Hacking Smart Meters: Attack Vectors on the Communication Infrastructure of Energy Suppliers

Dipl.-Ing. Hubert Schölnast, BSc
St. Pölten University of Applied Sciences

Science for Peace and Security (2024)
Energy infrastructure resilience in response to war and other hazards
Advanced Research Workshop (ARW) supported by NATO

POLAND, Rzeszów, 23.09.2024

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

Agenda

- What you need to know when you want to hack smart meters
- The “Kreisläufer” incident: What can go wrong in smart meter communication
- What you can see in a fully encrypted network

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

What you need to know to hack smart meters

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

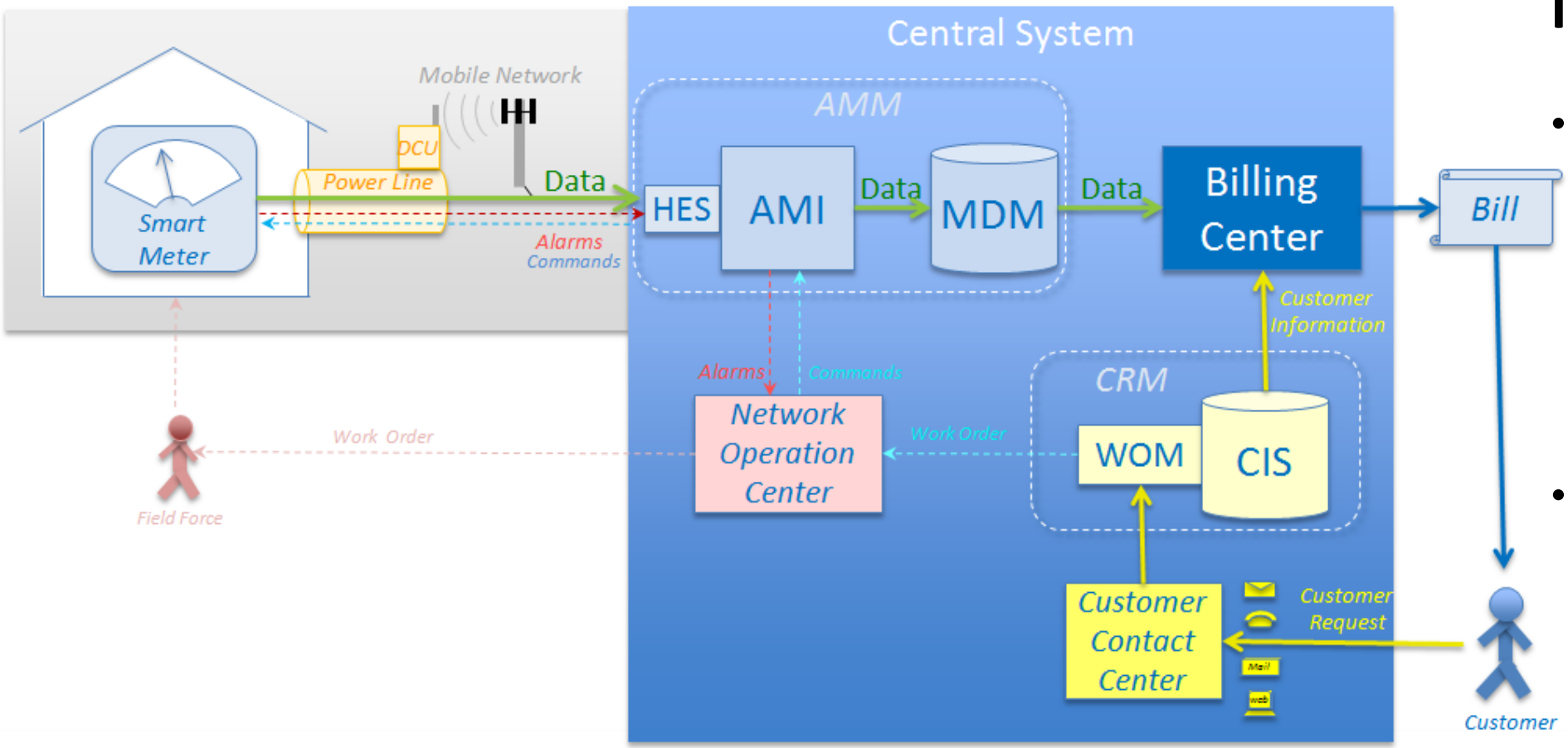
What is a Smart Meter?

- A smart meter is a device that measures the energy flowing through it to a consumer.
- A smart meter always includes a communications unit that allows the device to transmit data to the utility's control center and, in some cases, to communicate with other devices on the same communications network.
- Many smart meters also have a (a circuit breaker) controlled by the energy supplier that can be used to connect or disconnect the consumer from the utility's grid.

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

Outdoor infrastructure
(communication network)

Indoor infrastructure
(central system)



Smart Metering Infrastructure

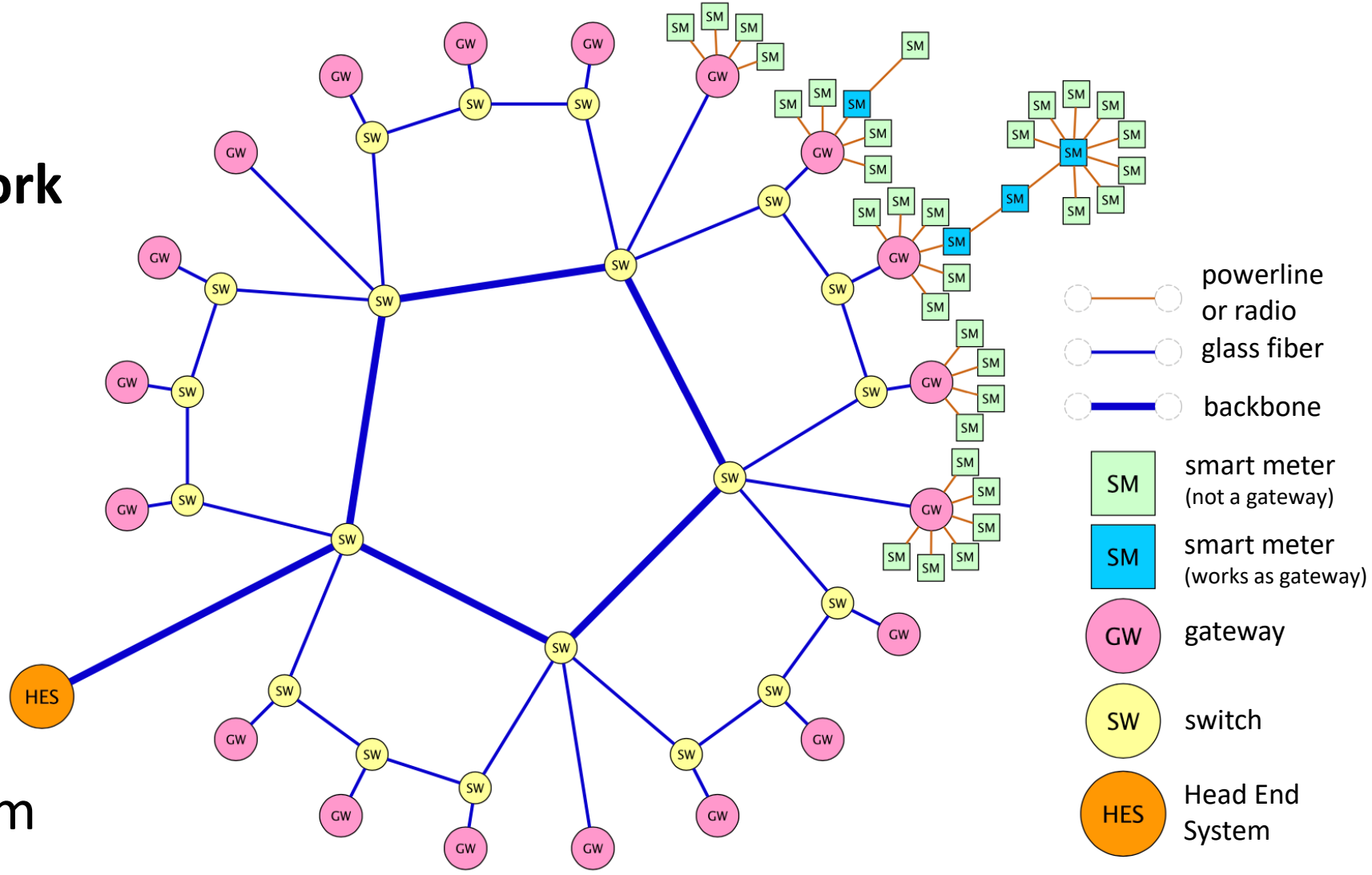
- **A**dvanced **M**eter **M**anagement
  - **H**ead **E**nd **S**ystem
  - **A**dvanced **M**etering **I**nfrastructure
  - **M**eter **D**ata **M**anagement
- **C**ustom **R**elationship **M**anagement
  - **W**ork **O**rder **M**anagement
  - **C**ustomer **I**nformation **S**ystem

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

Topography of a communication network

Example city: Wels in Austria

- About 55.000 smart meters
- About 400 gateways
- Some switches (unknown amount)
- One Head End System

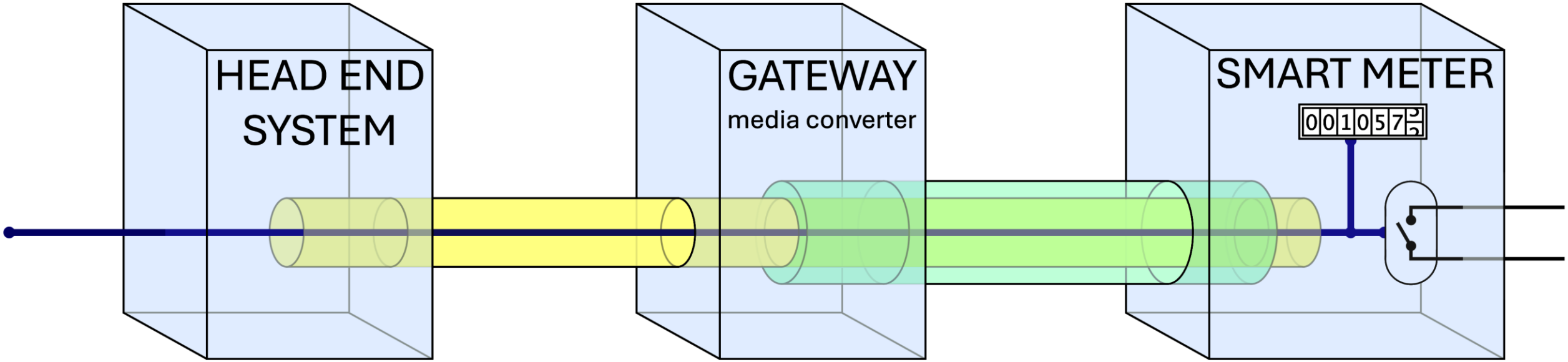


NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

central system

glass fiber,
ethernet, etc.

powerline



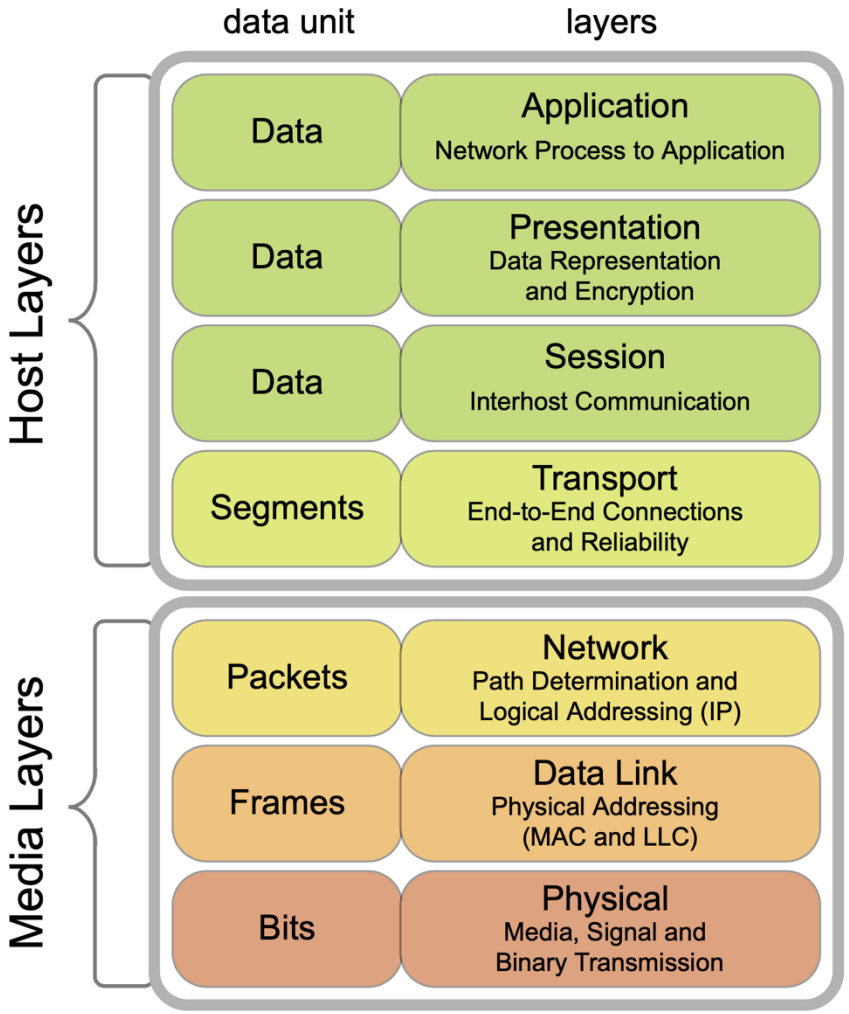
cleartext

end-to-end
encryption

additional
protocol encryption
(G3-PLC)

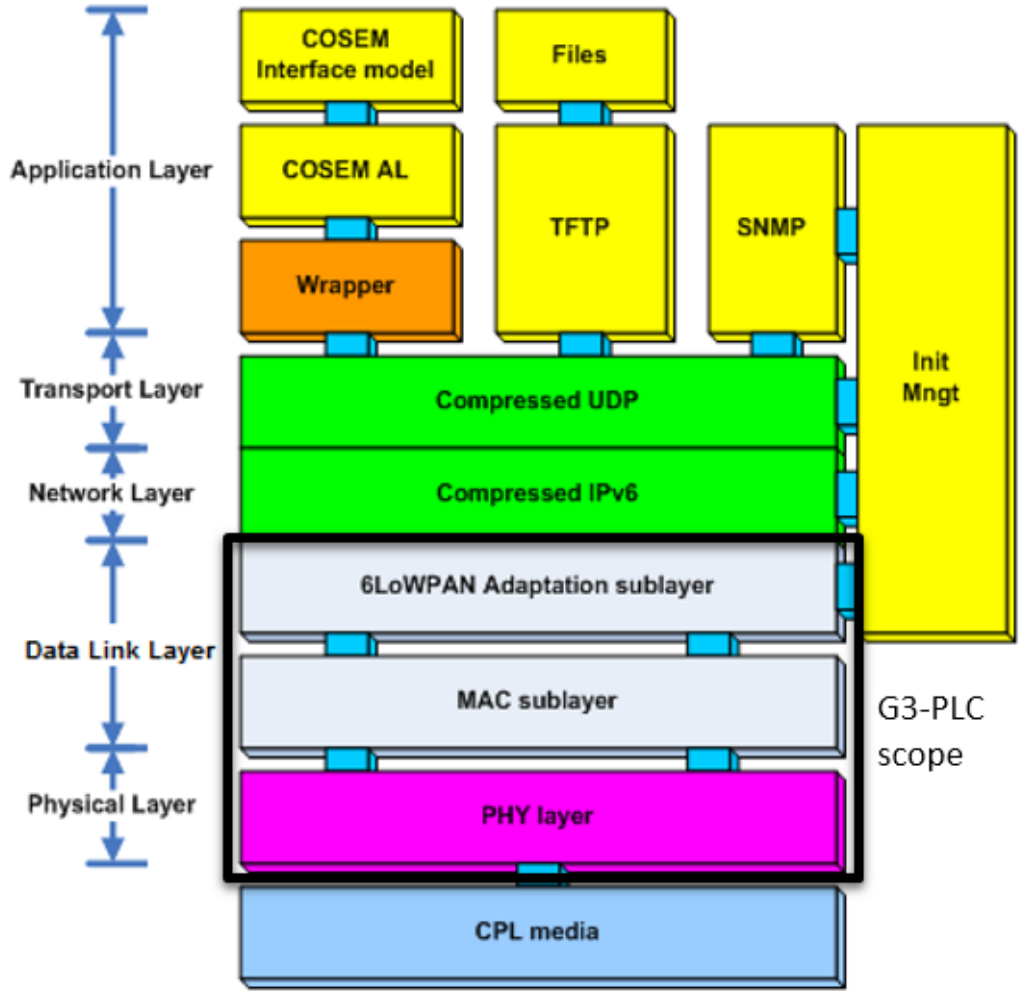
cleartext

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme



Communication protocols

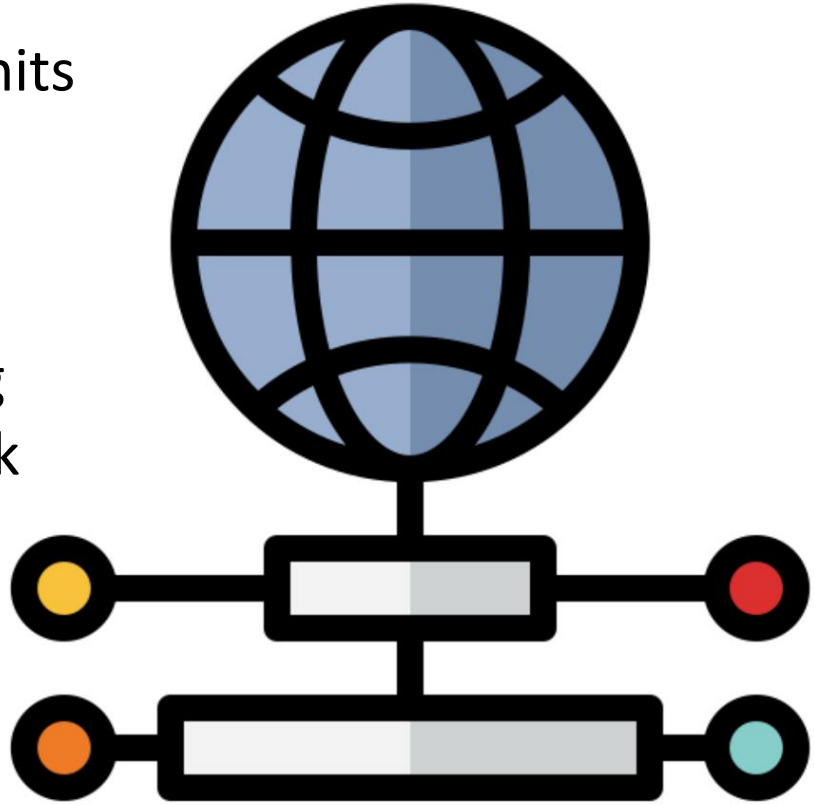
- Left: TCP/IP stack for glass fiber
- Right: G3-PLC for powerline



NATO OTAN
This workshop is supported by:
The NATO Science for Peace and Security Programme

Protocols in the Application Layer

- **DLMS** = Device Language Message Specification
  - Concept for abstract modeling of communication units
  - Identification of devices
  - Data transfer
  - Designed to cooperate with COSEM and OBIS
- **COSEM** = COmpanian Specification for Energy Metering
  - Set of rules for data transfer in smart meter network
  - Interface model for the communication
- **OBIS** = OBject Identification System
  - Hierarchical codes to identify objects
  - Standard IEC 62056-61



NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

The “Kreisläufer” incident

German “Kreisläufer” = English ”circle runner”

Affected: South of Germany and whole Austria (Home of 33 million people)
Duration: May 2, 2013 to May 7, 2013 (5 days)

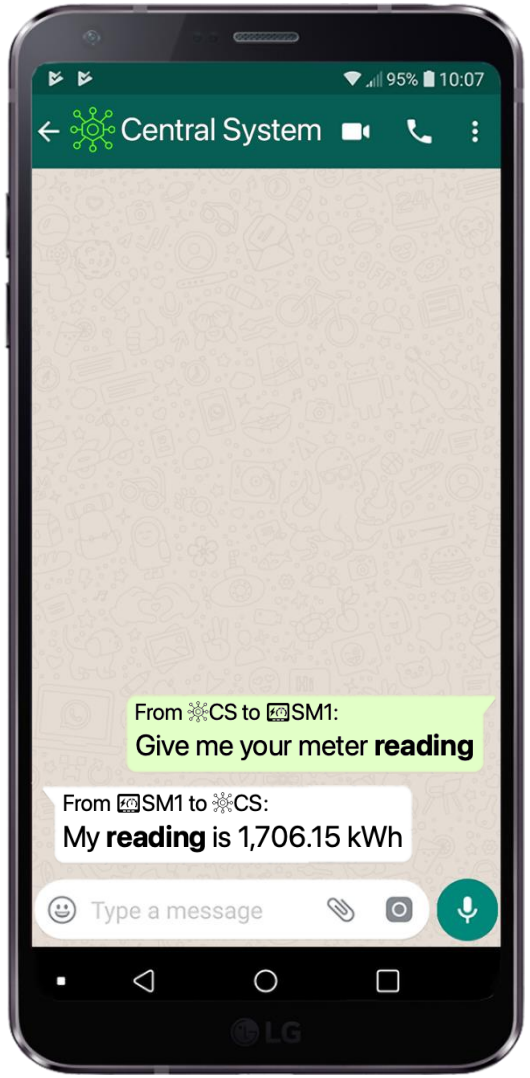
NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

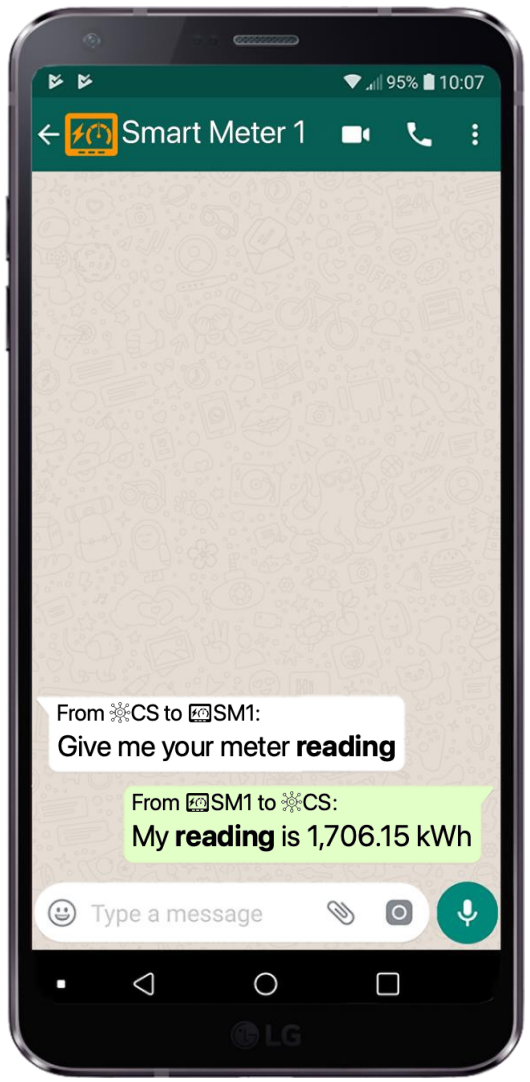
Usual meter reading query

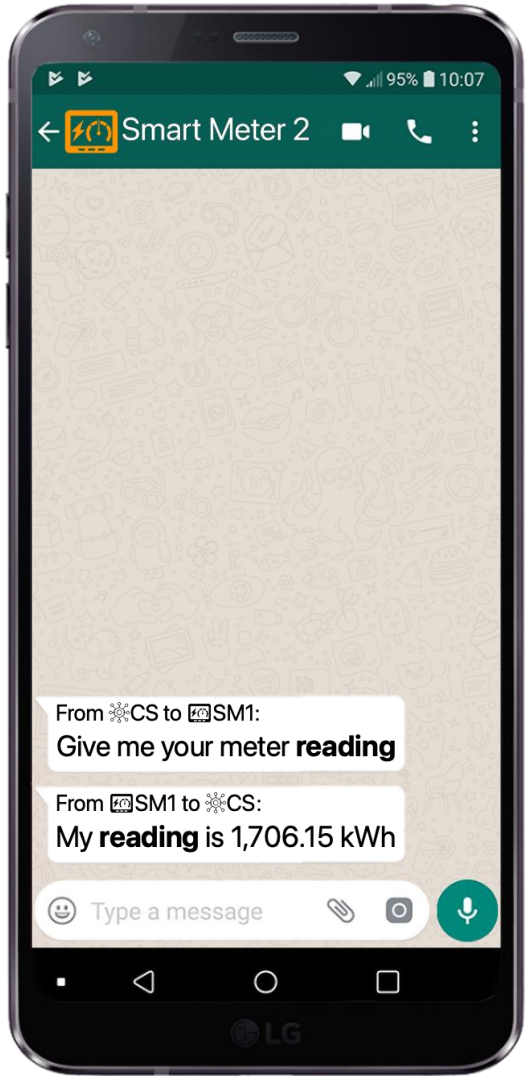
NATO OTAN
This workshop is supported by:
The NATO Science for Peace and Security Programme

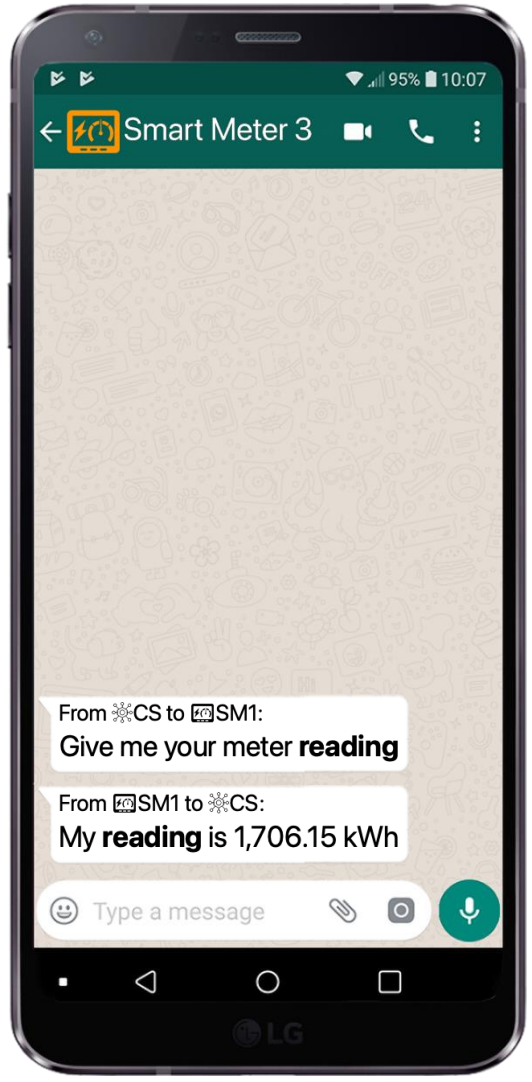
Usual meter reading query

End of communi-cation





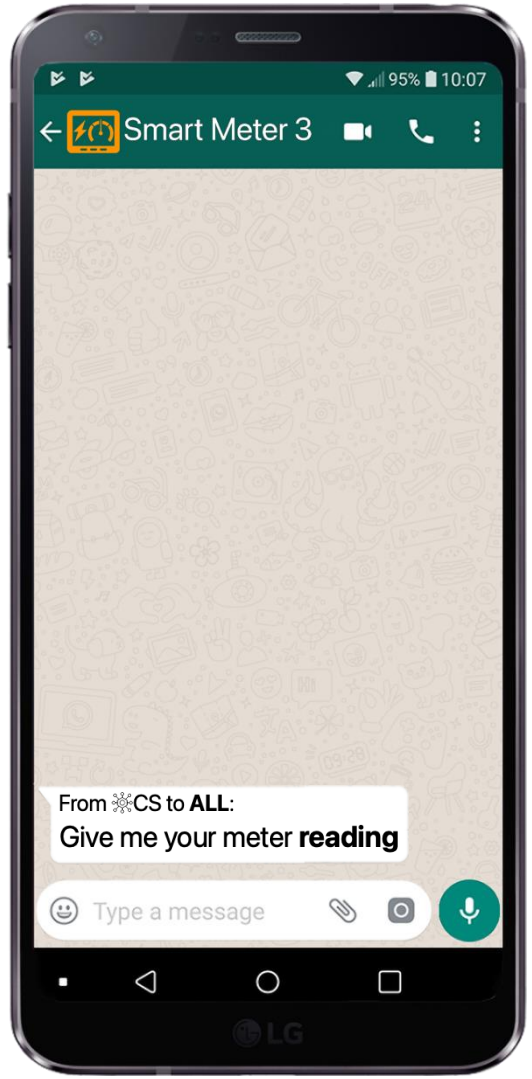




NATO OTAN
This workshop is supported by:
The NATO Science for Peace and Security Programme

Broadcast meter reading query

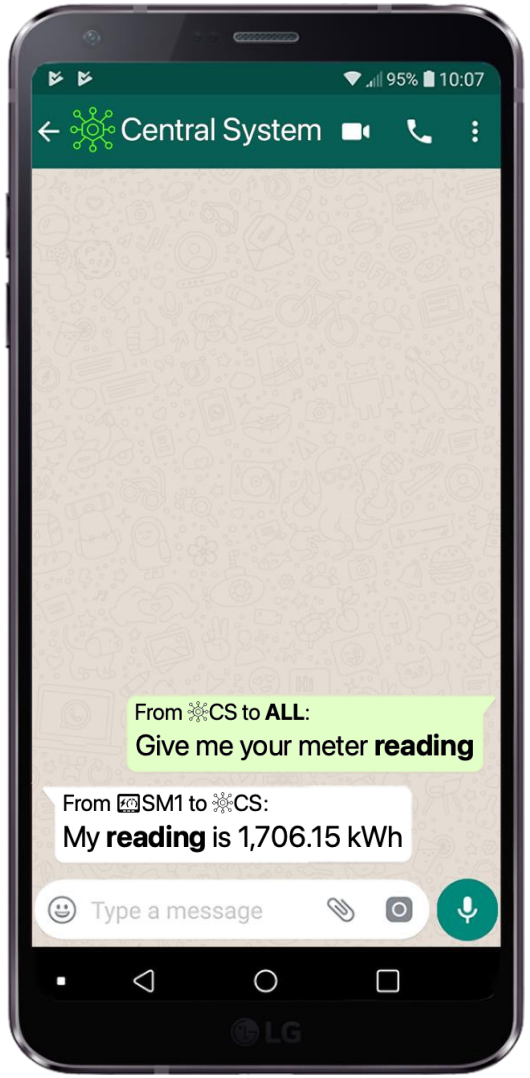
On a normal day

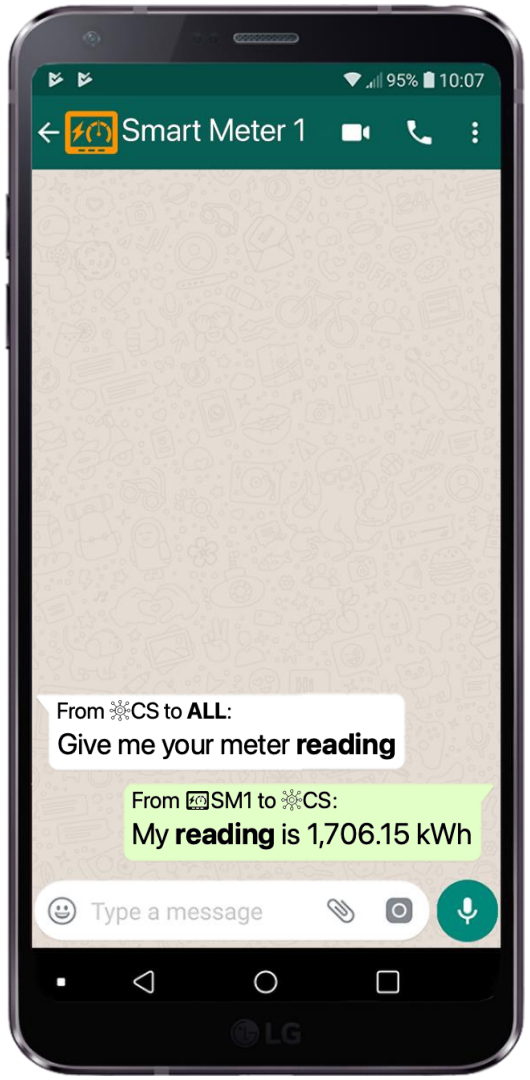


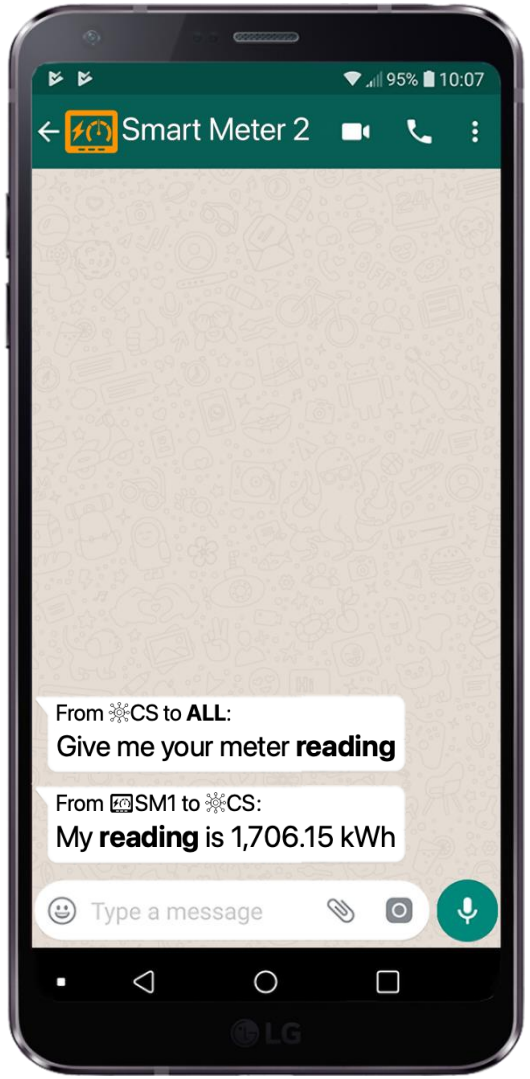
NATO OTAN
This workshop is supported by:
The NATO Science for Peace and Security Programme

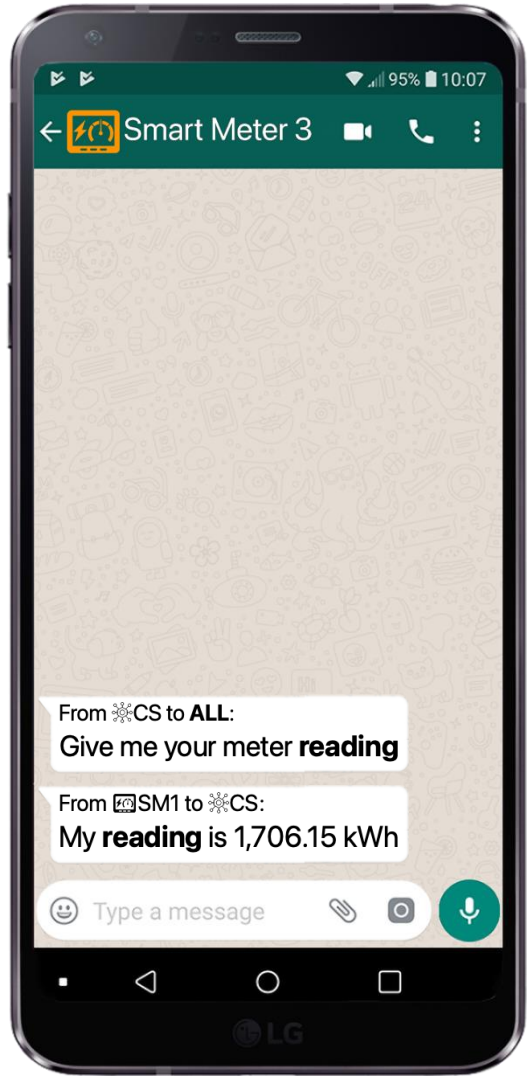
Broadcast meter reading query

On a normal day





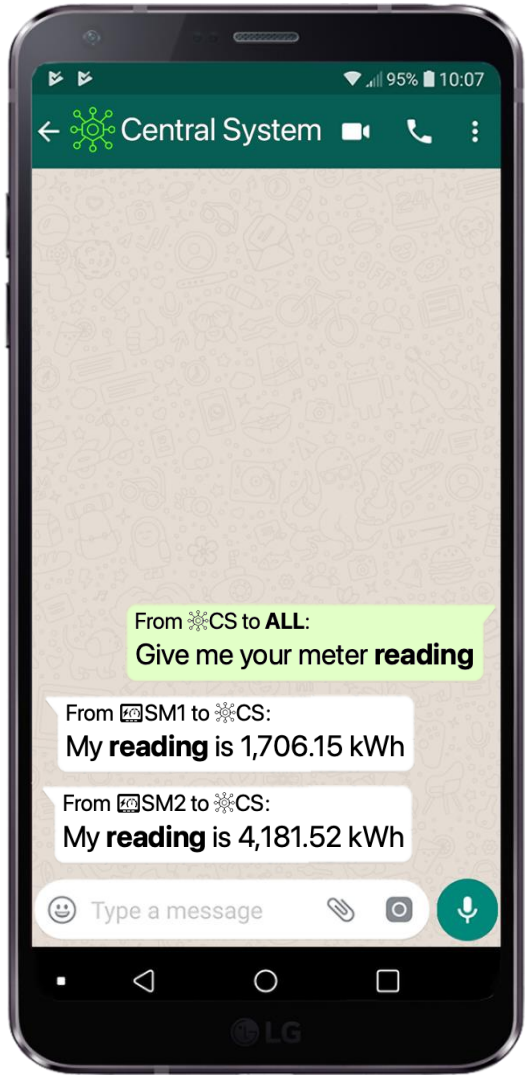


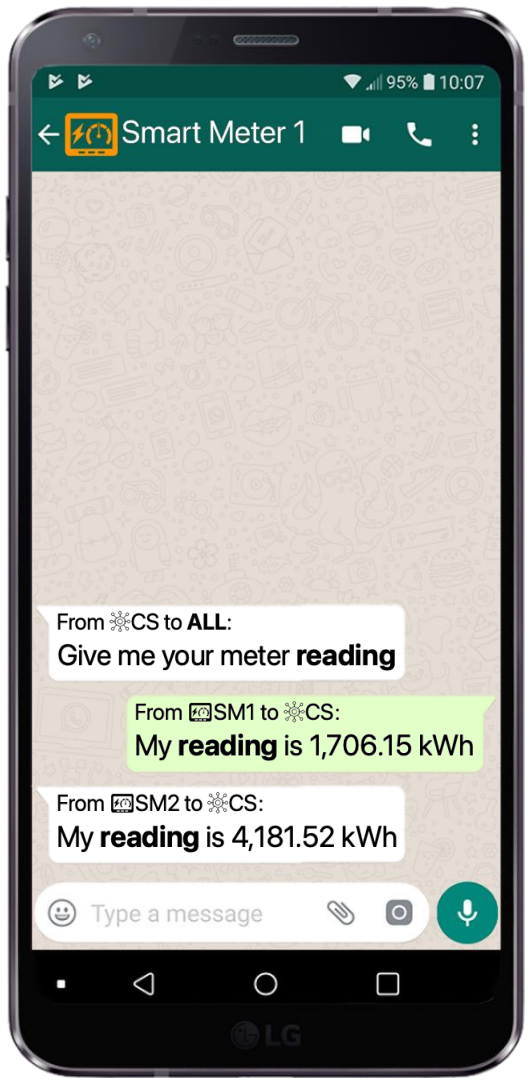


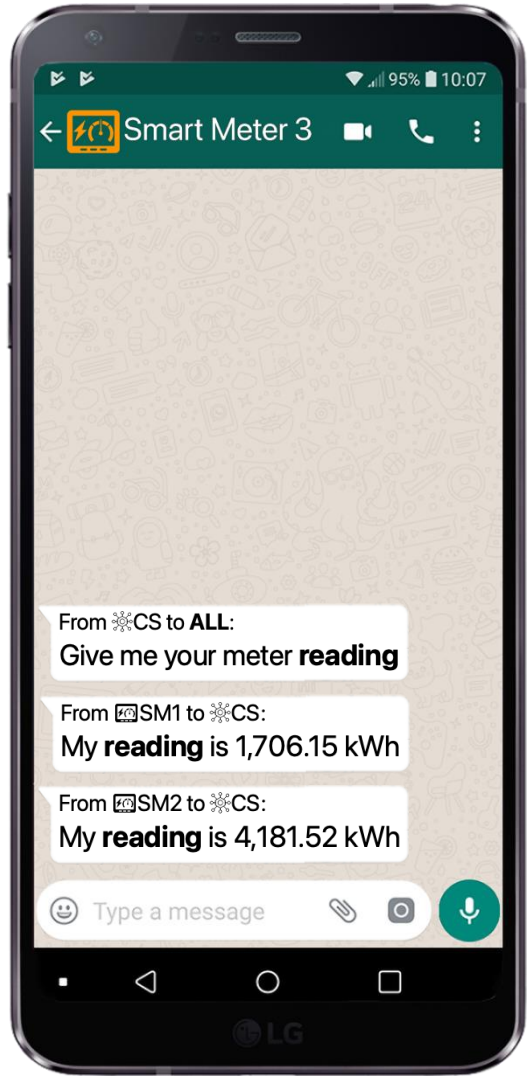
NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

Broadcast meter reading query

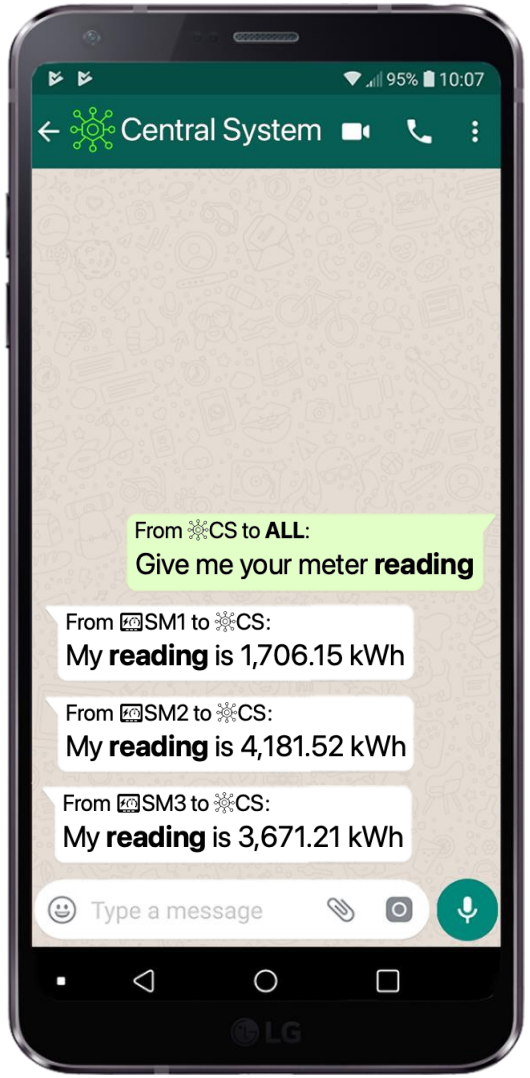
On a normal day







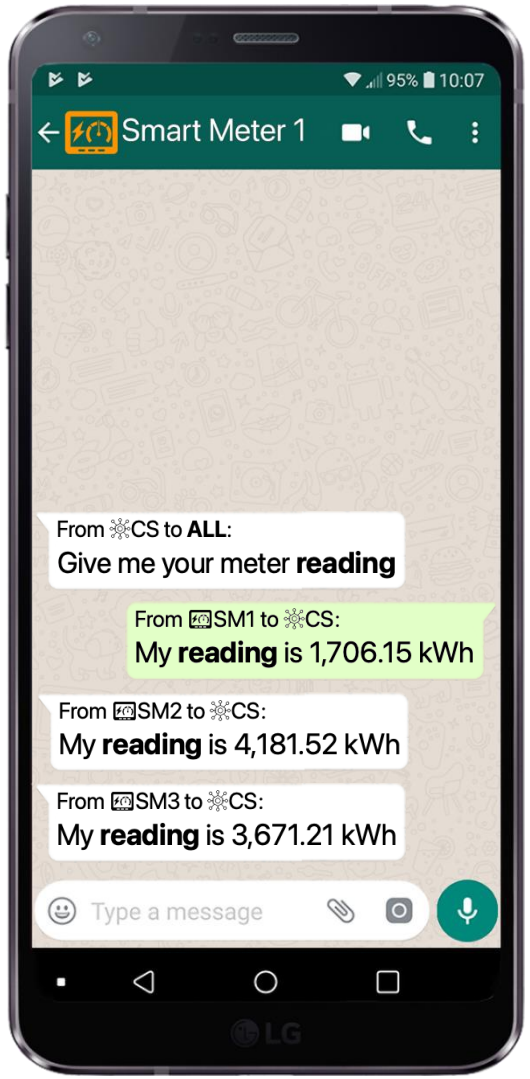
NATO OTAN
This workshop is supported by:
The NATO Science for Peace and Security Programme

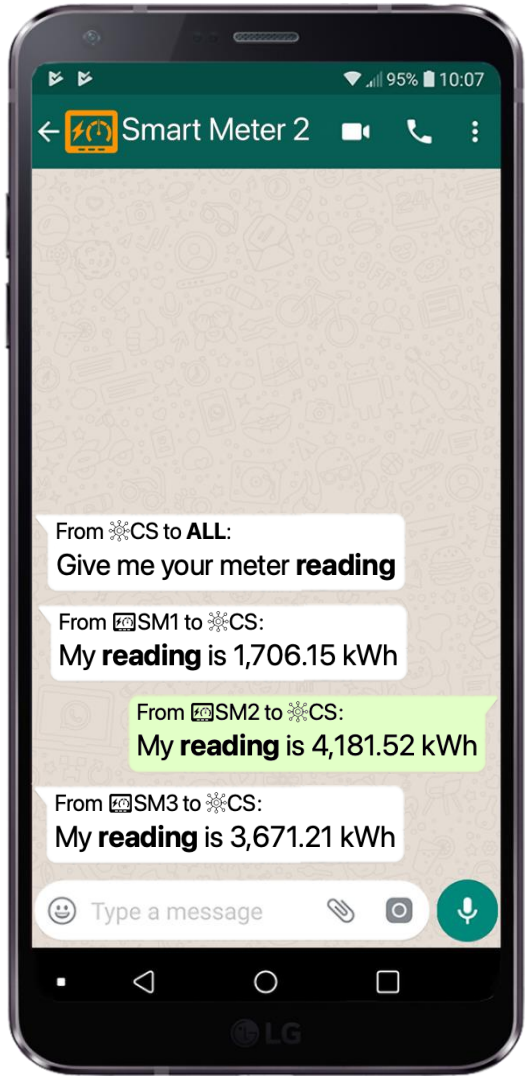


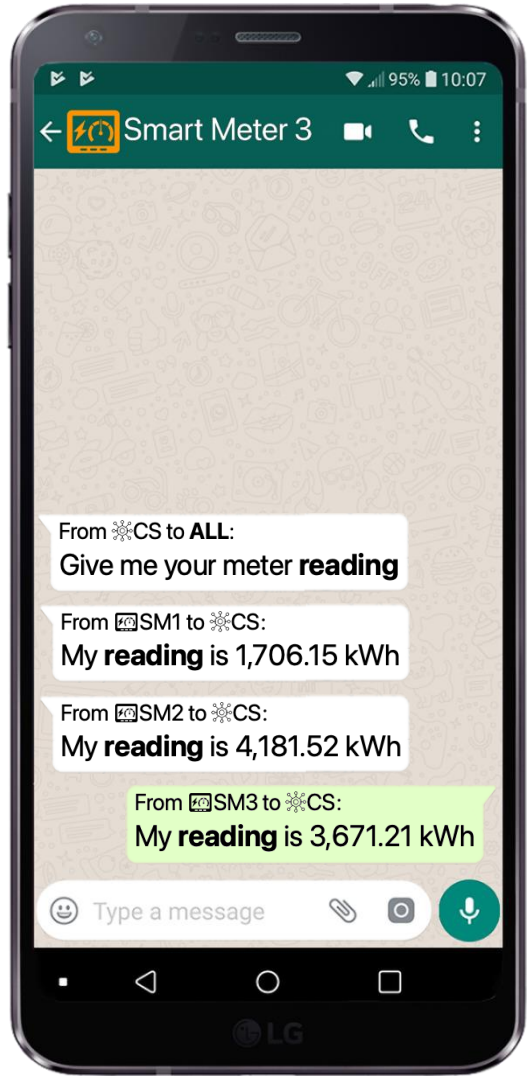
Broadcast meter reading query

On a normal day

End of communi-cation

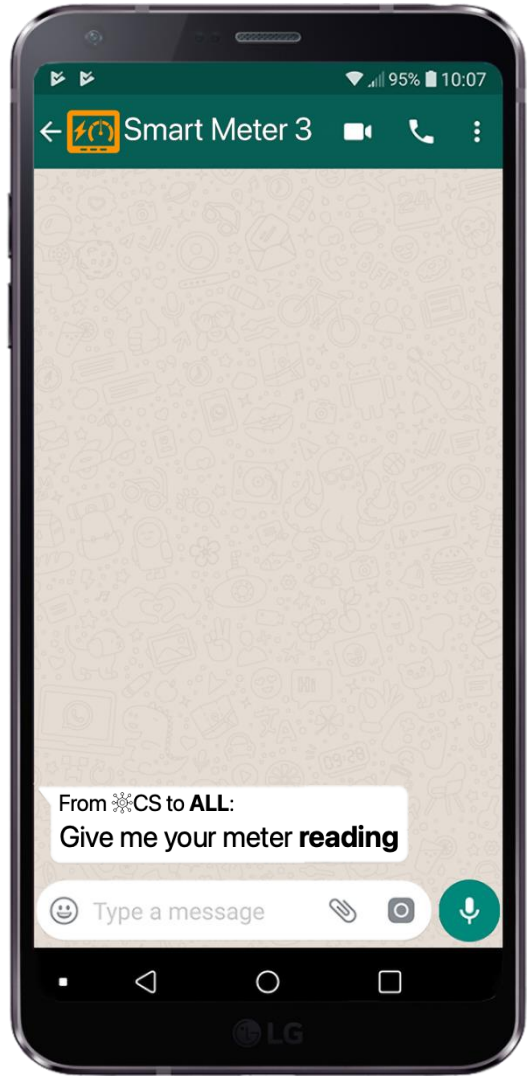






Broadcast meter reading query

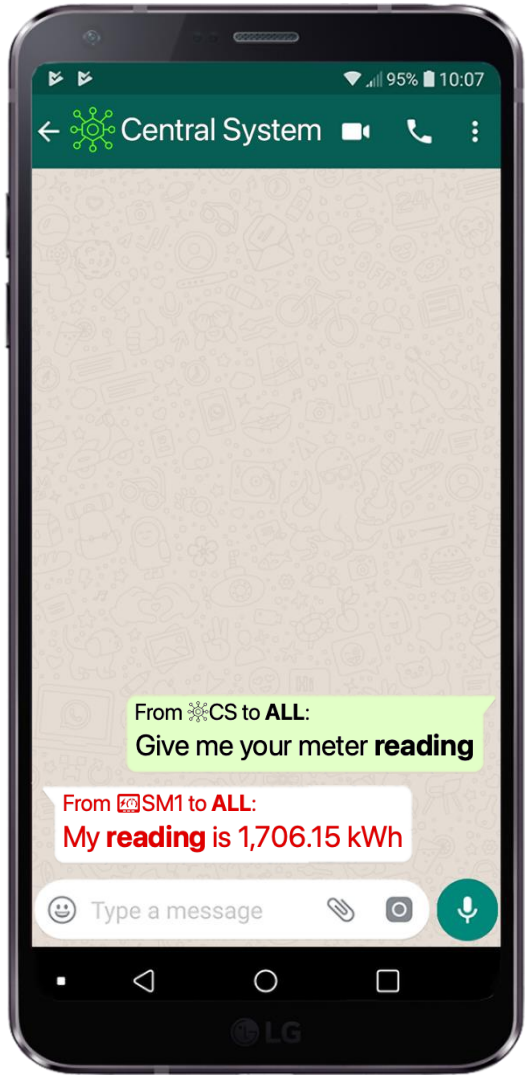
When it did go wrong

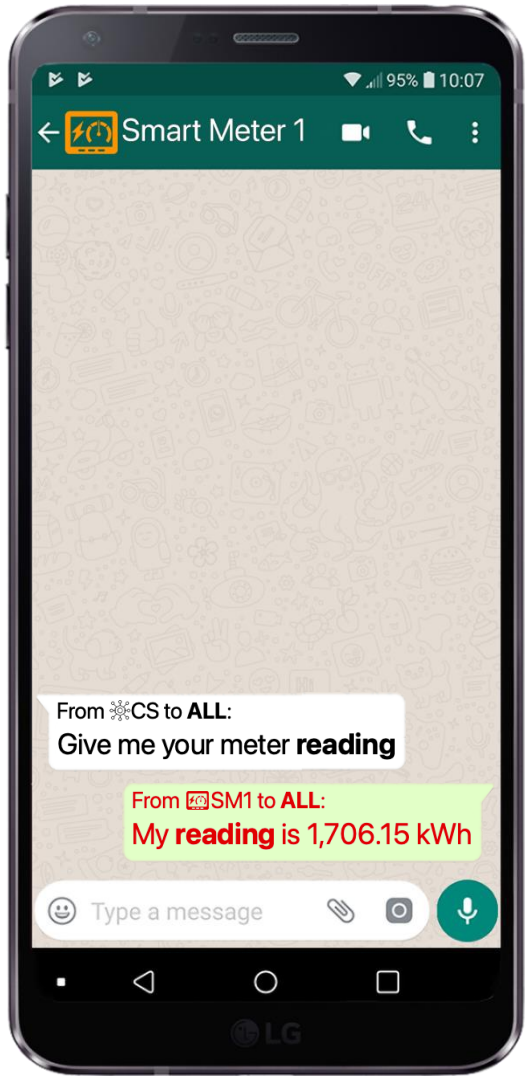


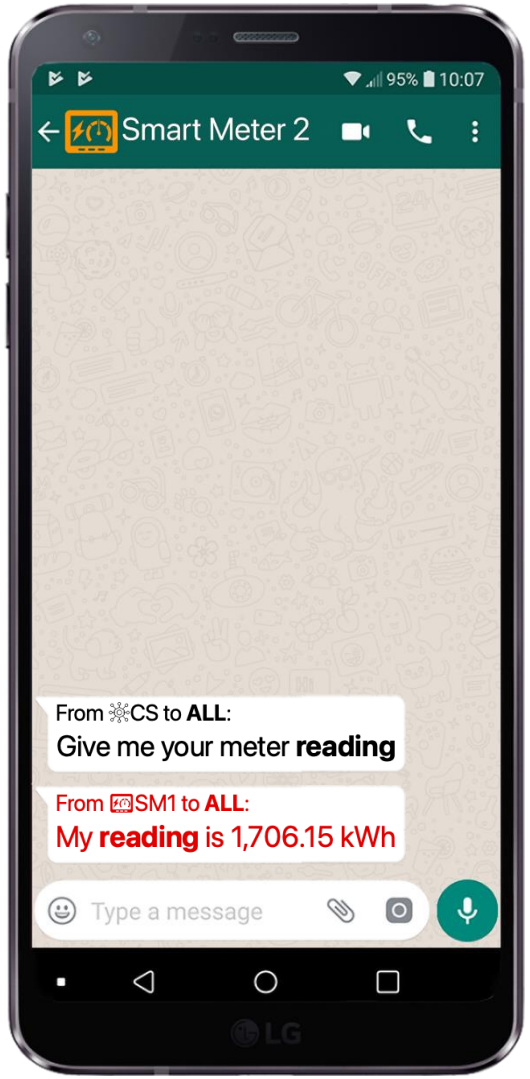
NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

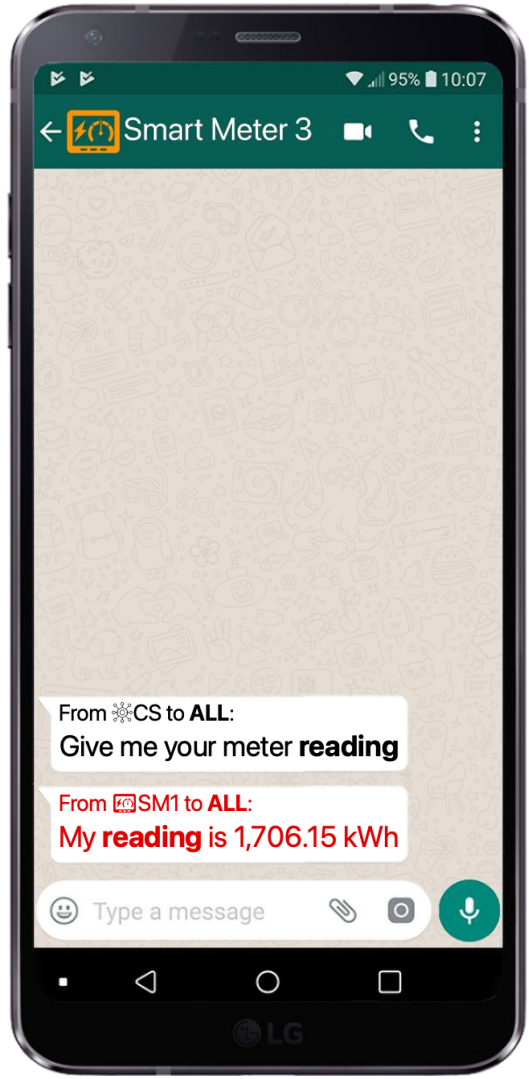
Broadcast meter reading query

When it did go wrong





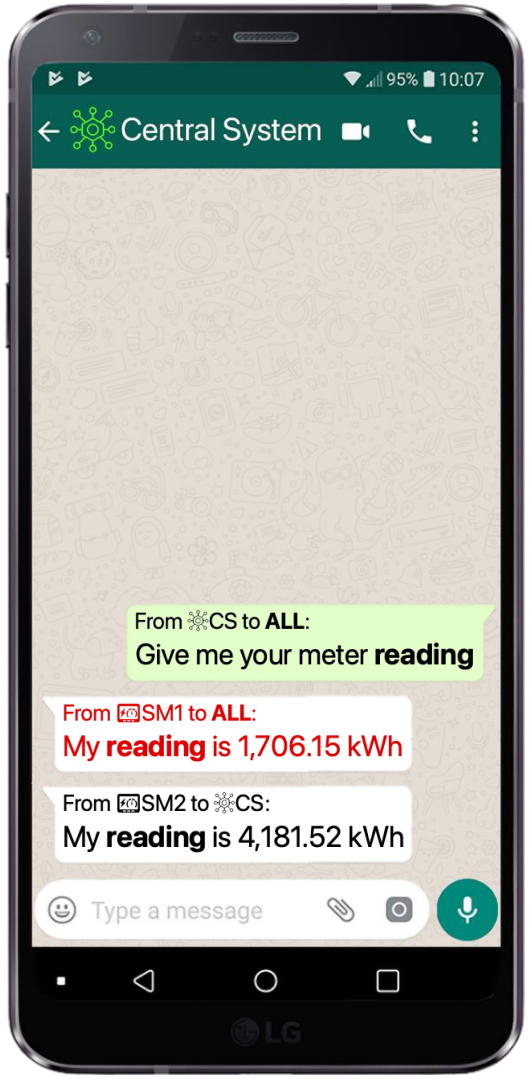


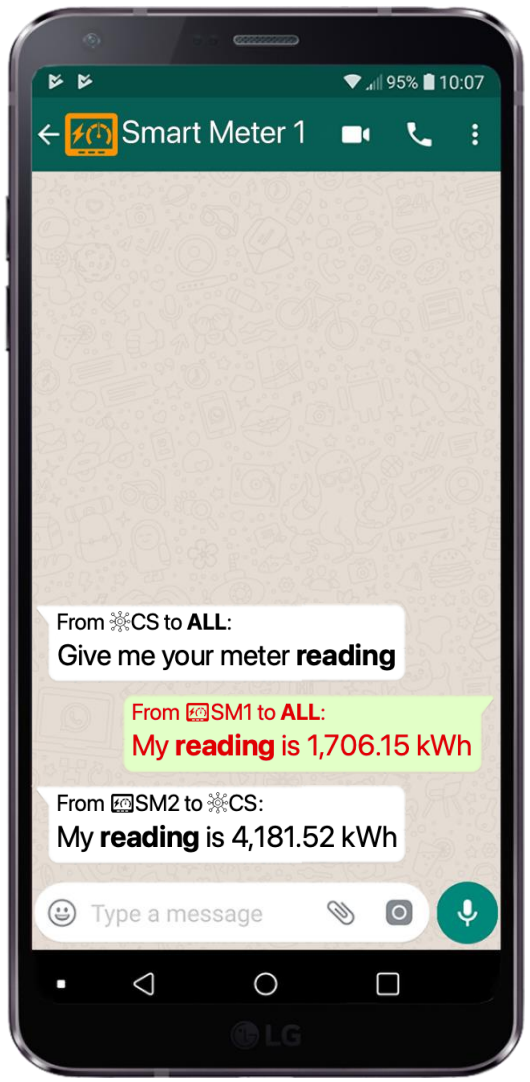


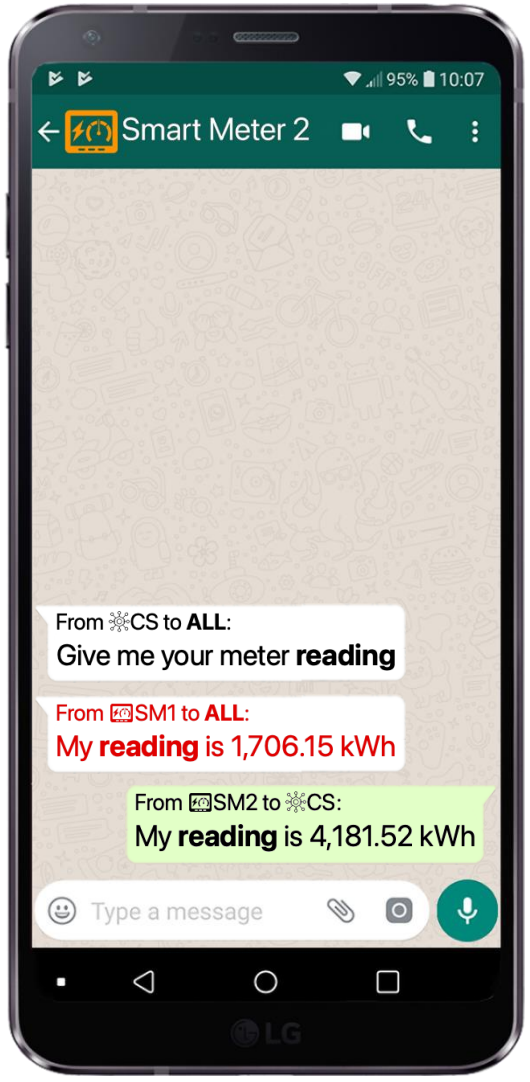
NATO OTAN
This workshop is supported by:
The NATO Science for Peace and Security Programme

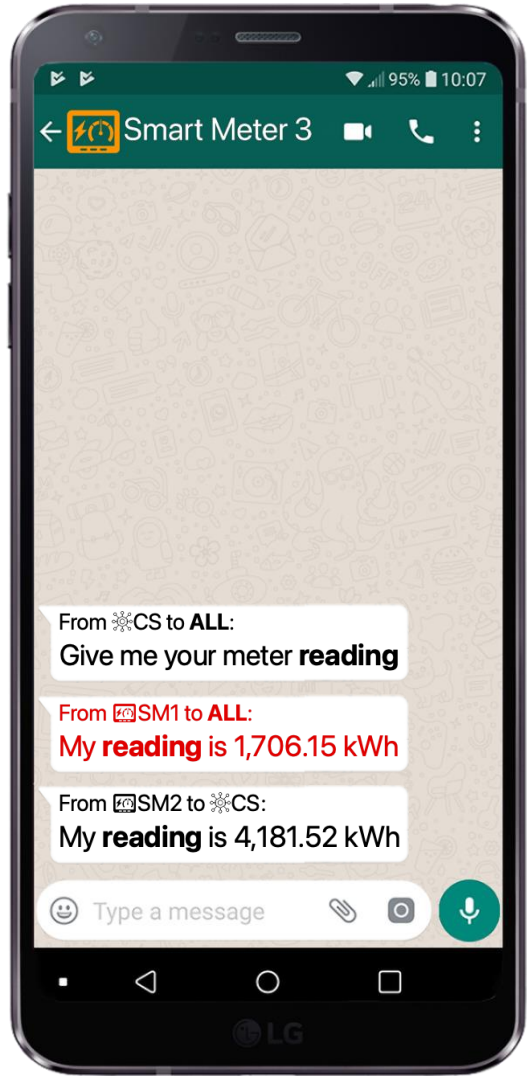
Broadcast meter reading query

When it did go wrong





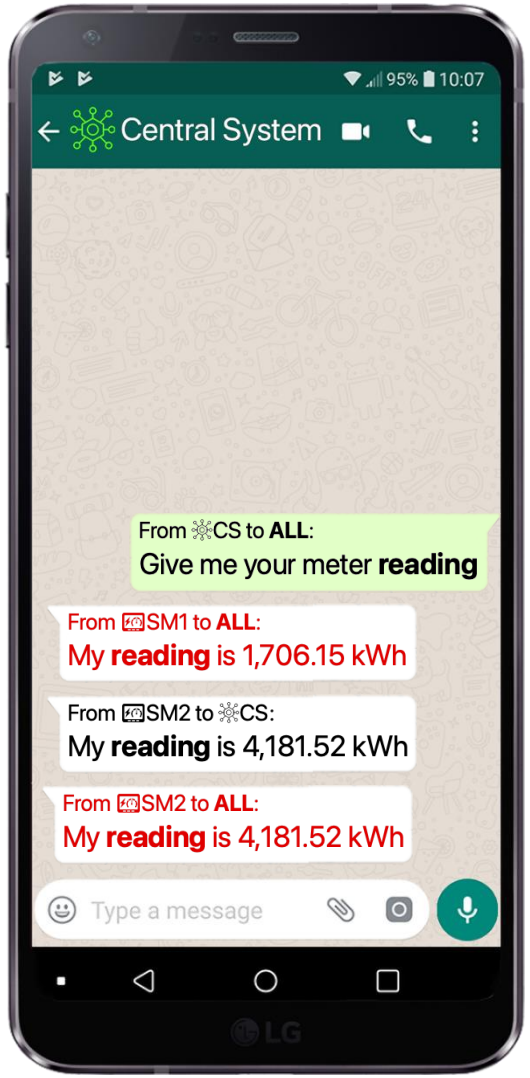


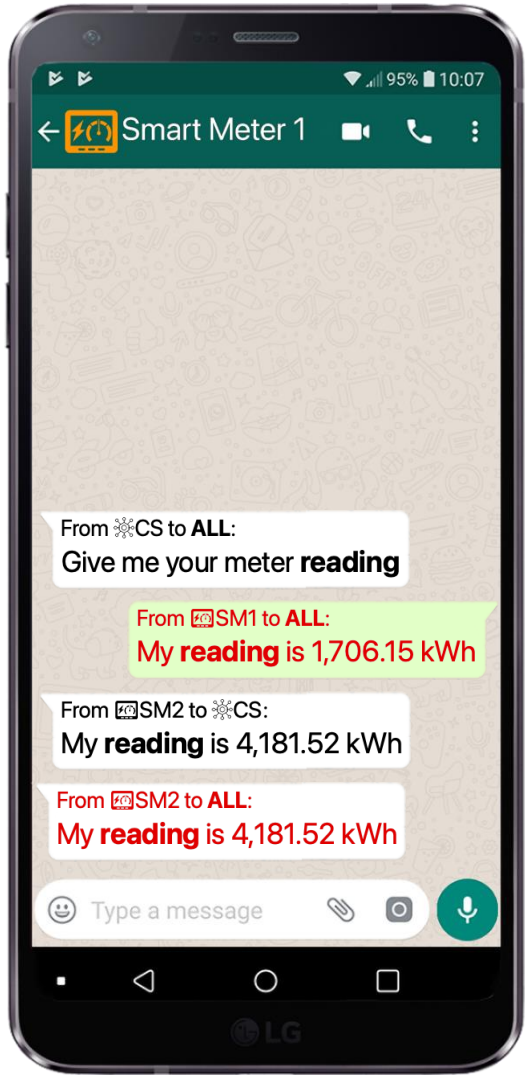


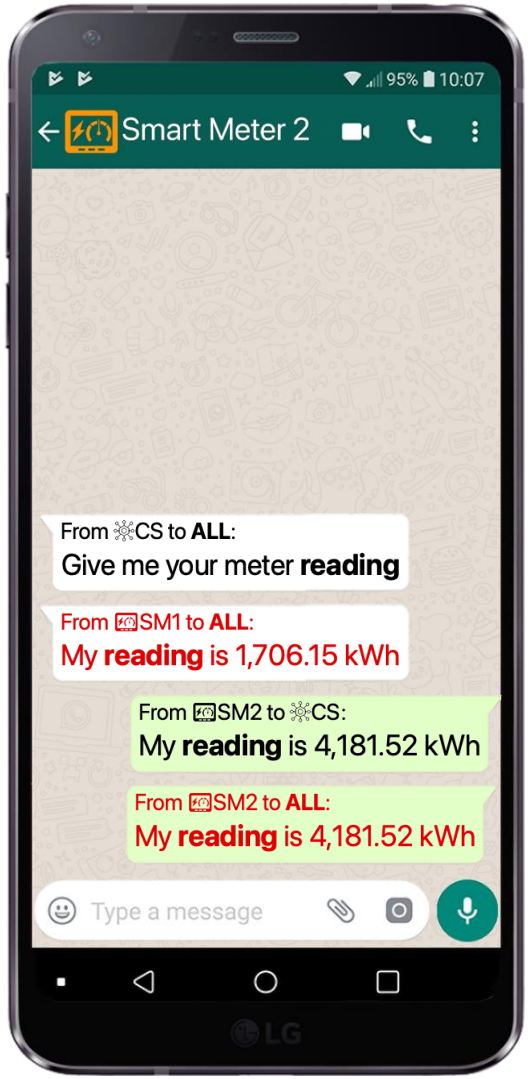
NATO OTAN
This workshop is supported by:
The NATO Science for Peace and Security Programme

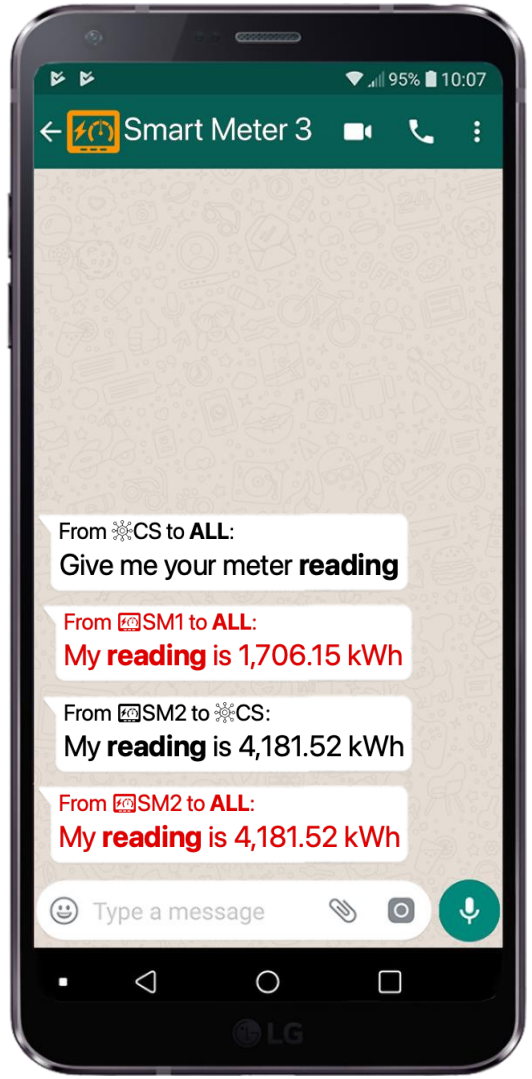
Broadcast meter reading query

When it did go wrong





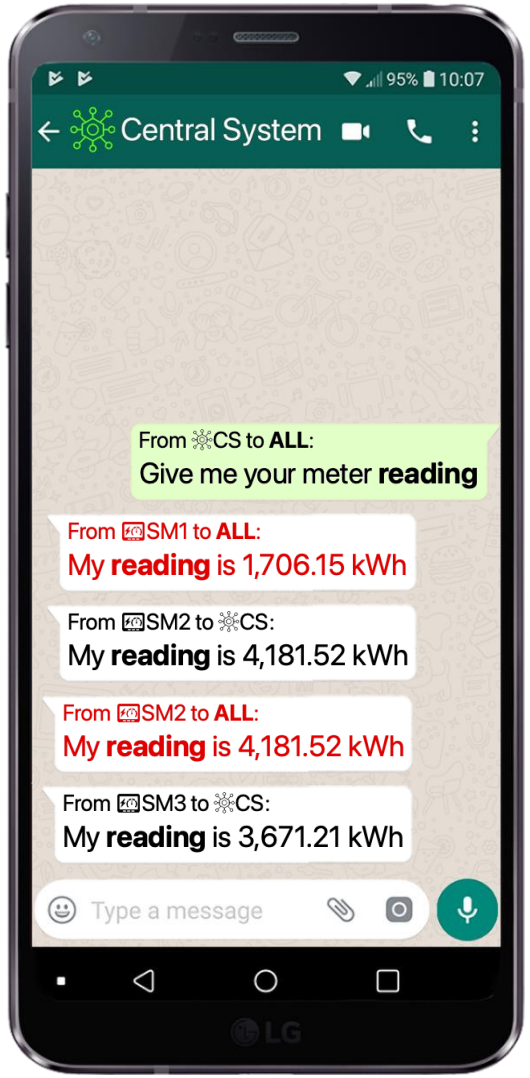


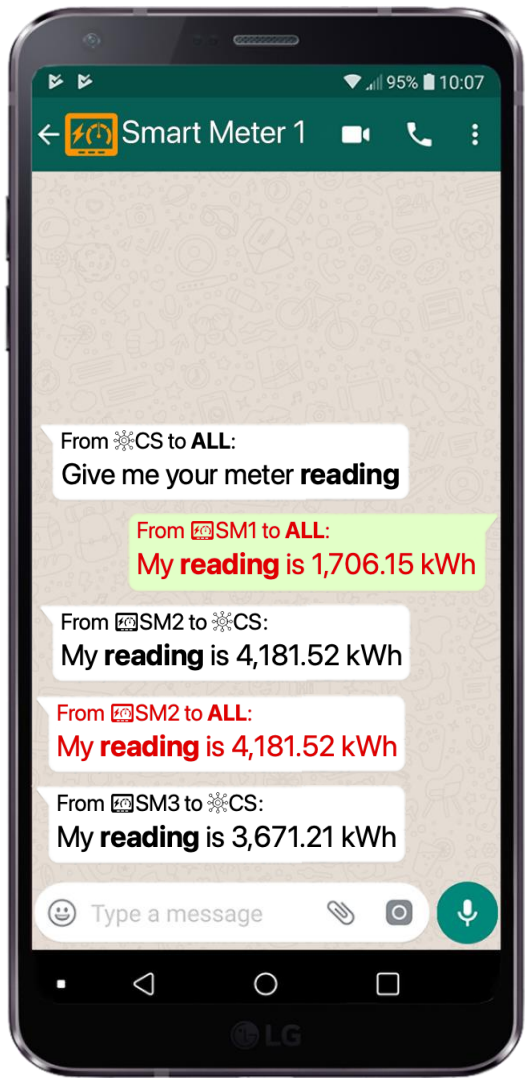


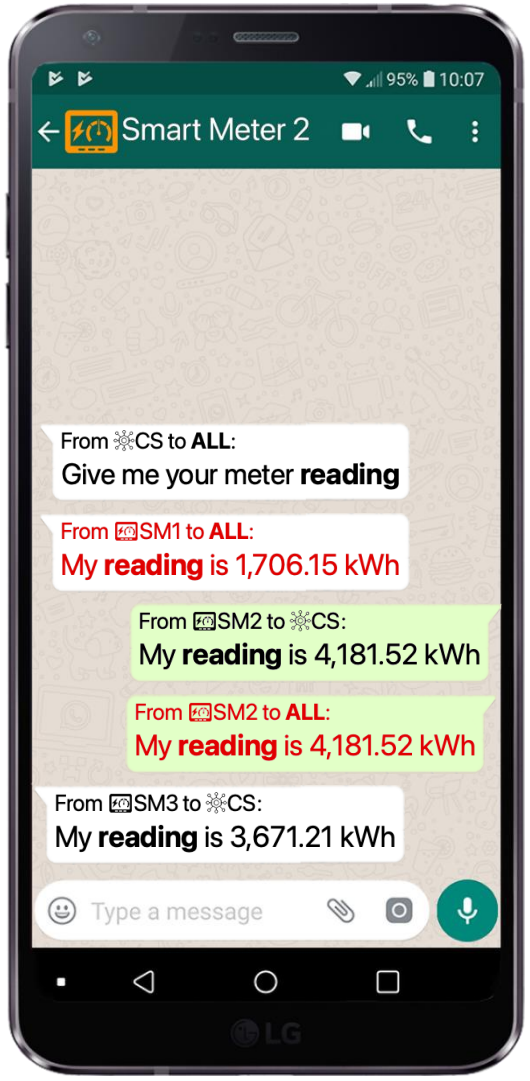
NATO OTAN
This workshop is supported by:
The NATO Science for Peace and Security Programme

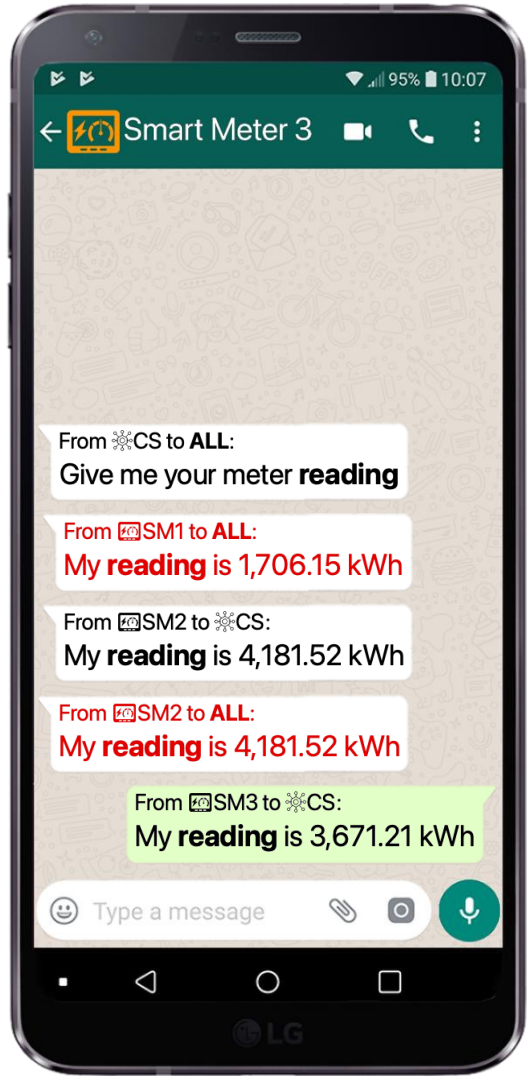
Broadcast meter reading query

When it did go wrong





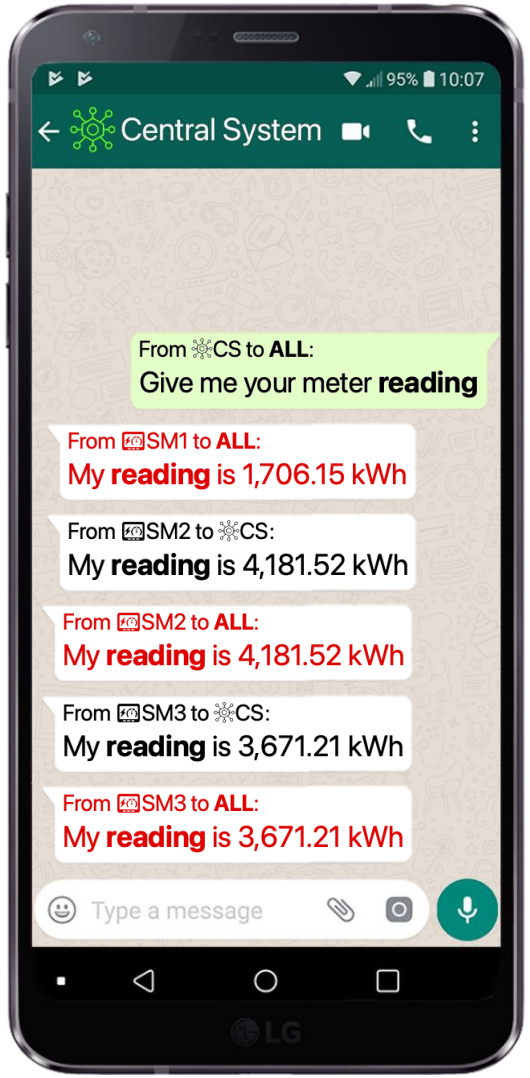


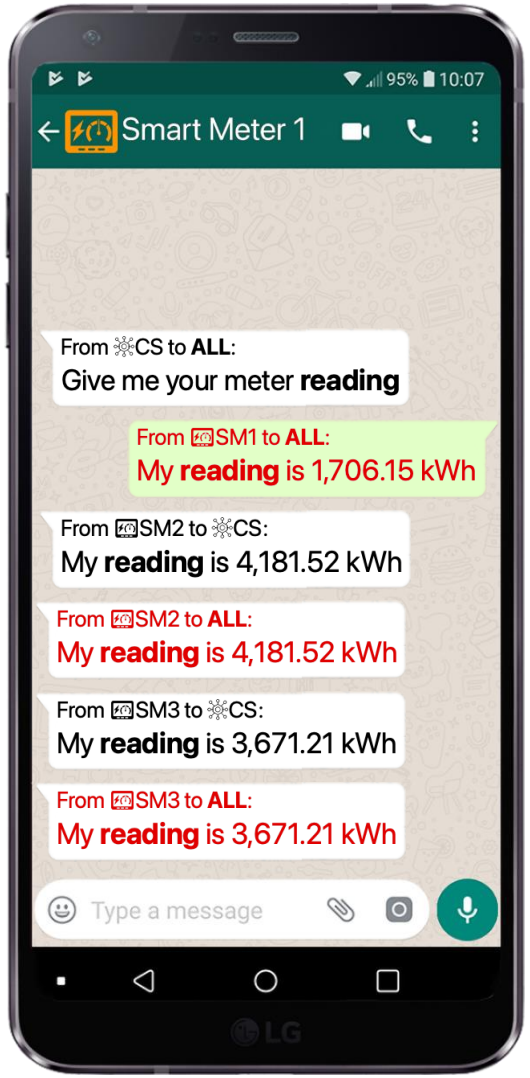


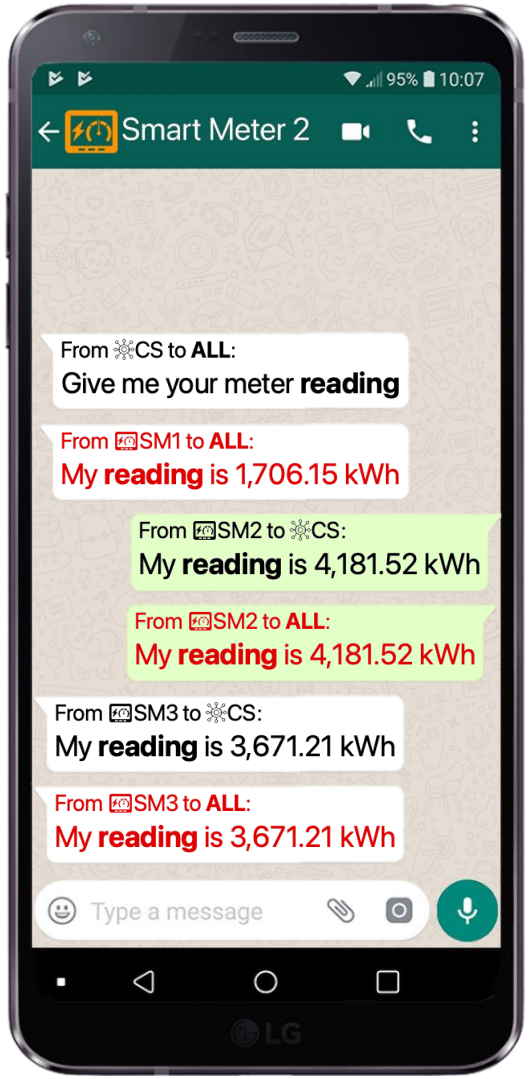
NATO OTAN
This workshop is supported by:
The NATO Science for Peace and Security Programme

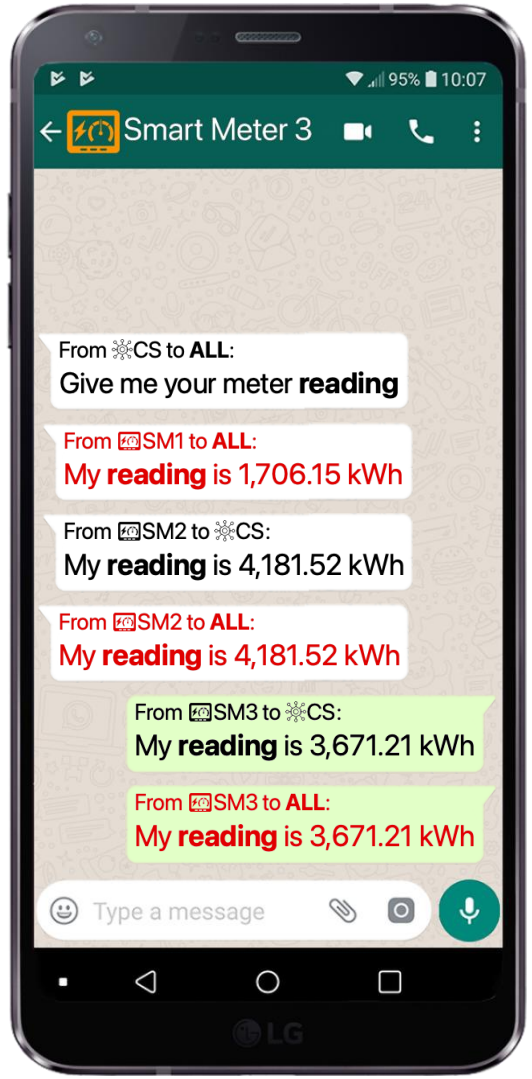
Broadcast meter reading query

When it did go wrong







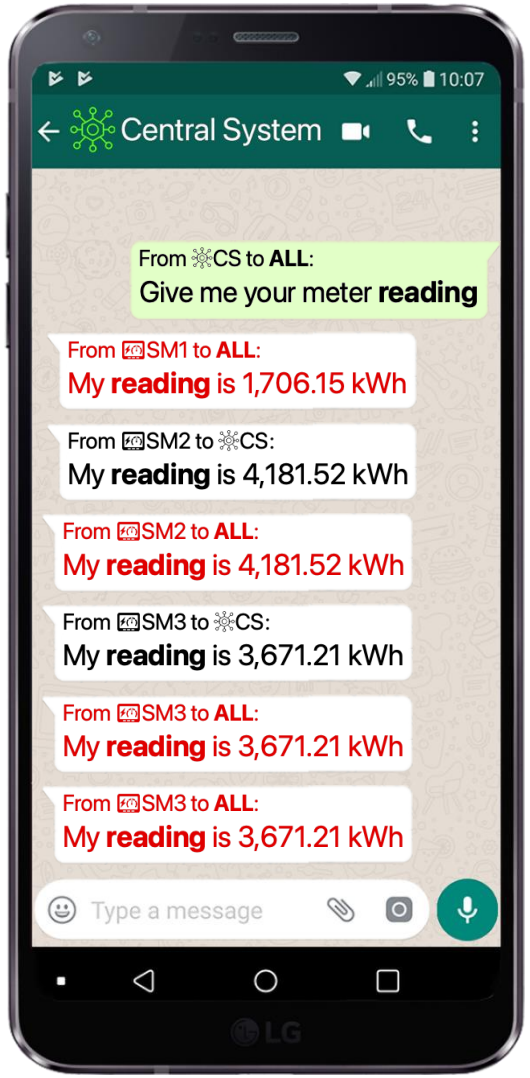


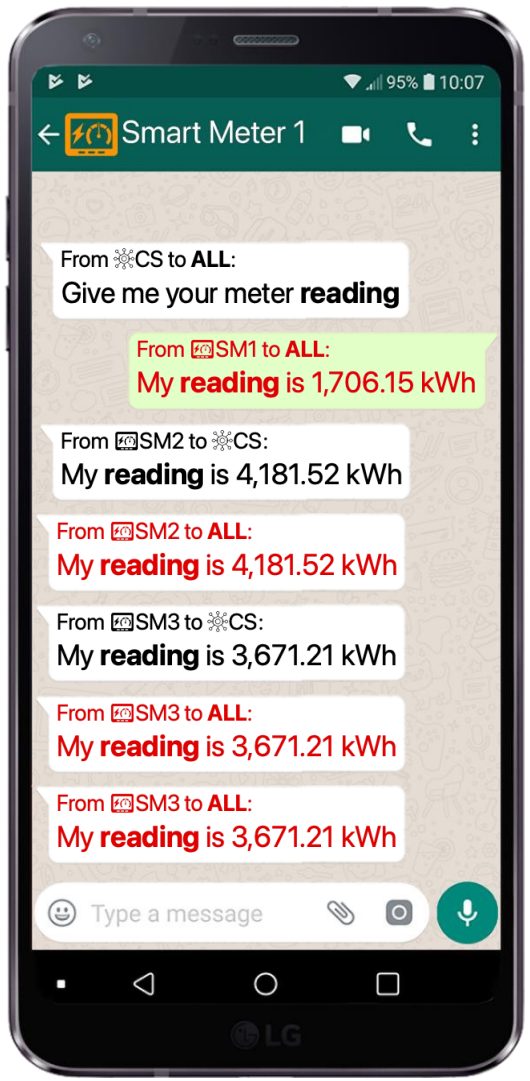
Hubert Schölnast
Hacking Smart Meters

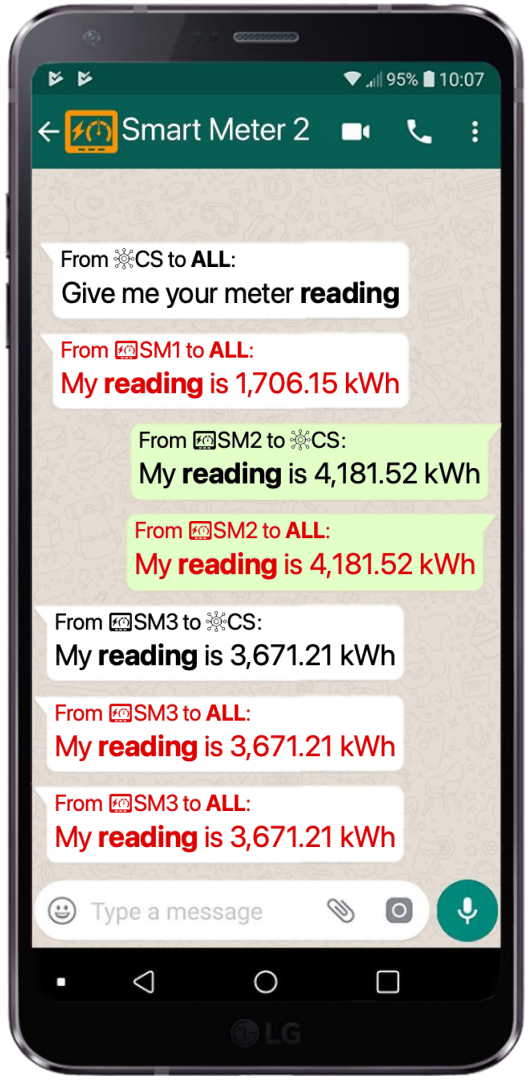
NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

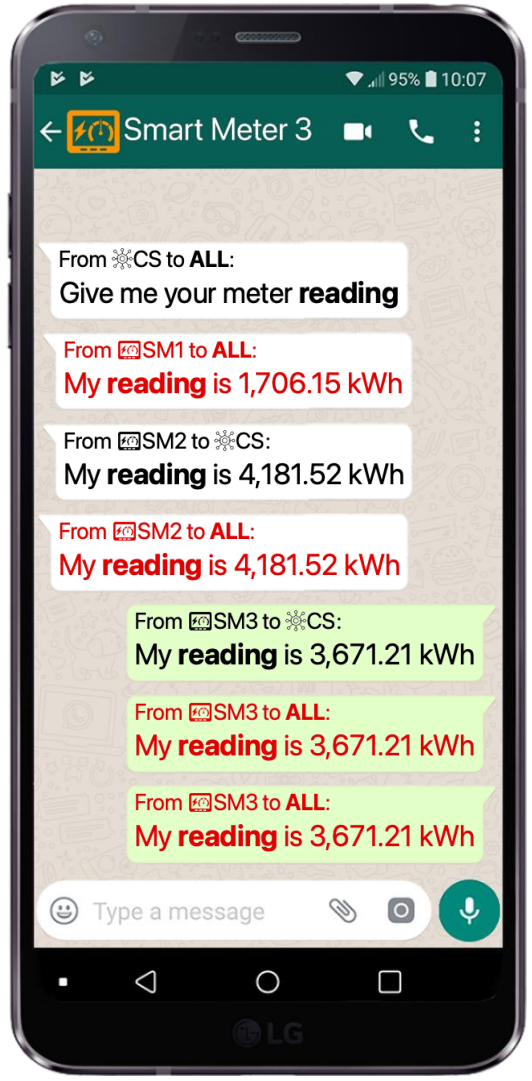
Broadcast meter reading query

When it did go wrong





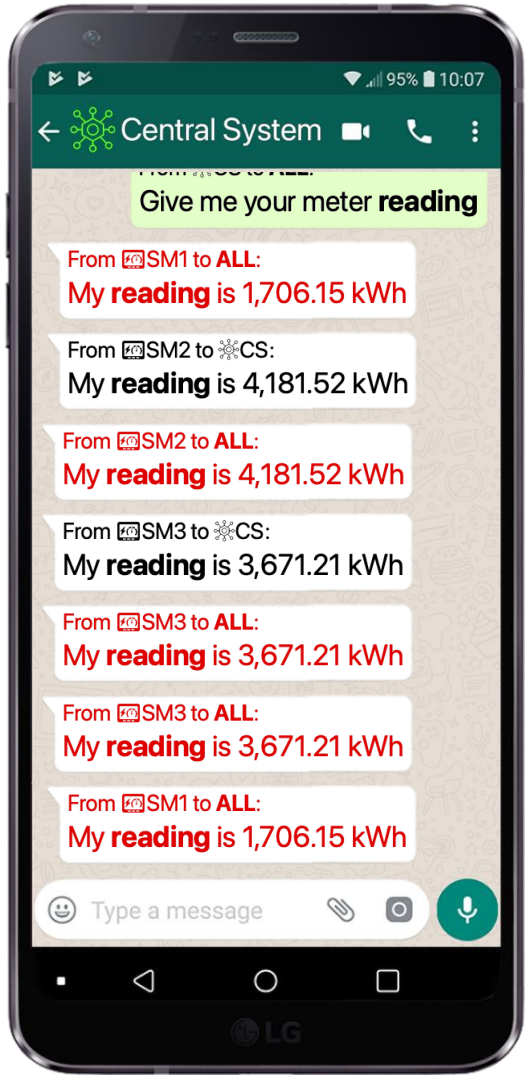


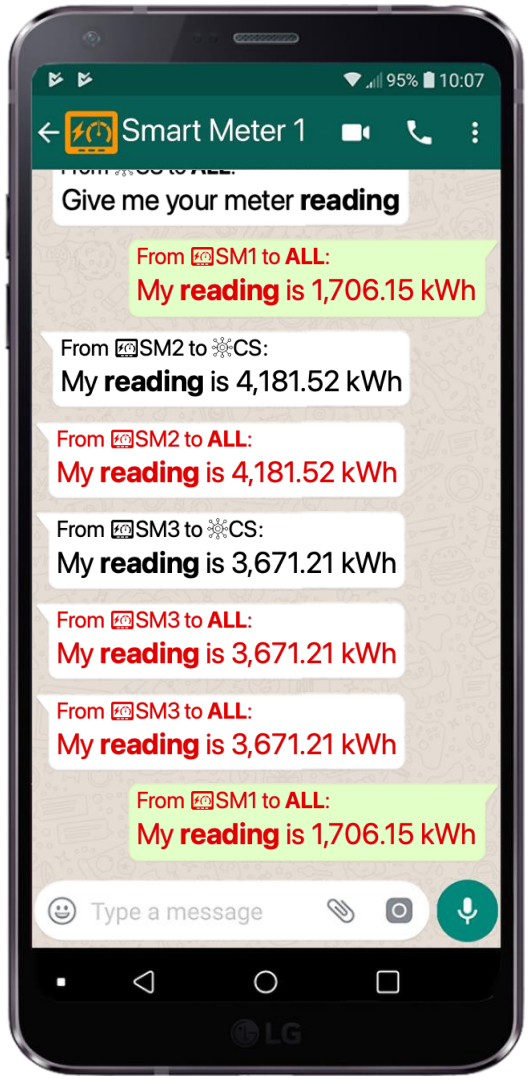


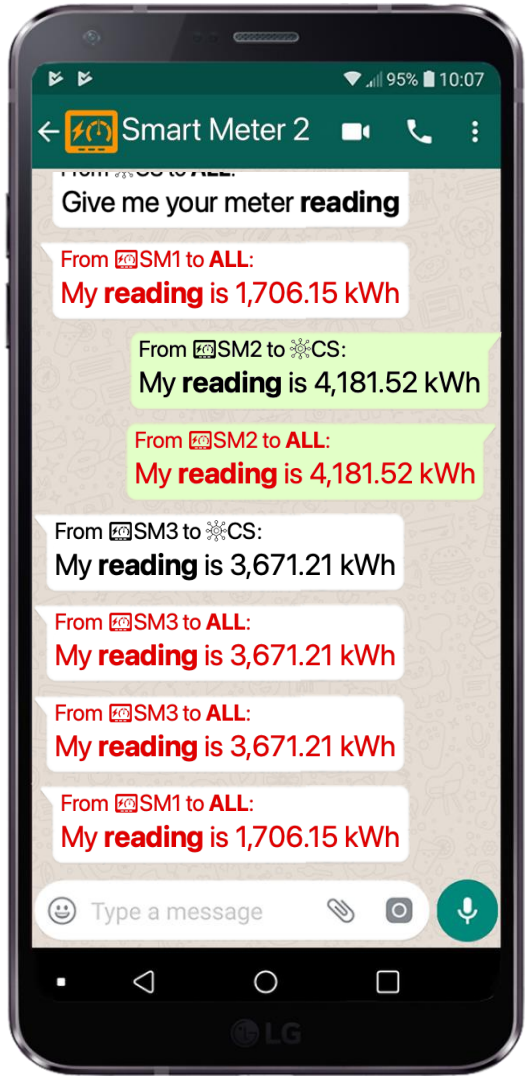
NATO OTAN
This workshop is supported by:
The NATO Science for Peace and Security Programme

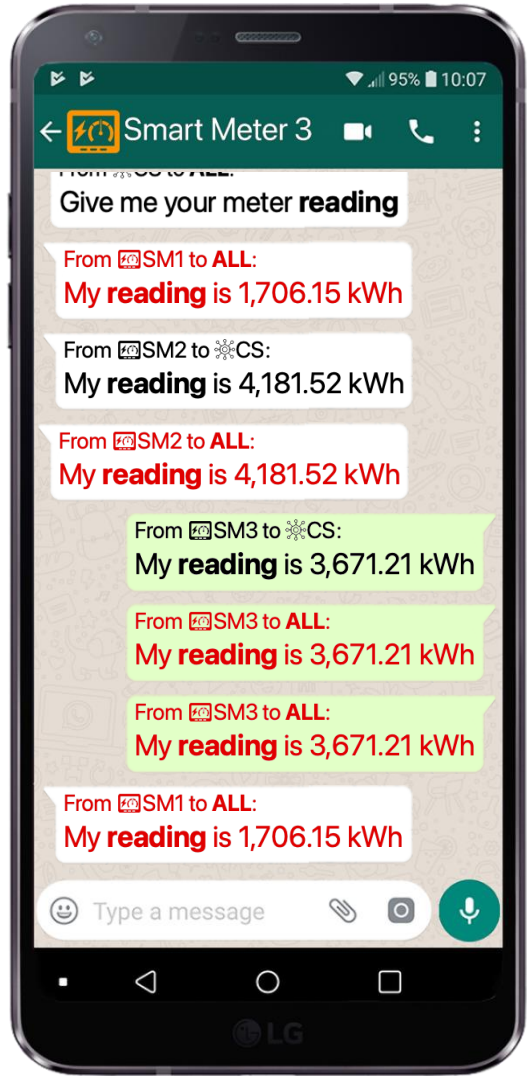
Broadcast meter reading query

When it did go wrong







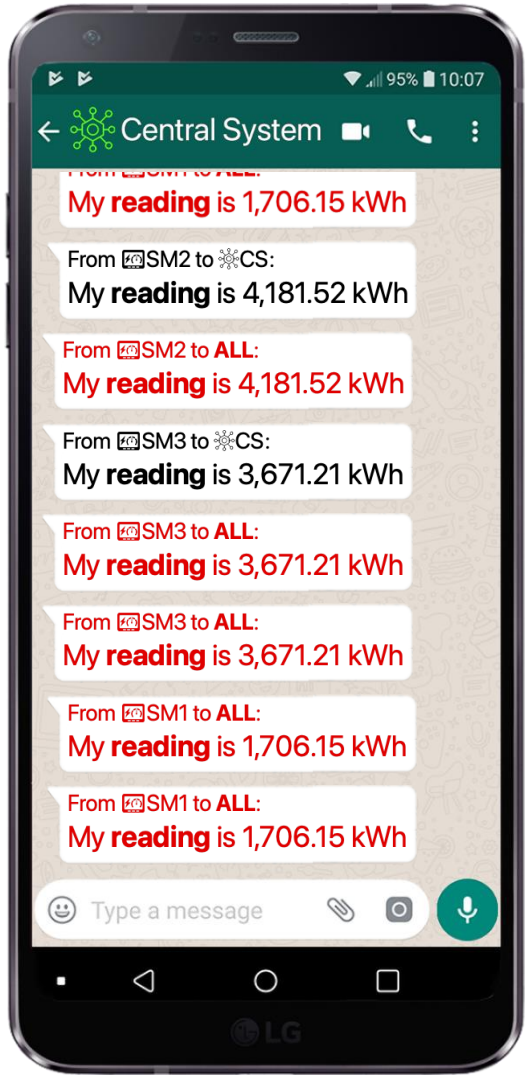


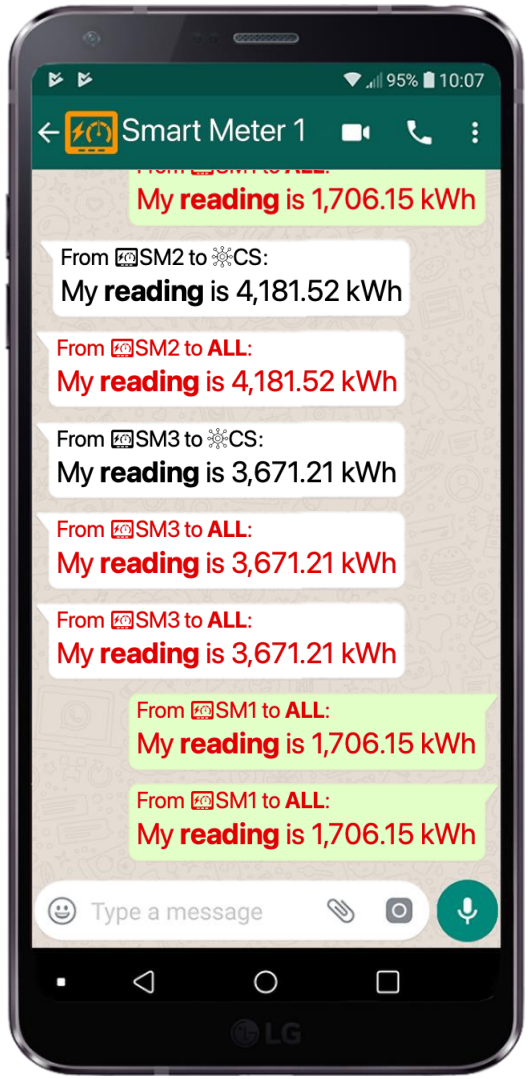
Hubert Schölnast
Hacking Smart Meters

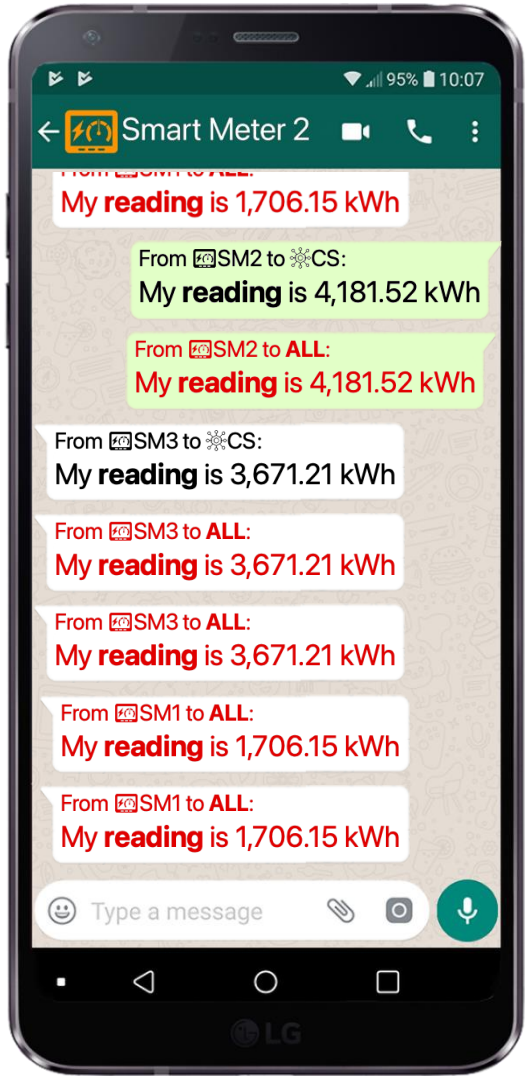
NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

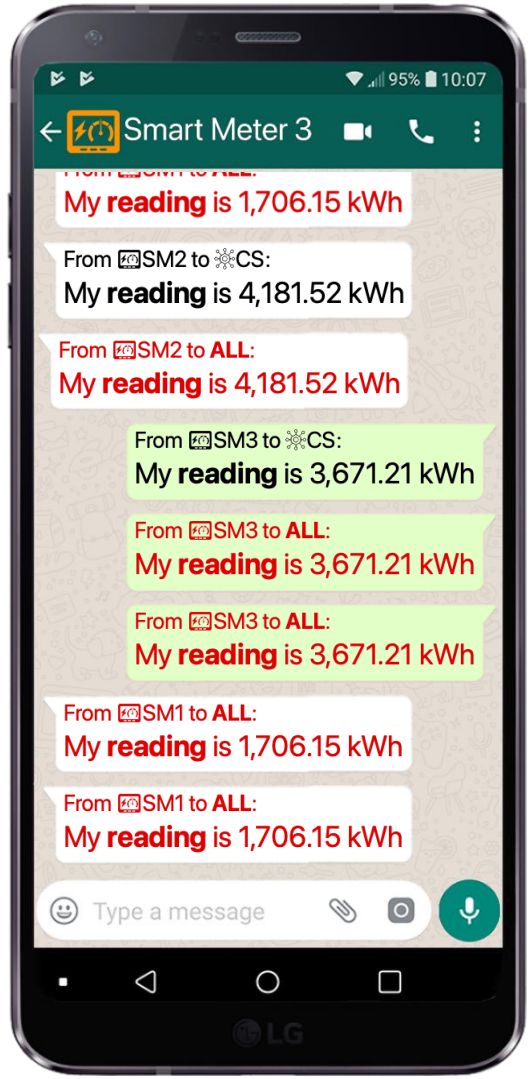
Broadcast meter reading query

When it did go wrong





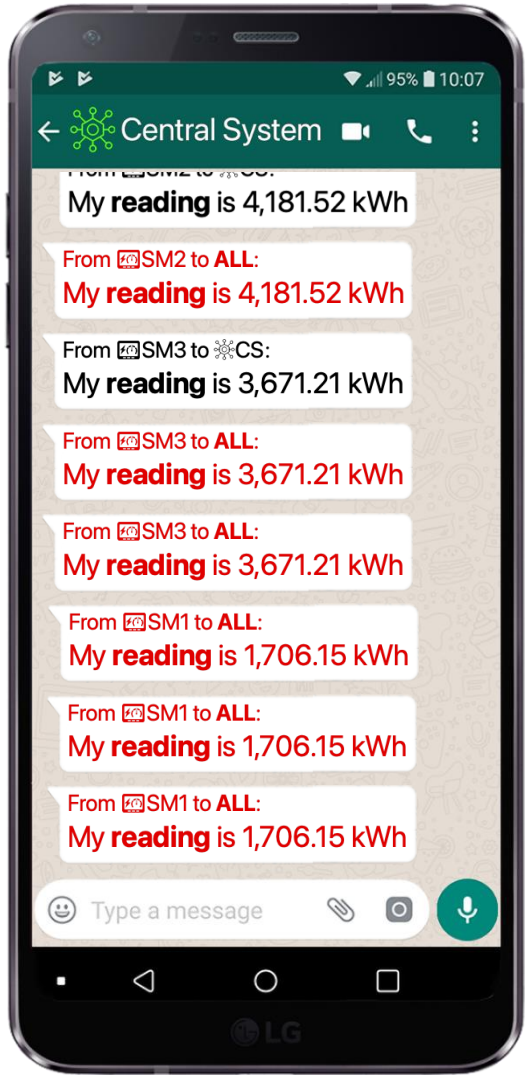


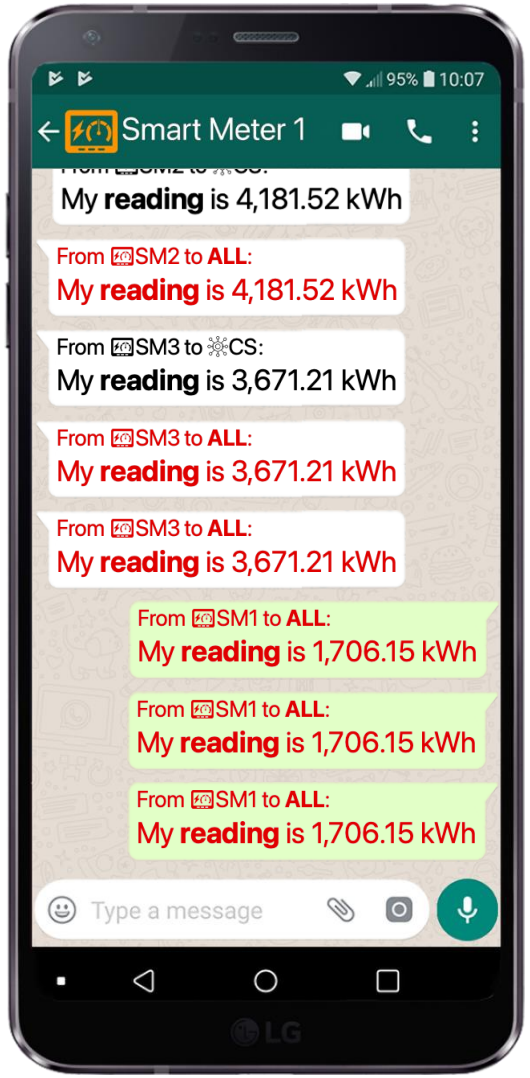


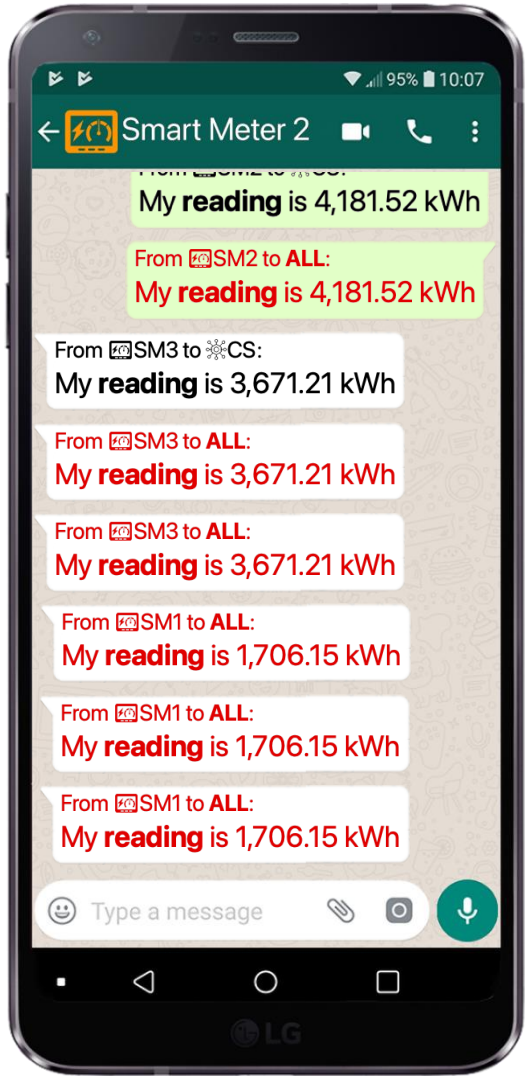
NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

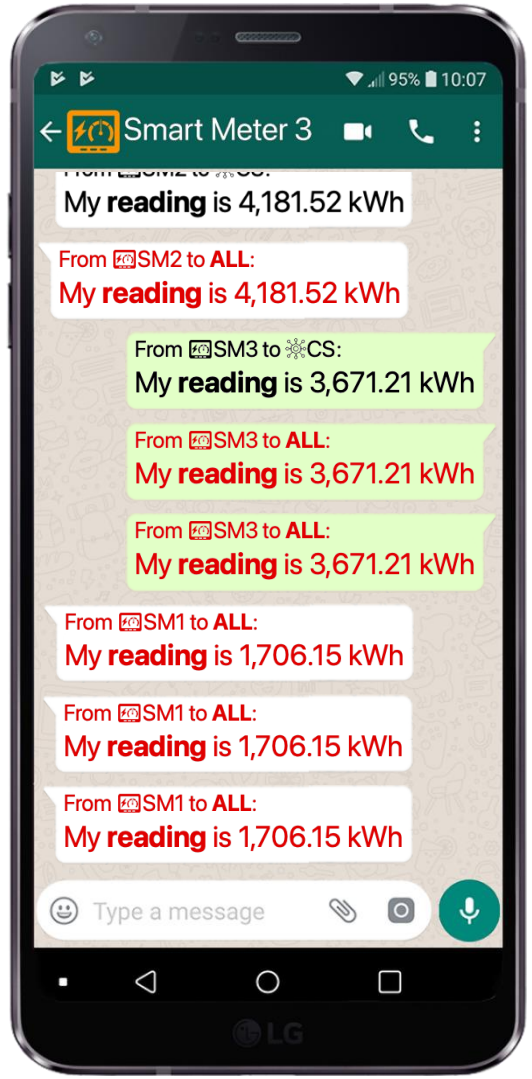
Broadcast meter reading query

When it did go wrong









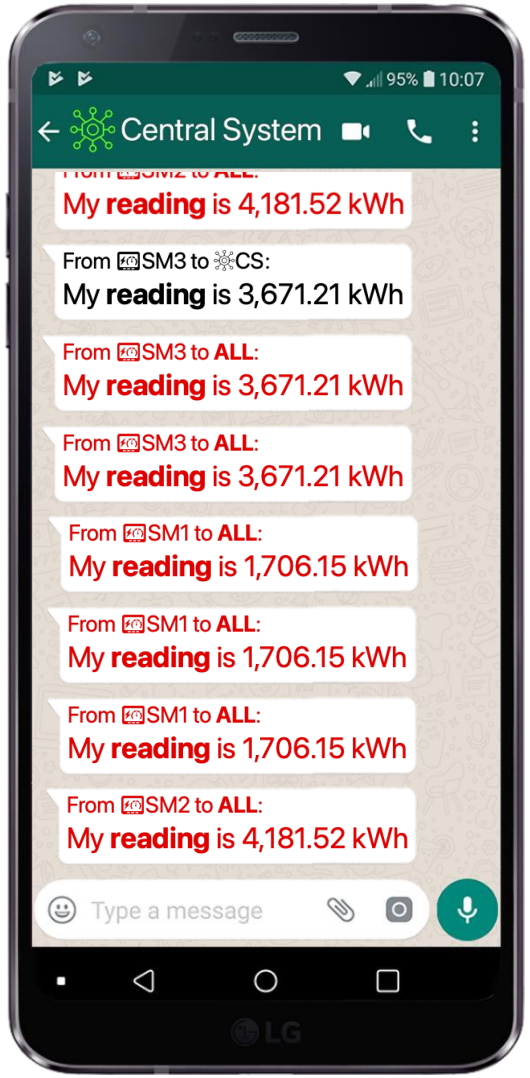
Hubert Schölnast
Hacking Smart Meters

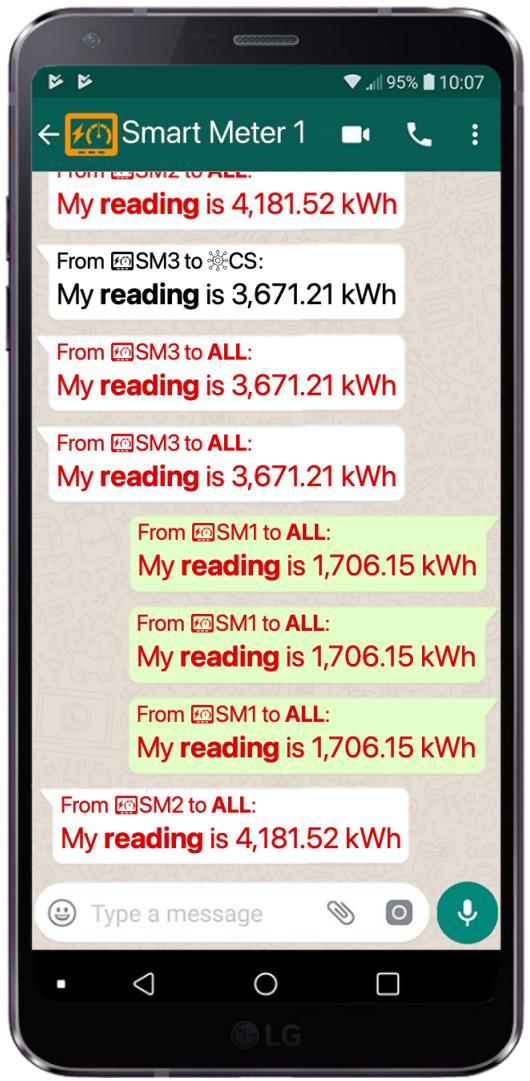
NATO OTAN
This workshop is supported by:
The NATO Science for Peace and Security Programme

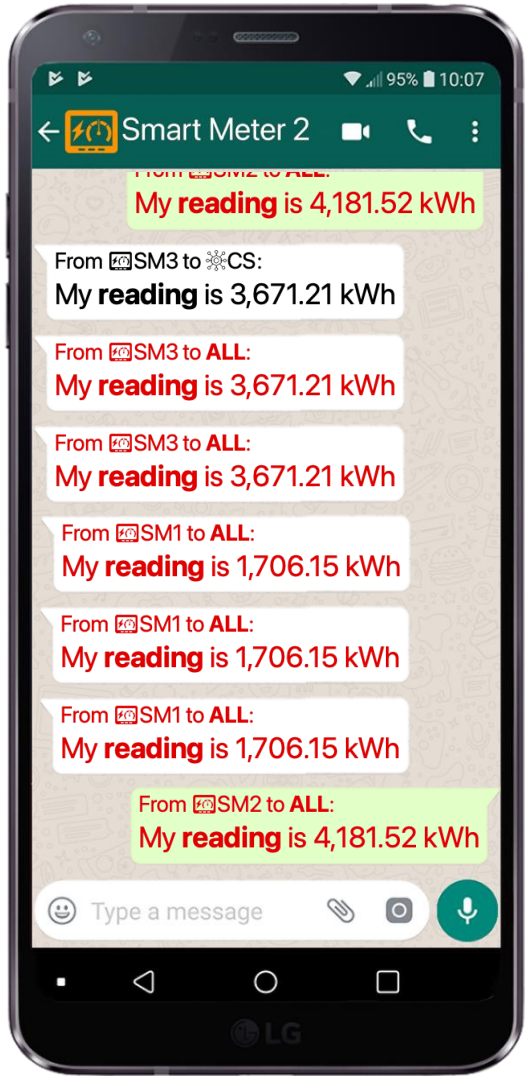
Broadcast meter reading query

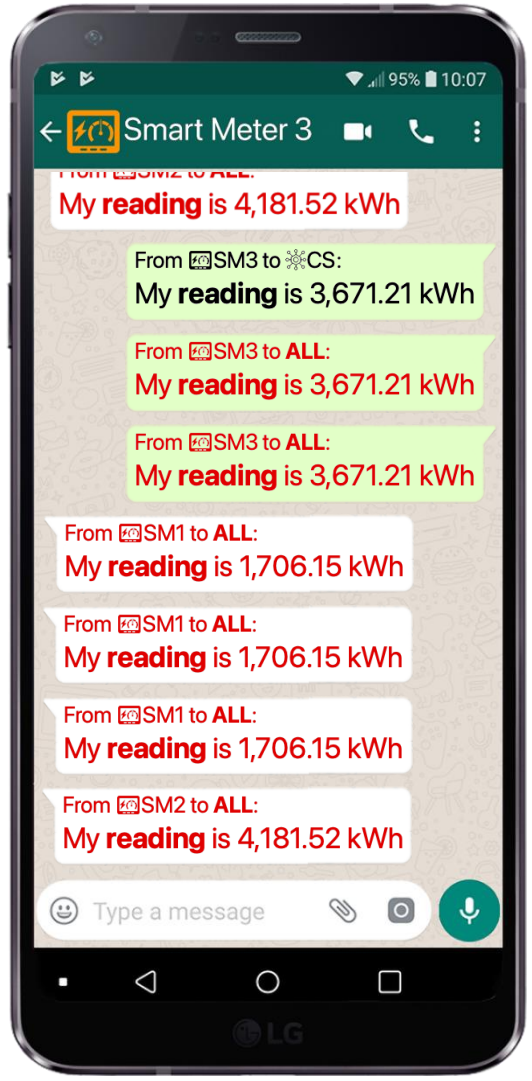
When it did go wrong

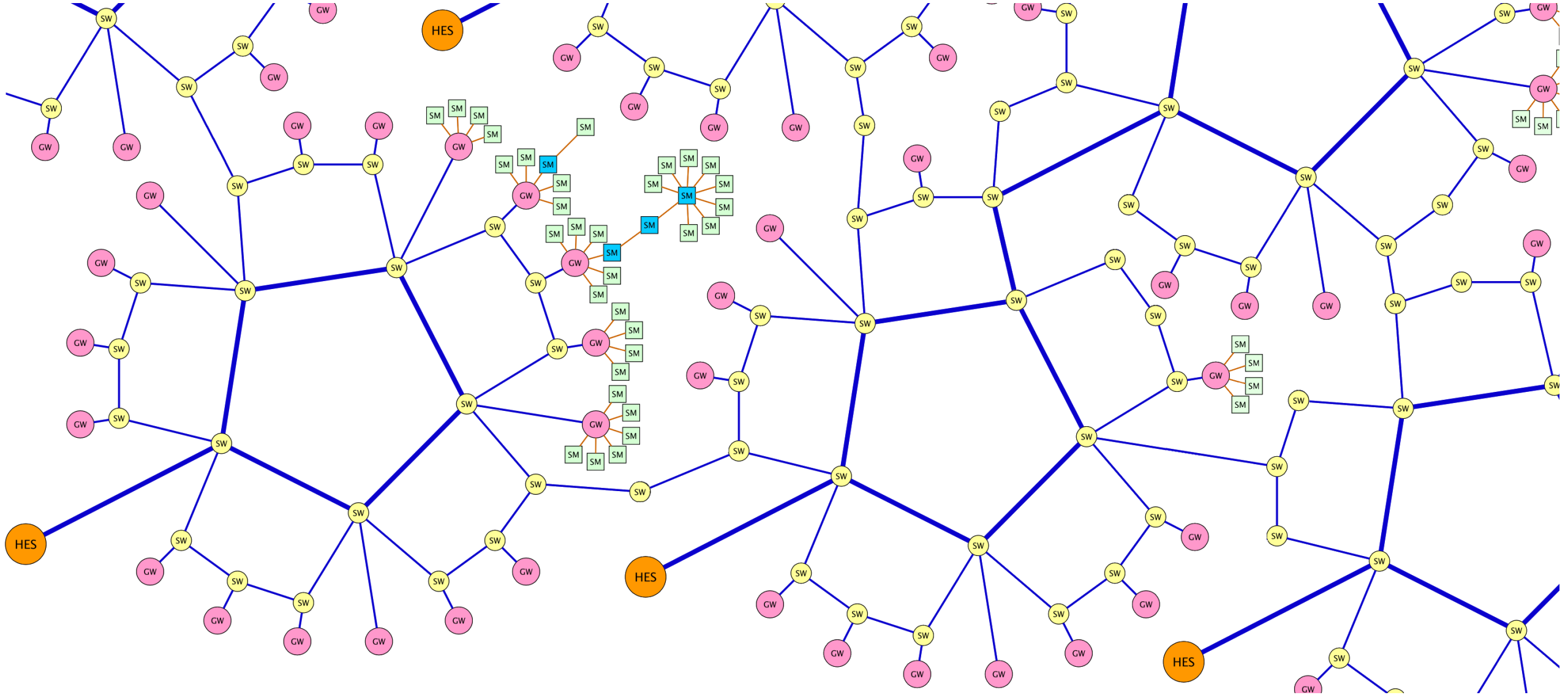
and so on











Hubert Schölnast
Hacking Smart Meters

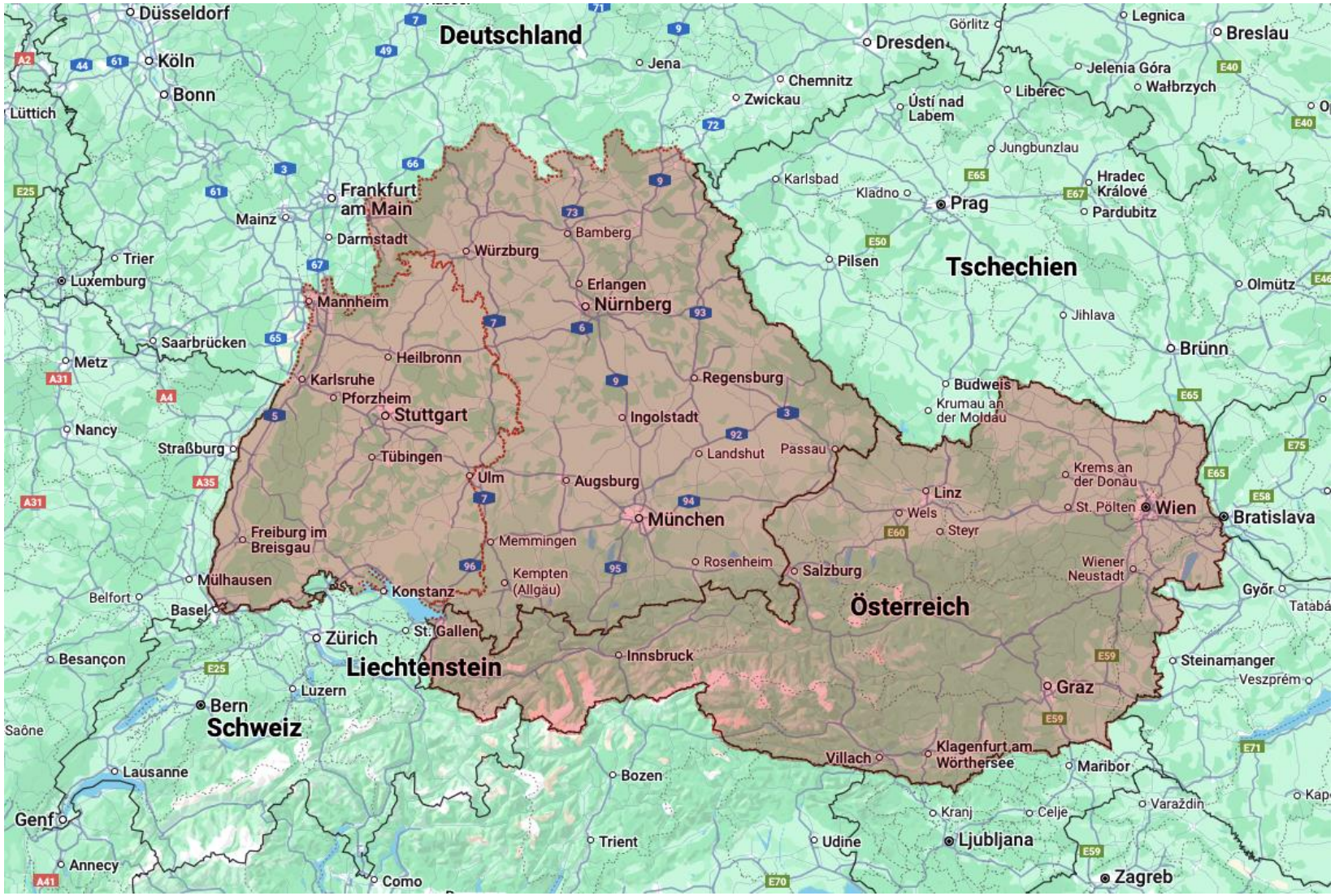
NATO OTAN
This workshop is supported by:
The NATO Science for Peace and Security Programme

The spread of the flood of messages

- There are only rumors about how and where exactly it started.
  - Some say it started as a test in a test environment that was too weakly closed.
  - Some say it was a deliberate hacker attack.
- But it is known that it started somewhere in Baden-Württemberg in the southeast of Germany.
- The toxic news broke through almost all protective walls and quickly spread throughout the whole state of Baden-Württemberg.
- From there they flooded over Bavaria and then even across the national border to Austria.

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

Affected regions	Population
Baden-Württemberg	11.3 million
Bavaria	13.4 million
Austria	9.1 million
Total	33.8 million



NATO OTAN
This workshop is supported by:
The NATO Science for Peace and Security Programme

The danger of this flood of messages

- The toxic messages pushed all communication systems to their capacity limits.
- Once the maximum was reached, new messages were lost.
- This included almost all of the "normal" messages needed to control the flow of energy through the electrical backbone.
- Also, the communication between substation was shut down.
- Engineers no longer knew what was going on in their system.
- Any small instability could quickly spread and grow unnoticed.
- The risk of a blackout in the affected region became greater and greater.
- Only a hastily developed software update for the gateways was able to stop the flood after 5 days of instability.

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

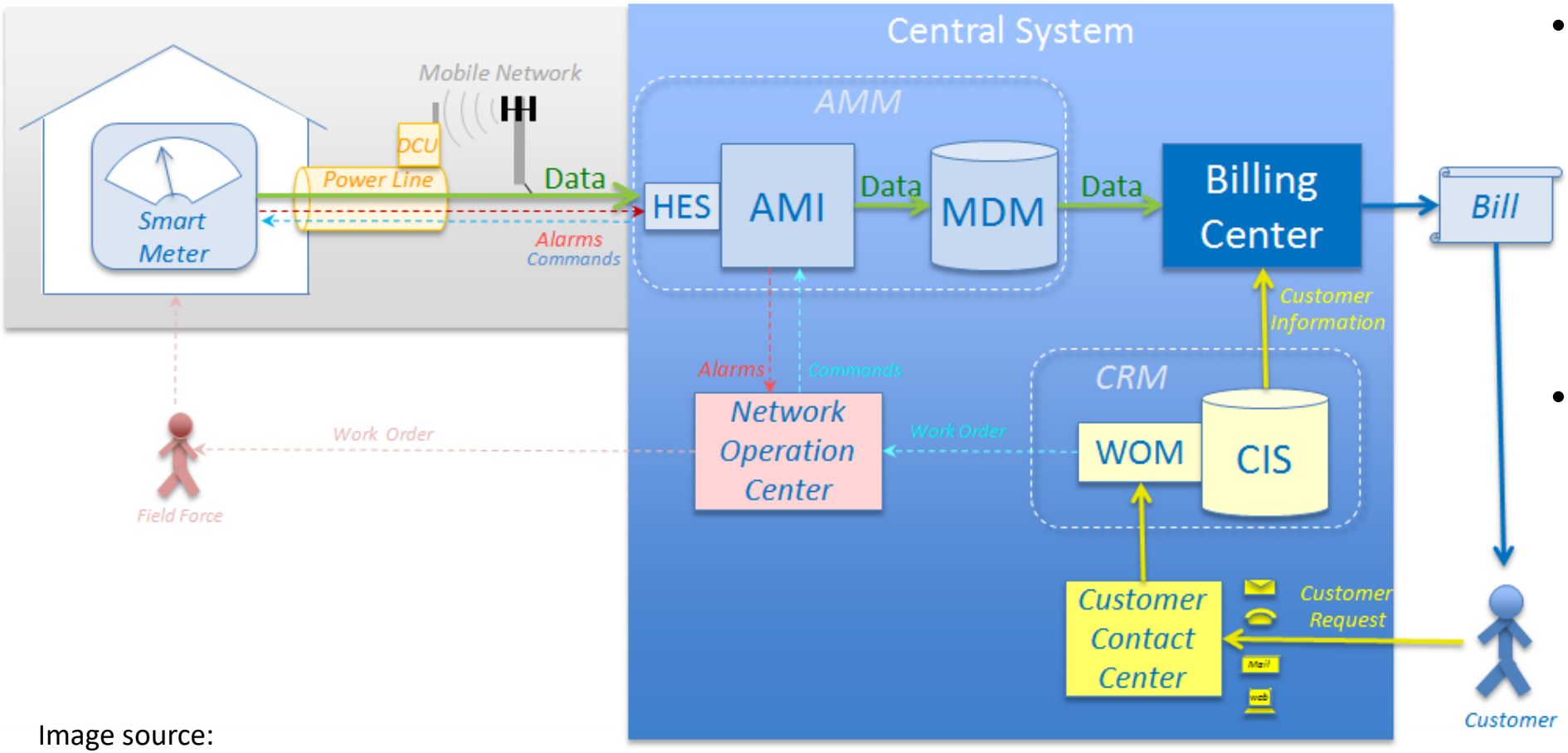
What you can see in a fully encrypted network

Results of the project “Energy Network Security”
Nov. 2018 – Oct. 2020
St. Pölten University of Applied Sciences
(Paul Tavolato, Hubert Schölnast, Oliver Eigner)
in cooperation with Wels Strom GmbH

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

Outdoor infrastructure
(communication network)

Indoor infrastructure
(central system)



Smart metering infrastructure

- **A**dvanced **M**eter **M**anagement
  - **H**ead **E**nd **S**ystem
  - **A**dvanced **M**etering **I**nfrastructure
  - **M**eter **D**ata **M**anagement
- **C**ustom **R**elationship **M**anagement
  - **W**ork **O**rder **M**anagement
  - **C**ustomer **I**nformation **S**ystem

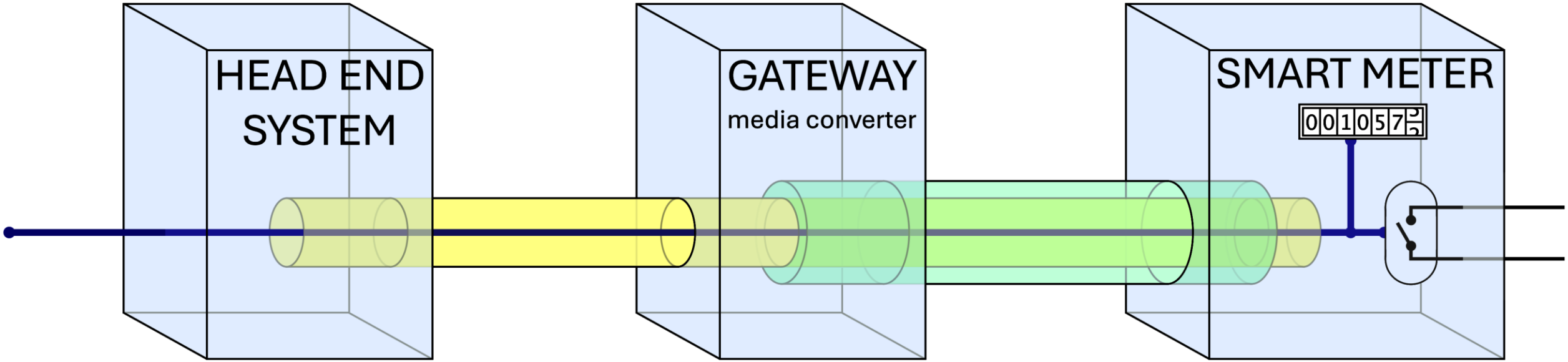
Image source:
https://de.wikipedia.org/wiki/Datei:Smart_Meter_Infrastructure.png

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

central system

glass fiber,
ethernet, etc.

powerline



cleartext

end-to-end
encryption

additional
protocol encryption
(G3-PLC)

cleartext

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

Every message belongs to one **52 defined use cases** (message types)

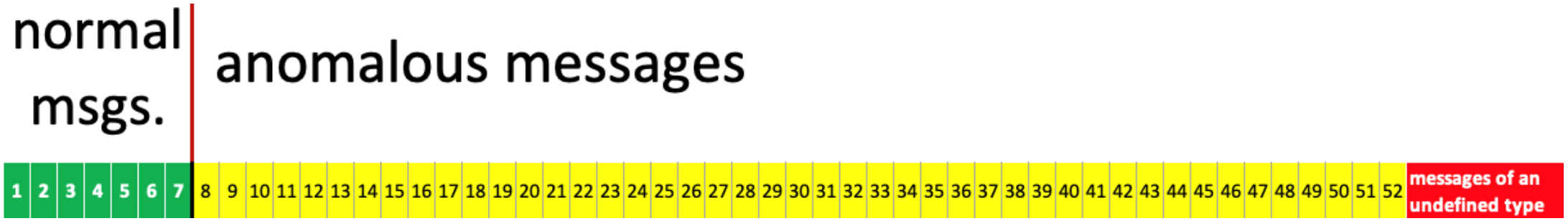
• Meter reading	**4** use cases
• Disconnect breaker, ready to reconnect breaker	**6** use cases
• Parametrization of the device	**12** use cases
• Firmware upgrade	**6** use cases
• Alarms and events	**2** use cases
• Load switching	**5** use cases
• Calibration/testing	**1** use case
• User interface activation/deactivation	**2** use cases
• Prepayment	**2** use cases
• Registration and deregistration of the end device	**2** use cases
• Activation and deactivation of gateway function	**5** use cases
• Security (cryptographic parameters)	**5** use cases

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

From these 52 allowed messages only these 7 are used in day-to-day operation of the environment:

- A Switching off the load switching device
- B Breaker status query
- C Direct switching on the load switching device
- D Enabling to switch on the load switching device
- E Meter reading query
- F Load profile query
- G Parameterization (Setting a threshold for the power limitation on the meter)

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

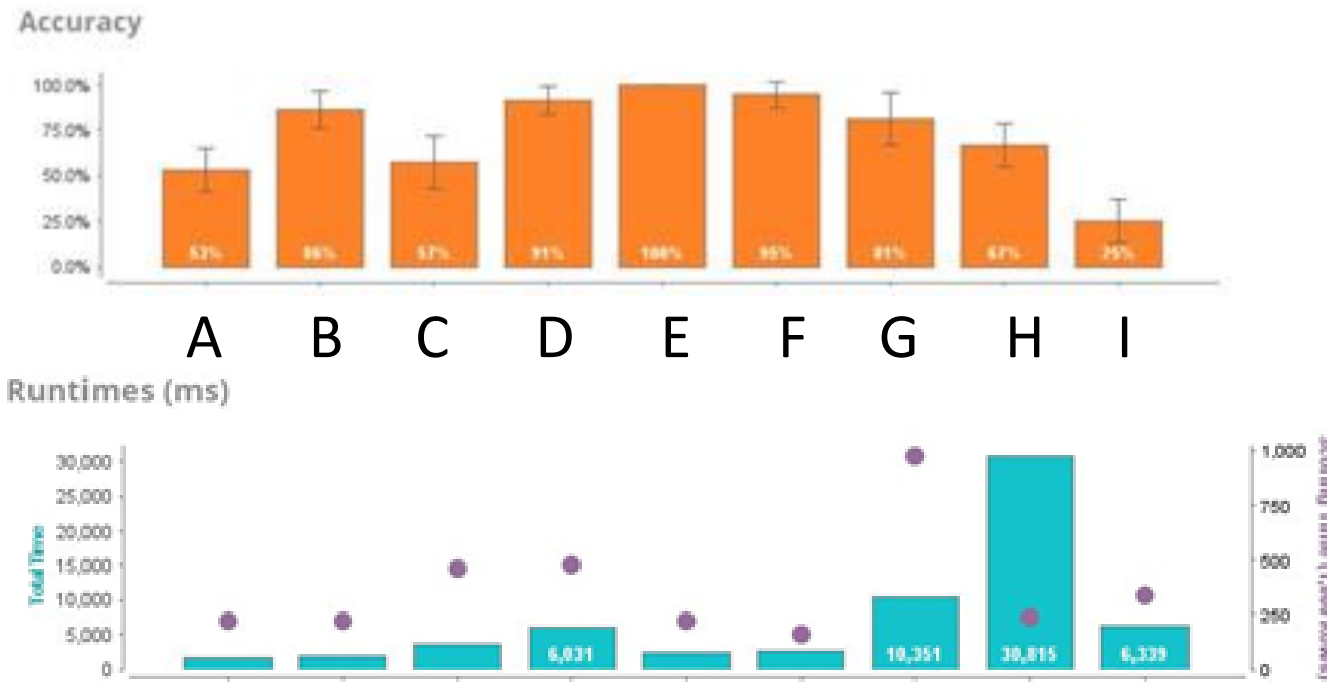


These 7 message types can be identified by properties of their meta data

- Length of IP-header
- Length of TCP-header
- Length of TCP-payload
- Number of packages per message
- Time delay between two packages
- many other features

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

We tried different methods of machine learning



A Naive Bayes

B Generalized Linear Model

C Logistic Regression

D Fast Large Margin

E Deep Learning

F Decision Tree

G Random Forest

H Gradient Boosted Trees

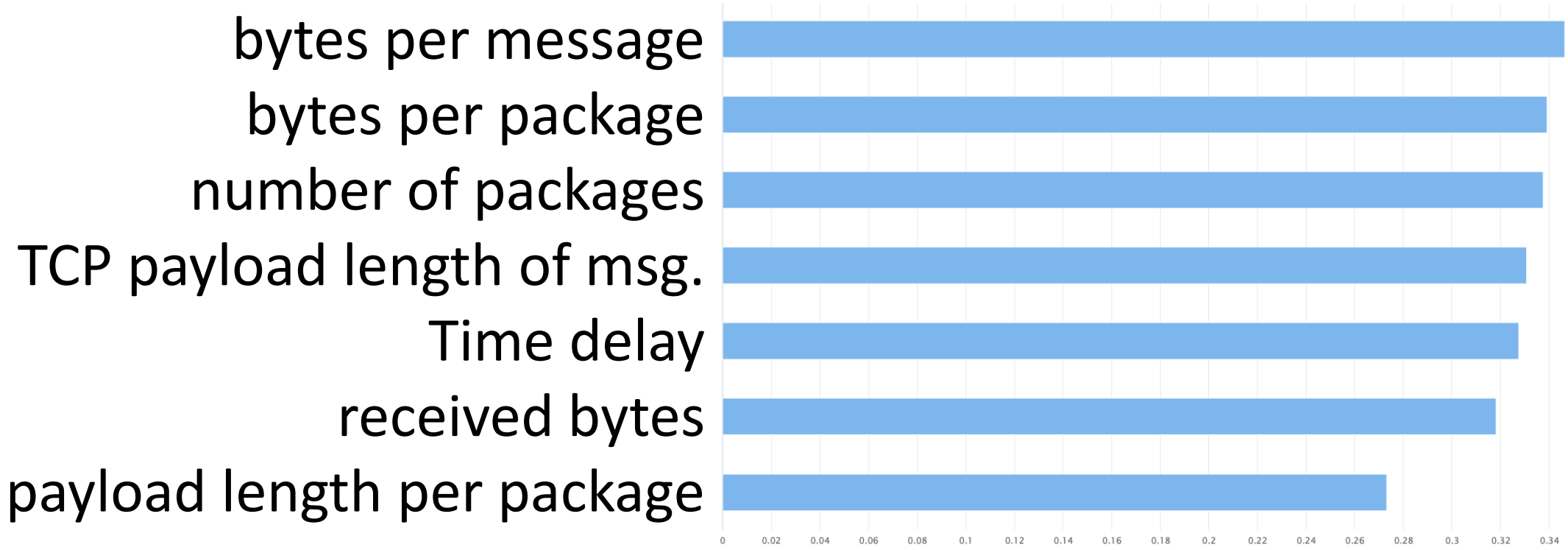
I Support Vector Machines

Hubert Schölnast

NATO OTAN

This workshop is supported by: The NATO Science for Peace and Security Programme

Deep learning found these features to be the most important:



Hubert Schölnast

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

Confusion matrix

prediction \ is really	A	B	C	D	E	F	G	class precision	
A	10	0	0	0	1	0	0	90,9%	Switching off
B	0	13	1	0	0	0	0	92,9%	Breaker status query
C	1	0	11	1	0	0	0	84,6%	Direct switching on
D	0	0	0	10	0	0	0	100,0%	Enabling to switch on
E	0	0	0	0	25	0	0	100,0%	Meter reading query
F	0	0	0	0	0	11	0	100,0%	Load profile query
G	0	0	0	0	0	0	5	100,0%	Parameterization
class recall	90,9%	100,0%	91,7%	90,9%	100,0%	100,0%	100,0%		

total accuracy: 95,5% of all packages correctly classified

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

Conclusion

- Types of message types can be clearly identified by machine learning although they are end-to-end encrypted
- A higher number of messages and a combination of machine learning approaches can increase accuracy to almost 100%
- “Normal” messages, which should theoretically make up 100% of all communication, will be recognized as such and can be ignored.
- All other messages will be reported to the operator
- Small devices performing this analysis of messages can be connected to the gateways, so operators will get informed about unusual traffic even if this traffic maybe don’t reach the HES directly.

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme

University of Applied Sciences
St. Pölten, Austria
Institute of Information
Security Research

UNIVERSITY OF APPLIED SCIENCES

Thank you very much
for your attention!

Dipl.-Ing. Hubert Schölnast, BSc

NATO OTAN
This workshop is supported by: The NATO Science for Peace and Security Programme