



# Energy Fraud and Orchestrated Blackouts

## Issues with Wireless Metering Protocols (wM-Bus)

Black Hat USA 2013, Las Vegas, Aug 1<sup>st</sup> 2013

cyrill.brunschwiler@csnc.ch

Compass Security AG  
Werkstrasse 20  
P.O. Box 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
[team@csnc.ch](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)

# Agenda

## Intro

- ❖ Making Of
- ❖ Smart Grids
- ❖ Smart Metering

## Wireless M-Bus

- ❖ Application
- ❖ Protocol Stack
- ❖ Protocol Overview (Frames, Transport Layer, Data Headers)
- ❖ Protocol Analysis (Privacy, Confidentiality, Integrity)

## Demo

- ❖ Setup
- ❖ Attacks and Issues

## Conclusion



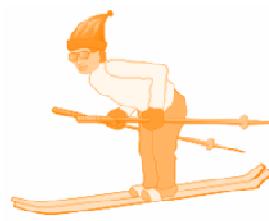
# Intro

Compass Security AG  
Werkstrasse 20  
P.O. Box 2038  
CH-8645 Jona

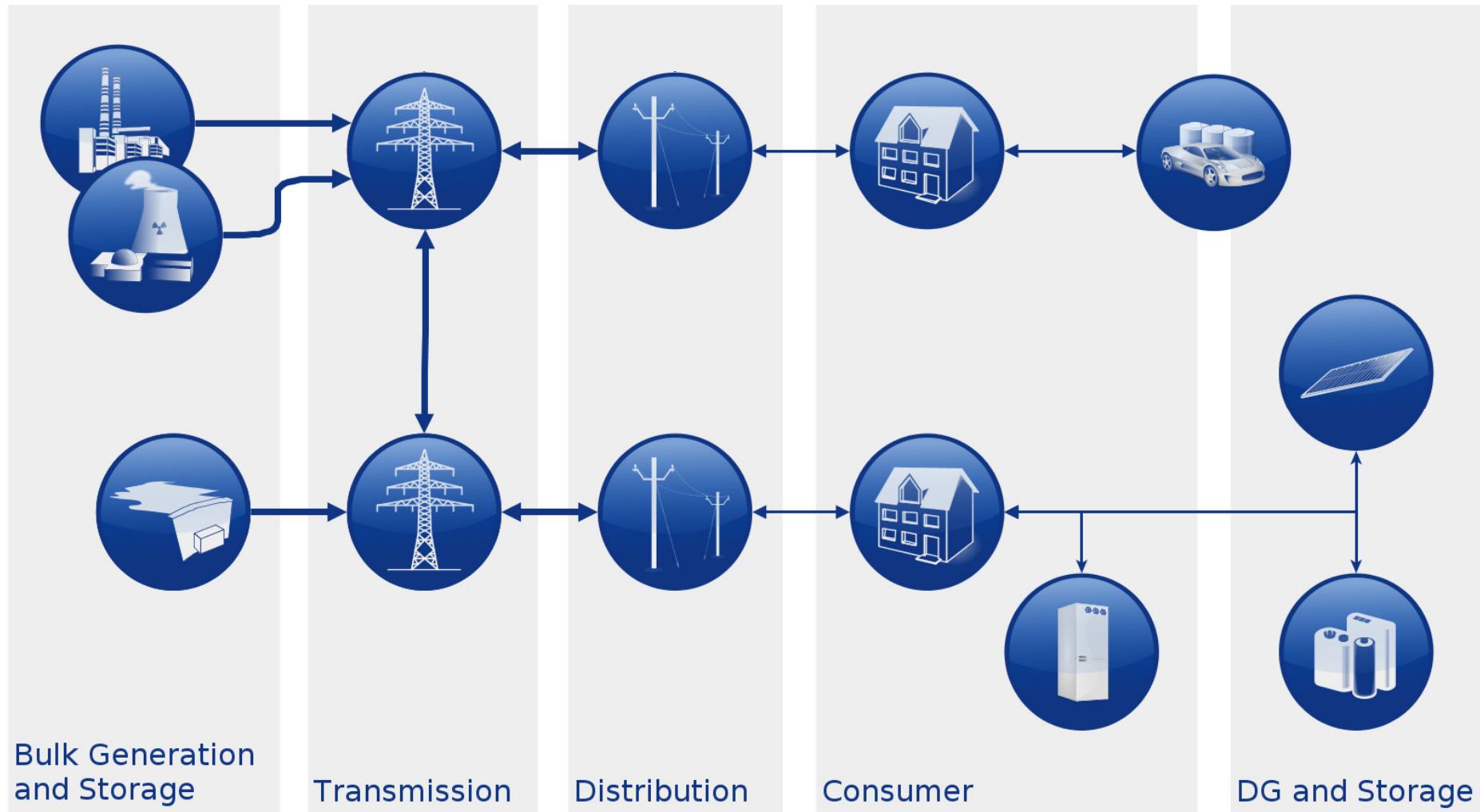
Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
[team@csnc.ch](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)

## Timeline

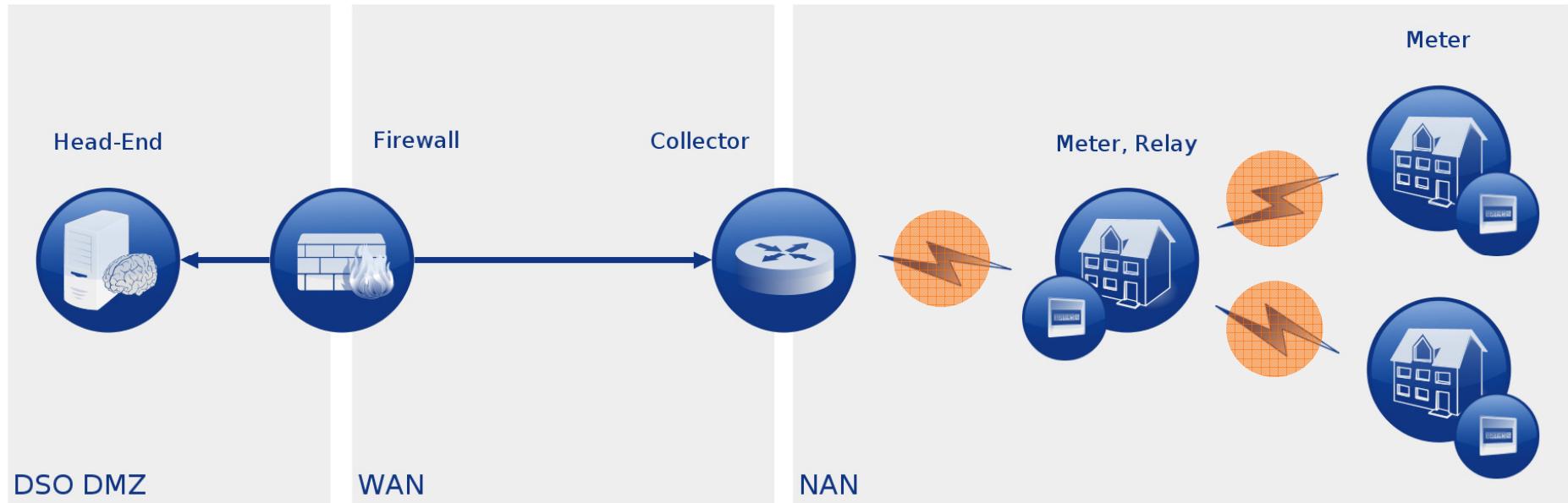
- ❖ Summer 2011: Got attention of wireless M-Bus
- ❖ Autumn 2012: Started MSc thesis
- ❖ X-mas 2012: German BSI/OMS group published „Security Report“
- ❖ X-mas 2012: Short mention of M-Bus being „inadequate“
- ❖ February 2013: Spent some time digging through EN paperwork
- ❖ February 2013: Spent some time in an M-Bus lab environment
- ❖ March 2013: Finished analysis of M-Bus current resp. draft standards
- ❖ March 2013: German BSI mentions wM-Bus security being insufficient
- ❖ Summer 2013: Publication at Black Hat USA



## Smart Grid Blue Print



## Metering Infrastructure Blue Print



## Legend

- ❖ DSO Distribution System Operator
- ❖ NAN Neighbourhood Area Network
- ❖ Wireless M-Bus

## Collectors

- ◆ Various Vendors
- ◆ Neuhaus is just an example of a Multi Utility Controller (MUC)

## Support Head-end side

- ◆ GPRS
- ◆ Ethernet (Web Interface)
- ◆ WLAN
- ◆ WiMAX

## Support Meter side

- ◆ Wired Serial (RS-485)
- ◆ Wired M-Bus
- ◆ ZigBee
- ◆ Wireless M-Bus



# Intro – Smart Metering – Collector GUI



VARIOMUC-Manager 1.2.3.14

Datei Trennen Short Info Einstellungen Sonderfunktionen Sensoren

Benutzer		Nr.	Servernummer	Zählernummer	Status
Gast		1	000475F72E0F		18.07.2013
Endanwender		2	01242375034010640E	HYD 10400375 Bus-/System-Komponente	18.07.2013
MUC-Betreiber		3	01242376034010640E	HYD 10400376 Bus-/System-Komponente	18.07.2013
Messstellenbetreiber		4	012D2C077194150102	KAM 15947107 Elektrizität	18.07.2013
Messdienstleister		5	012D2C400649150102	KAM 15490640 Elektrizität	18.07.2013
Lieferant		6	019315773535030002	ELS 03353577 Elektrizität	18.07.2013
Hersteller		7	01A205440000570C37	AMB 57000044 Funkwandler (Zählerseitig)	18.07.2013
LAN/DSL		8	01A511198105423003	DME 42058119 Gas	18.07.2013
IPT		9	01A815000216945802	FMH 94160200 Elektrizität	18.07.2013

OBIS	OBIS	Wert	Scaler	Einheit	Status	Zeit
8181C78203FF	129-129:199.130.3*255	AMB				
0000616100FF	0-0:97.97.0*255	0				
0000600101FF	0-0:96.1.1*255	A2 05 44 00 00 57 0C 37				
0000600109FF	0-0:96.1.9*255	BMBER wireless Testmodul! T Mode				

## Electricity Meters

- ❖ Various Vendors
- ❖ Kamstrup is just an example

## Interfaces

- ❖ Optical
- ❖ Wired Interfaces
- ❖ GPRS
- ❖ ZigBee
- ❖ Wireless M-Bus

## Functionality

- ❖ Meter reading
- ❖ Pre-payment
- ❖ Tariffs
- ❖ Disconnect





# Wireless M-Bus

Compass Security AG  
Werkstrasse 20  
P.O. Box 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
[team@csnc.ch](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)

## Market segment

- ❖ Popular in remote meter reading
  - ❖ Heat, Water, Gas, Electricity
- ❖ 15 million wireless devices deployed (figures from 2010)
- ❖ Mainly spread across Europe

## Usage

- ❖ Remote meter reading
- ❖ Drive-by meter reading
- ❖ Meter maintenance and configuration
- ❖ Becoming popular for smart metering applications
  - ❖ Tariff schemes, real-time-pricing
  - ❖ Demand-response
  - ❖ Pre-payment
  - ❖ Load-limit
  - ❖ Remote disconnect

# Protocol Stack



## Involved Standards

Layer	Standard	Description
Application	prEN 13757-3	M-bus dedicated application layer (specified application layer security)
Network	EN 13757-5	Wireless relaying (optional for meters supporting the router approach)
Data Link	prEN 13757-4	Wireless meter readout (specifies link layer security)
Physical	prEN 13757-4	Wireless meter readout (specifies use of frequency bands)

## Legend

- ❖ EN European Norm
- ❖ pr Draft Standard



# Protocol Overview

Compass Security AG  
Werkstrasse 20  
P.O. Box 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
[team@csnc.ch](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)

## Physical Layer

- ◆ Frequency Spectrums
  - ◆ 868 MHz
  - ◆ 434 MHz
  - ◆ 169 MHz
- ◆ Distance
  - ◆ Up to 5 miles (LoS)
- ◆ Line coding (depends on communication mode)
  - ◆ 3 of 6 code (constant-weight code)
  - ◆ Manchester coding
  - ◆ NRZ coding

## Data Link Layer

- ❖ Frames (typical)

Frame Header

Data Header

Data Records

- ❖ CRCs
- ❖ Device addressing
- ❖ Specification of data (application layer)
  - ❖ Response
  - ❖ Command
  - ❖ Alerts and Errors...

- ❖ Extended Link Layer

- ❖ CRCs
- ❖ Provides encryption at link layer

# Protocol Overview - Data Link Layer



## First Block (Frame Header)

Example Capture (Sent by meter, CRCs removed)

**1E 44 2D 2C 07 71 94 15 01 02** 7A B3 00 10 85 BF  
5C 93 72 04 76 59 50 24 16 93 27 D3 03 58 C8

Field	Value	Interpretation
Length	1E	30 bytes frame length (exclusive length byte)
Control	44	Indicates message from primary station, function send/no reply (SND-NR)
Manuf. ID	2D 2C	Coded for Kamstrup (KAM) calculated as specified in prEN 13757-3. ID is managed by the flag association.
Address	07 71 94 15 01 02	Identification: 15 94 71 07 (little-endian) Device Type: 02 (electricity meter) Version: 01

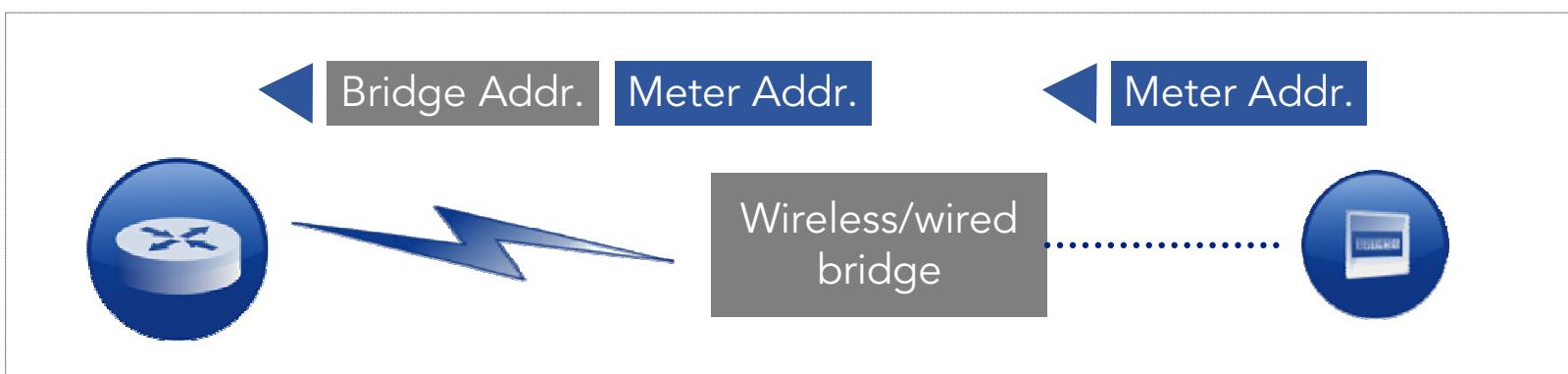
## Data Header Types

Frame Header

Data Header

Data Records

- ❖ No header
- ❖ Short header
  - ❖ Indicates access number
  - ❖ Signals errors and alerts
  - ❖ Indicates encryption mode
- ❖ Long header
  - ❖ Additionally signals addresses behind bridges or virtual devices



# Protocol Overview – Application Layer



## Data Header Example

Example Capture (Sent by meter, CRCs removed)

1E 44 2D 2C 07 71 94 15 01 02 7A **B3** **00** **10** **85** BF  
5C 93 72 04 76 59 50 24 16 93 27 D3 03 58 C8

Field	Value	Interpretation
Access number	B3	Current access number is 179. The standard mandates to choose a random number on meter start. The standard suggests to use timestamps and sequence counters since ACC is insufficient to prevent replay.
Status field	00	Message is meter initiated and there are no alarms or errors.
Configuration	10 85	Encryption mode is 5 <sub>h</sub> which is AES-128 in CBC mode. 10 <sub>h</sub> indicates a single encrypted block containing meter data (without signature). The field further indicates a short window where the meter listens for requests (8 <sub>h</sub> )

## Data Records

Frame Header

Data Header

Data Records

- Structured using data information fields (DIF) and value information fields (VIF) incl. relevant extensions (DIFE, VIFE)

## Data Record Example

04 83 3B 08 34 05 00

Field	Value	Interpretation
DIF	04	Instantaneous readout value, no extension fields
VIF	83	Primary VIF, Unit: Energy $10^0$ Wh, has extension (VIFE0)
VIFE0	3B	Forward flow contribution only
Data	08 34 05 00	The value is coded LSB first and it represents a value of 341000 respectively: 341 kWh

# Wireless M-Bus Sniffer



**Protocol sniffers display wireless M-Bus data record contents provided you know the key. The standard suggests "at least 8 bytes of the key shall be different for each meter"**

```
root@debian:/home/user/git/scambus# ./scanner.py -i /dev/ttyUSB0 -v
FF 03 11 44 24 23 75 03 40 10 64 0E 70 F0 02 FD 17 30 00 61
Jul 29 15:57:05 HYD 10 40 03 75 SND-NR Data: F0 02 FD 17 30 00 61
CI Detail:    70 (Application error from device without Transport La
w/o header:   True
short header:  False
long header:   False
F0 02 FD 17 30 00 61
-----
FF 03 5F 44 79 16 17 00 17 13 06 02 7A 37 00 50 05 45 96 8A A5 6B 0E 6
  60 59 EA 4F 51 91 1B 3F BA A7 BB 70 E8 66 A5 5E 63 4B A3 B7 03 EF B5
  7
Jul 29 15:57:07 ESY 13 17 00 17 SND-NR Data: 45 96 8A A5 6B 0E 6C 08 F
  EA 4F 51 91 1B 3F BA A7 BB 70 E8 66 A5 5E 63 4B A3 B7 03 EF B5 48 D7
CI Detail:    7A (EN 13757-3 Application Layer with short Transport
w/o header:   False
short header:  True
long header:   False
has errors:   False
```



# wM-Bus Protocol Analysis

Compass Security AG  
Werkstrasse 20  
P.O. Box 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
[team@csnc.ch](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)

## Dedicated Application Layer (DAL) Encryption Modes

- ❖ 0 no encryption
- ❖ 1 reserved
- ❖ 2 DES in CBC mode, zero IV
- ❖ 3 DES in CBC mode, non-zero IV
- ❖ 4 AES-128 in CBC mode, zero IV
- ❖ 5 AES-128 in CBC mode, non-zero IV
- ❖ 6 reserved for future use
- ❖ 7ff reserved

## Extended Link Layer (ELL) Encryption Modes

- ❖ 0 no encryption
- ❖ 1 AES-128 in CTR mode



## Are we safe with AES?



Compass Security AG  
Werkstrasse 20  
P.O. Box 2038  
CH-8645 Jona

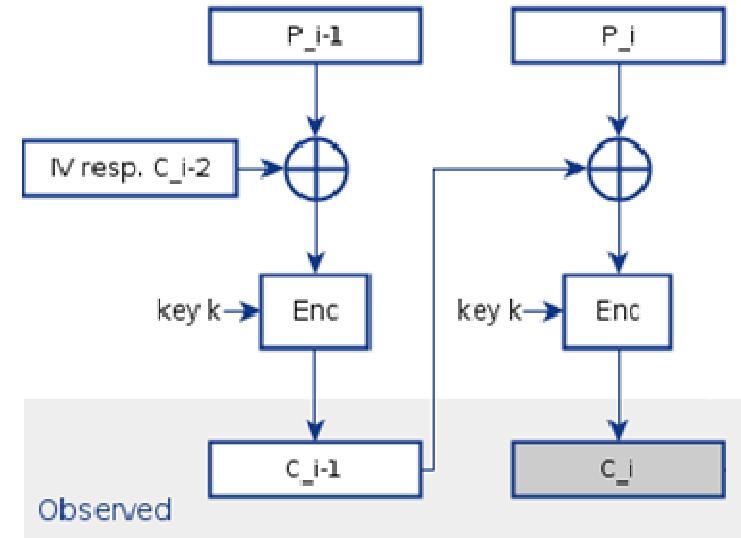
Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
[team@csnc.ch](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)

# Are we safe with AES?



## Encryption Mode 4 (DAL)

- ❖ AES-128 in CBC mode
- ❖ All-zero IV
- ❖ Uses static key k
- ❖  $C_1 = \text{Enc}_k(P_1 \oplus \text{IV})$   
=  $\text{Enc}_k(P_1 \oplus 00\ 00\ \dots\ 00\ 00)$   
=  $\text{Enc}_k(P_1)$
- ❖ Equal PT result in same CT



## Standard workaround

- ❖ Standard mandates to prefix value with date and time record
- ❖ Date and time (record type F) maximum granularity is minutes

## Side note

- ❖ Type I and J records allow for a granularity of seconds

## Encryption Mode 5 (DAL)

- ◆ AES-128 in CBC mode
- ◆ Non-zero IV
- ◆ Uses static key k
- ◆ IV built from frame info and data header

## Mode 5, IV Example

Example Capture (Sent by meter, CRCs removed)

1E 44 **2D** **2C** 07 71 94 15 01 02 7A **B3** 00 10 85 BF  
5C 93 72 04 76 59 50 24 16 93 27 D3 03 58 C8

### Initialization Vector (IV)

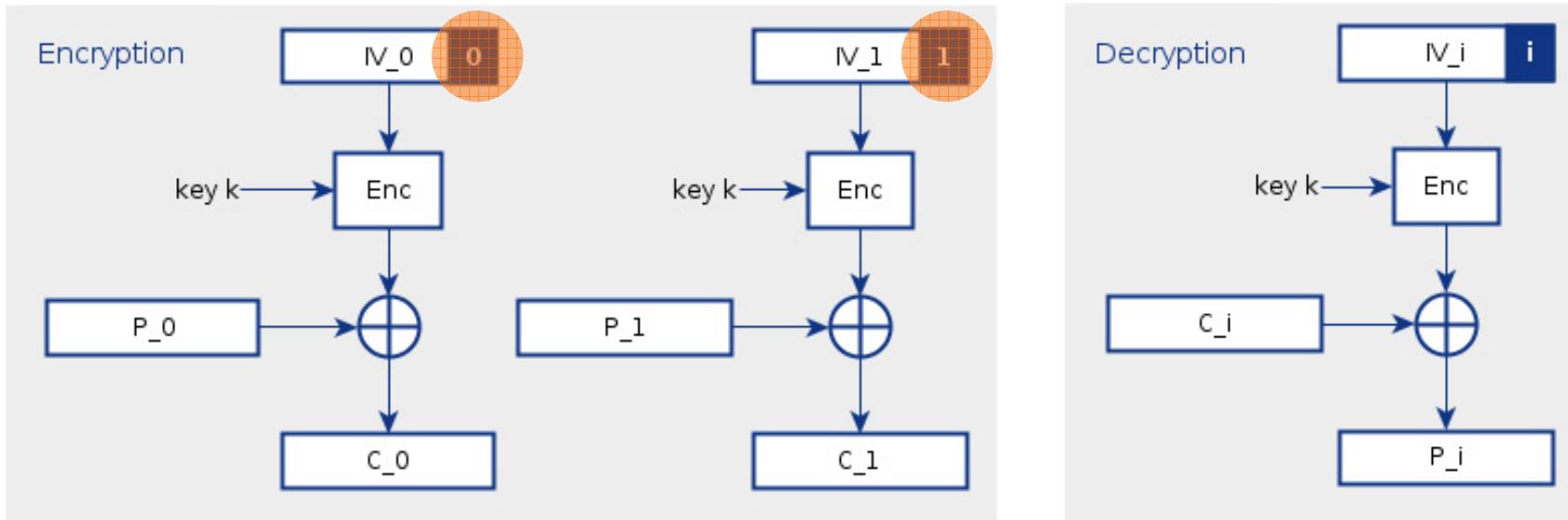
Manuf.	Address								Padding with Access Number							
2D	2C	07	71	94	15	01	02	B3	B3	B3	B3	B3	B3	B3	B3	B3

# How about Counter Mode?



## Encryption Mode 1 (ELL)

- ★ AES-128 in CTR mode



# How about Counter Mode?



## Keystream repetition in CTR mode

$$C_a = \text{Enc}_k(\text{IV}) \oplus P_a$$

$$C_b = \text{Enc}_k(\text{IV}) \oplus P_b$$

## Apply Mathemagic

$$P_a \oplus P_b = C_a \oplus C_b$$

## Example of Keystream Repetition

$$P_a = 04\ 83\ 3B\ \textcolor{orange}{08}\ \textcolor{blue}{34}\ \textcolor{blue}{05}\ \textcolor{blue}{00}\ 2F\dots\ (341'000\ \text{Wh})$$

$$P_b = 04\ 83\ 3B\ \textcolor{blue}{14}\ \textcolor{blue}{34}\ \textcolor{blue}{05}\ \textcolor{blue}{00}\ 2F\dots\ (341'012\ \text{Wh})$$

$$P_a \oplus P_b = 00\ 00\ 00\ \textcolor{orange}{1C}\ 00\ 00\ 00\ 00\dots$$

$$C_a \oplus C_b = 00\ 00\ 00\ \textcolor{orange}{1C}\ 00\ 00\ 00\ 00\dots$$

# How about Counter Mode?



We observed a difference of 0x1C. So what?

Think about the construction of 0x1C out of two values

$$\begin{array}{rcl} \text{Max. difference: } & 1 & 1100 = 28 \\ & -0 & 0000 = 0 \\ & & = \mathbf{28 \text{ Wh}} \end{array}$$

$$\begin{array}{rcl} \text{Min. difference: } & 1 & 0000 = 16 \\ & -0 & 1100 = 12 \\ & & = \mathbf{4 \text{ Wh}} \end{array}$$

Consumption must have changed between 4 and 28 Wh

# How about Counter Mode?



## IV in encryption mode 1

Manuf.	Address	CC	SN	FN	BC
2 bytes	6 bytes	1 byte	4 bytes	2 bytes	1 byte

- ❖ CC Signal communication direction, prioritise frames ...
- ❖ SN Encryption mode, time field, session counter (4 bits)
- ❖ FN Frame number
- ❖ BC Block counter
  
- ❖ Predictable IVs result in 85-bits security due to TMTO

## How to get the key stream to repeat?

- ❖ Cause device to reuse the same IV
- ❖ If someone could adjust the device time the IV could be repeated

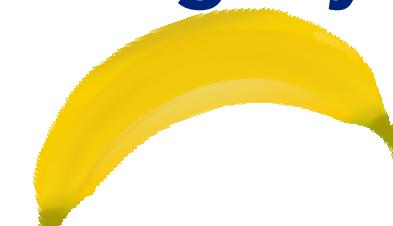
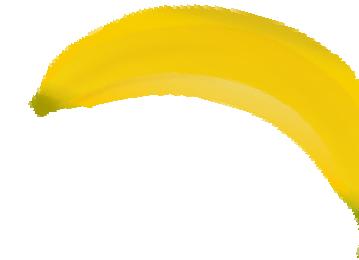
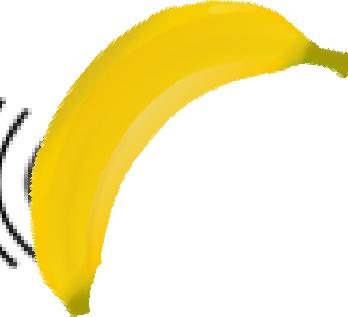
## Encryption in Special Protocols

- ◆ Alarms and errors
  - ◆ Signalled within status byte
  - ◆ Header is not subject to encryption
- ◆ Application resets (CI 50<sub>h</sub>)
  - ◆ Special upper layer protocol
  - ◆ Security services of the DAL and ELL do not apply
- ◆ Clock updates
  - ◆ Special upper layer protocol
  - ◆ Set, add and subtracts (TC field)

CI	Long Data Header	Check Bytes	TC	Payload	Cmd Verify
1 byte	12 bytes	2F 2Fh	1 byte	9 byte	2F 2F 2F 2Fh



# Issues with message integrity?



Compass Security AG  
Werkstrasse 20  
P.O. Box 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
[team@csnc.ch](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)

## General

- ❖ There are two mention on how one could approach authentication. However there are neither authentication methods nor protocols specified

## DAL Integrity Protection

- ❖ CRCs
  - ❖ There are CRCs at the frame level
  - ❖ CRCs are not considered integrity protection
- ❖ Signatures
  - ❖ Encryption mode 5 and 6 can signal digitally signed billing data
  - ❖ Not widely used => due to meter display has priority
- ❖ MACs
  - ❖ Not available

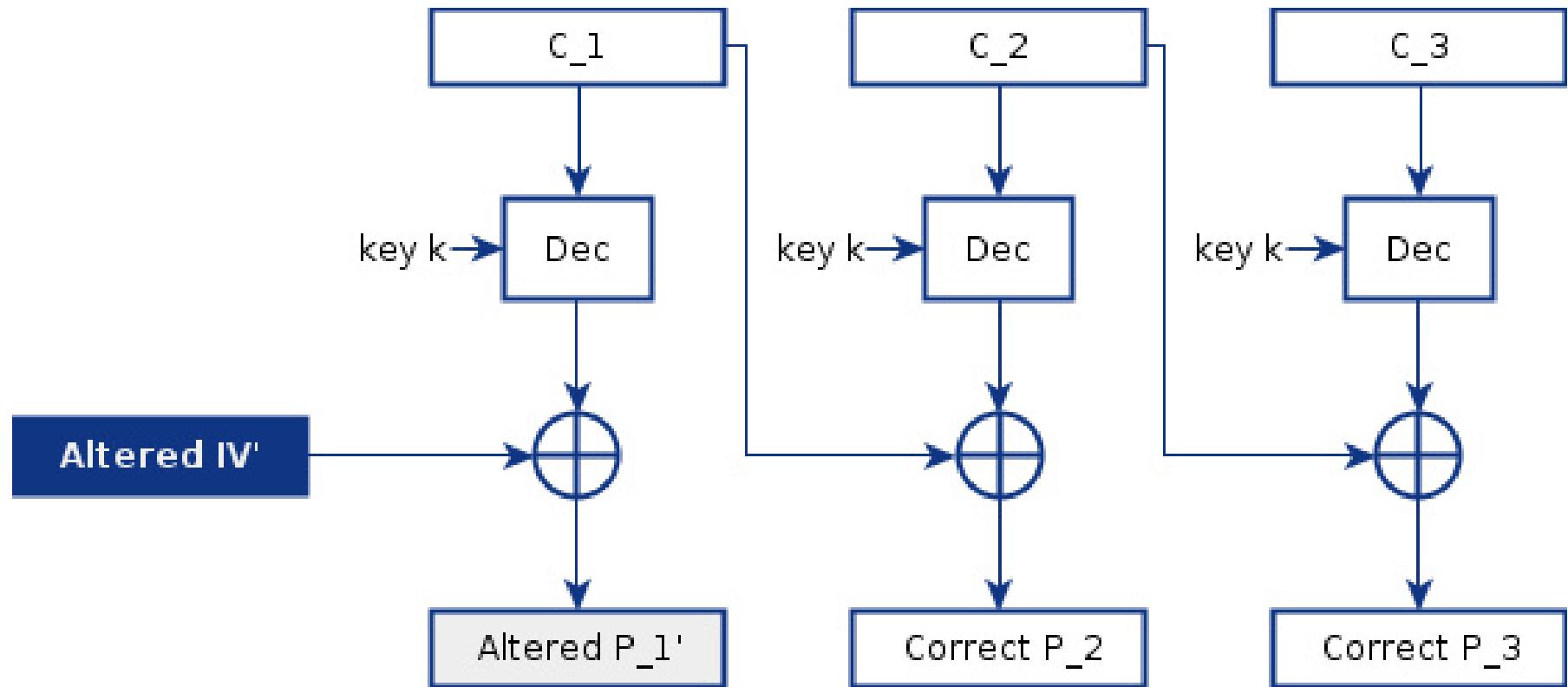
## Manipulation of Ciphertexts or IVs

- ❖ In CBC mode, the manipulation of ciphertexts is pointless
- ❖ Manipulation of the IV is difficult but feasible

# IV Manipulation in CBC



## CBC Mode of Decryption



## Feasibility of IV manipulation

	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16
<b>IV</b>	Manuf. ID	Device Address					Vers.	Type	ACC	ACC	ACC	ACC	ACC	ACC	ACC	ACC
<b>P1</b>	Leading 2F	DIF	VIF	VIFE	Consumption	Value							Trailing 2F			

## Issues

- ❖ Manipulation of manufacturer or address => key not found
- ❖ Manipulation of version, type => key not found (receiver specific)
- ❖ Manipulation of ACC => destroys trailing 2F (receiver specific)
- ❖ What if devices share the same key?

# IV Manipulation Example



## Example of Consumption Value Manipulation

$$P_1' = \text{Dec}_k(C_1) \oplus IV' \Rightarrow \text{Dec}_k(C_1) = P_1' \oplus IV' = P_1 \oplus IV$$

$$P_1' = P_1 \oplus IV \oplus IV'$$

## Precondition

- Original value read from meter display 341 kWh (08 34 05 00 )

## Calculate Plaintext $P_1'$

$P_1$	2F	2F	04	83	3B	<b>08</b>	<b>34</b>	<b>05</b>	<b>00</b>	2F						
IV	2D	2C	07	71	94	15	01	02	B3	B3	B3	B3	B3	B3	B3	B3
$IV'$	2D	2C	07	71	94	15	01	<b>05</b>	B3	B3	B3	B3	B3	B3	B3	B3
$P_1'$	2F	2F	04	83	3B	<b>08</b>	<b>34</b>	<b>02</b>	<b>00</b>	2F						

## Result

- $P_1' 144'392 \text{ Wh (08 34 02 00)}$

## Partial Encryption

- ◆ Dedicated Application Layer allows for partial encryption
- ◆ How does the receiver handle doubled data records?

## Expansion Attack Example

Value in CT: 04 83 3B 08 34 **05** 00 (341'000 Wh)

**1E** 44 2D 2C 07 71 94 15 01 02 7A B3 00 10 85 **BF**  
**5C** **93** **72** **04** **76** **59** **50** **24** **16** **93** **27** **D3** **03** **58** **C8**

Value attached: 04 83 3B 08 34 **02** 00 (144'392 Wh)

**25** 44 2D 2C 07 71 94 15 01 02 7A B3 00 10 85 **BF**  
**5C** **93** **72** **04** **76** **59** **50** **24** **16** **93** **27** **D3** **03** **58** **C8** **04**  
**83** **3B** **08** **34** **05** **00**

## ELL Integrity Protection

- ◆ CRC at the frame level
- ◆ Another CRC at the ELL level (subject to encryption)
- ◆ No MACs, no signatures

## ELL CRC calculation

Frame Header	ELL Header	Encrypted Data				
		CRC	DIF	VIF	VIFE	CMD
		CC	22	01	FD	1F

## Data Link Layer: CRC calculation using reveng

```
cbrunsch@tortuga: ~/Documents/rhul/thesis/software/reveng-1.1.0
$ ./reveng -h
CRC RevEng, an arbitrary-precision CRC calculator and algorithm finder
...
Copyright (C) 2010, 2011, 2012, 2013 Gregory Cook
This is free software; see the source for copying conditions. There
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PU
Version 1.1.0                                         <http://reveng.sourceforge.net>
$
$ ./reveng -D | grep 13757
width=16  poly=0x3d65  init=0x0000  refin=false  refout=false  xorout=
=0xc2b7  name="CRC-16/EN-13757"
$
$ ./reveng -m CRC-16/EN-13757 -c 01FD1F01
cc22
$ ./reveng -m CRC-16/EN-13757 -c 01FD1F00
f147
$ 
```

## ELL Manipulation Example

$P_a = CC\ 22\ 01\ FD\ 1F\ 01$  (On Command)

$P_b = F1\ 47\ 01\ FD\ 1F\ 00$  (Off Command)

$C_a = E7\ 8E\ 1B\ 7B\ 9D\ 86$  (Intercepted Ciphertext)

$C_b = C_a \square P_a \square P_b$

$C_b = E7\ 8E\ 1B\ 7B\ 9D\ 86\ \square$

$CC\ 22\ 01\ FD\ 1F\ 01\ \square$

$F1\ 47\ 01\ FD\ 1F\ 00$

$C_b = DA\ EB\ 1B\ 7B\ 9D\ 87$  (**Manipulated Ciphertext**)

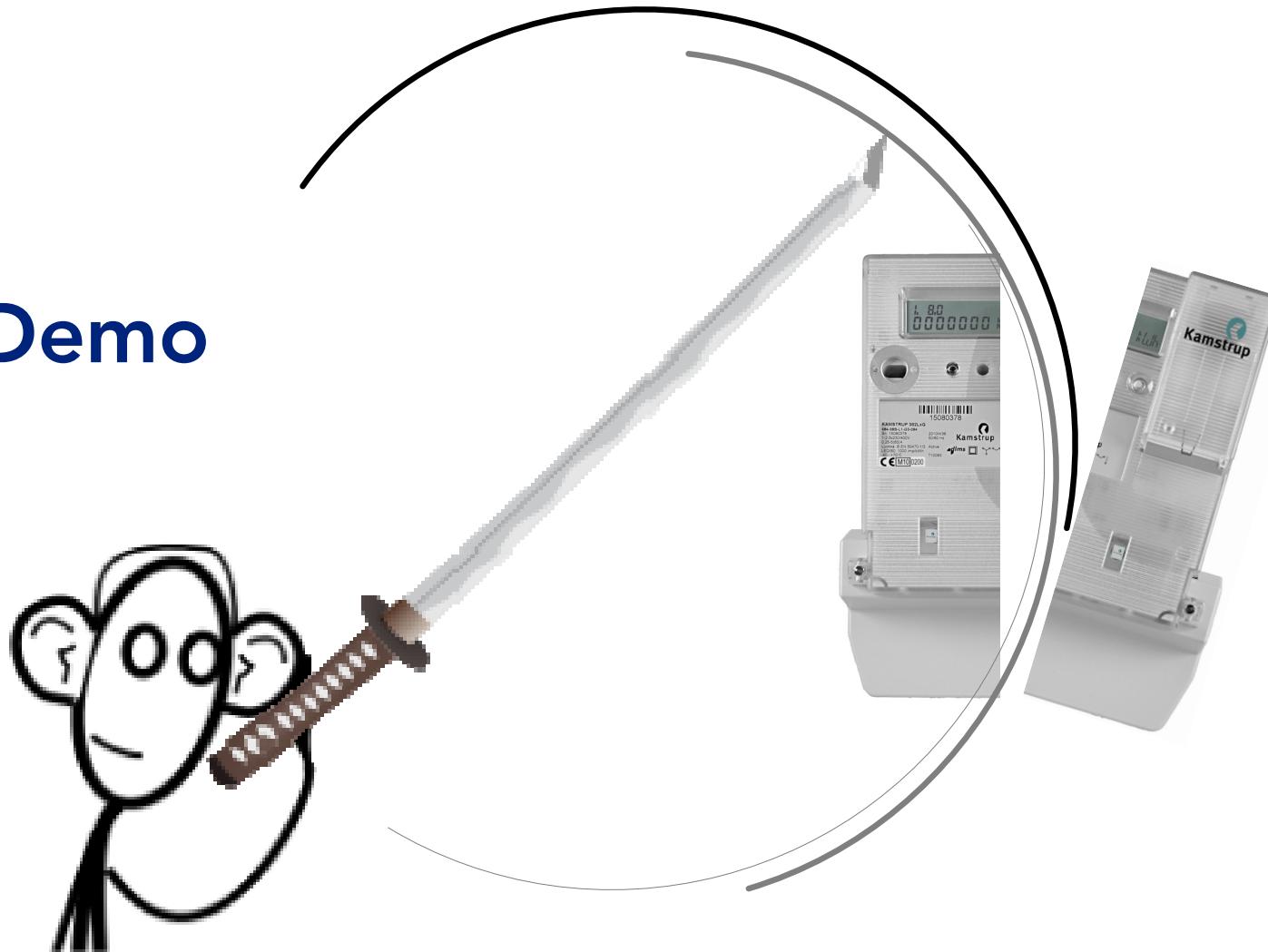
# Which messages are affected?



## Integrity with Special Protocols

- ❖ No integrity protection at all
  - ❖ Alarms and errors
  - ❖ Application resets
  - ❖ Clock synchronization
  - ❖ Commands
  - ❖ Network management
  - ❖ Precision timing

# Demo



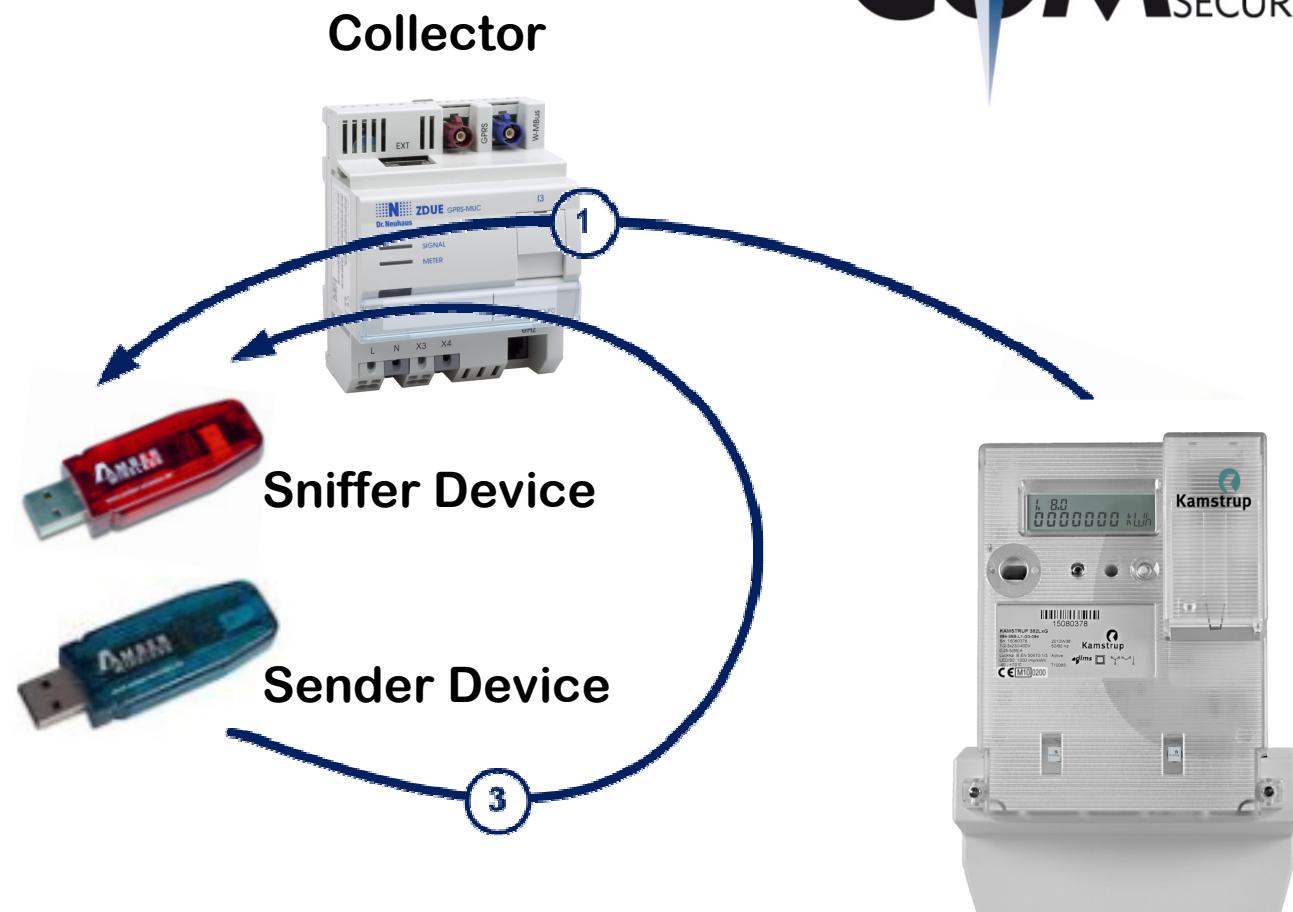
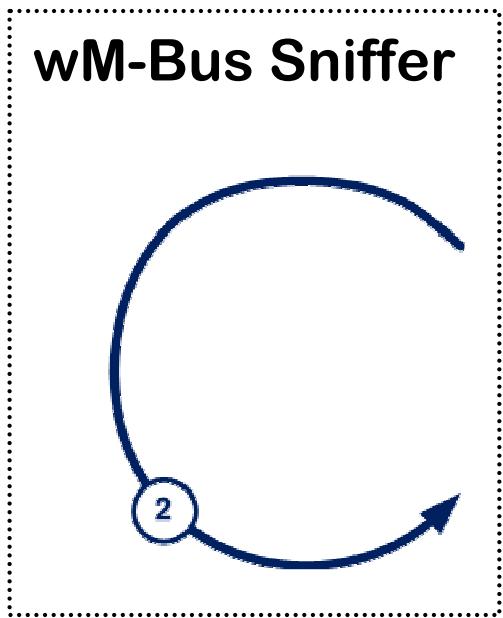
Compass Security AG  
Werkstrasse 20  
P.O. Box 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
[team@csnc.ch](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)

# Energy Fraud Demo



## Setup



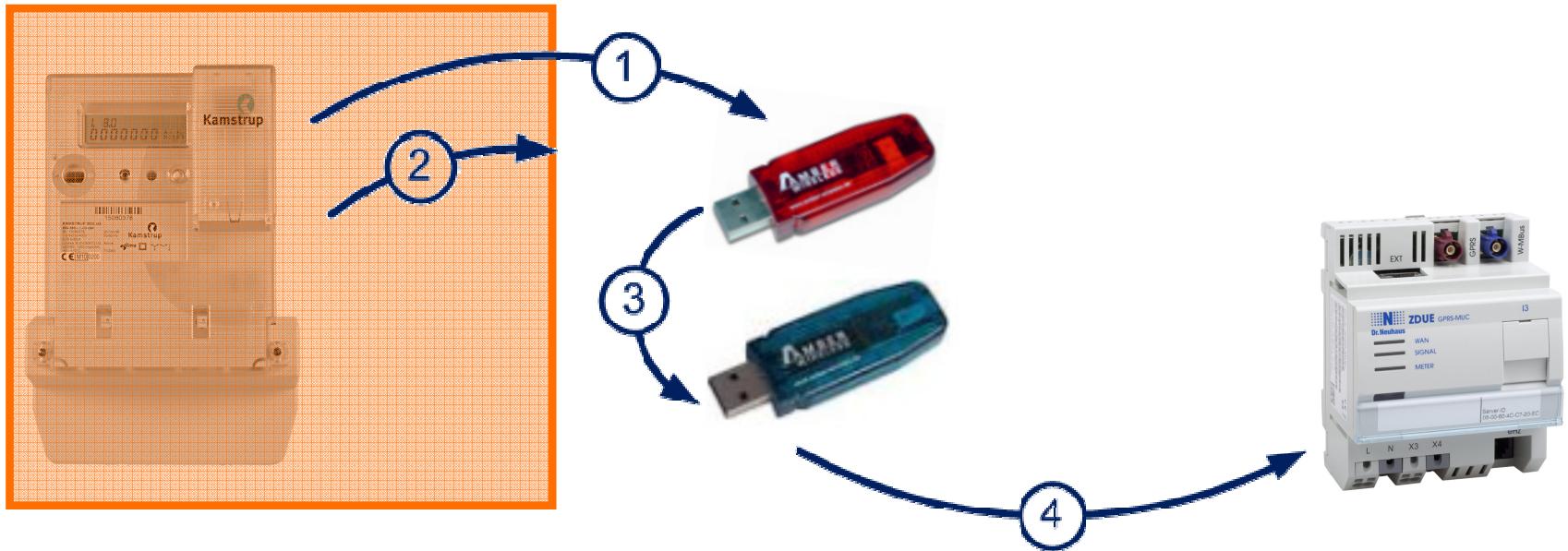
## Hardware

- ◆ Amber Sticks <http://amber-wireless.de/406-1-AMB8465-M.html>
- ◆ TI Transceiver <http://www.ti.com/lit/ds/symlink/cc1101.pdf>
- ◆ TI App Note <http://www.ti.com/lit/an/swra234a/swra234a.pdf>

# Issues with Packet Replay



## Shield and Replay I

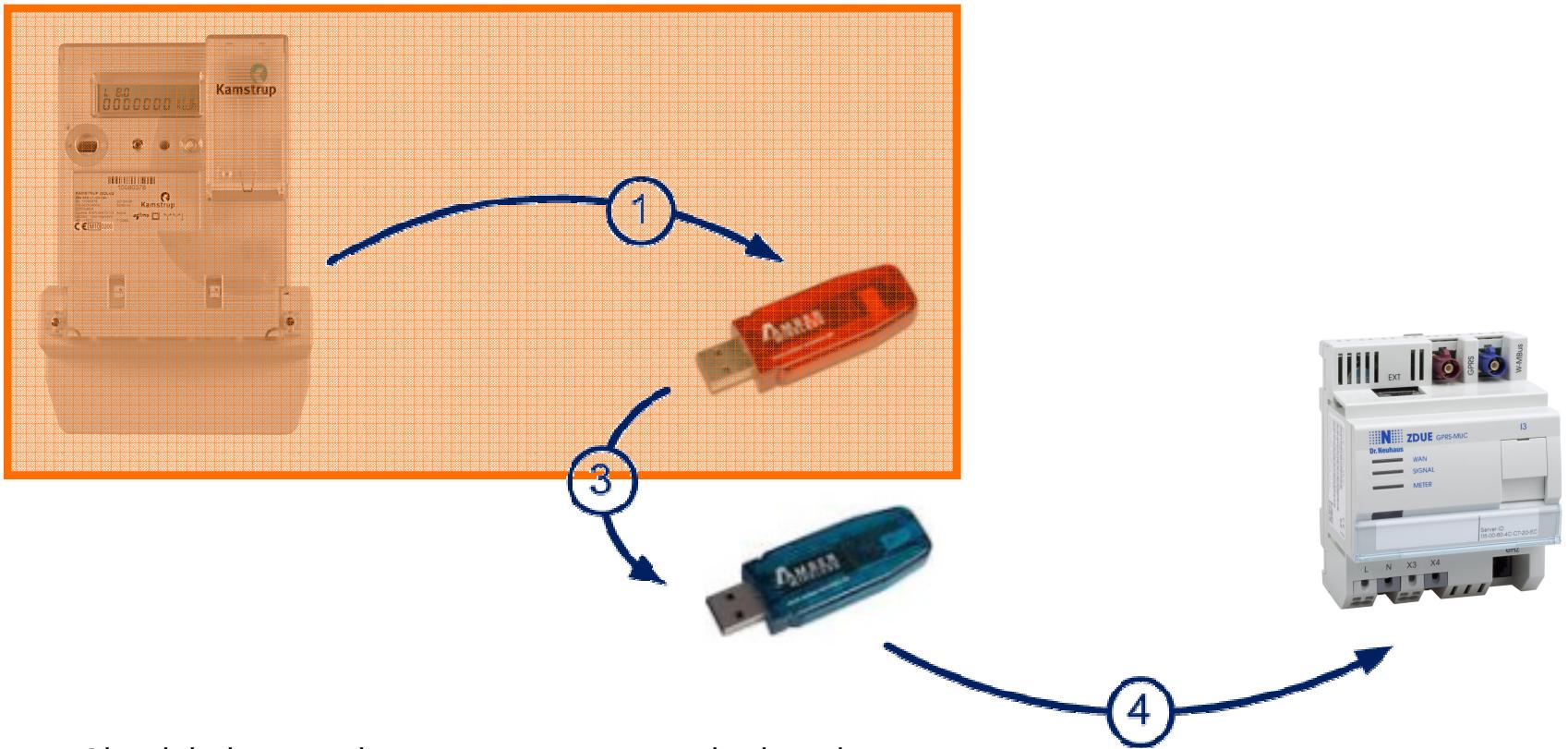


- ❖ Capture messages from original device
- ❖ Shield device and replay messages

# Issues with Packet Replay



## Shield and Replay II



- ◆ Shield device, have a receiver with the device
- ◆ Submit messages to collector at maybe lower pace

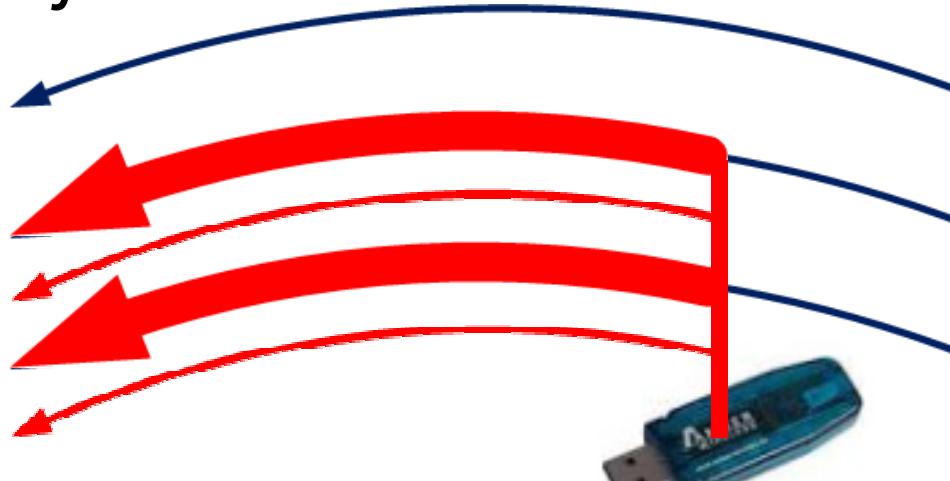
# Issues with Packet Replay



## Jam and Replay



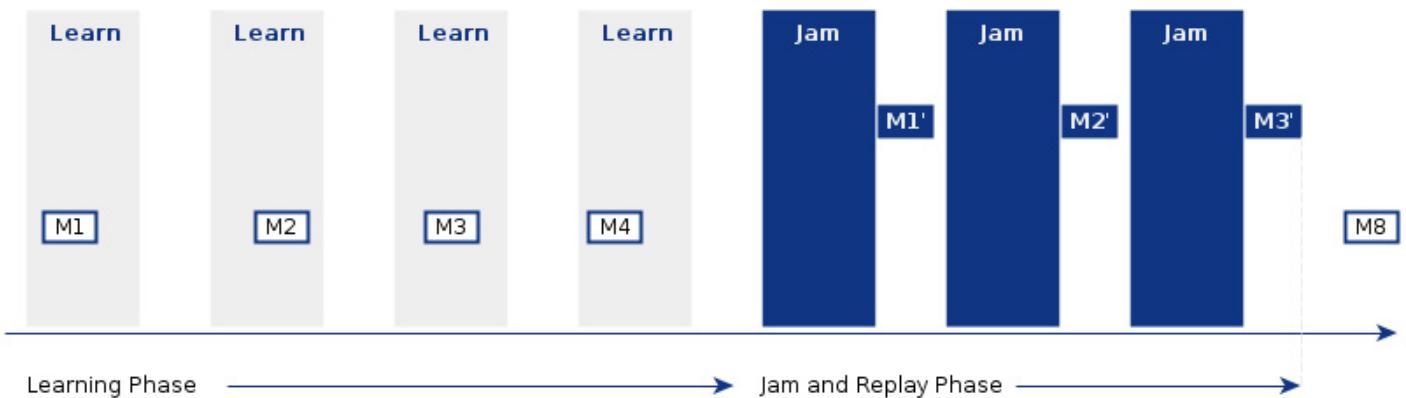
Collector



Sender Device



Meter

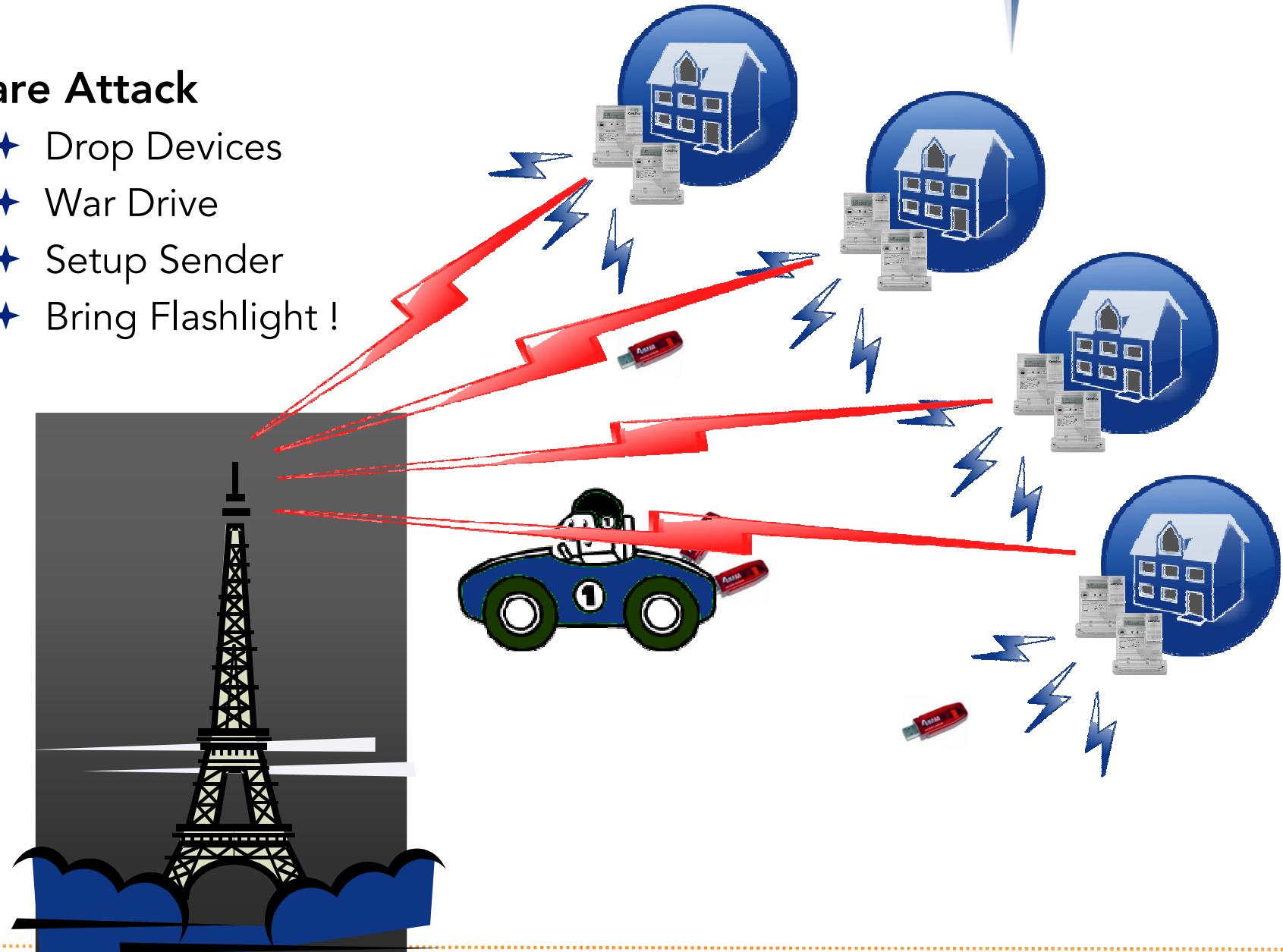


# Orchestrated Blackouts



## Prepare Attack

- ❖ Drop Devices
- ❖ War Drive
- ❖ Setup Sender
- ❖ Bring Flashlight !





# Conclusion

Compass Security AG  
Werkstrasse 20  
P.O. Box 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61  
[team@csnc.ch](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)

# Conclusion



Screenshot of the Allmess website (<http://www.allmess.de/index.php?id=157>) showing the TeleControl M-Bus system.

The page features a banner with the text "Take the Original" and the Allmess logo. The menu includes links for Kundenwelten, Service, Unternehmen, and Newsletter. The sidebar lists various products and systems, with "TeleControl M-Bus" highlighted in red.

**Fernauslese-Systeme  
TeleControl M-Bus**

Der M-BUS ist als kabelgebundenes Fernauslesesystem in der Europäischen Norm EN 1434-3 standardisiert.

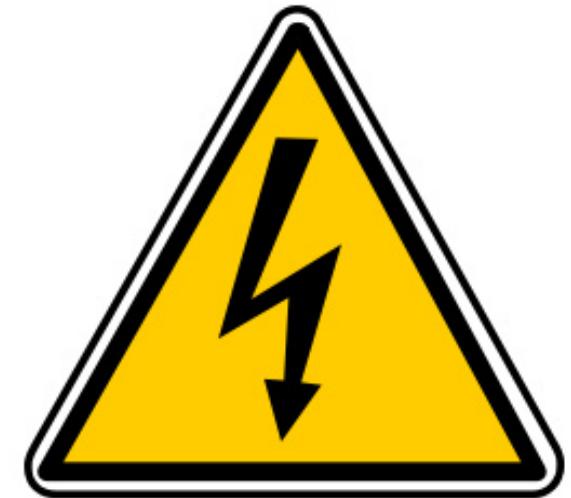
The diagram illustrates the M-Bus system architecture. It shows a cross-section of a house with various rooms and components. Numbered callouts point to specific parts:

- ①: Two analog meters on a wall panel.
- ②: An electrical control cabinet containing internal wiring and components.
- ③: A handheld remote device.
- ④: A small electronic module or sensor.
- ⑤: A central control unit, likely a computer terminal or a concentrator.

The diagram also depicts a network of lines connecting the different components, representing the M-Bus communication network.

## General Issues

- ❖ Key size 64 bits
- ❖ Zero consumption detection
- ❖ Disclosure of consumption values
- ❖ Plaintext errors and alarms
- ❖ Information Disclosure
- ❖ Man-in-the-middle in routed environments
- ❖ Key disclosure



## Energy Fraud

- ❖ Manipulation of consumption value

## Orchestrated Blackouts

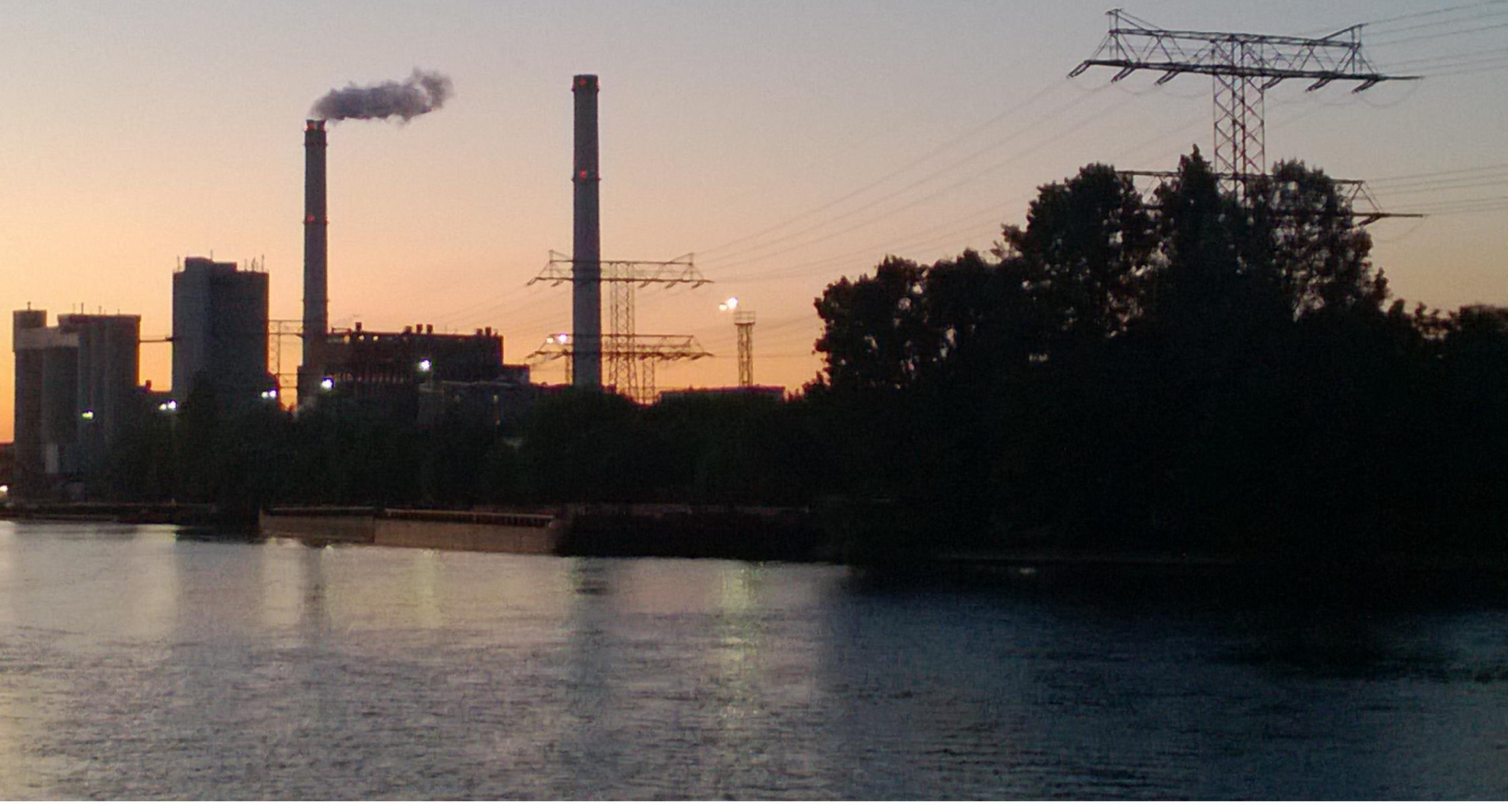
- ❖ Manipulation of valve and breaker open/close commands

## Counter Measures

- ❖ Efforts of the OMS Group and the German Federal Office for Information Security (BSI Germany)
  - ❖ Integrity-preserving authentication and fragmentation layer (AFL),
  - ❖ Additional encryption mode relying on AES-128 in CBC mode using ephemeral keys
  - ❖ TLS 1.2 support for wM-Bus
  - ❖ Published on X-Mas 2012
- ❖ Looks promising, no independent public analysis so far



# Battery pack empty.



**Presentation**

[http://www.csnc.ch/misc/files/2013/energy\\_fraud\\_and\\_blackouts.pdf](http://www.csnc.ch/misc/files/2013/energy_fraud_and_blackouts.pdf)

**Whitepaper**

[http://www.csnc.ch/misc/files/2013/wmbus\\_security\\_whitepaper.pdf](http://www.csnc.ch/misc/files/2013/wmbus_security_whitepaper.pdf)

**Sniffer & MUC (credits [lukas@statuscode.ch](mailto:lukas@statuscode.ch))**

<https://github.com/CBrunsch/WMBus-Sniffer-MUC>

**Python Sniffer**

<https://github.com/CBrunsch/scambus>

**GNU Radio wM-Bus (credits [neundorf@kde.org](mailto:neundorf@kde.org))**

<https://github.com/oWCTejLVIxFyNztcBnOoh/gr-wmbus>

**Cliparts**

<http://openclipart.org>