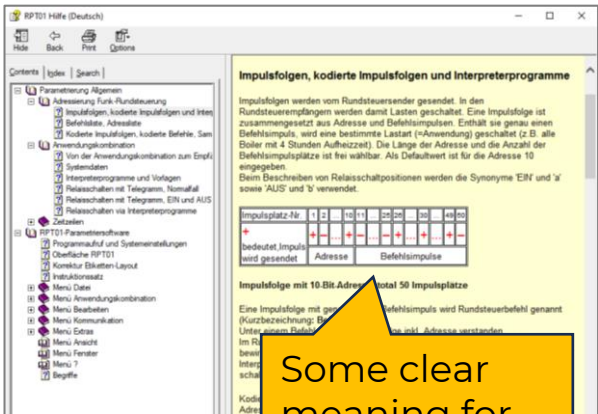
And these symbols?

We still don't know how to use those device IDs and addresses...

S We improved our knowledge by digging into help pages and old documents

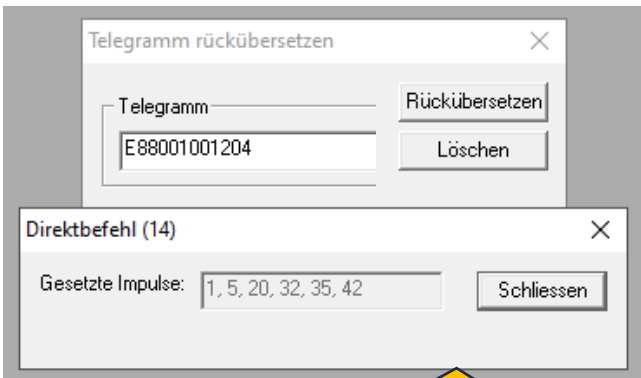


RPT01's built-in help pages are actually helpful



Some clear meaning for those bit numbers and +/- symbols

RPT01 allows encoding and also decoding of payloads



"Telegramme rückübersetzen" feature yields commands and their parameters

Semagyr was proudly presented in 1993

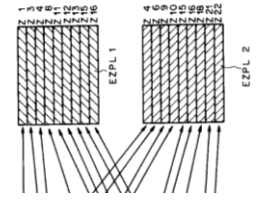


<https://www.tib.eu/en/search/id/tema:TEMAE93071412292/Semagyr-TOP-eine-Erweiterung-von-Rundsteuersystemen>

Patents reveal other details

⊙ Rundsteuerverfahren und Rundsteuerempfänge

⊙ Eine Menge von Handlungen, die von Rundsteuerempfängern auszuführen sind, sind in einer Rundsteuer-Sendezentrale in einer Liste von zeitlich festgelegten Befehlen formuliert und abgespeichert. In den Rundsteuerempfängern wird ein Abbild desjenigen Teils der Liste abgespeichert, der demjenigen Rundsteuerempfänger durchzuführen ist. Die Liste ist vorzugsweise eine Sendezentrale-Zeitprogramm-Liste (SZPL), deren Zeilen (Z1 bis Z23) je eine Informations-Einheit enthalten. Das Abbild ist dann eine Empfänger-Zeitprogramm-Liste (EZPL1



<https://patents.google.com/patent/EP0588006A1>

Concepts and terminology

Combining all docs and features, we finally fully understood the Semagyr world 😊

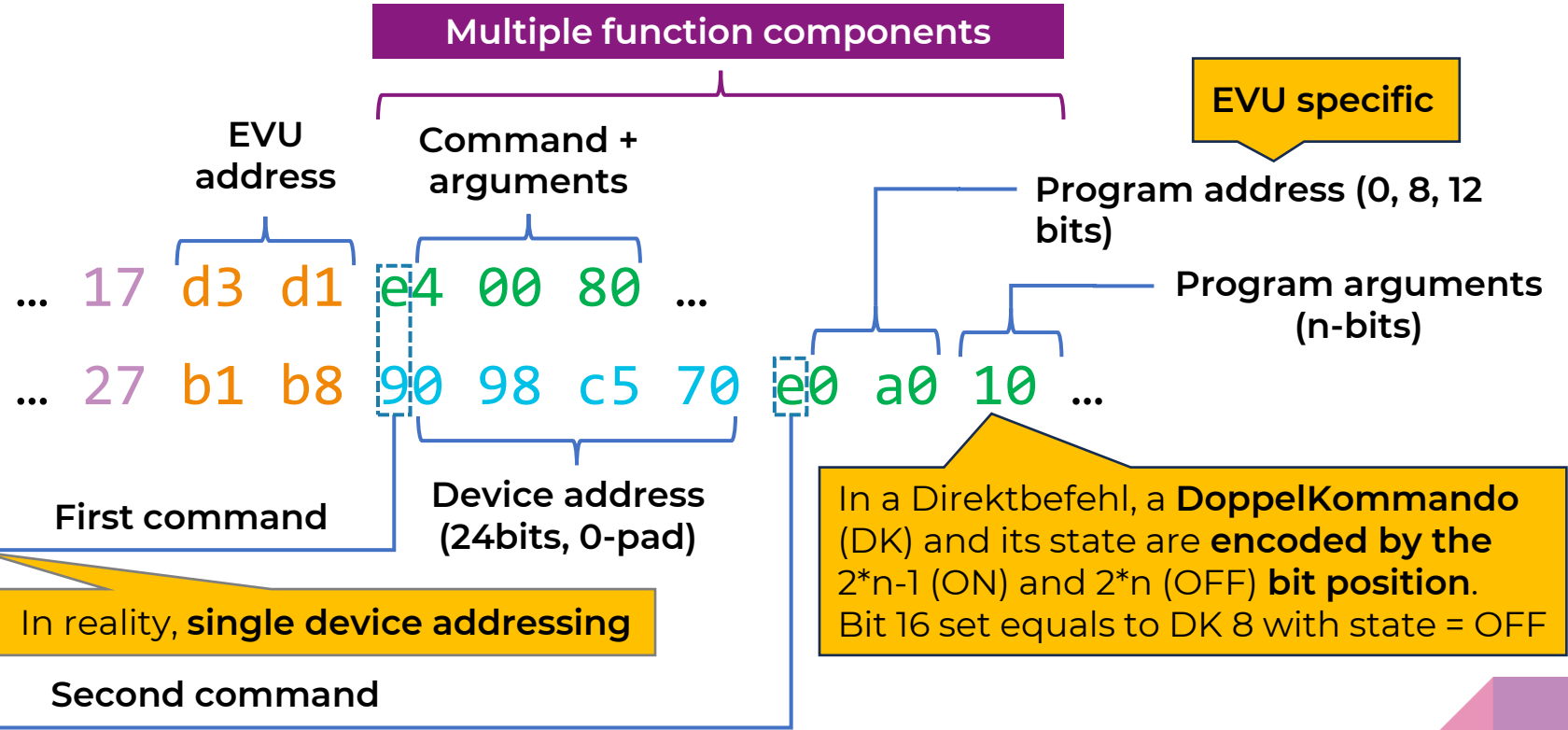
S Finally, received telegrams could be decoded and new ones can be crafted



Decoding a Semagyr-TOP (DIN 43861-402) telegram

Functions can (de)activate and **manually trigger** stored programs

Funktion	Beschreibung
0000	Herstellerspezifische Funktionserweiterung
0001	für Funktionserweiterung reserviert
0010	Rundsteuer-Wochentag synchronisieren
0011	Teilprogramme synchronisieren
0100	Eintrag ... vornehmen; mit Datumsbereich
0101	Eintrag ... vornehmen; ohne Datumsangabe
0110	Eintrag ... entfernen
0111	Ausführung Eintrag ... sperren
1000	Ausführung Eintrag ... freigeben
1001	für Funktionserweiterung reserviert
1010	Timerwerte parametrieren
1011	Flags parametrieren
1100	Ausführung Indexbereich A sperren und B freigeben
1101	Eintrag 2 Zeitzeilen mit identischem Datum vornehmen
1110	Direktbefehl
1111	für Funktionserweiterung reserviert



Great, we understand addresses and program arguments, but **what do programs do?**

Programs can be found by guessing addresses; their behavior revealed through real-world tests



We need a way to **map and classify** the wide variety of programs being used to **identify the useful ones**

Captured telegrams provide a nice view of the parameters

```
e0 80 02 00 12 01
e0 80 02 00 12 04
e0 80 02 00 12 06
...
e0 80 08 00 10 0e
e0 80 08 00 22 01
e0 80 08 00 22 04
...
e1 20 20 00 47 06
e1 20 40 00 12 e6
...
e1 40 20 00 23 01
e1 40 20 00 23 04
```

Parameters
Program address

RPT01 contains various program definitions

Complex example

```
Programm Nr. 6 (TYP Z48)
1      11      21
-----+-----+*-----+-----+-----+-----+-----+-----+
If DK 7 (WH8Nv)
Einlf
  set NV-Flag 2
  If not Flag 0
    Aus Relais K2
    Ein Relais K5
  Endlf
Auslf
  clear NV-Flag 2
  Aus Relais K5
  If NV-Flag 1
    If not Flag 0
      If not NV-Flag 0
        Ein Relais K2
      Endlf
    Endlf
  Endlf
Endlf
End.
```

The * indicates which bit will be used in the IF statement

Aside of input bits, internal state is used

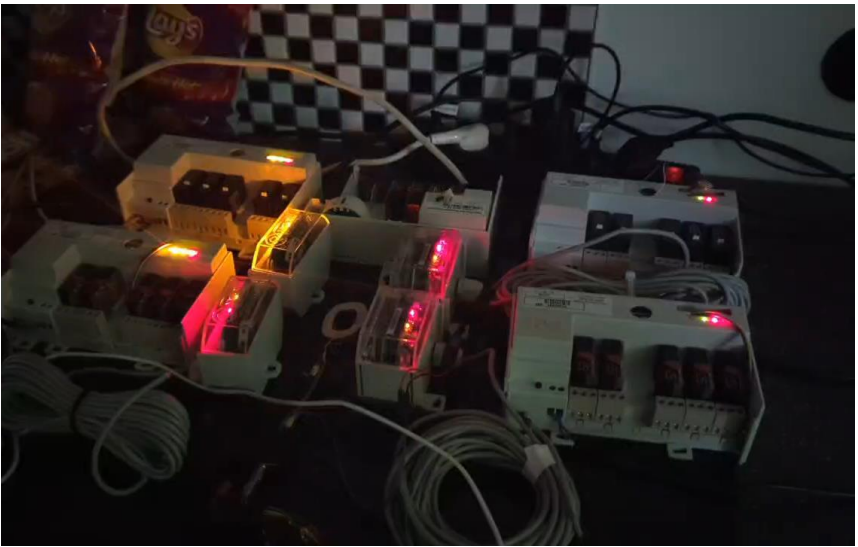
Simple example

```
Programm Nr. 2 (TYP X01)
1      11      21
-----+-----+*-----+-----+-----+-----+
DK 7 Relais K1 (WTALG)
End.
```

This program simply sets one output relay based on the input

Can we find more of these?

Telegram fuzzing can reveal programs



Through fuzzing and an electrical feedback loop, we could identify simple relay-switching programs!

Attack 3: Relay program discovery

Most devices store simple programs that can directly switch relays



Relays can be steered individually over radio

Test program DK 25 can switch relays, no matter what address!

Name	DK	EIN	AUS	Adresse	Kommentar
25	25	49	50	Ohne Adresse	Testsendung
0310	10	19	20	A03 +++++---	Strassenbeleuchtung A
0510	10	19	20	A05 +++++---	Strassenbeleuchtung B

By sending these requests we can change relay states at will

Finally, we have a way to switch both Versacom and Semagyr devices!



So what about the BlinkenCity idea?



Feasibility

- Radio-controlling individual street lamps is possible
- To display content, one needs to know the correct individual ID for each lamp:
 - Extract single addressing IDs from recordings
 - Read out individual ID via infrared
 - After finding one, enumerate consecutive IDs
 - Map ID to location, potentially from a drone

Limitations

- Low “fps” (~2 pixels/regions per second and sender)
- Requires sufficient sending power to cover the city
- Requires prior mapping from street lamp to location

Could be done (within limitations and with permissions!),
probably best as a timelapse

“AskTheState” how many displays there are



While a few cities consider it sensitive information, others respond with more detail than asked for

The screenshot shows the FragDenStaat website interface. At the top, there are navigation links for 'Anfragen', 'Recherchen', 'Klagen', and 'Kampagnen'. Below this, a search bar contains the query 'Steuerung von Straßenbeleuchtung' and a 'Suchen' button. The search results show a response from 'Stadtwerke Bielefeld / mobiel' dated 'am 01.04.2020'. The response text is as follows:

Sehr [redacted]

vielen Dank für Ihre Anfrage. Die Bielefelder Straßenbeleuchtung wird über eine Funk-Rundsteueranlage ein- und wieder ausgeschaltet. Den Ein- bzw. Ausschaltimpuls erhält die Anlage von zwei Dämmerungssensoren. Der eine Sensor ist in der Stadtmitte und der andere im Bielefelder Süden installiert. Dies ist den unterschiedlichen Lichtverhältnissen in den Stadtgebieten geschuldet, die durch den Kamm des Teutoburger Waldes getrennt sind. Je nachdem welcher Sensor zuerst den Schaltimpuls ausgibt, wird die Anlage über den einen oder den anderen Sensor geschaltet. So wird sichergestellt, dass die Straßen im gesamten Stadtgebiet zum gleichen Zeitpunkt ausgeleuchtet werden. Um auf die Trends der Smart City reagieren zu können, soll die Funk-Rundsteueranlage perspektivisch durch ein modernes System abgelöst werden. Weitere Technologien sind aktuell nicht produktiv im Einsatz.

https://fragdenstaat.de/anfrage/steuerung-von-straenbeleuchtung-bei-den-stadtwerken-bielefeld/#nachricht-475436

New Hacking Tool



Thanks to FragDenStaat, and Thomas Blinn for performing the requests!

Hamburg has **just** finished migrating to the “future-proof” radio ripple control system



radio-controllable now!



<https://t3n.de/magazin/chaos-computer-club-246437/>

Zukunftsfähiges System

Hamburg stellt Technik für Beleuchtungsanlagen um

26. August 2024 Pressemitteilung

In Hamburg erfolgt die Ansteuerung der öffentlichen Beleuchtungsanlagen seit vielen Jahren mithilfe der sogenannten Tonfrequenzrundsteuerung (TFR), kabelgebunden über das städtische Stromnetz. Die TFR-Technik wird seit Jahrzehnten von Stromnetz Hamburg (SNH) bzw. den Vorgängerunternehmen in Hamburg als Steuersignal für verschiedenste Anwendungen zur Verfügung gestellt. Zum Beispiel beim Ein- und Ausschalten von Nachtspeicheröfen, Beleuchtungsanlagen bei privaten Kleingartenvereinen oder auch den öffentlichen Beleuchtungsanlagen. Die Technik ist in die Jahre gekommen und entspricht nicht mehr den aktuellen Bedürfnissen. Beim bevorstehenden Netzbau des städtischen Stromnetzes wird die Technik daher nicht weiter verbaut werden. Die dazu genutzte Signalübermittlung wird von der SNH zum 31. Dezember 2024 endgültig abgeschaltet. Damit Hamburg zum Jahreswechsel nicht im Dunkeln steht, muss eine technische Alternative installiert werden. Hamburg Verkehrsanlagen installiert daher seit Dezember 2021 eine neue Ansteuerungstechnik auf Basis der Europäischen Funkrundsteuerung namens EFR.

Für die erfolgreiche Umsetzung mussten im Hamburger Stadtgebiet insgesamt 49.000 einzelne Empfänger ersetzt werden, die künftig über den Langwellenradioweg zentral von den Maststandorten bei Mainflingen bei Frankfurt am Main und Burg bei Magdeburg angesteuert werden und die rund 126.000 Beleuchtungsanlagen ein- oder ausschalten. Diese Ansteuerung geschieht in Hamburg

In other news: Hiccup in Hesse

Im Südkreis wird es dunkel
In mehreren Kommunen sind am Dienstagabend großflächig die Straßenlaternen ausgefallen
Die Spekulationen über die Ursachen reichten von Einsparmaßnahmen bis zur leichteren Suche nach einem Brandstifter in Riedstadt oder einem Hackerangriff. Wie die Pressestelle des zuständigen

Radio ripple controlled, "technical defect" (Not us!)

Our talk is too late for Hamburg, but maybe not for others?

Three conditions need to be met to cause grid instabilities



Now, radio ripple control telegrams have been reversed: **is that sufficient to cause a blackout?**

We are not experts, but we imagine that at least these 3 conditions have to be met:

A large enough amount of power has to be involved

+

The radio control signal has to be overcome/hijacked

+

Optimal timing has to be chosen



- How much power is controlled via radio ripple receivers?
- How much power would need to be taken away to cause trouble?



Two options:

- Overpowering EFR signal with antennas in multiple areas. This seems not an easy task, but we will do a feasibility study on it
- Gain control of EFR's transmitters, either by hacking their IT infrastructure, or by physically breaching into the tower sites



Some elements can affect the damage produced by the attack:

- How utilized are the controlled plants?
- Is there any real-time information about the current grid status?

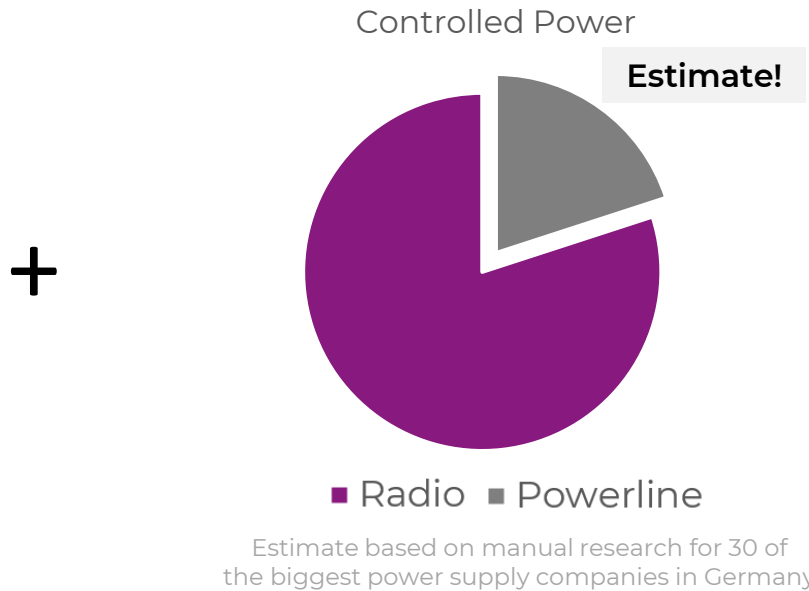
EVUs use radio ripple control to manage small and medium solar plants in Germany



Radio ripple control is **widespread** and legally required for a large portion of PV **roof installations**

Installed power	Remote control
< 30kW	Optional. Demanded by some EVUs.
30 – 100kW	Required by law (EEG). Almost exclusively implemented via ripple control.
> 100kW	Required by law (EEG). More advanced “Fernwirktechnik” needs to be installed.

Type of ripple control



But does it mean that FREs are not in use in this case?



And how about very large solar parks?

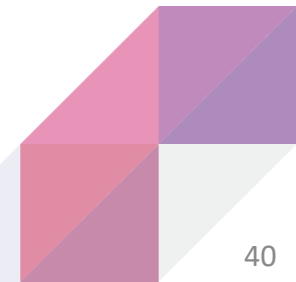


Still today, FREs are used to control also massive renewable power generation plants



Each FRE controls 20MW!

<https://www.youtube.com/watch?v=OaaLkQ0gzZ4>; Video from 2021, confirmed to still be in use today



Solarpark Senftenberg/Schipkau


🌐 2 languages ▾

Article [Talk](#)

From Wikipedia, the free encyclopedia

Enough for ~200.000 households,
or ~8 times Berlin street lighting

Read [Edit](#) [View history](#) [Tools](#) ▾

Coordinates:  51°32′42″N 13°58′48″E﻿ / ﻿51.54500°N 13.97999°E﻿ / 51.54500; 13.97999

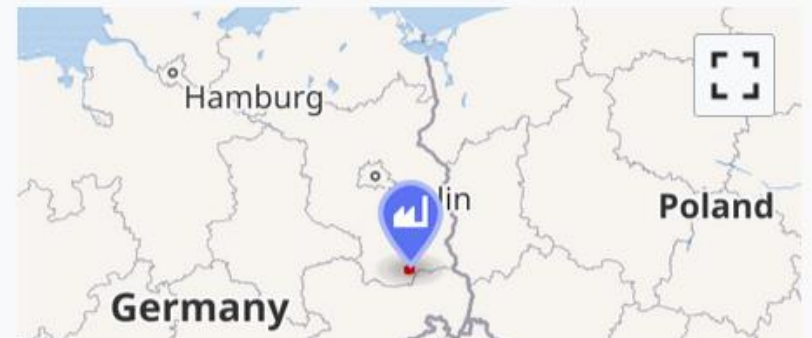
Solarpark Senftenberg/Schipkau is a **166 megawatt (MW)** photovoltaic power station located in Germany near the border of [Senftenberg](#) and [Schipkau](#) (near the village of Meuro). The plant was built on the now closed [Meuro lignite mine](#)^[1] and **is the country's largest solar park.** By now, the 3rd largest solar park national solar project of the year in 2012.^[4]

The park consist of Solarpark Schipkau (72 MWp), Solarpark Senftenberg I (12 MWp) and Solarpark Senftenberg II & III (78 MWp).^[5]

The **PV system** uses about 636,000 **solar panels** provided by [Canadian Solar](#) and 20k-string inverters from [REFUso](#). It is also the first solar park to use a 690VAC gridvoltage for some of REFUso's 333k HV central inverters.

https://en.wikipedia.org/wiki/Solarpark_Senftenberg/Schipkau

Solarpark Senftenberg/Schipkau



Several documents confirm the existence of >100kWp producers controlled by FREs



	Technische Mindestanforderungen Umsetzung des Einspeisemanagements nach § 9 EEG für Erzeugungsanlagen	Seite: 4/8 Stand: 09/2014
	Strom	

Wird bei PV-Anlagen das Signal zur Reduzierung der Einspeiseleistung über einen FRE übermittelt, kommen im Netzgebiet der Netze BW GmbH leistungsabhängig derzeit zwei unterschiedlich parametrisierte FRE zum Einsatz. Bei der Bestellung ist sicherzustellen, dass der jeweils passende FRE bestellt und verwendet wird.

- Für alle PV-Anlagen, bis einschließlich 100 kW, wird ein Empfänger mit einer für das jeweilige Netzgebiet spezifischen Parametrierung eingesetzt.
- Alle PV-Anlagen, die gemäß § 9 Abs. 3 EEG als Anlagen mit mehr als 100 kW gelten, werden über einen FRE mit einer eigenen Parametrierung angesteuert.



Allgemeines

Im Netzgebiet der EWR Netz GmbH wird für das Einspeisemanagement die **Funkrundsteuertechnik** der Fa. EFR GmbH eingesetzt. Zur Umsetzung werden Funkrundsteuerempfänger (FRE) verwendet. Hierbei handelt es sich um technische Einrichtungen zur ferngesteuerten Reduzierung der Einspeiseleistung einer Erzeugungsanlage.

Bei einer Modulleistung von höchstens 100 kWp:

- Mehrstufige Leistungsreduzierung (100 % - 60 % - 30 % - 0 %)


Alternative zum FRE (zulässig bei einer Modulleistung von höchstens 25 kWp)

- Dauerhafte Reduzierung, d. h. Begrenzung der Wirkleistungseinspeisung auf 70 % der installierten Leistung

Bei einer Modul- bzw. Generatorleistung von mehr als 100 kW(p):

- Mehrstufige Leistungsreduzierung (100 % - 60 % - 30 % - 0 %)

Die Syna GmbH realisiert das Netzsicherheitsmanagement mit Hilfe der sogenannten Funkrundsteuertechnik. Hierzu ist bei EEG- und KWK-Anlagen mit einer installierten elektrischen Leistung > 25 kW und < 950 kW ein Funkrundsteuerempfänger zu installieren.

	Anschlusschema und Parametrierung eines Funkrundsteuerempfängers für EEG/KWK-Anlagen zur Reduzierung der Einspeiseleistung	ZZM 49.1000
		Teil – Seite 4/7
		Fachbereich: DRZ-O-PD

Alle Angaben in kW

Leistungs-klasse	Energieart					
	1	2	3	4	5	6
	Windenergie	Deponiegas Grubengas Klärgas Biomasse	Wasserkraft	Solare Strahlungs- energie (PV)	BHKW-/IKW- Anlagen mit konventionellen Energieträgern (z.B. Erdgas, Öl), KWK-gefördert	Geothermie
I	≥ 10.000	≥ 2.000	≥ 1.000	≥ 500	≥ 1.000	≥ 5.000
II	≥ 1.000 und < 10.000	≥ 500 und < 2.000	≥ 500 und < 1.000	≥ 100 und < 500	≥ 100 und < 1.000	≥ 500 und < 5.000
III	< 1.000	< 500	< 500	< 100	< 100	< 500



Die Avacon Netz GmbH setzt für die Stadtwerke Burg die neue Parametrierung ebenfalls unter Verwendung der alten Identifikationsnummer FAE6.3143 als Typ 6_UW031_SF43 ein.

für Avacon Netz GmbH nach alter Parametrierung:

Einspeisemanagement Typ IV für PV ≤ 100 kWp ... nur Relais 4 aktiv für 100%

Einspeisemanagement Typ III Wind (alt PV ≤ 100kWp) ... alle Relais deaktiviert

Einspeisemanagement Typ II für PV > 100 kWp ... nur Relais 4 aktiv für 100%

Our estimate is that 40 GWp of supply and 20 GW of load are controlled with FREs



We collected and correlated information from various sources to **estimate FRE-controllable power**

Bundesnetzagentur
MaStR
Marktstammdatenregister

Datendownload

Gesamtdatenauszug vom Vortag

Download Daten [ZIP / 2.220.324 KB] | Beschreibung des Exports [ZIP / 2.100 KB]

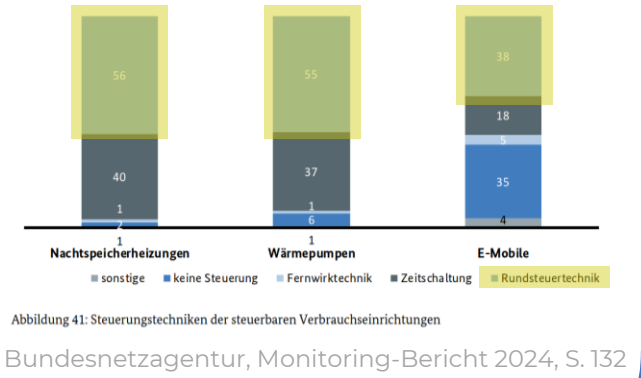
<https://www.marktstammdatenregister.de/MaStR/Datendownload>

From [redacted]
To 'fabian@positive.security' <fabian@positive.security> @
Subject **Steuerung von EE-Anlagen über FRE bei** [redacted]

3. Wie setzt sich dieser zusammen? Also wie viele Gigawatt werden pro Energieart und Kraftwerkgröße (<10kW, <100kW, <1MW, <10MW, >10MW) über die Funkrundsteuertechnik angesprochen?

< 10 kW: ca. 500 Anlagen; Leistung ca. 1,4 MW
>10 kW – 30 kW: ca. 2.200 Anlagen; ca. 25,4 MW
>30 kW – 100 kW: 5.409 Anlagen; 294 MW

Regional energy provider, data from 01.11.2024



Power generation

Energy loads

Estimate!

Solar (<30kW): 4 GWp
Solar (30-100kW): 10 GWp
Solar (>100kW): 6 GWp (?)

Estimate!

Wind: 20 GWp (?)

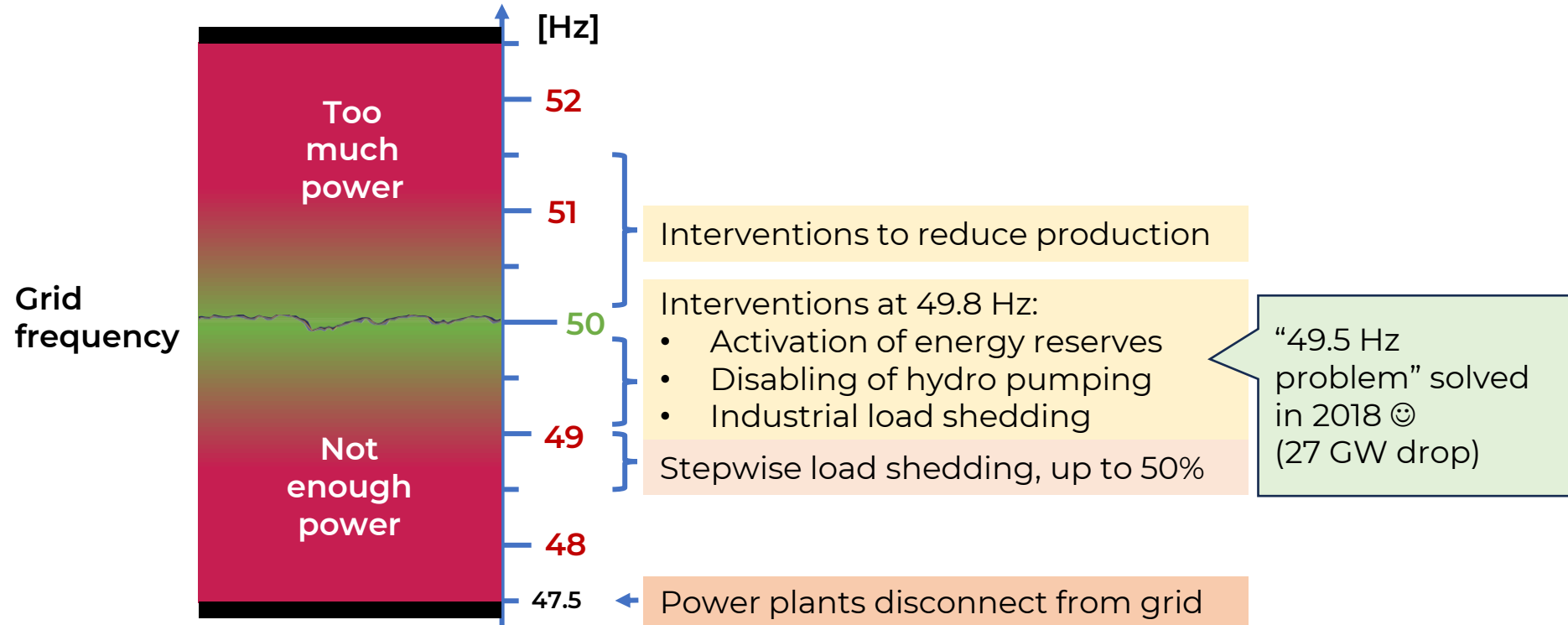
(extrapolating only the 5 wind production companies that were mentioned with numbers by EFR, unconfirmed if FREs are still in use)

Estimate!

Night storage heating: 10 GW
Heat pumps: 8 GW
Wallboxes: 2 GW

The overall controlled load is **hard to estimate** exactly, **but** it is a **significant** portion. For comparison, Germany has ~70 GW peak energy usage and 250 GW of installed production. (This estimate does not consider energy types other than solar/wind and countries other than Germany)

Much less than 60GW is needed to cause serious instabilities in the European grid



In theory, in a fully loaded European grid at 300 GW:
1 Hz change requires **18 GW** imbalance

<https://netzfrequenz.info/regelleistung>

In practice, during an incident on May 17, 2021:
49.84 Hz after a sudden loss of **3.32 GW** of power

https://eepublicdownloads.entsoe.eu/clean-documentsnews/2022/220318_Final_report_Rogowiec_incident.pdf

Sudden regional imbalances can also cause cascade effects!

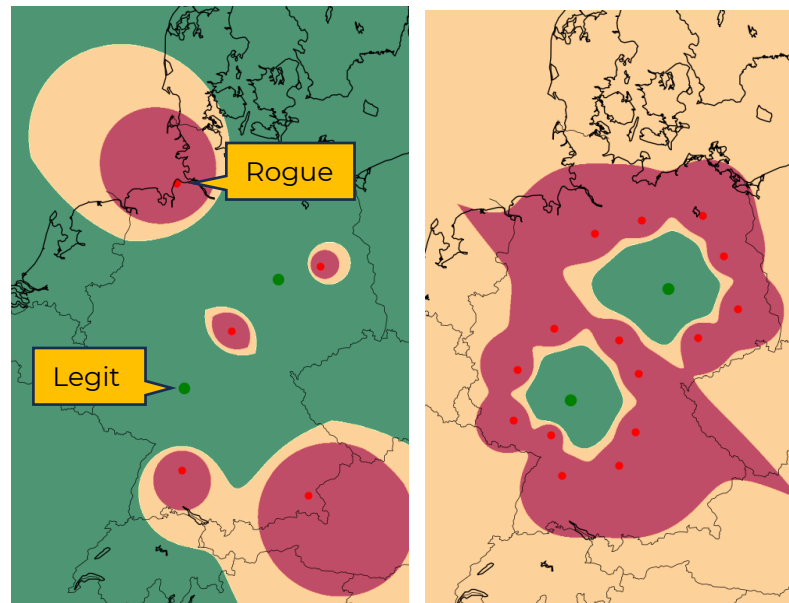
Multiple deployment strategies can be leveraged to create a network of decentralized transmitters



How to overpower EFR transmitters?

Our calculations (together with a longwave expert) suggest that with:

- **550m** antenna
 - **10kW** radio amplifier (~500€)
 - **10kWp** power station (~100€/day)
 - **300km** distance to EFR tower
- the legitimate signal can be sufficiently **overpowered within 70-240 km**



Orange Jammed Red Hijacked

Antenna mount option

High floor

A tall building from which one can drop a cable

Length

50-150m

Price (€)

100

Limitations

Fixed location

Kite

Kite models designed for aerial photography (KAP)

Full size (550m)

500

Requires wind

Balloon

Tethered weather balloons filled up with helium

Full size (550m)

1K

Helium refill, low wind

Drone

Heavy duty commercial or custom drones

Full size (550m)

3-30K

Short operational time

Trailer with mast

Civil or military trailers with a telescopic mast

40m

10K (used)
200K (new)
60/day

Slow to move, availability

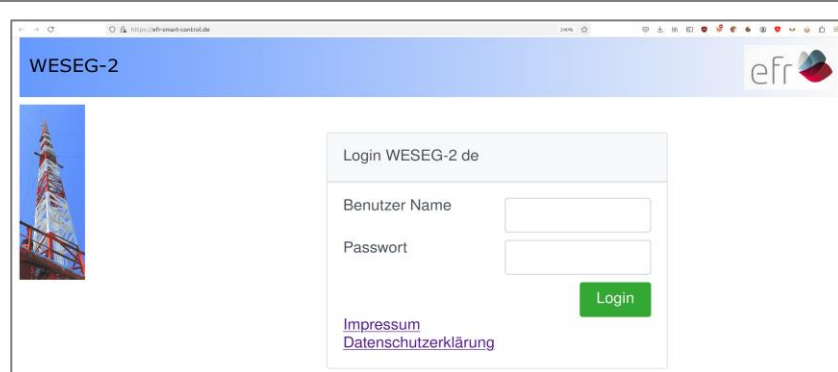


Alternatively, an attacker could attempt to abuse EFR's own radio transmitters



An attacker could try to leverage the existing radio infrastructure **by hacking EFR, or getting physical access** to the sending station (both not the focus of this talk)

Attack option 1: Remote access



Via internet recon, we identified:

- official customer portals and APIs
- information leaks on forgotten websites (now removed)
- outdated software, e.g. a 12-year-old Typo3 CMS (now fixed)

Attack option 2: Physical access



The radio transmitter sites do not seem to be particularly well secured

Illegal Instructions

Let's adopt the perspective of an attacker



Inspired by this 32c3 talk, we will now discuss how a real attack to the grid could look like, assuming FRE control is possible

Wie man einen Blackout verursacht
und warum das gar nicht so einfach ist.

Mathias Dalheimer

62 min 2015-12-30 305305 Fahrplan

https://media.ccc.de/v/32c3-7323-wie_man_einen_blackout_verursacht



Step 1: Find good locations to place senders

Rogue radio transmitters should be close to power plants and away from real ones

Kraftwerkskarte/-liste Kraftwerkskarte Kraftwerksliste

Unternehmen: Alle Regelzone: Alle

Umkreis 100 km Nennleistung

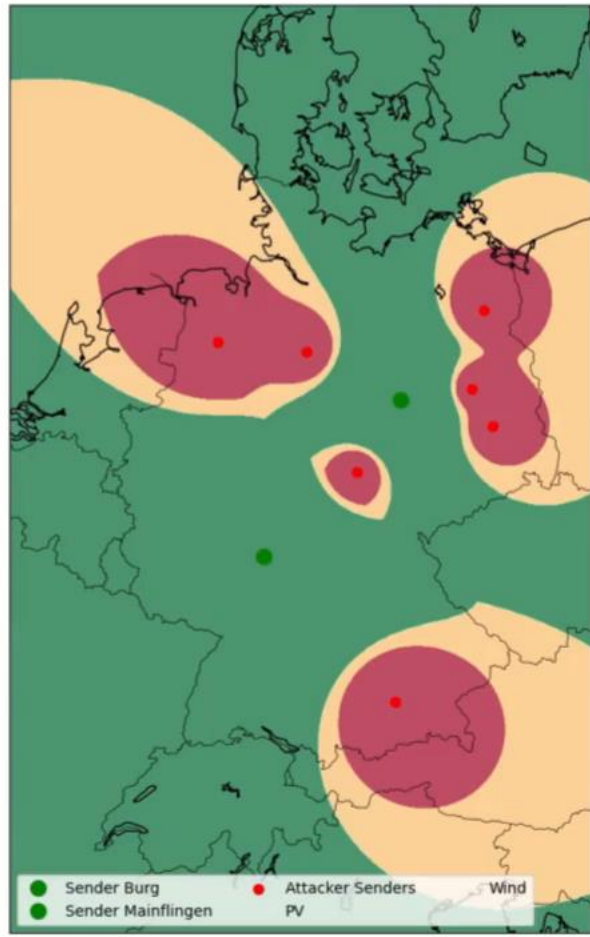
Unternehmen: Bundesland: Alle

Karte Satellit **Illustrative**

Legend:
● EFR transmitter locations
● Potential attacker sending site

Name	Ort	Energieträger	Nennleistung
+ 11 Windkraftanlagen	Ahlen	Wind (Onshore)	25,3 MW
+ 1Heiz Energie GmbH	Eberswalde	Biomasse	20 MW
+ 2000-7317	Treia	Wind (Onshore)	16,8 MW
+ Abfallentsorgungszentrum Asdonkshof	Kamp-Lintfort	Mineralölprodukte	20,8 MW
+ Abfallheizkraftwerk Neunkirchen	Neunkirchen	Abfall	11,6 MW
+ Abwinden-Asten	Luftenberg/Asten	Laufwasser	168 MW
+ ADM Heizkraftwerk	Hamburg	Erdgas	23,73 MW
+ Ahrensfelde	Ahrensfelde	Erdgas	148,4 MW
+ alpha ventus	Nordsee	Wind (Offshore)	60 MW
+ Alt-Bennebek	Alt Bennebek	Wind (Onshore)	15,3 MW

Type, size and location of many power plants



Optimize Locations

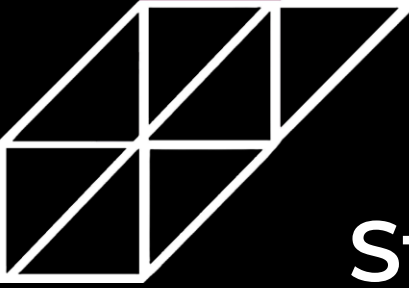
Show Wind

Show PV

+3dB needed

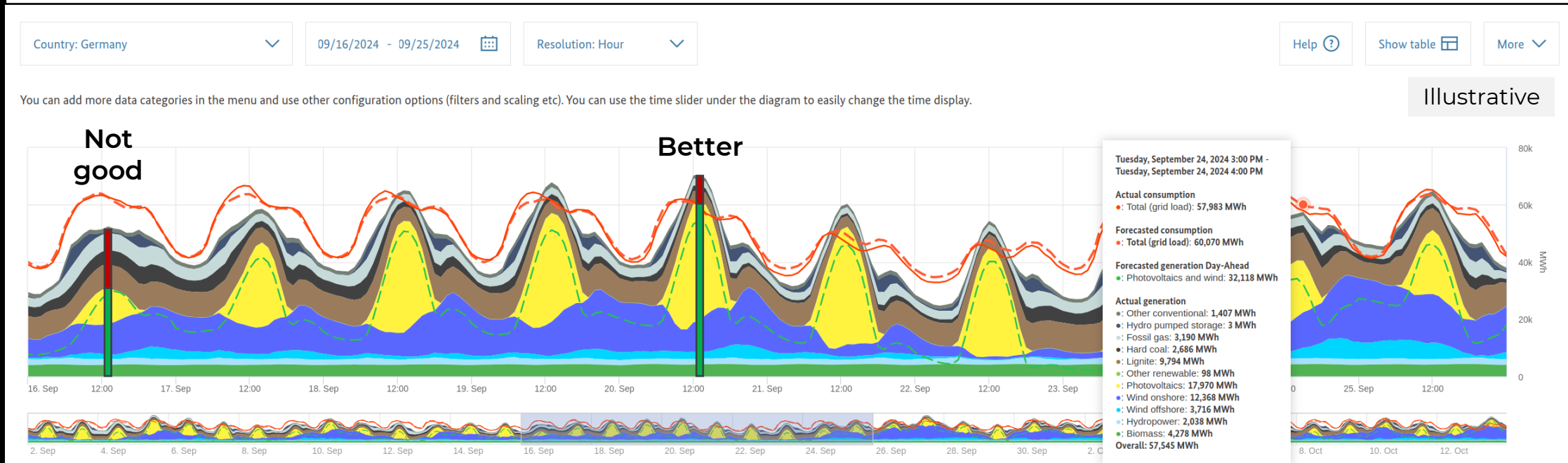
Total Power: Hijacked=0.0 MW, Safe=0.0 MW, Jammed=0.0 MW





Step 2: Choose the right time

Wait for massive solar and wind production with non-renewables at a low



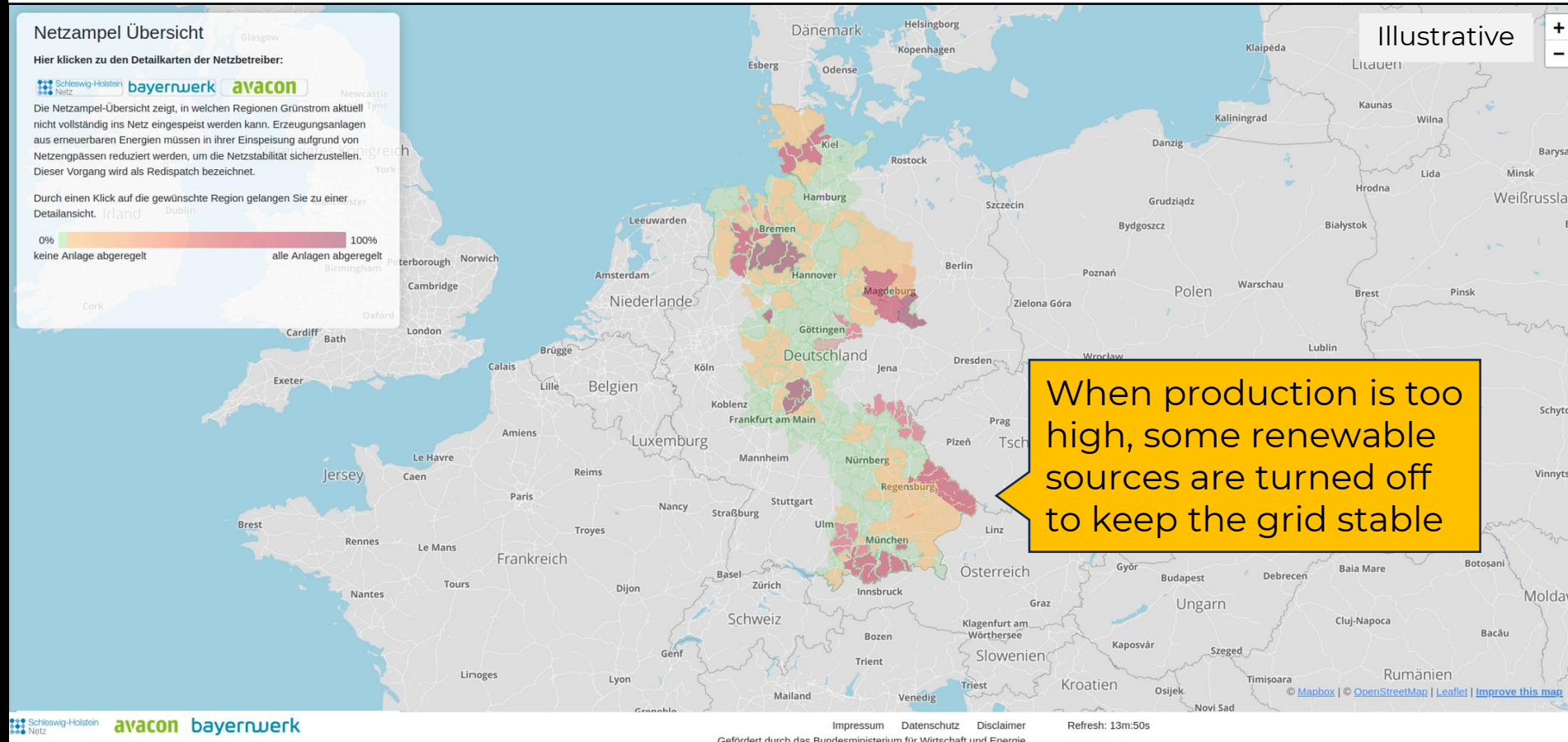
<https://www.smard.de/home>

- Non-renewable
- Renewable

Step 2b: Verify it's the right time



Wait until many renewables are already turned off



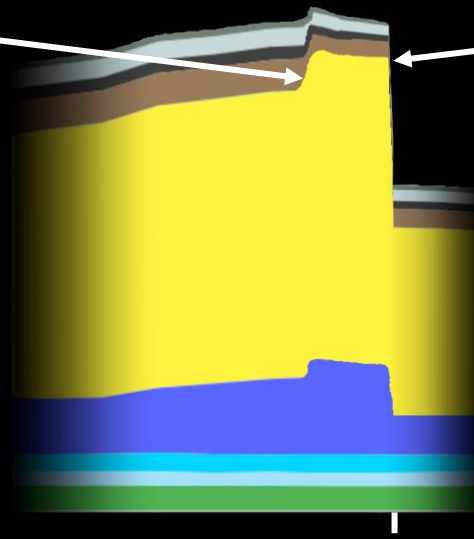
Step 3: Perform the attack



Illustrative

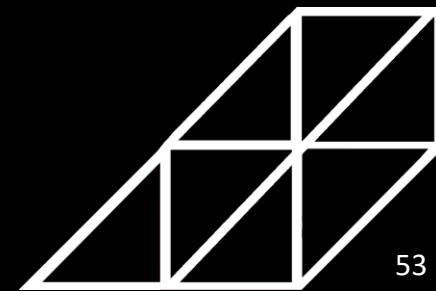
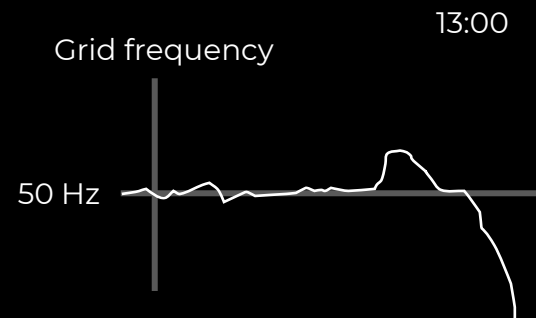
1. Switch on all renewables

- With many renewables off, switch all of them on
- Reduces supply from uncontrolled power plants ("amplification attack")
- Wait for return to 50 Hz



2. Switch renewables off and loads on

- Possible optimizations:
- Time it with the change of hour
 - Multiple on-off-rounds synced with grid's resonance frequency
 - Add an "FRE deactivation" message in the end and jam the frequency



In our opinion, this attack scenario has potential to cause grid instabilities



A large enough amount of power has to be involved

+

The radio control signal has to be overcome/hijacked

+

Optimal timing has to be chosen

The biggest unknown.

However, with our estimate of FRE-controlled supply and load, the European grid could experience a never-before-seen unexpected loss of power

The biggest obstacle.



Overpowering the signal with own transmitters requires a significant coordinated effort

For a state-sponsored attacker, hijacking of the actual transmitter might be the more plausible attack vector

Comparably trivial.

Public information about production and loads is available in real-time

Note: If an attack does not cause a blackout or brownout, it could still have short-term effects on energy prices and/or result in a network split



But we're not experts, so SPIEGEL asked one



Thanks to Prof. Dr. Albert Moser, university professor at "Institut für Elektrische Anlagen und Netze, Digitalisierung und Energiewirtschaft" at RWTH Aachen for taking the time to provide his assessment

"Ein Angriff in dieser Größenordnung könnte durchaus zum ersten europaweiten Stromausfall in der Geschichte führen"

Translation: "An attack of this magnitude could indeed lead to the first Europe-wide power outage in history"

EFR took our disclosure seriously ... and involved their lawyers



2024-09-12: Reported our findings to EFR via email

2024-11-06: In-person meeting with EFR

- Some issues already known, reported by Prof. Dr. Christoph Ruland and Matthias Schneider from the University of Siegen in 2013 (mainly unencrypted/unauthenticated time stamp, our attack #1) ^[1]
- In 2015, an encrypted protocol replacement was developed, but "the market did not demand it"
- Use of FREs in large power plants was not intended and not known

Umsetzungspflicht. EFR hat im vergangenen Jahr eine Möglichkeit der Verschlüsselung der Langwellensignale erarbeitet, die implementiert werden kann, sobald der Markt dies fordert. Im laufenden Jahr ist ein Schwerpunkt die Sicherheit der Kommunikation im System der EFR zu verbessern, um hier

Source: EFR "Jahresabschluss zum Geschäftsjahr" 2015

2024-11-07: Filed report to BSI, which forwarded it also to BNetzA and BMWK

2024-12-05: EFR told us they will inform customers next week and warn of FRE usage in large power plants

2024-12-10: EFR sent us a letter via their lawyers, urging us not to proceed with this talk and demanding removal of their company name, also from the Fahrplan talk description

2024-12-28: Public disclosure at 38C3

§ 130a Abs. 1 StGB erfüllen. Es handelt sich im buchstäblichen Sinne um „illegal instructions“, was zwar dem Motto des diesjährigen 38C3 entsprechen mag, für Sie persönlich aber **erhebliche nachteilige Folgen** haben kann.

Source: EFR lawyer's letter

Note: EFR quickly mitigated some low-hanging internet perimeter issues that we stumbled upon and reported

Last Minute Update:

EFR is now publicly denying the possibility to overpower their senders with a decentralized network



2024-12-10:

Diese Darstellung übergeht aber, welcher enorme technische Aufwand erforderlich ist, um flächendeckend ein stärkeres Signal als die Sendeanlagen unserer Mandantin auszusenden. Hierfür wären sehr viele geeignete Sender von **über zoom Höhe** erforderlich.

Source: EFR lawyer's letter

2024-12-28:

Die EFR wiederum weist das Angriffsszenario mit den selbstgebauten, fliegenden Antennen strikt zurück. Die Firma schreibt auf SPIEGEL-Anfrage noch deutlicher: »Die Einschätzung, dass die Funkrundsteuerung über Langwelle großflächig manipuliert werden kann«, sei schlicht »falsch«.

Source: <https://www.spiegel.de/netzwelt/web/stromversorgung-koennten-hacker-blackouts-ueber-funk-ausloesen-a-53c29240-425b-4603-852e-5a1c0a1e5400>

While EFR **has agreed** with our assessment in their lawyer letter ("one would need many transmitters with >200m height"), they are **now outright denying** this possibility towards media

Our offer still stands: **Let us validate it in a real-world test!**

The way forward: Implement remote management using a more secure alternative



This is the proposed successor technology
Currently, certified devices are produced by:
EFR, EMH, Sagemcom, Theben, Power Plus



**iMSys
(intelligentes
Messsystem)**

Public LTE-M
or NB-IoT

KRITIS-only
LTE 450MHz

Ethernet



LoraWAN



TETRA



Strompager



Broadband
over Power
Lines (BPL)



The rollout of iMSys started, but could speed up and it seems to prioritize the wrong targets



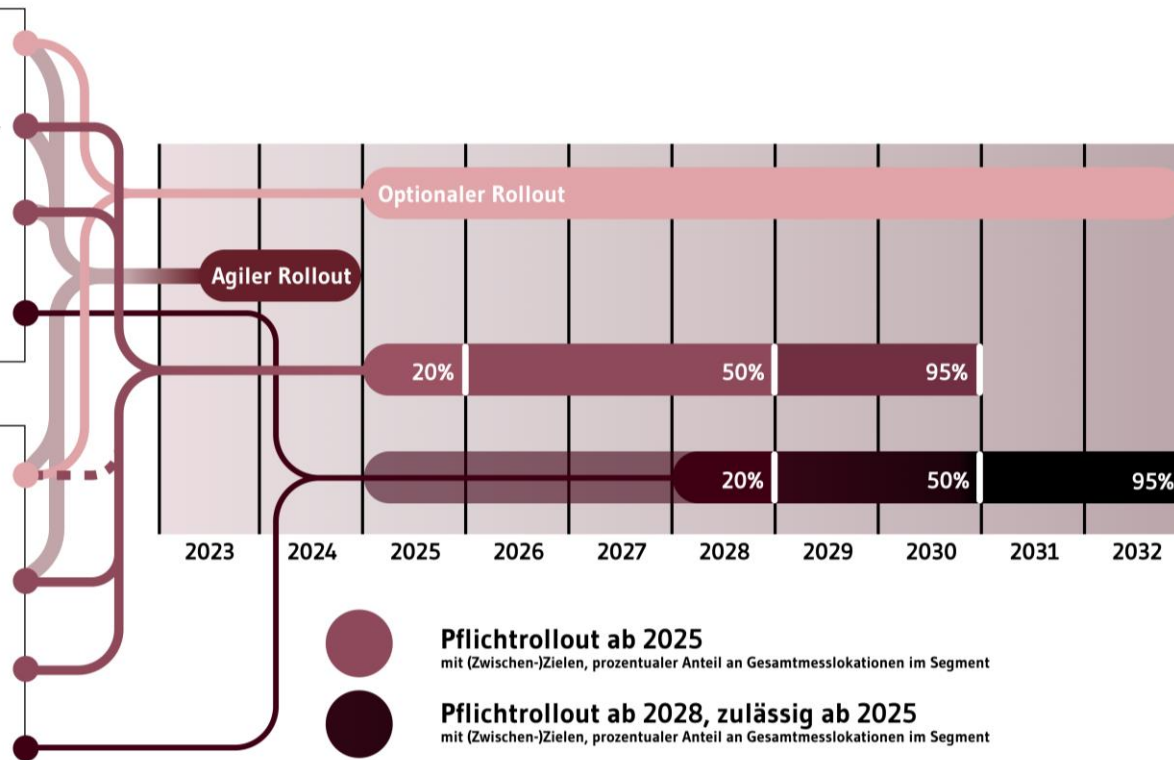
Initially planned for 2017, iMSys gateways will “soon” really be required in Germany (probably)

Letztverbraucher

- Unter 6.000 kWh/Jahr**
für Verbraucher unter einem Verbrauch von 6000 kWh/Jahr
-> ist seit 2023 der agile Rollout gestartet
-> ist der Rollout ab 2025 optional, auch auf Wunsch des Kunden
- 6.000 bis 100.000 kWh/Jahr**
für Verbraucher ab 6000 kWh/Jahr bis einschließlich 100.000 kWh/Jahr
-> ist seit 2023 der agile Rollout gestartet
-> ist der Rollout ab 2025 verpflichtend
- §14a EnWG Verbrauchseinrichtung**
für Verbrauchseinrichtungen nach §14a EnWG, i. d. R. mit einer Leistung über 6,2 kW
-> ist seit 2023 der agile Rollout gestartet
-> ist der Rollout ab 2025 verpflichtend
- Über 100.000 kWh/Jahr**
für Verbraucher ab 100.000 kWh/Jahr
-> ist der Rollout ab 2025 zulässig
-> ist der Rollout ab 2028 verpflichtend

EEG-/KWKG-Erzeuger

- 1 kW bis 7 kW**
für Erzeuger bis einschließlich 7 kW installierter Leistung
-> ist seit 2023 der agile Rollout gestartet
-> ist der Rollout ab 2025 optional
- und mit §14a Verbrauchseinrichtung ab 2025 verpflichtend
Ausnahme für Steckersolargeräte bis 2kWp:
-> kein Anschluss nötig
- 7 kW bis 25 kW**
für Erzeuger ab 7 bis einschließlich 25 kW installierter Leistung
-> ist seit 2023 der agile Rollout gestartet
-> ist der Rollout ab 2025 verpflichtend
- 25 kW bis 100 kW**
für Erzeuger ab 25 bis einschließlich 100 kW installierter Leistung
-> ist der Rollout ab 2025 verpflichtend
- Über 100 kW**
für Erzeuger über 100 kW installierter Leistung
-> ist der Rollout ab 2028 verpflichtend



Wait... why are the **fewer most important** targets (large plants/loads) onboarded at the **latest**?

We wish the regulator could change the plan, and **push for those ones first**, and fast!

<https://ariadneprojekt.de/media/2024/10/Gesetzlicher-Smart-Meter-Rolloutplan.png>

Takeaways



Cities with radio controllable street lights can be turned **into cool art installations** (if allowed)



Radio ripple receivers can be **locally abused for fraud** (tariff switching, no power limitations)



Compromising receivers at scale could result in **grid instabilities and potentially blackouts**

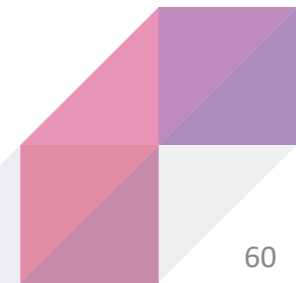


iMSys rollout should speed up to replace radio ripple control devices in large power plants



In general, all **legacy systems need scrutiny** by security experts, so **go and find the next one!**

Our wish, if you're on the receiving side: **Collaborate with good-faith researchers** instead of threatening to sue them



Illustrative

Parody



Thanks to:

- Jakob Lell
- Maximilian Kirchmeier
- Dr. Markus Vester

Questions?

Contact us:

- fabian@positive.security
- luca@positive.security