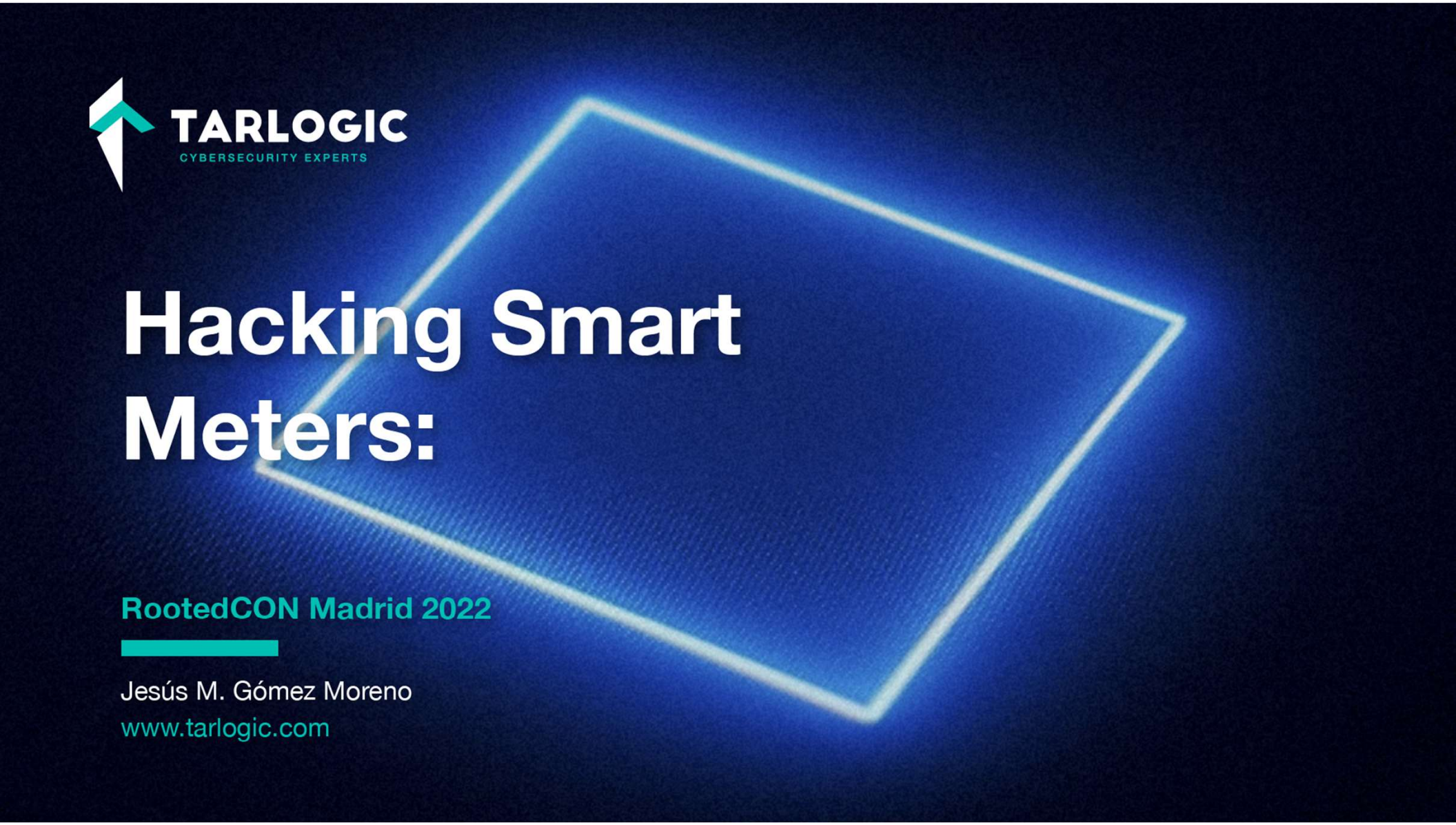
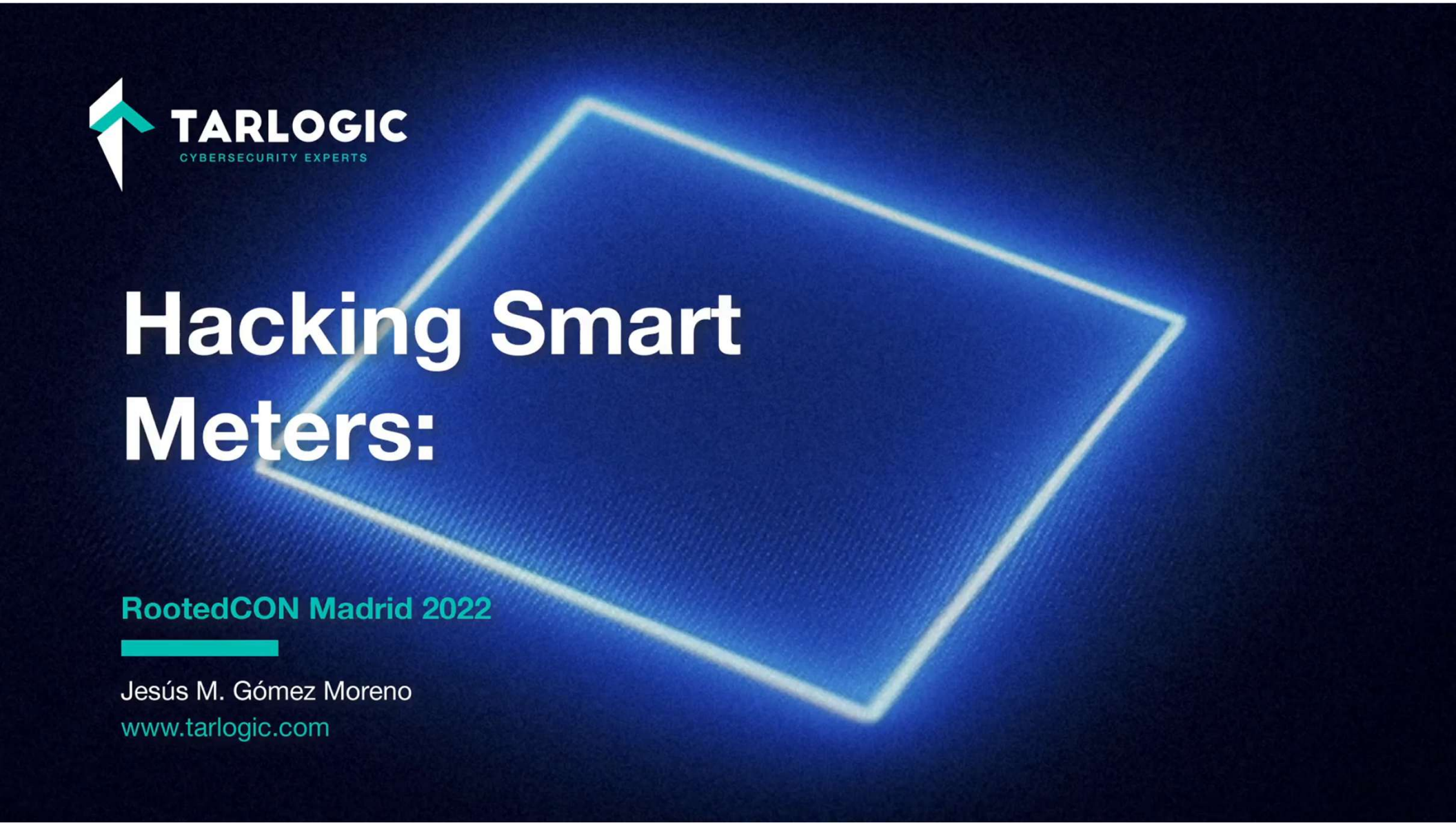


Jesús M. Gómez Moreno
www.tarlogic.com



Jesús M. Gómez Moreno
www.tarlogic.com

Hacking Smart Meters

www.tarlogic.com

Jesús M. Gómez Moreno

TARLOGIC
CYBERSECURITY EXPERTS

$ whoami

Jesús M. Gómez Moreno

@zus_999
jesus.gomez@tarlogic.com

#**Research Engineer** en Tarlogic Security

TARLOGIC
CYBERSECURITY EXPERTS

PRECEDENTS

Hindawi
Security and Communication Networks
Volume 2017, Article ID 7369684, 18 pages
https://doi.org/10.1155/2017/7369684

WILEY | Hindawi

Research Article

Cybersecurity Vulnerability Analysis of the PLC PRIME Standard

Miguel Seijo Simó, Gregorio López López, and José Ignacio Moreno Novella

Universidad Carlos III de Madrid, Madrid, Spain

Correspondence should be addressed to Miguel Seijo Simó; mseijo@it.uc3m.es

Received 20 February 2017; Accepted 18 May 2017; Published 5 July 2017

Academic Editor: Sherali Zeadally

Security in critical infrastructures such as the power grid is of vital importance. The Smart Grid puts power grid classical security approach on the ropes, since it introduces cyberphysical systems where devices, communications, and information systems must be protected. PoweRline Intelligent Metering Evolution (PRIME) is a Narrowband Power-Line Communications (NB-PLC) protocol widely used in the last mile of Advanced Metering Infrastructure (AMI) deployments, playing a key role in the Smart Grid. Therefore, this work aims to unveil the cybersecurity vulnerabilities present in PRIME standard, proposing solutions and validating and discussing the results obtained.

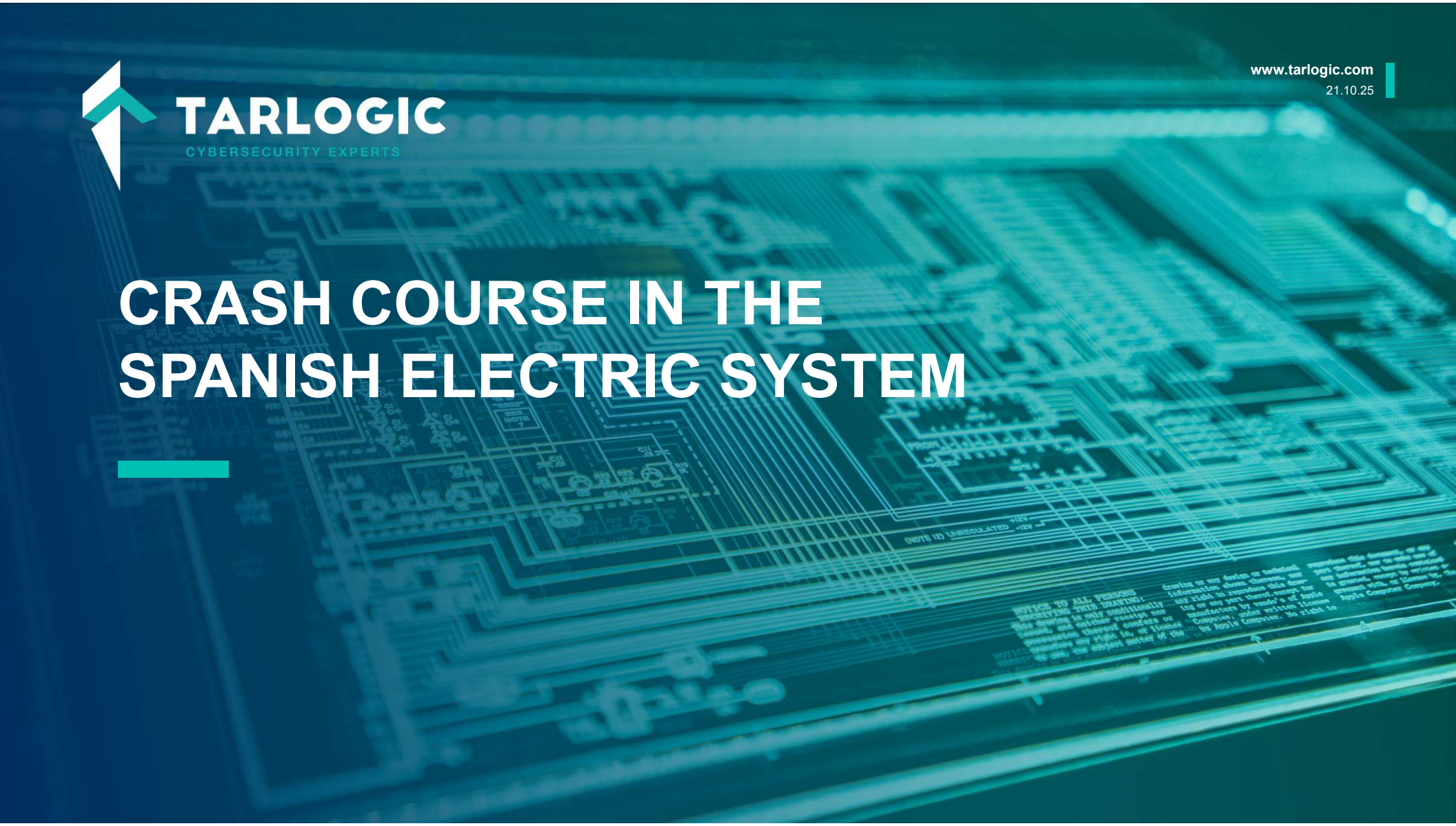
1. Introduction

with smart meters by 2018, which means a deployment of

TARLOGIC
CYBERSECURITY EXPERTS

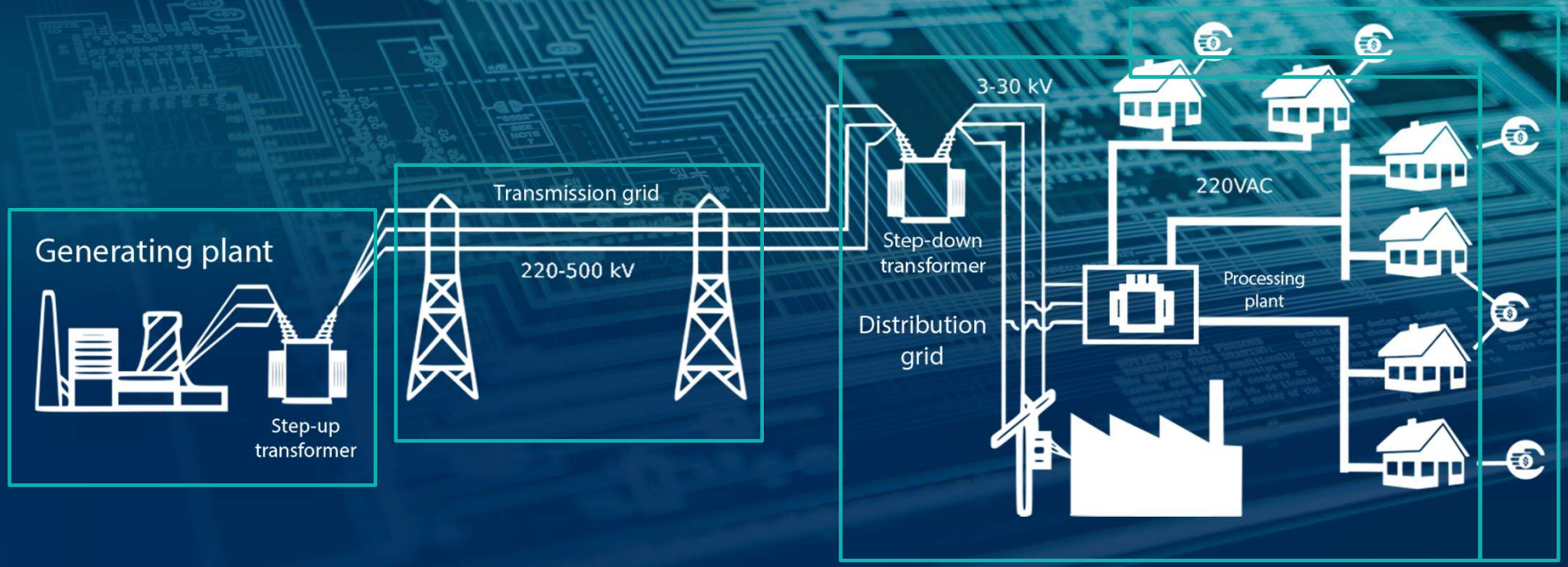
www.tarlogic.com
21.10.25

CRASH COURSE IN THE SPANISH ELECTRIC SYSTEM



ELECTRIC SYSTEM STAGES

GENERATION | **TRANSPORT** | **DISTRIBUTION** | **COMERCIALIZATION**



REMOTE MANAGEMENT

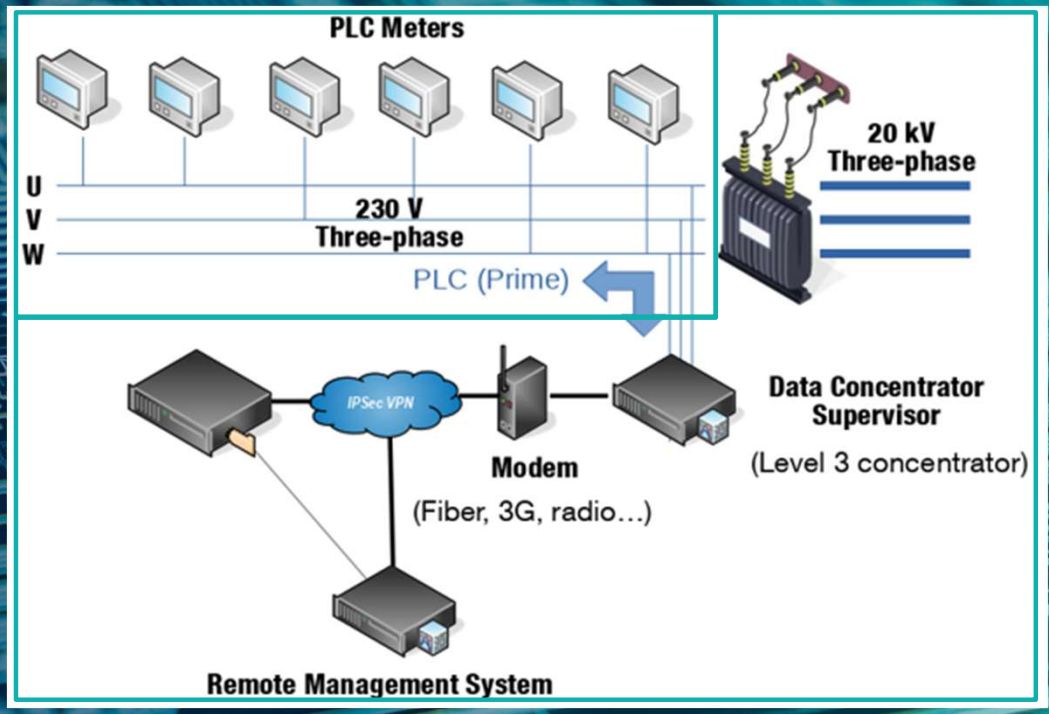
Point of Delivery

- PLC Meters

Electrical Transformation Plant

- Data Concentrator Supervisor

Remote Management Infrastructure
(customer type 5)



TARLOGIC
CYBERSECURITY EXPERTS

www.tarlogic.com
21.10.25

SMART METERS AND RELATED TOPICS

WHAT DO SMART METERS DO?

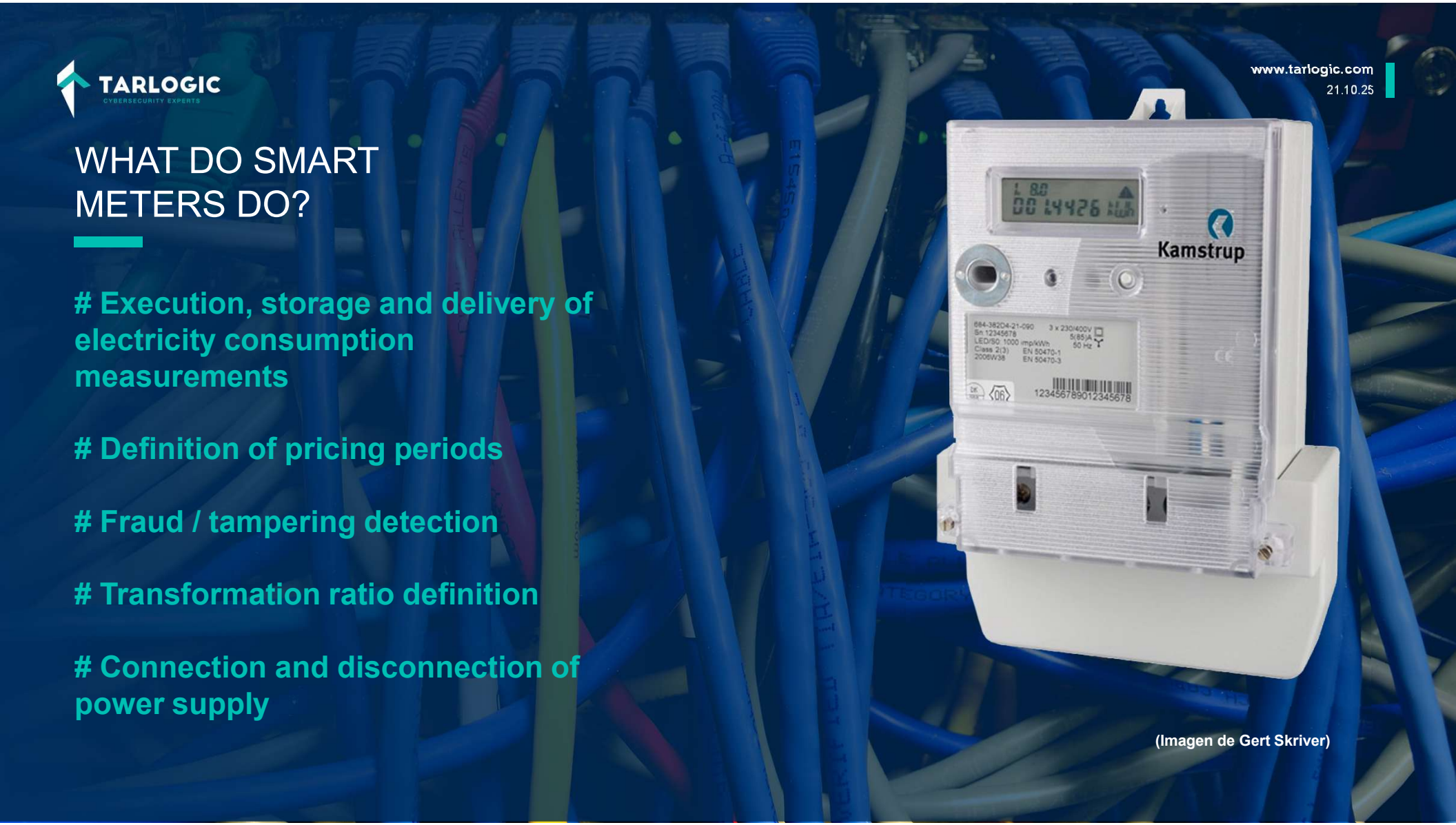
 # Execution, storage and delivery of electricity consumption measurements

 # Definition of pricing periods

 # Fraud / tampering detection

 # Transformation ratio definition

 # Connection and disconnection of power supply



(Imagen de Gert Skriver)

POWER LINE COMMUNICATION

 # (Almost) Star network
- Meters connected to a central data concentrator (DC)

 # In Europe: CENELEC bands
- CENELEC A: 35 to 91 kHz
- CENELEC B: 98 to 122 kHz

 # Different communication protocols (MAC layer)
- PRIME
- G3
- Meters and More

 # Application layer protocols
- DLMS/COSEM

APPLICATION

PHY/MAC

TARLOGIC
CYBERSECURITY EXPERTS

www.tarlogic.com
21.10.25

THE PRIME STANDARD

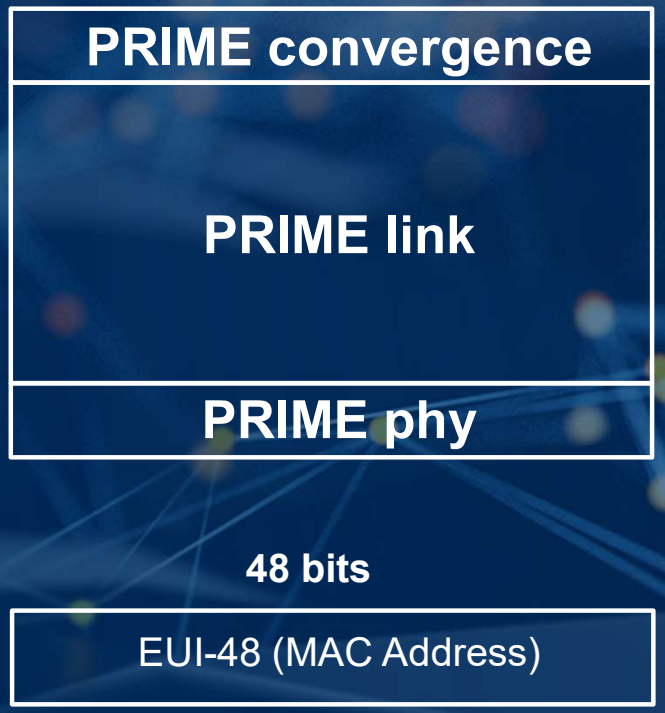
PRIME SUBLAYERS

 # Convergence layer

 # Overpowered MAC layer (LINK)

- MAC headers with CRC32
- Association between meters and DCs
- Connections for data multiplexion
- 48-bit MAC addresses (EUI-48)
- Local network addressing

 # Physical layer (PHY)



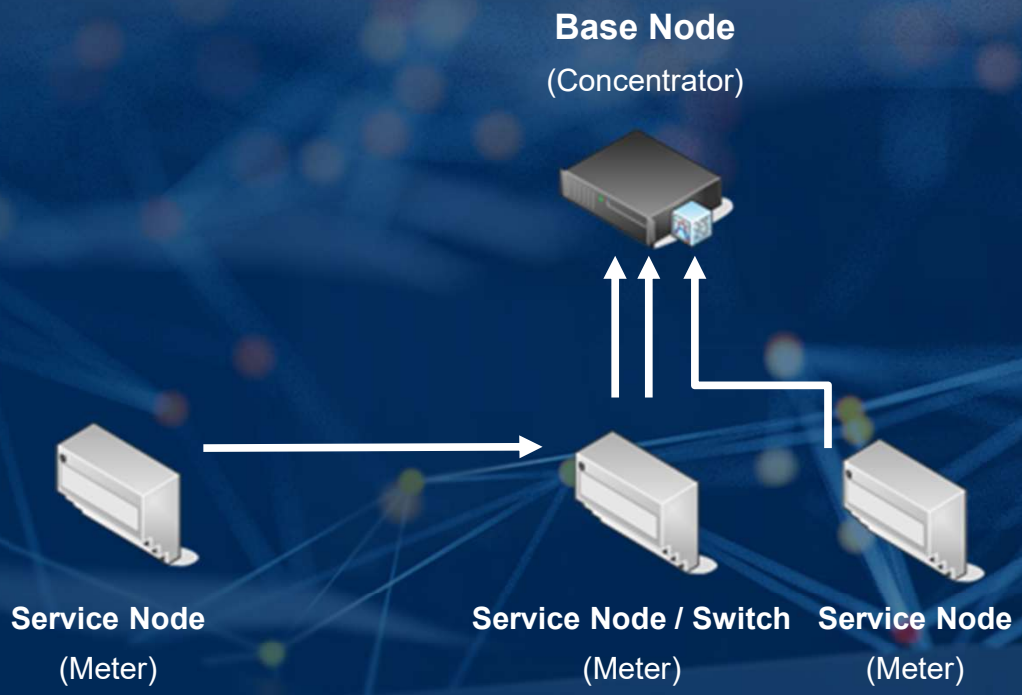
PRIME NODES

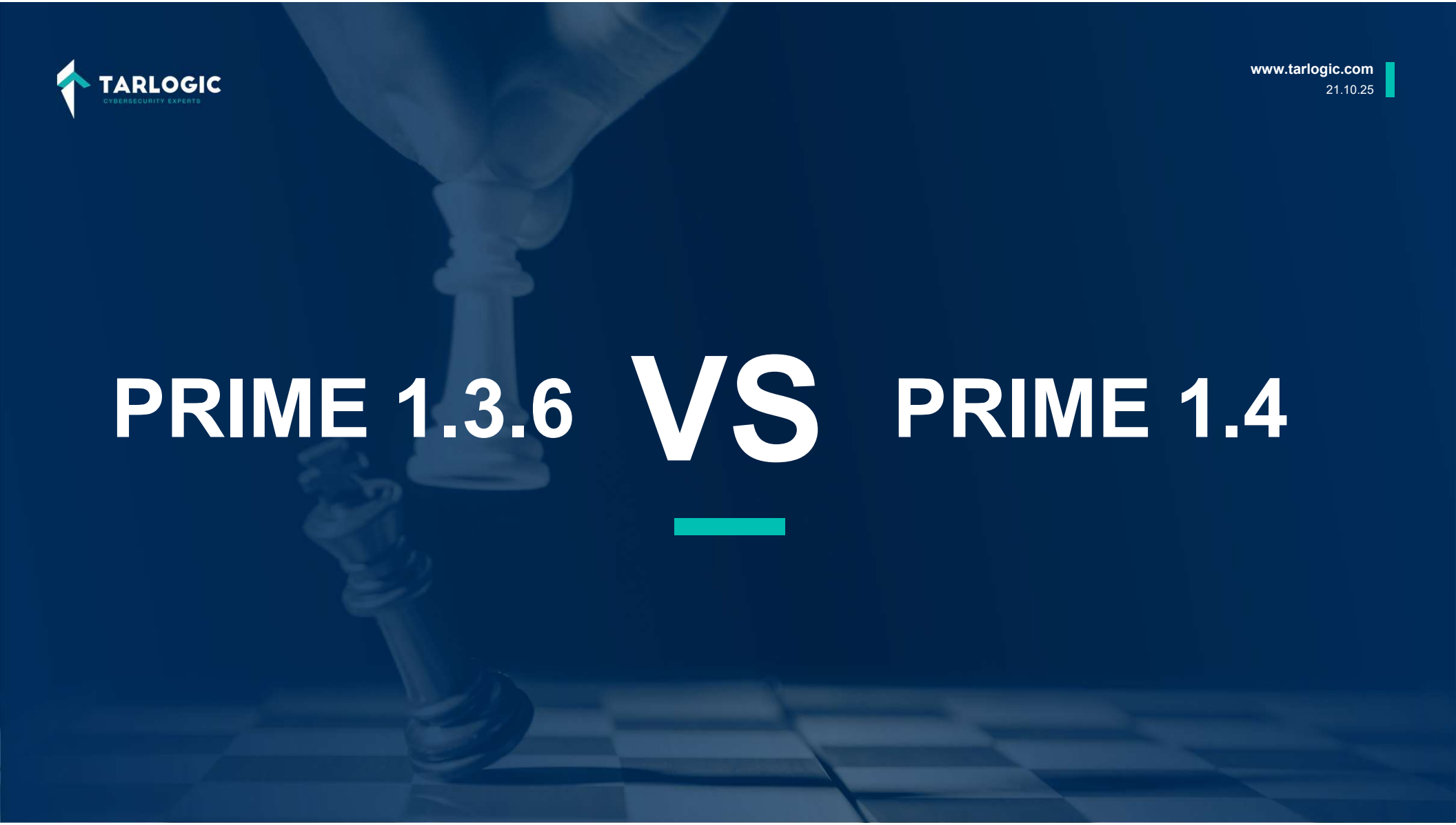
 # Two types of nodes

- Base node
- Service node

 # If a service node doesn't reach the base node, a promotion is requested

- A service node is promoted to switch
- A service node uses a switch as a repeater to reach the base node





PRIME 1.3.6 VS PRIME 1.4


TARLOGIC
CYBERSECURITY EXPERTS
www.tarlogic.com
21.10.25
DLMS/COSEM

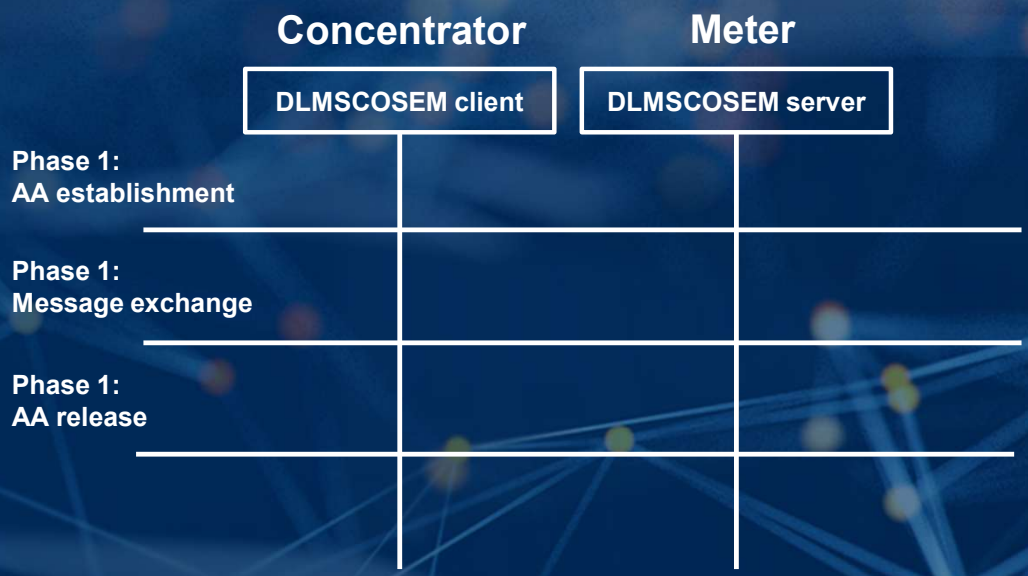
DLMS/COSEM

Client – Server architecture

- The client is the concentrator
- The server is the meter

Connection oriented operation

- AA is the name given to a connection
- After the messages have been exchanged, the connection is released



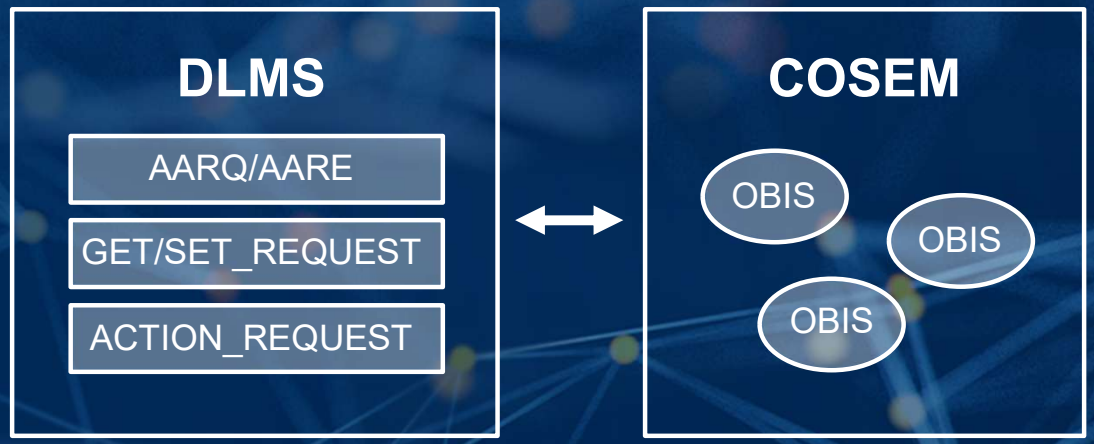
DLMS/COSEM

DLMS: Object-oriented message passing

- AARQ: Application Association Request
- GET_REQUEST / SET_REQUEST
- ACTION_REQUEST

COSEM: Object model

- Objects representing features of the meter
- Instances identified by OBIS (OBject Identification System) code




TARLOGIC
CYBERSECURITY EXPERTS
www.tarlogic.com
21.10.25
SECURITY IN PRIME AND DLMS/COSEM

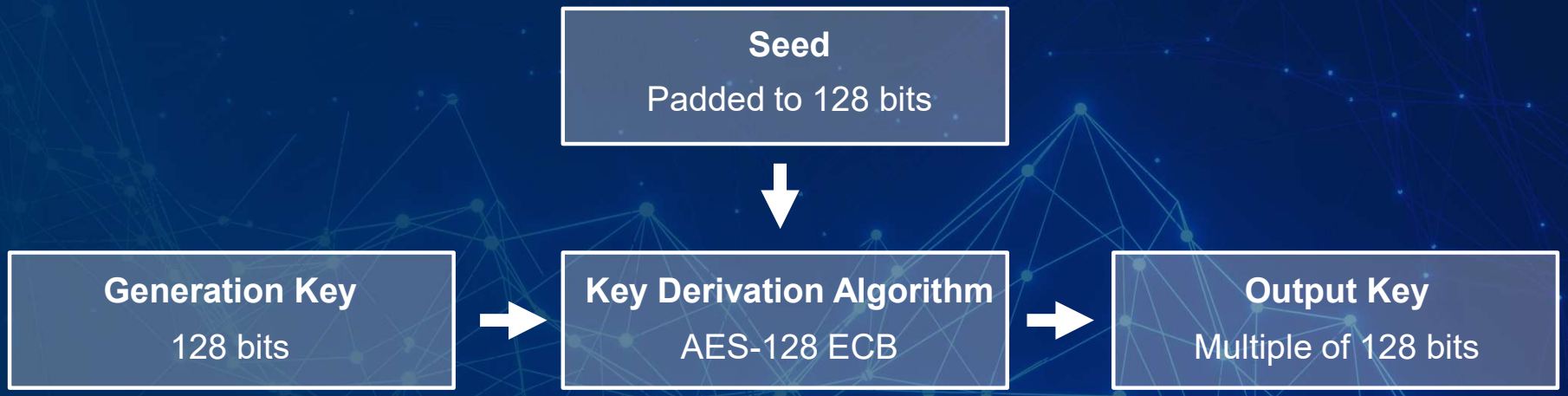
SECURITY IN PRIME 1.3.6

Two security profiles

- Profile 0 (no security)
  - No security at all, used in test deployments
- Profile 1 (basic security)
  - Some degree of information security, with partial encryption and secure CRC
  - Equivalent to no security if you can impersonate the DC

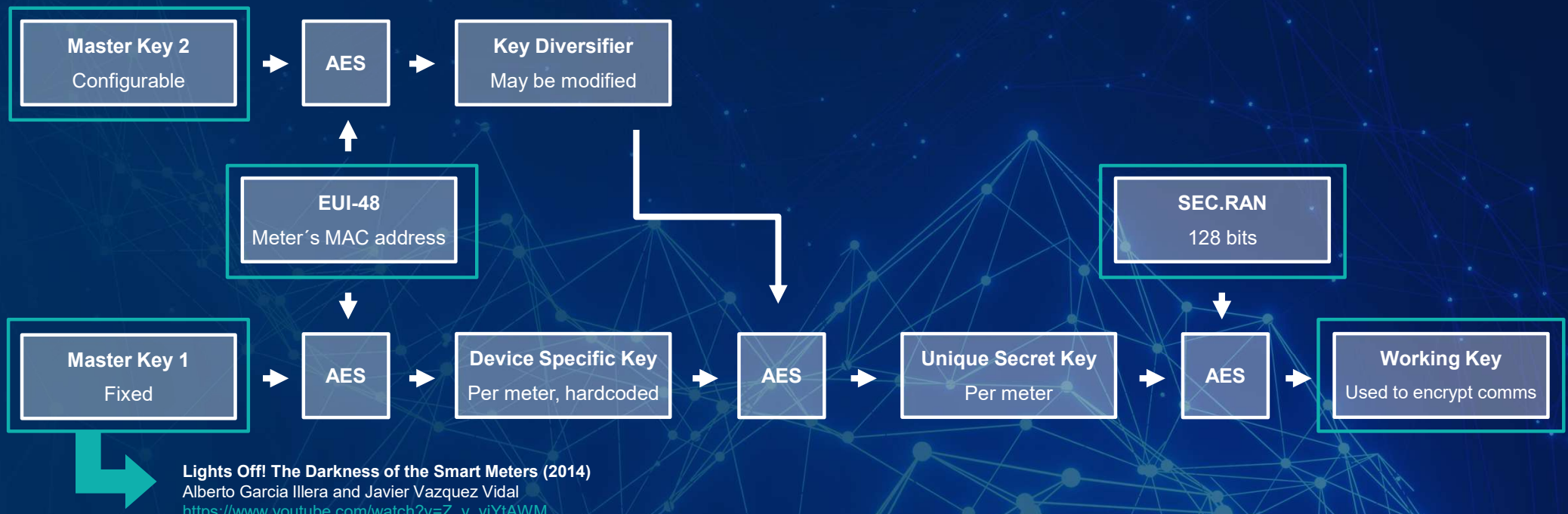
PROFILE 1 IS NOT AN OPTION

Key derivation



PROFILE 1 IS NOT AN OPTION

Key derivation



Lights Off! The Darkness of the Smart Meters (2014)
Alberto Garcia Illera and Javier Vazquez Vidal
https://www.youtube.com/watch?v=Z_y_vjYtAWM

SECURITY IN PRIME 1.4

No backwards compatibility with 1.3.6

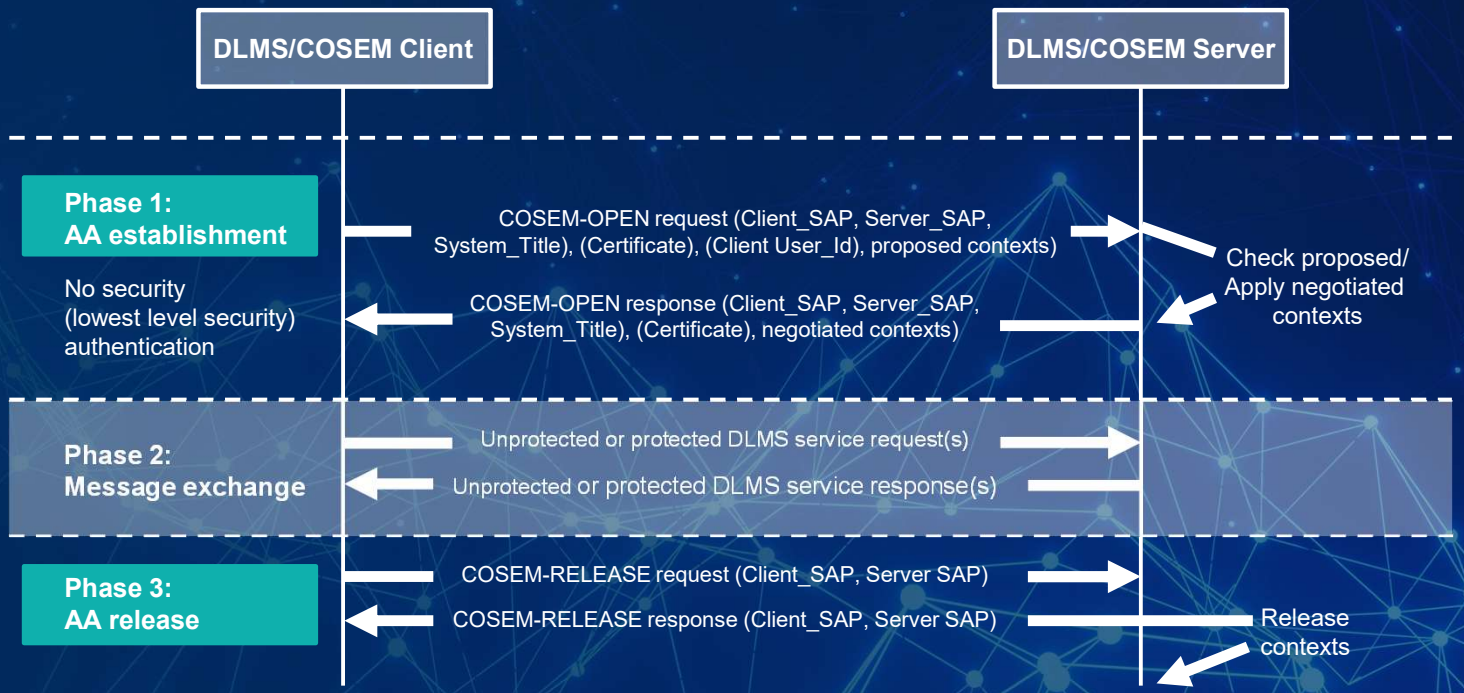
- Attempt to solve PRIME 1.3.6 security issues.
- Old devices will not be compatible.
  - Not all manufacturers implement it.
- New key derivation scheme (**incompatible** too with PRIME 1.3.6)

Three security levels

- Additional profile: Profile 2
  - Encrypts more frames than Profile 1.3.6

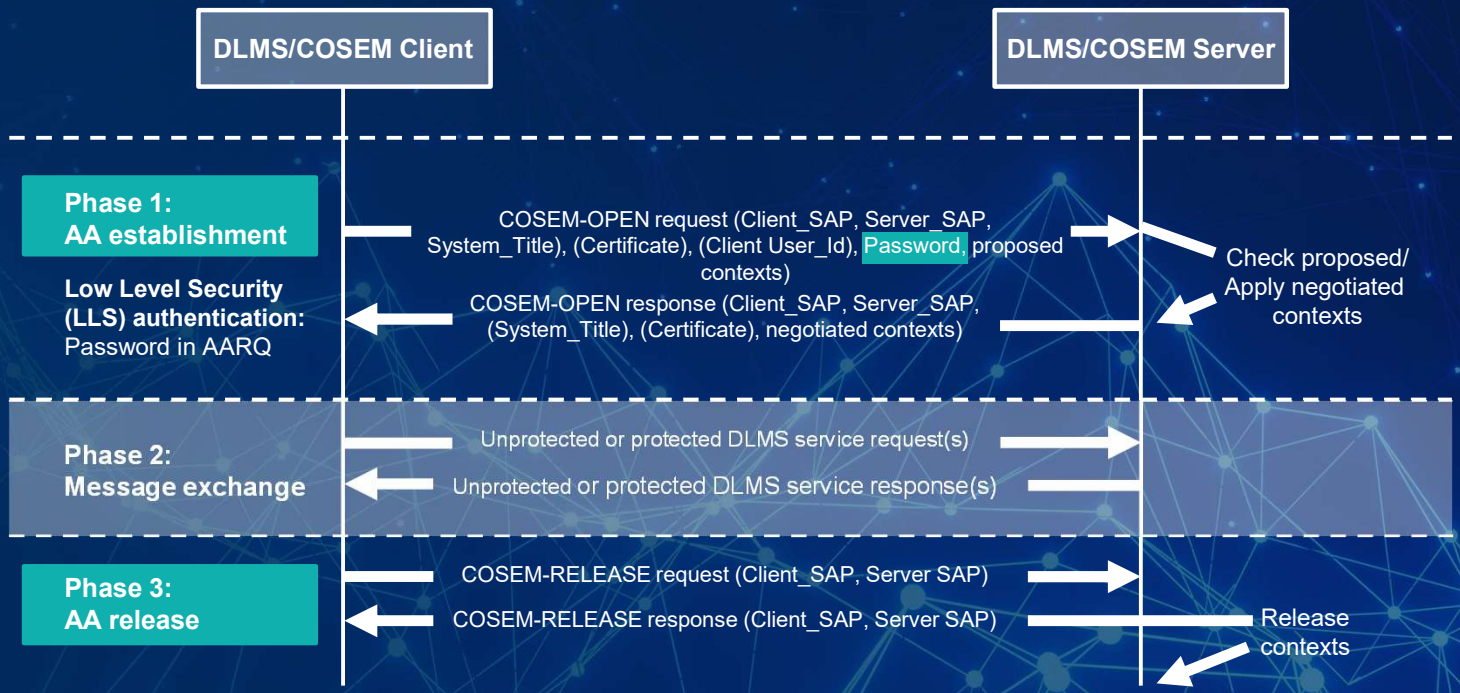
SECURITY IN DMLS

Lowest Level Security



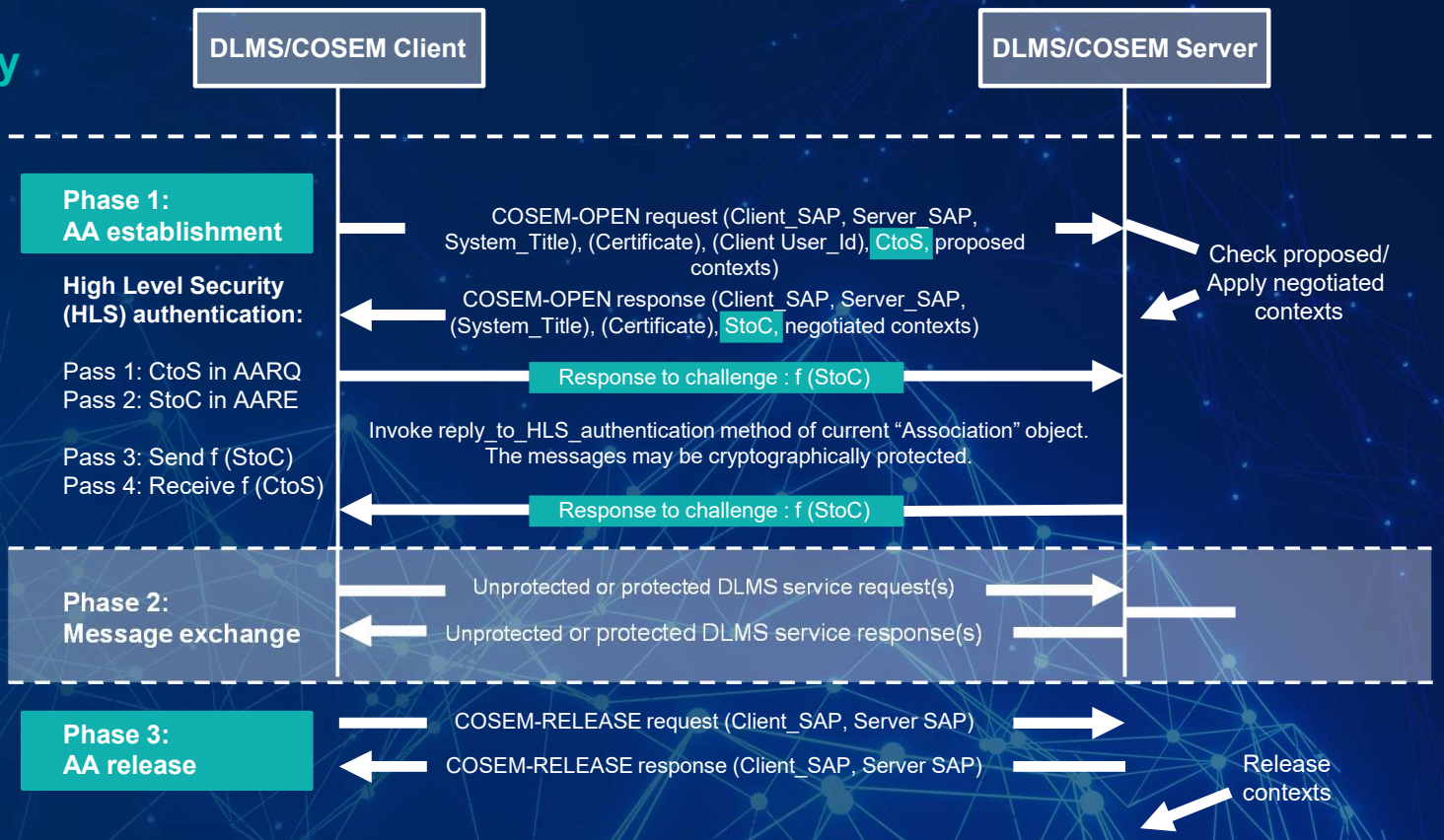
SECURITY IN DMLS

Low Level Security



SECURITY IN DMLS

High Level Security



TARLOGIC
CYBERSECURITY EXPERTS

CURRENT SITUATION

SECURITY IN ACTUAL METERS

 # All of this doesn't matter because every PRIME network observed so far uses…

PRIME 1.3.6 PROFILE 0 (no security)

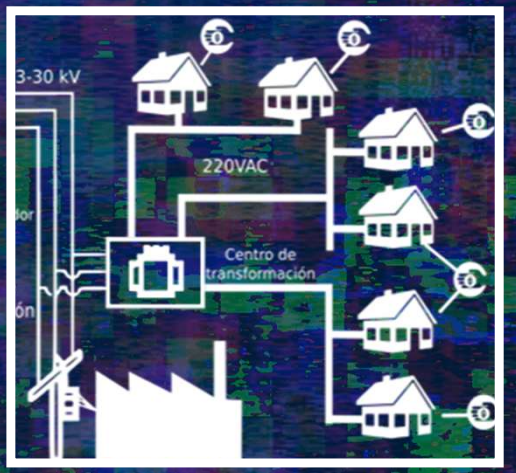
AND

DLMS Low Level Security (cleartext authentication)

JUST UPDATE SECURITY?

 # Updating security configuration is not so simple…

- To update PRIME version, new hardware is needed
- Compatibility must be preserved in the network
- Compatibility must be preserved between meters
- Compatibility must be preserved between concetrators and meters



MORE PROBLEMS

Until now

- Measurements should be taken hourly and be stored for a month

New EU regulations

- Measurements should be taken every 15 minutes
- Measurements should stored for a month
- Measurements should be read every day from management servers
- **Many current meters have capacity for only 16 days**
- **PRIME 1.3.6: CENELEC A (35 to 91 kHz) and CENELEC B (98 to 122 kHz)**
- **Not enough bandwidth for daily recovery of measurements**
- **Due to the noise, many packets are lost**

MORE PROBLEMS

PRIME 1.4 Meters

- Reaches up to 500 kHz
- Allows for an improved measurement recovery rate and is less sensitive to noise
- Increased memory to store required measurements

PRIME 1.4 Challenges

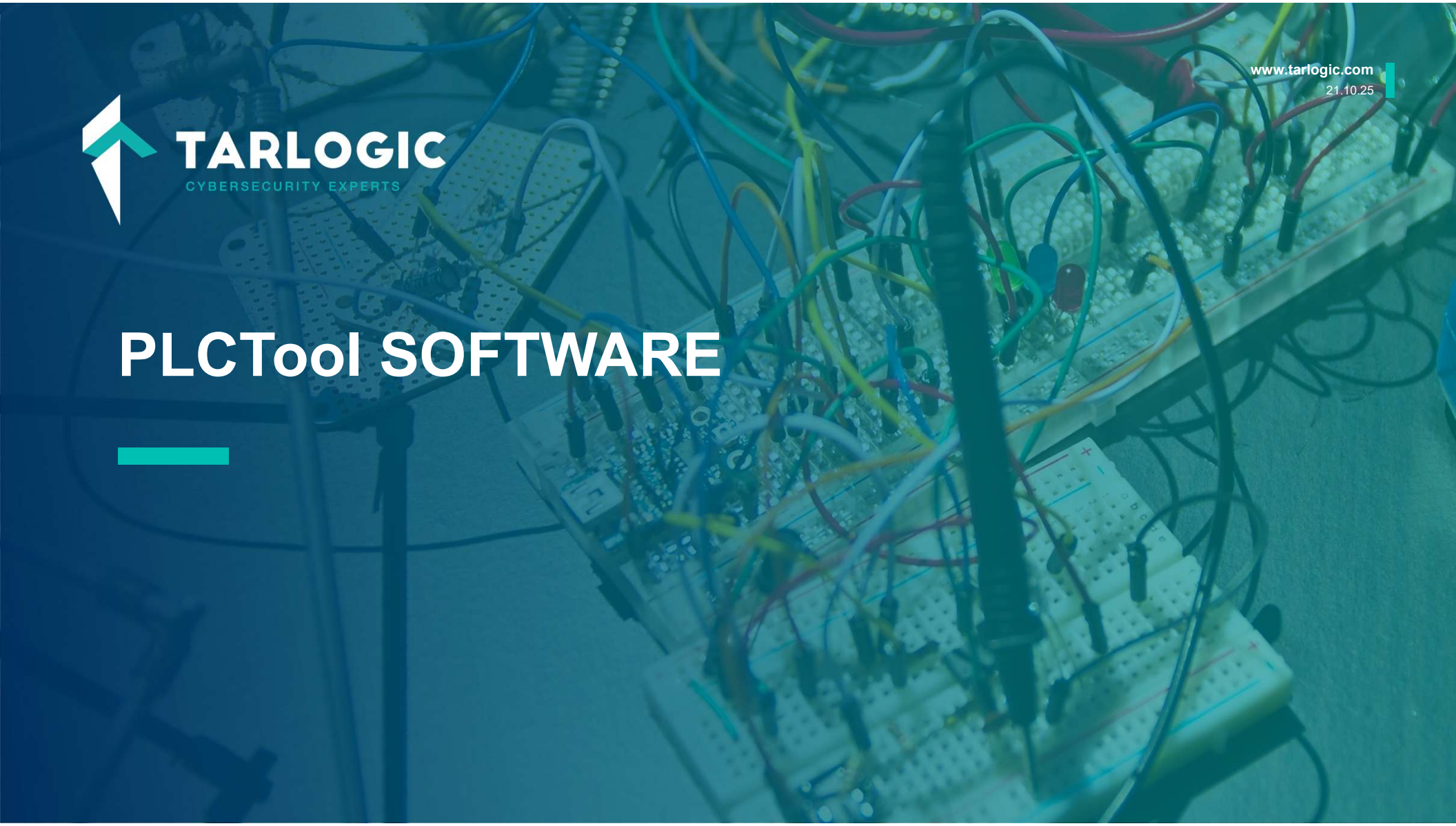
- Due to differences in bandwidth, **PRIME 1.3.6 and PRIME 1.4 are incompatible**
- **Heavily regularized and slow market**
- **Currently, only six manufacturers**:
  - Circutor, Sagem, Elsewedy, ZIV, ORBIS and LANDIS

MORE PROBLEMS

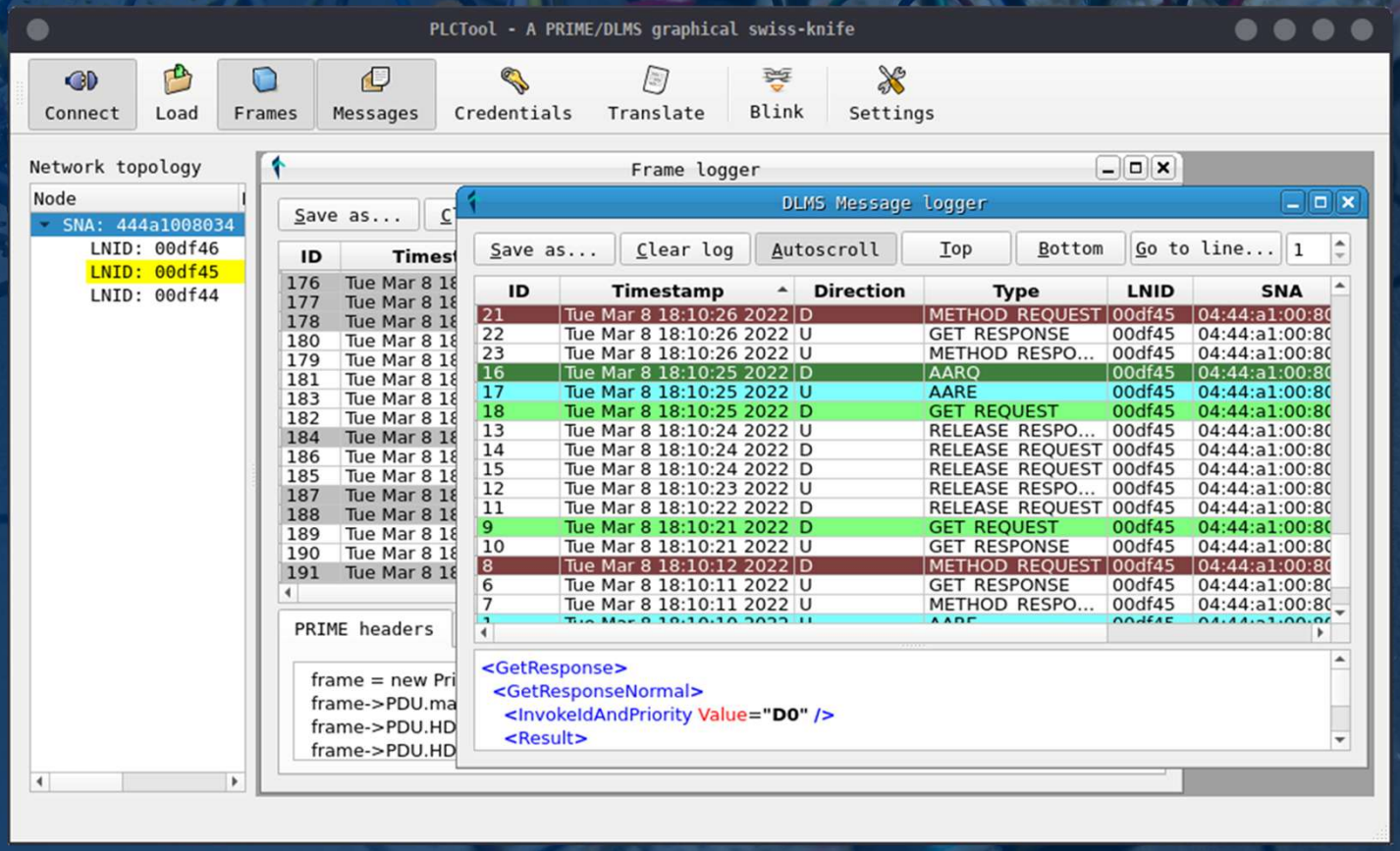
Meters are still not available

- Tests are still being run to allow PRIME 1.3.6 and PRIME 1.4 to work together using bridges
- PRIME 1.4 Meters are not yet on the market

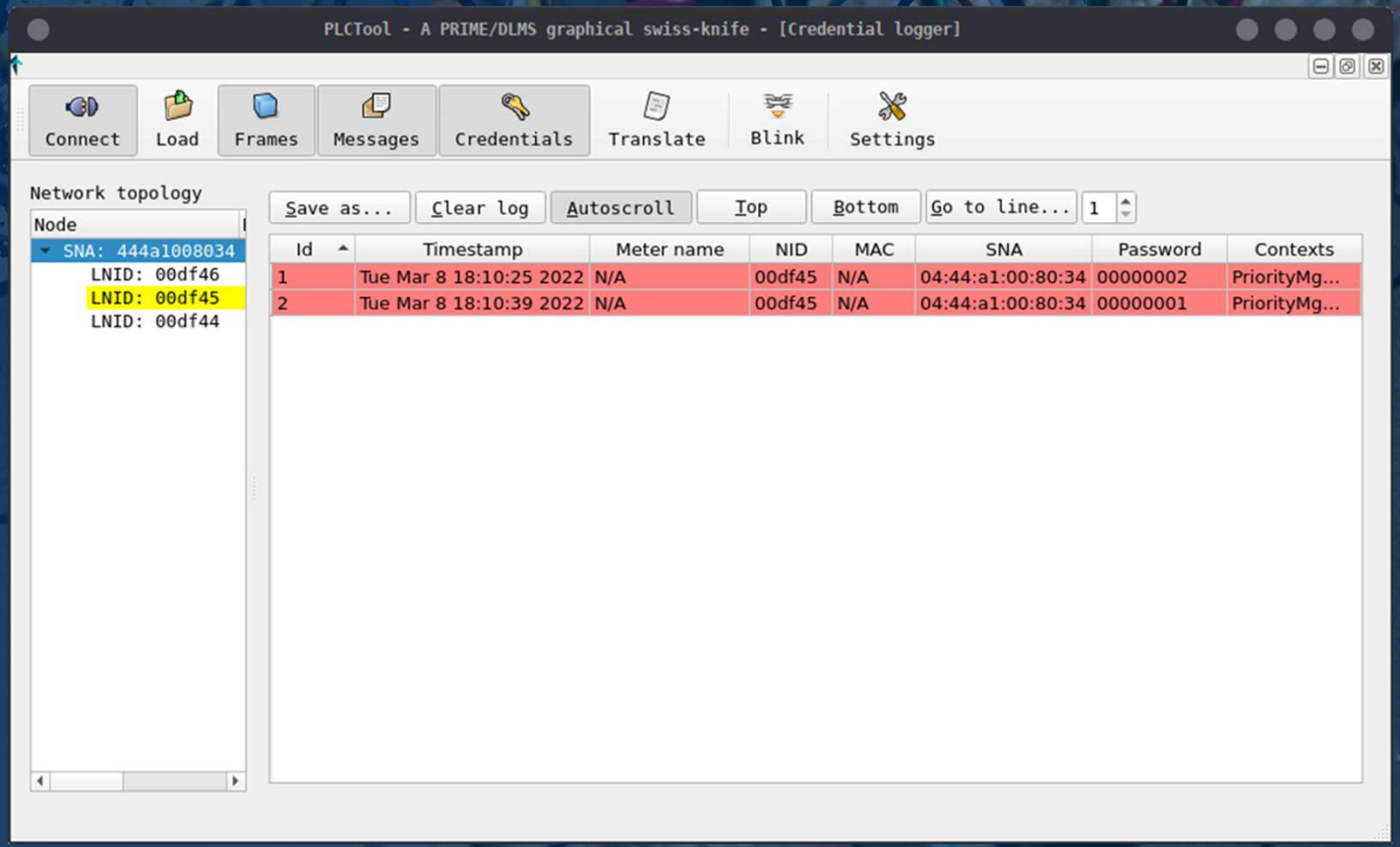
COULD TAKE YEARS TO RENEW


TARLOGIC
CYBERSECURITY EXPERTS
www.tarlogic.com
21.10.25
PLCTool SOFTWARE

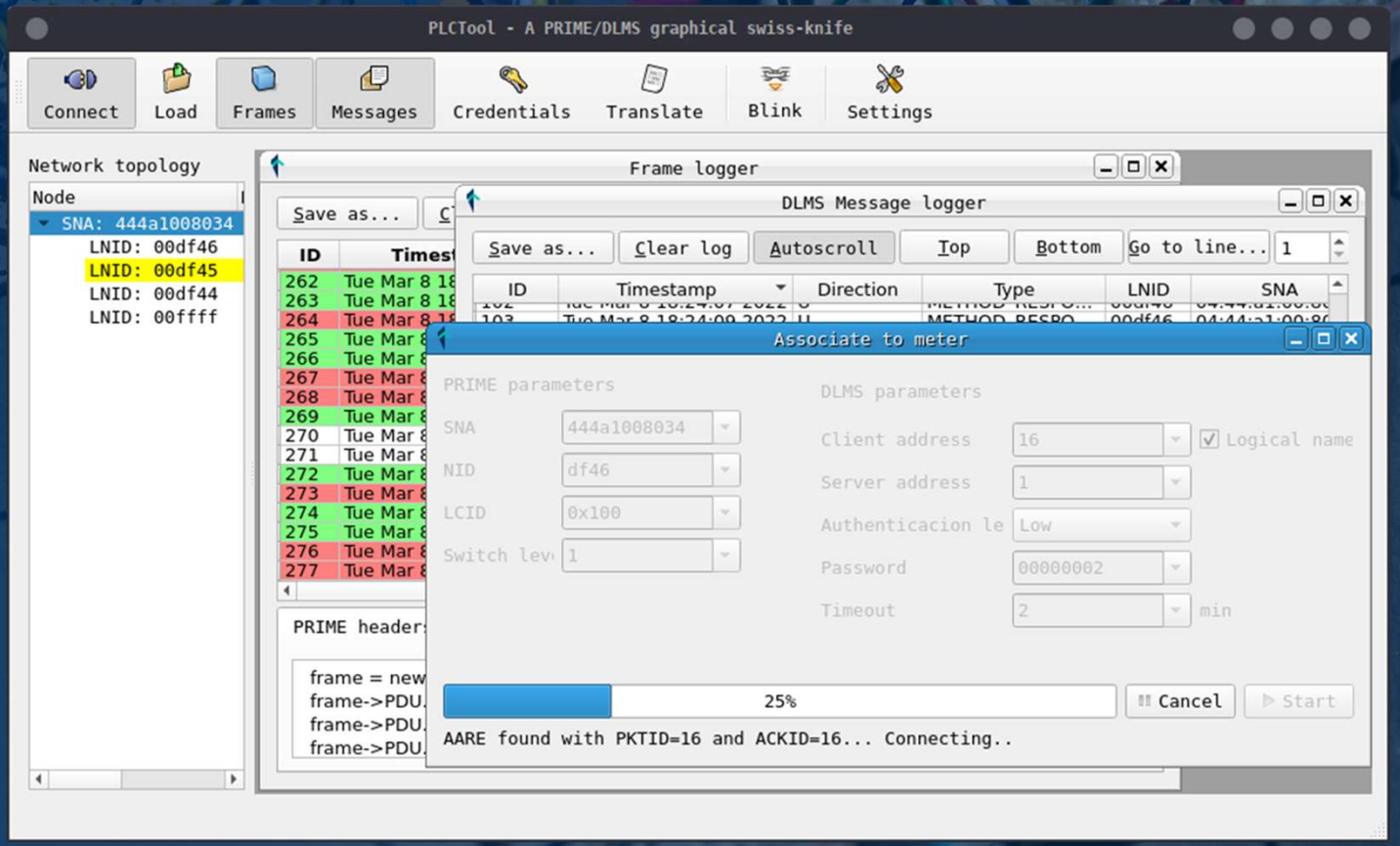
THE TOOL


PLCTool - A PRIME/DLMS graphical swiss-knife
Connect
Load
Frames
Messages
Credentials
Translate
Blink
Settings
Network topology
Node
SNA: 444a1008034
LNID: 00df46
LNID: 00df45
LNID: 00df44
Frame logger
Save as...
ID
Timest
176 Tue Mar 8 18
177 Tue Mar 8 18
178 Tue Mar 8 18
180 Tue Mar 8 18
179 Tue Mar 8 18
181 Tue Mar 8 18
183 Tue Mar 8 18
182 Tue Mar 8 18
184 Tue Mar 8 18
186 Tue Mar 8 18
185 Tue Mar 8 18
187 Tue Mar 8 18
188 Tue Mar 8 18
189 Tue Mar 8 18
190 Tue Mar 8 18
191 Tue Mar 8 18
PRIME headers
frame = new Pri
frame->PDU.ma
frame->PDU.HD
frame->PDU.HD
DLMS Message logger
Save as...
Clear log
Autoscroll
Top
Bottom
Go to line...
1
ID
Timestamp
Direction
Type
LNID
SNA
21 Tue Mar 8 18:10:26 2022 D METHOD_REQUEST 00df45 04:44:a1:00:80
22 Tue Mar 8 18:10:26 2022 U GET RESPONSE 00df45 04:44:a1:00:80
23 Tue Mar 8 18:10:26 2022 U METHOD RESPO... 00df45 04:44:a1:00:80
16 Tue Mar 8 18:10:25 2022 D AARQ 00df45 04:44:a1:00:80
17 Tue Mar 8 18:10:25 2022 U AARE 00df45 04:44:a1:00:80
18 Tue Mar 8 18:10:25 2022 D GET REQUEST 00df45 04:44:a1:00:80
13 Tue Mar 8 18:10:24 2022 U RELEASE RESPO... 00df45 04:44:a1:00:80
14 Tue Mar 8 18:10:24 2022 D RELEASE REQUEST 00df45 04:44:a1:00:80
15 Tue Mar 8 18:10:24 2022 D RELEASE REQUEST 00df45 04:44:a1:00:80
12 Tue Mar 8 18:10:23 2022 U RELEASE RESPO... 00df45 04:44:a1:00:80
11 Tue Mar 8 18:10:22 2022 D RELEASE REQUEST 00df45 04:44:a1:00:80
9 Tue Mar 8 18:10:21 2022 D GET REQUEST 00df45 04:44:a1:00:80
10 Tue Mar 8 18:10:21 2022 U GET RESPONSE 00df45 04:44:a1:00:80
8 Tue Mar 8 18:10:12 2022 D METHOD_REQUEST 00df45 04:44:a1:00:80
6 Tue Mar 8 18:10:11 2022 U GET RESPONSE 00df45 04:44:a1:00:80
7 Tue Mar 8 18:10:11 2022 U METHOD RESPO... 00df45 04:44:a1:00:80
<GetResponse>
<GetResponseNormal>
<InvokeIdAndPriority Value="D0" />
<Result>

THE TOOL


PLCTool - A PRIME/DLMS graphical swiss-knife - [Credential logger]
Connect
Load
Frames
Messages
Credentials
Translate
Blink
Settings
Network topology
Node
SNA: 444a1008034
LNID: 00df46
LNID: 00df45
LNID: 00df44
Save as...
Clear log
Autoscroll
Top
Bottom
Go to line...
1
Id
Timestamp
Meter name
NID
MAC
SNA
Password
Contexts
1
Tue Mar 8 18:10:25 2022
N/A
00df45
N/A
04:44:a1:00:80:34
00000002
PriorityMg...
2
Tue Mar 8 18:10:39 2022
N/A
00df45
N/A
04:44:a1:00:80:34
00000001
PriorityMg...

THE TOOL


PLCTool - A PRIME/DLMS graphical swiss-knife
Connect
Load
Frames
Messages
Credentials
Translate
Blink
Settings
Network topology
Node
SNA: 444a1008034
LNID: 00df46
LNID: 00df45
LNID: 00df44
LNID: 00ffff
Frame logger
Save as...
ID
Timest
262 Tue Mar 8 18
263 Tue Mar 8 18
264 Tue Mar 8 18
265 Tue Mar 8
266 Tue Mar 8
267 Tue Mar 8
268 Tue Mar 8
269 Tue Mar 8
270 Tue Mar 8
271 Tue Mar 8
272 Tue Mar 8
273 Tue Mar 8
274 Tue Mar 8
275 Tue Mar 8
276 Tue Mar 8
277 Tue Mar 8
PRIME header
frame = new
frame->PDU
frame->PDU
frame->PDU
DLMS Message logger
Save as...
Clear log
Autoscroll
Top
Bottom
Go to line...
1
ID
Timestamp
Direction
Type
LNID
SNA
Associate to meter
PRIME parameters
SNA
444a1008034
NID
df46
LCID
0x100
Switch lev
1
DLMS parameters
Client address
16
Logical name
Server address
1
Authenticacion le
Low
Password
00000002
Timeout
2
min
25%
Cancel
Start
AARE found with PKTID=16 and ACKID=16... Connecting..

FEATURES

Saves and loads previous captures

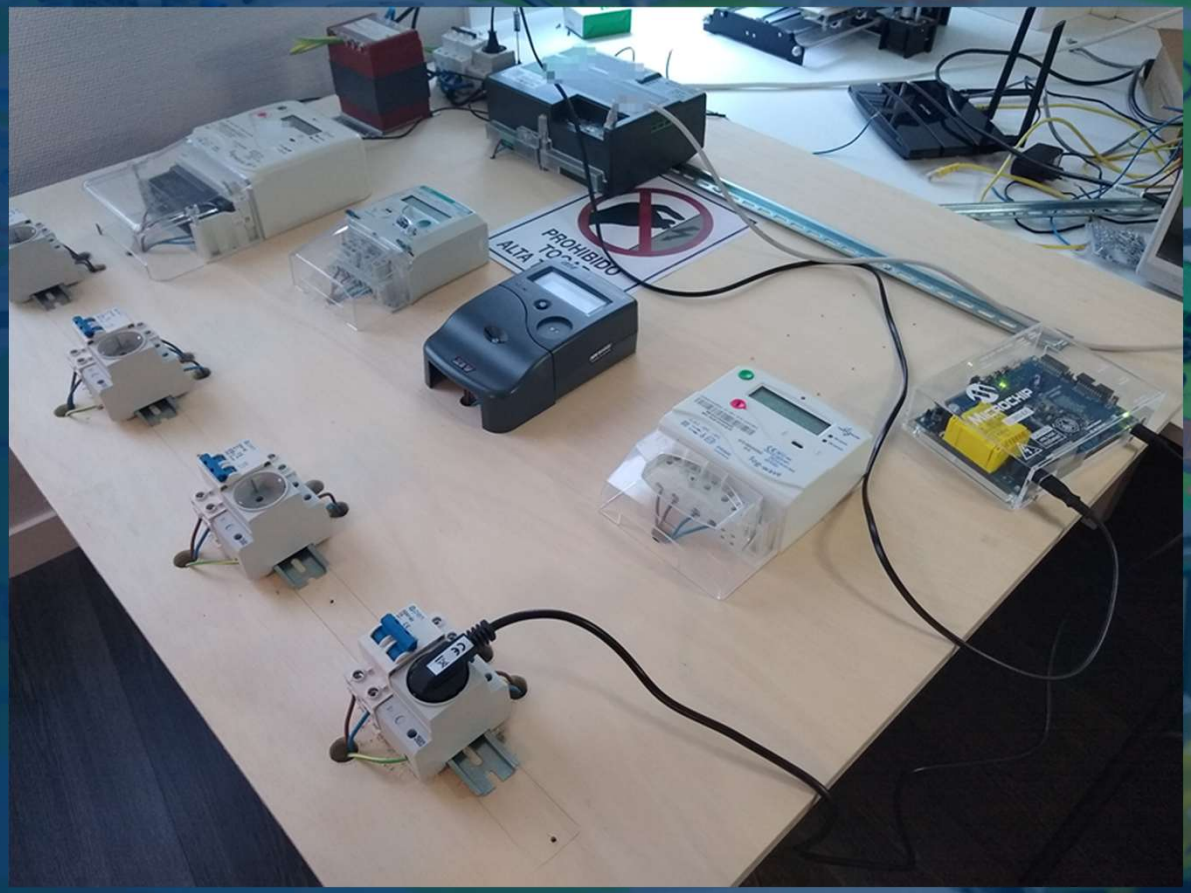
Modular design to implement new attacks and features

Basic attacks implemented

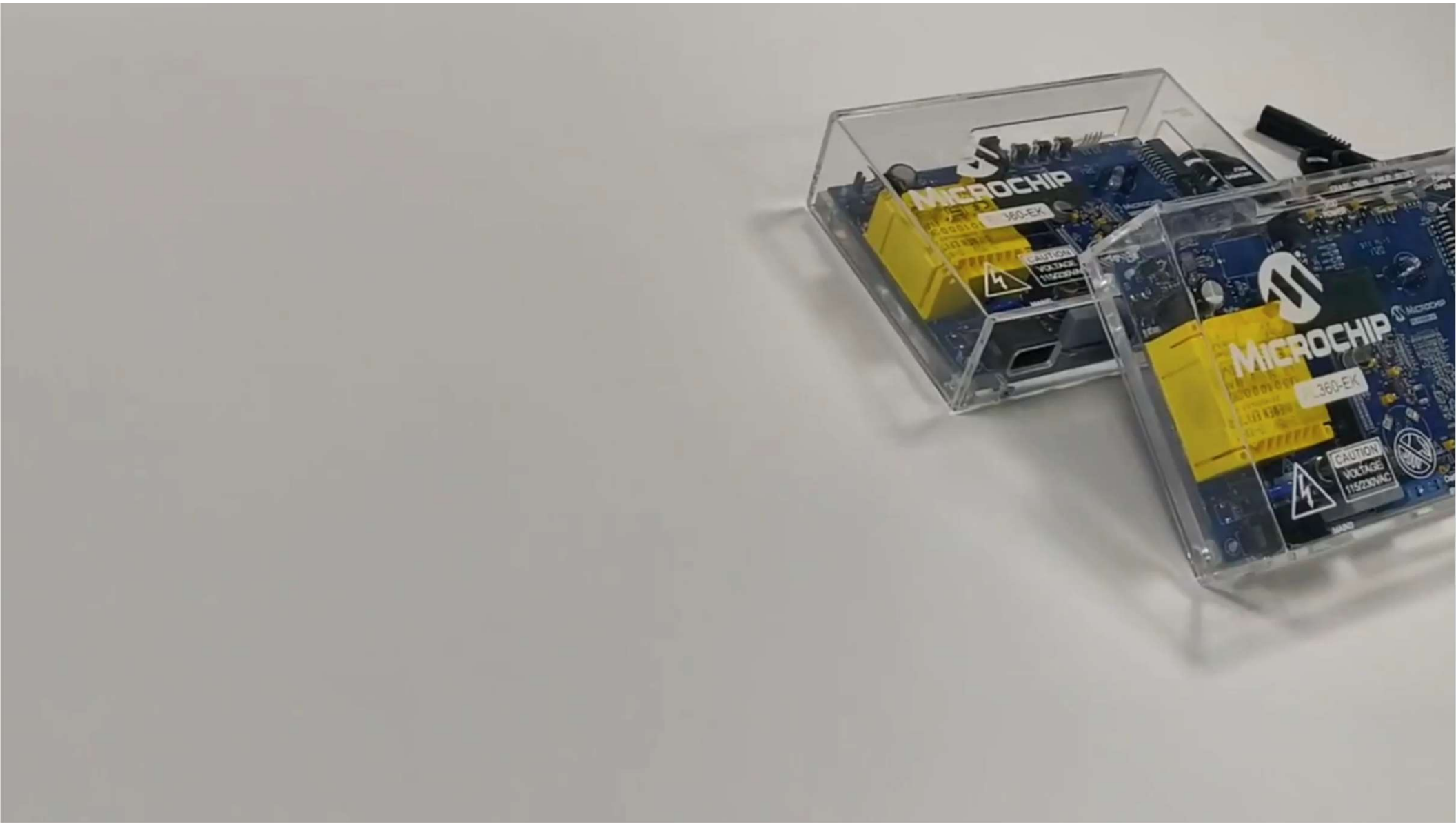
- Turning lights on and off
- Limiting power consumption
- Capturing credentials


TARLOGIC
CYBERSECURITY EXPERTS
www.tarlogic.com
21.10.25
TIME TO PLAY

DEMO



DEVELOPMENT KITS


MICROCHIP
MICROCHIP
CAUTION
VOLTAGE
115/230VAC