STORMSHIELD

Network Endpoint Data

Who am I

Davide **Pala**

Presales Stormshield

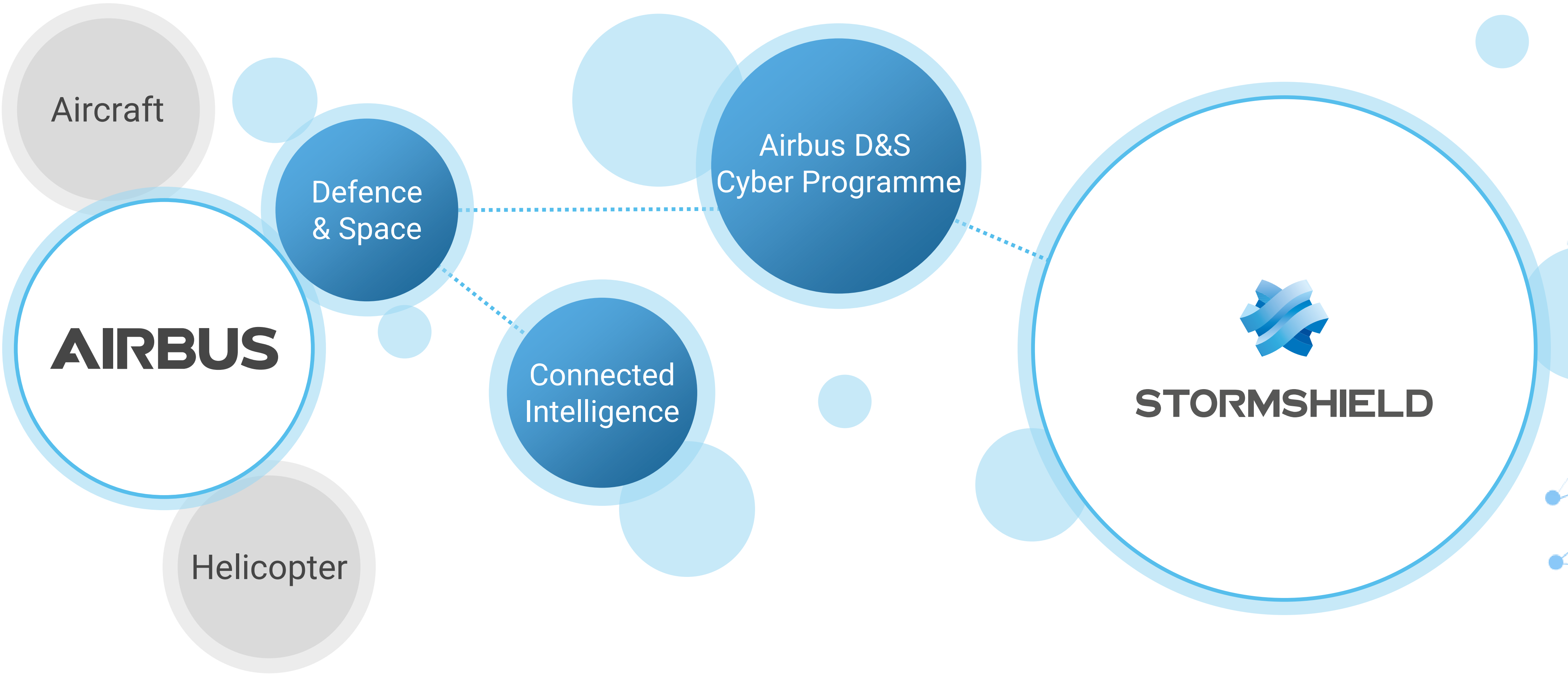
Cybersecurity passionate
and Cyber Saiyan co-founder

davide.pala@stormshield.eu

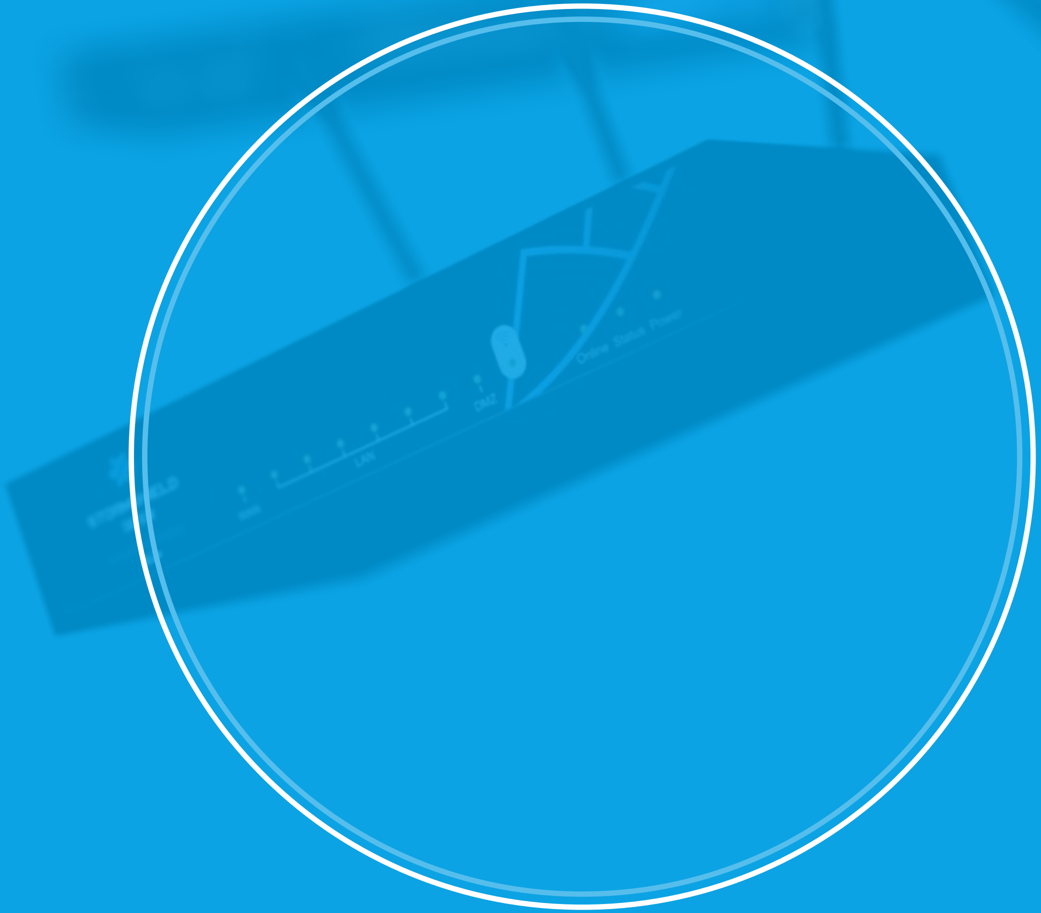
War in cyberspace

How to choose efficient OT cybersecurity solution using IEC 61850 power substations as an example

Subsidiary of Europe's greatest industrial success story



Our **solutions**



Stormshield

Network Security

A range of next generation firewalls & VPNs

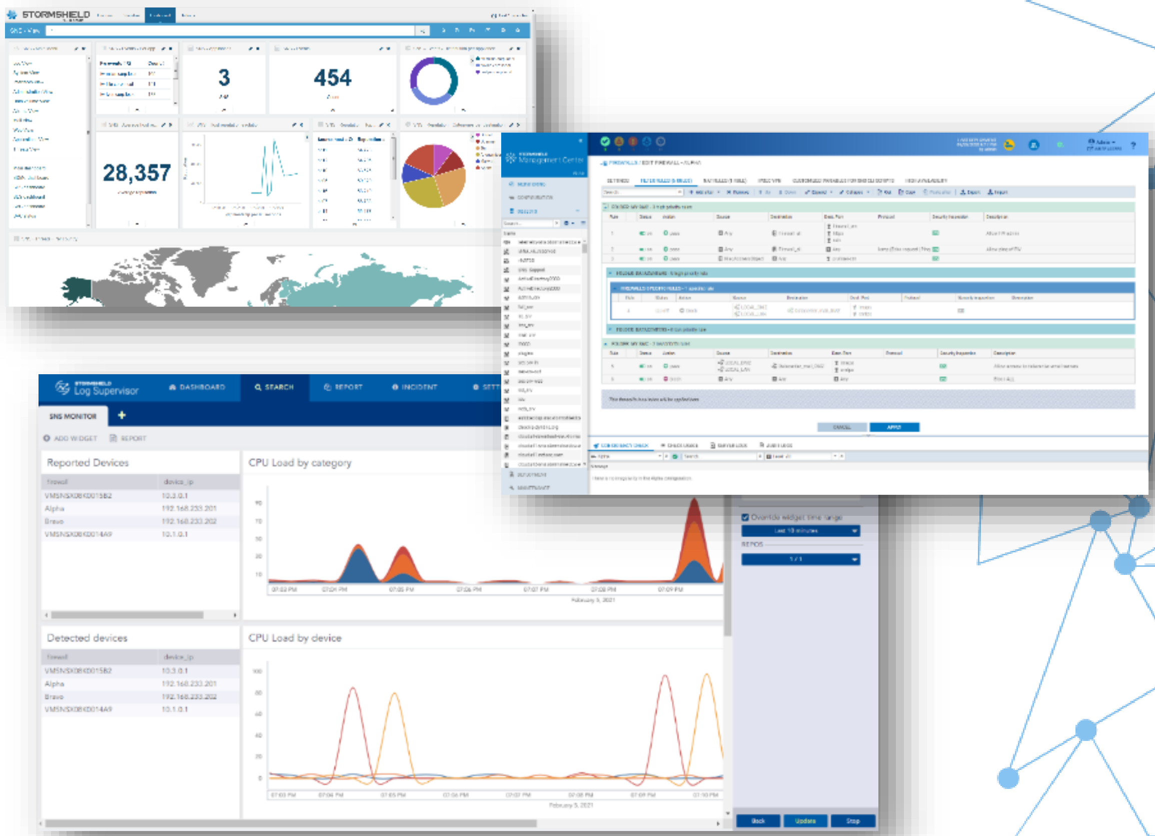
Stormshield advantages:
Unmatched performance at the best cost

Protection of all IT/OT and Cloud environments in one complete range and one administration software package

Stormshield

Network Security

Advanced administration tools



Reported Devices

firewall	device_ip
VMSNSX08KD015B2	10.3.0.1
Alpha	192.168.233.201
Bravo	192.168.233.202
VMSNSX08KD014A9	10.1.0.1

Detected devices

firewall	device_ip
VMSNSX08KD015B2	10.3.0.1
Alpha	192.168.233.201
Bravo	192.168.233.202
VMSNSX08KD014A9	10.1.0.1

Stormshield advantages:
Tools to optimise your security and the effectiveness of your protection

Stormshield Management Center - The centralized management tool for Stormshield firewalls

Stormshield Log Supervisor - Log Management on a larger scale

Stormshield

Endpoint Security

Advanced protection for Windows workstations

Stormshield advantages:
Unique, proactive, offline protection

Proactively blocks unknown attacks and provides detected investigational information

Stormshield

Data Security

End-to-end multi-device and multi-application encryption

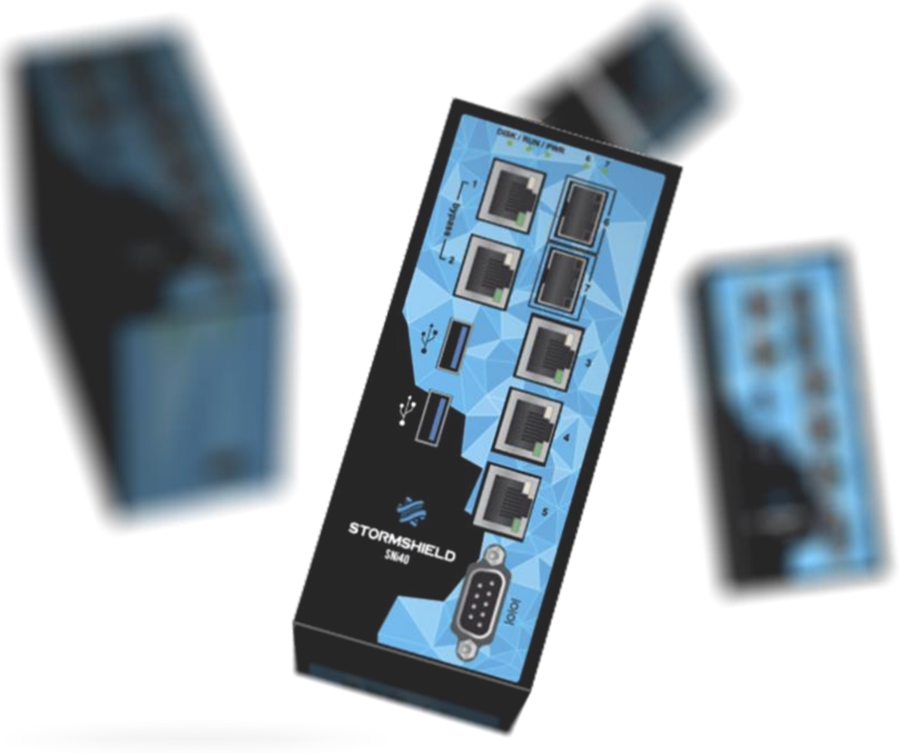
Stormshield advantages:
A solution for encrypting unstructured On-Premise & Cloud data

Encryption as close to the data as possible ensures end-to-end protection

Stormshield

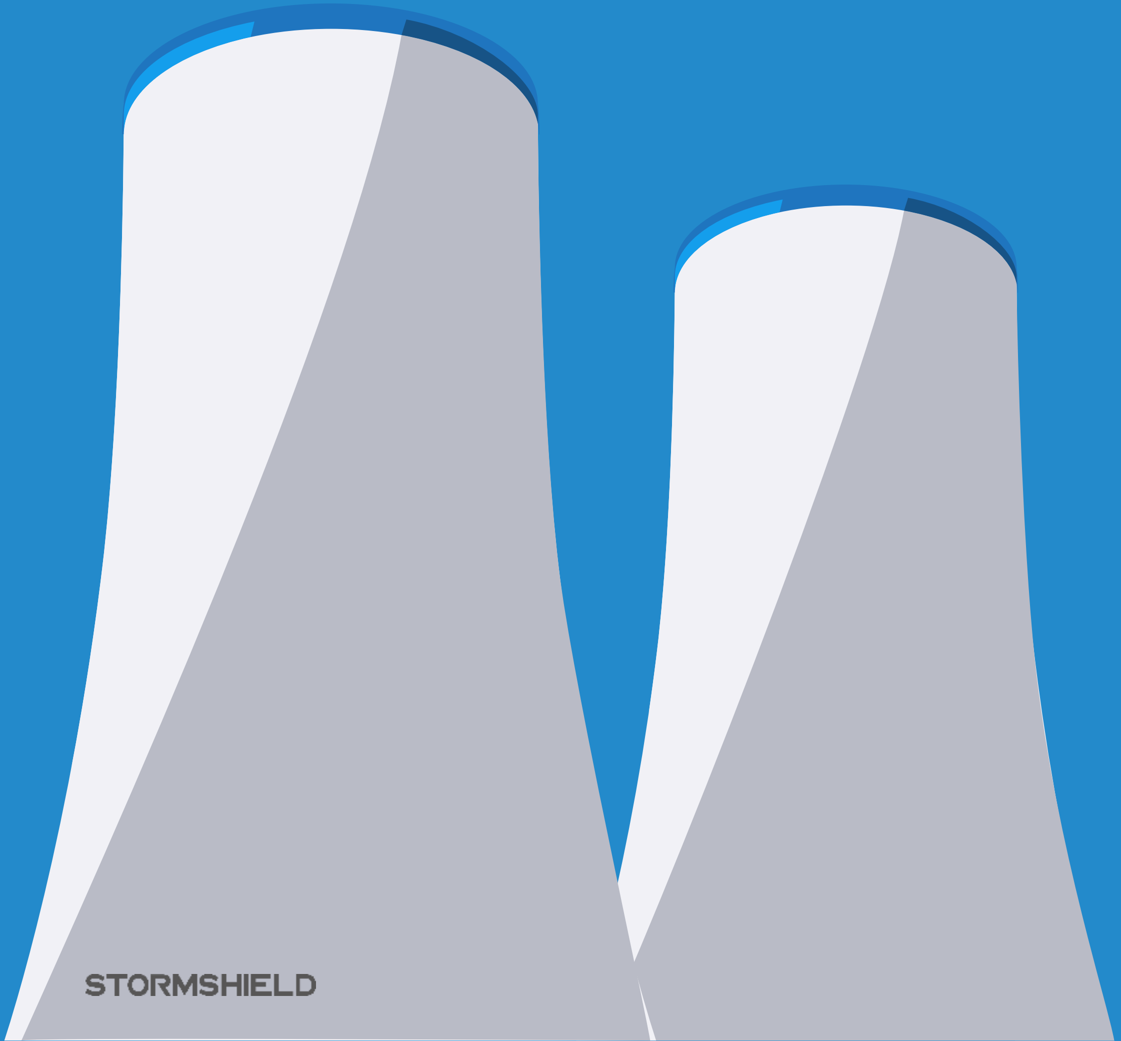
Industrial Business Line

OT infrastructure security with industrial firewalls and operational station protection



Stormshield advantages:
Comprehensive coverage of protection needs

Unique expertise in controlling commands to ensure the functioning of operational processes

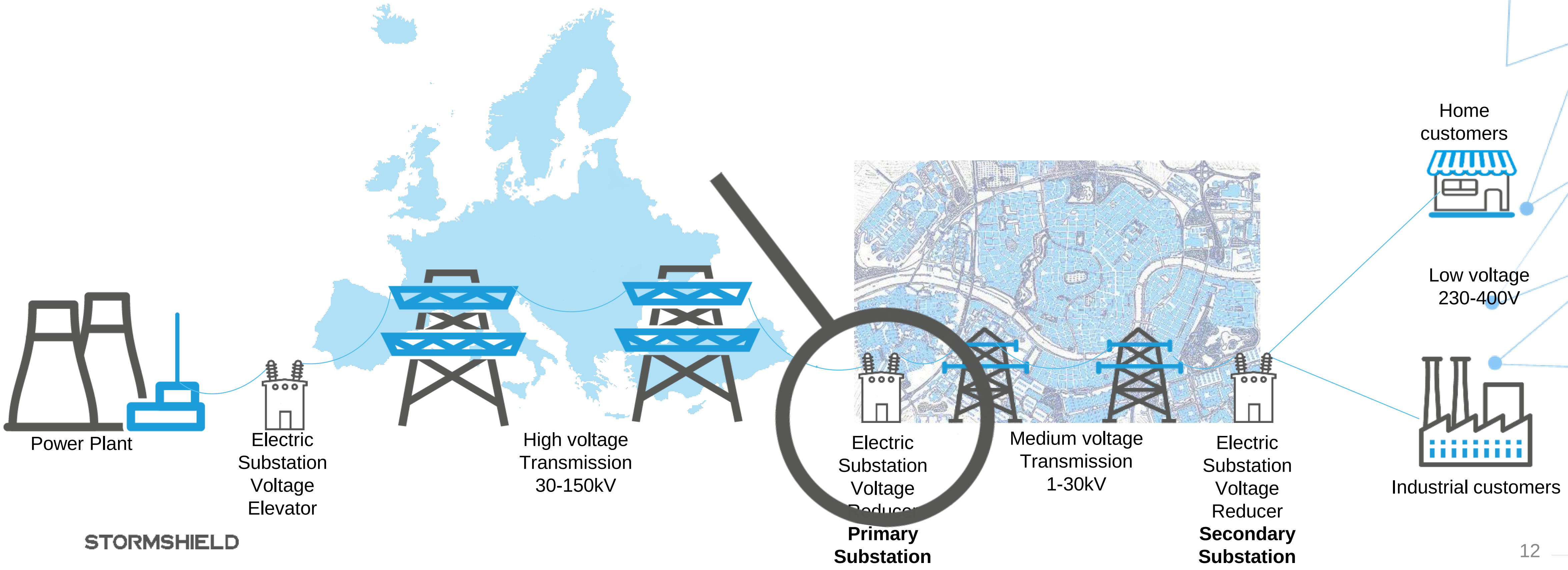


A story in the

Energy sector

The energy production and distribution process

- For hundreds of KM the voltage must be really high
- For few KM the voltage can be medium
- For local distribution the voltage can be low



Power Plant

Electric Substation Voltage Elevator

High voltage Transmission 30-150kV

Electric Substation Voltage Reducer **Primary Substation**

Medium voltage Transmission 1-30kV

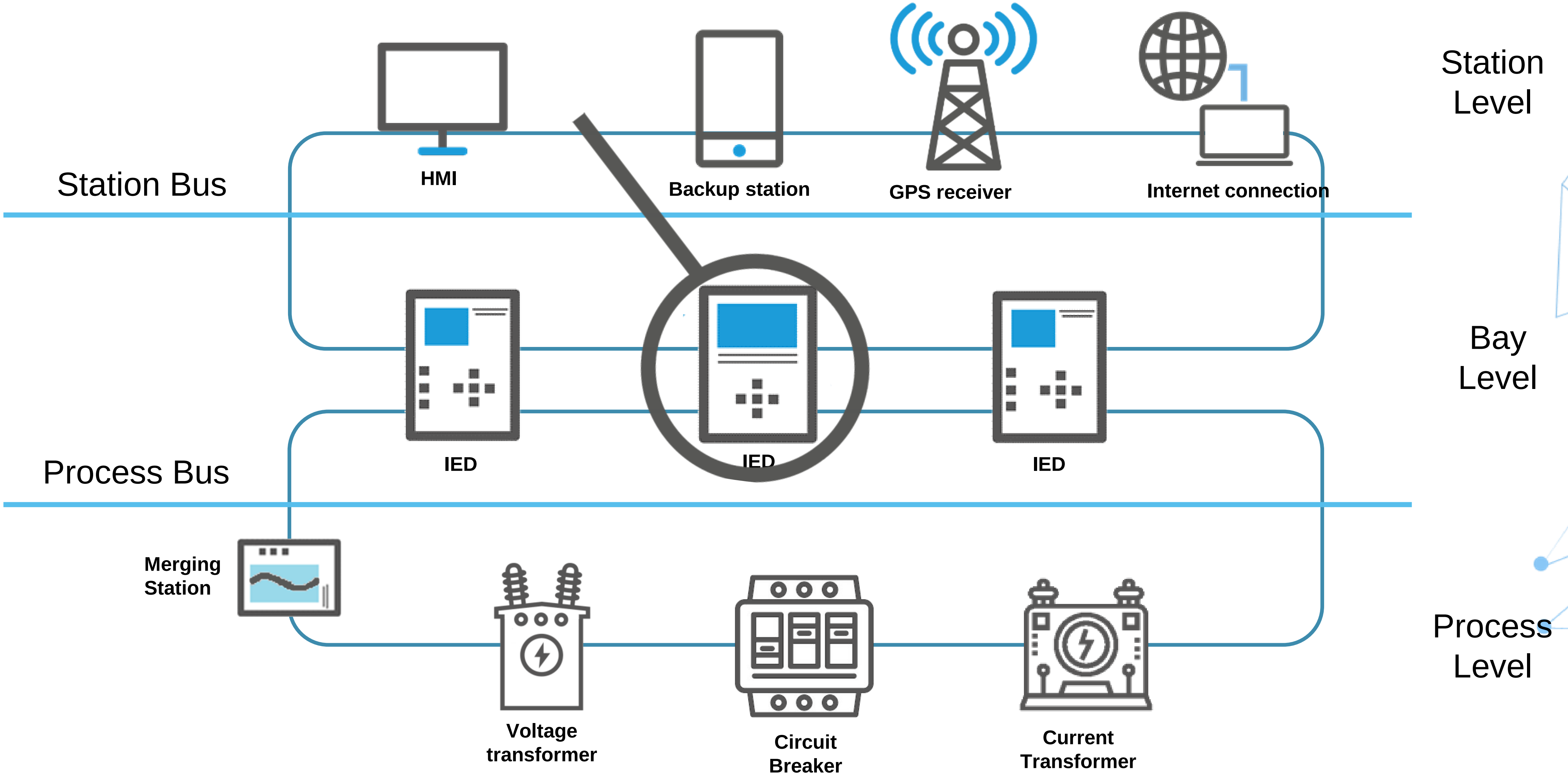
Electric Substation Voltage Reducer **Secondary Substation**

Home customers

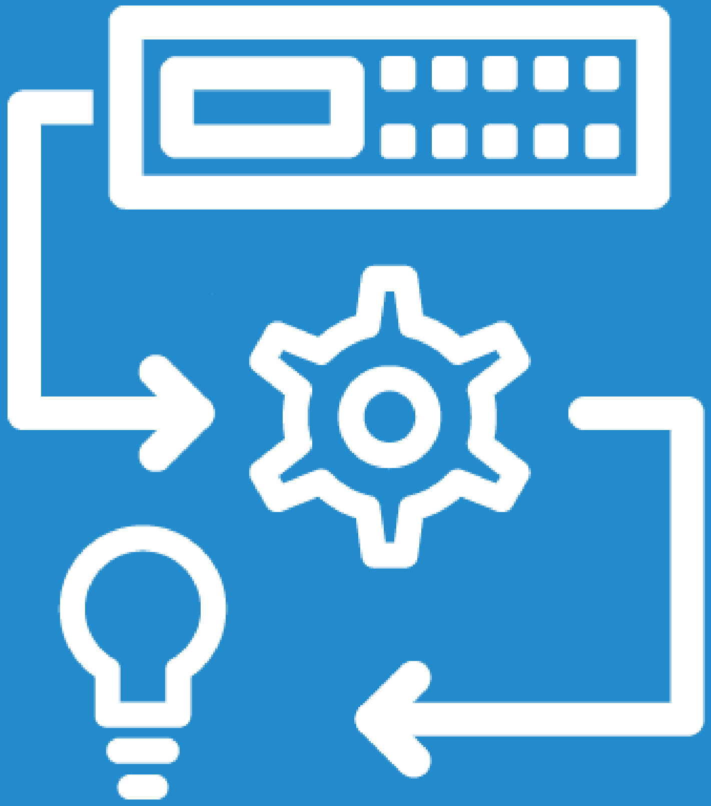
Low voltage 230-400V

Industrial customers

Power Substation

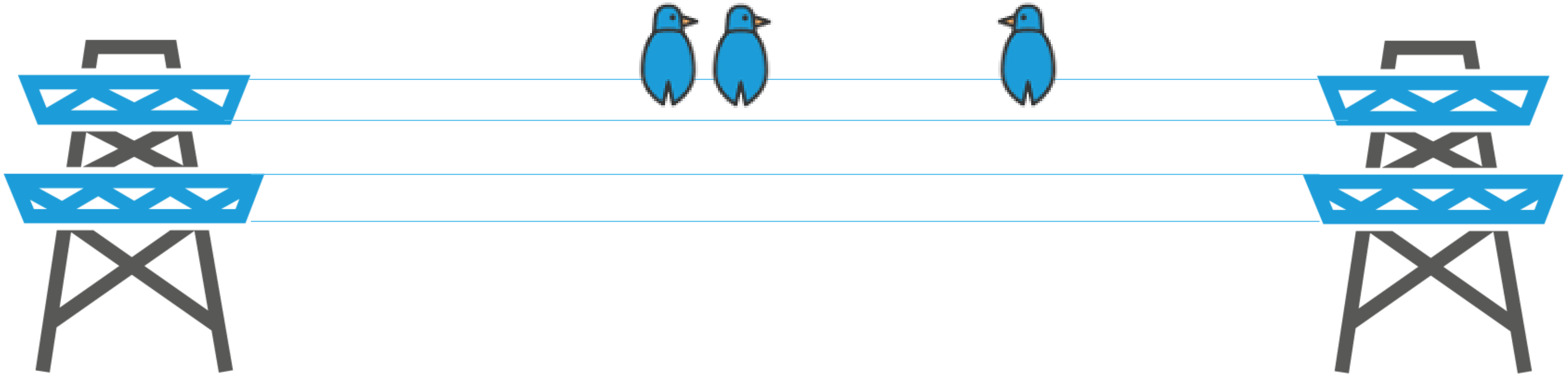


IEC 61850

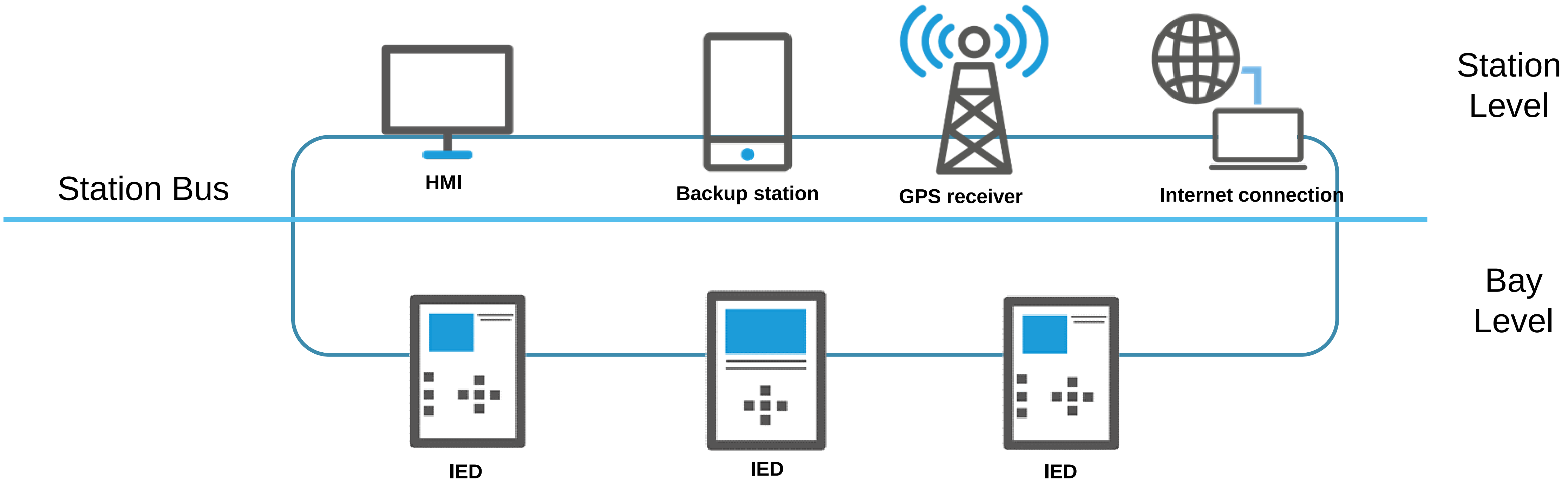


What is IEC61850?

- It’s a standard for the substation components integration and their functional characteristics.
- Defined by the IEC TC57 group (one of the IEC technical commissions).
- Composed by multiple protocols (ex: GOOSE,MMS, SMV).
- Used in the management and design of electric substation.



MMS - Manufacturing Message Specification

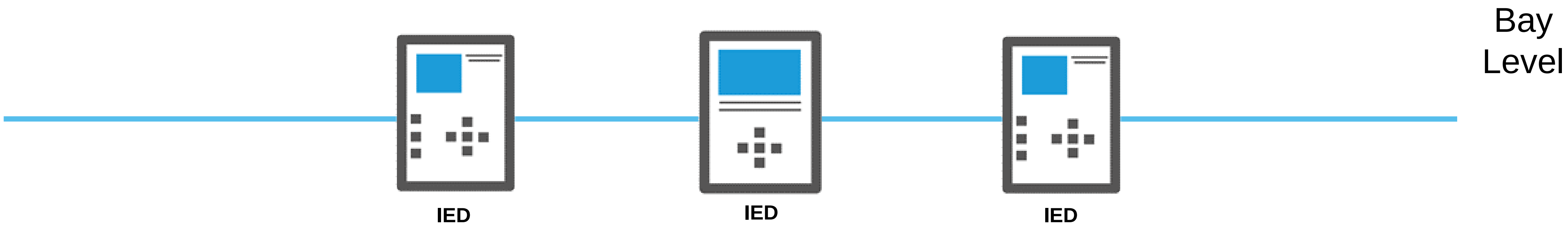


Application Layer	MMS
Transport Layer	TCP
Network Layer	IP
Link Layer	LAN

- Client/Server communication protocol
- Used between IED and SCADA
- Required speed: <100ms

GOOSE - Generic Object Oriented Substation Event

- Publish/Subscriber
- Required Speed: <10 ms
- No ACK but messages are repeated cyclically

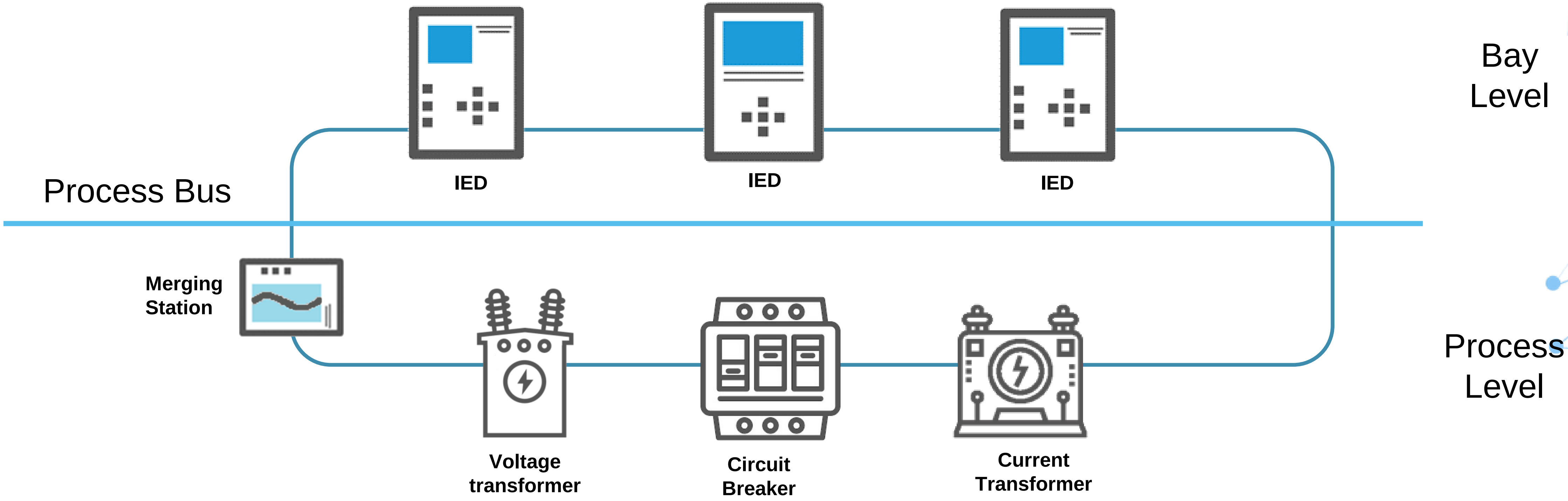


Application Layer	GOOSE
Transport Layer	
Network Layer	
Link Layer	LAN

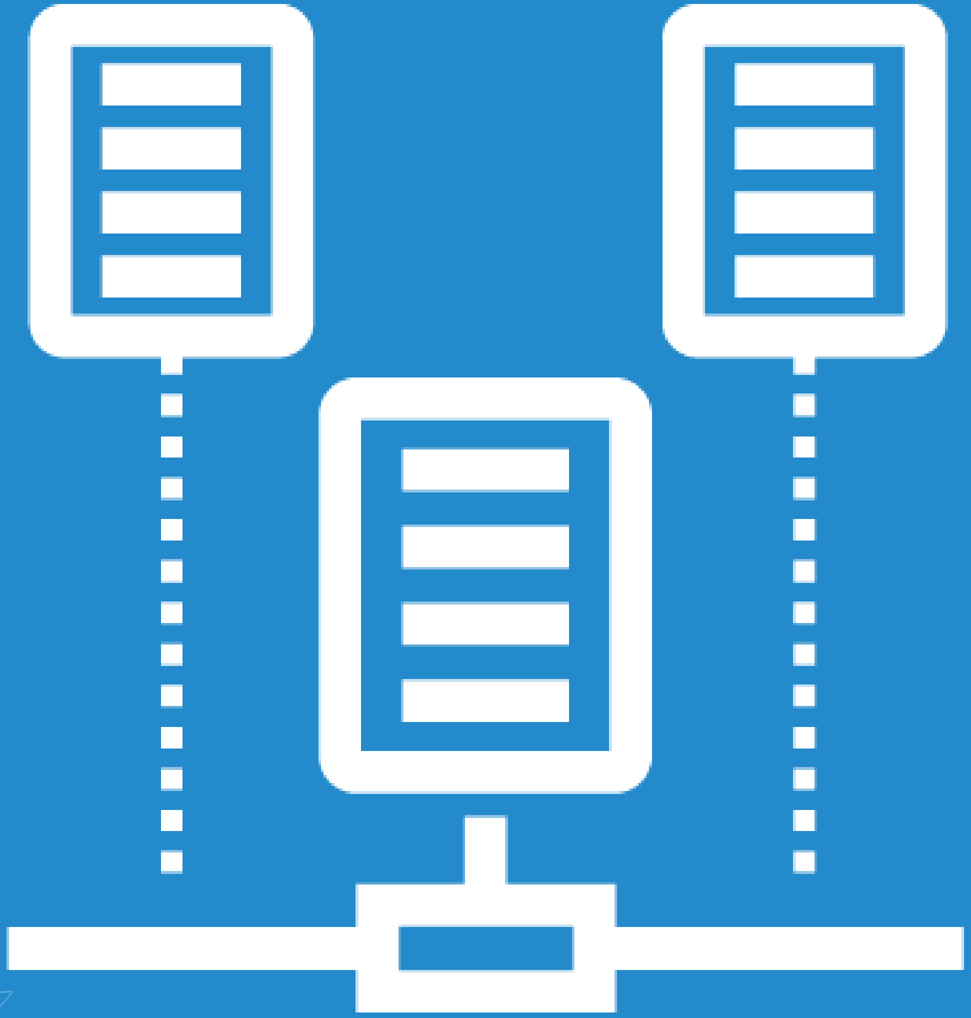
SMV - Sampled Measured Values

- Publish/Subscriber
- Required Speed <10 ms
- Require high bandwidth
- Just send measures with a timestamp
- NO ACK

Application Layer	SMV
Transport Layer	
Network Layer	
Link Layer	LAN



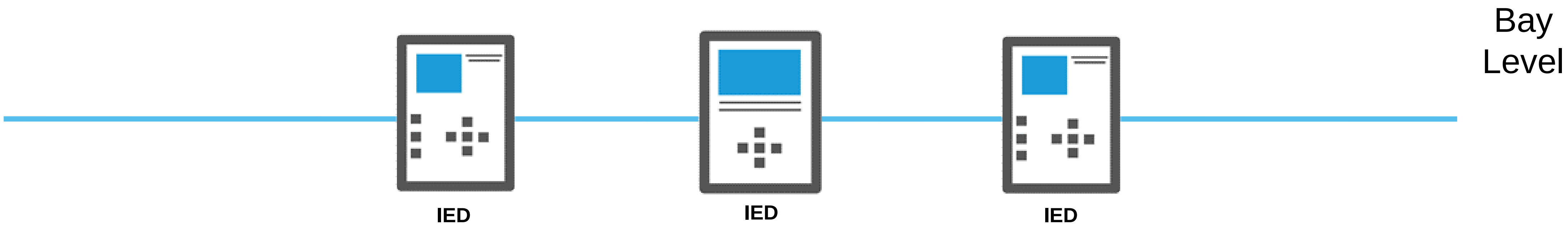
GOOSE



STORMSHIELD

GOOSE - Generic Object Oriented Substation Event

- Publish/Subscriber
- Required Speed: <10ms
- No ACK but messages are repeated cyclically



Application Layer	GOOSE
Transport Layer	↓
Network Layer	
Link Layer	LAN

Goose

Generic Substation Events is defined in IEC 61850 with the purpose to:
Provide a secure and reliable way to share data between substation
Provide a way to share event with multiple devices.

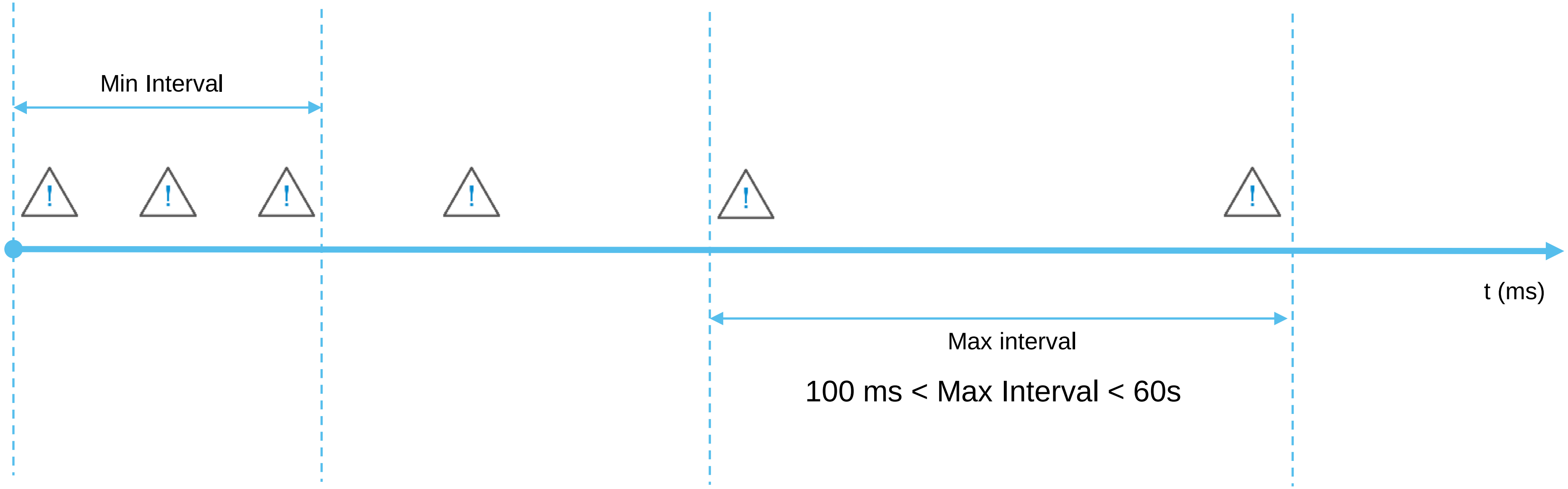
In order to do this it uses also multicast and broadcast.

GSE is divided in:
GOOSE (Generic Object Oriented Substation Events): many data types (binary, analog, integer)
GSSE (Generic Substation Status Events): only fixed structures of binary events. It’s progressively dismissed in favor of GOOSE.

GOOSE main characteristic:

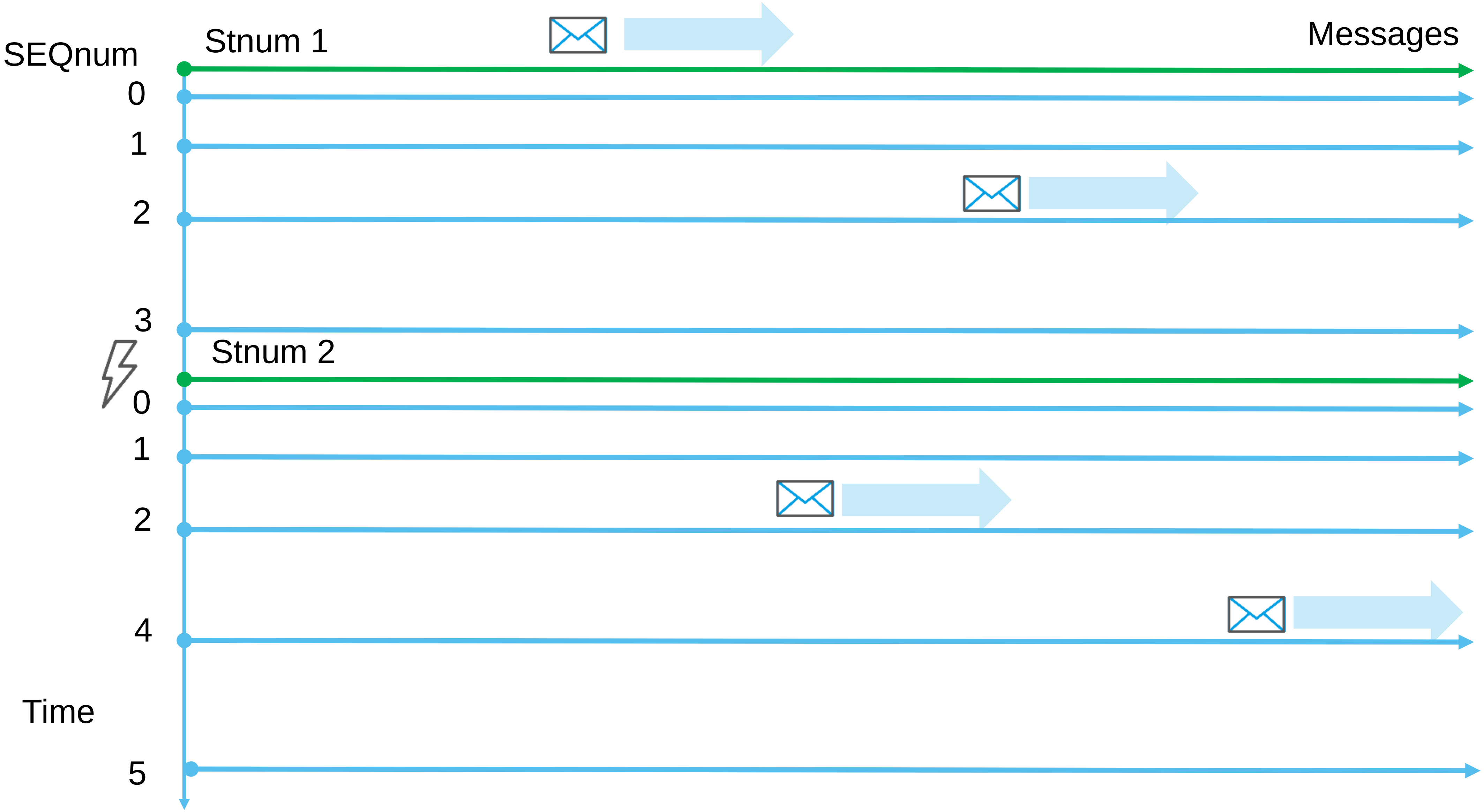
- Based on Ethernet to be faster
- Usage of Vlan in order to prioritize packets
- Usage of published subscriber methods
- Using a retransmission method to be sure that all the device receive the packet

GOOSE



GOOSE doesn’t require an ACK.
The same packet is re-transmitted periodically with an increasing time between the rentrasmission in order to be sure that it’s received.

GOOSE

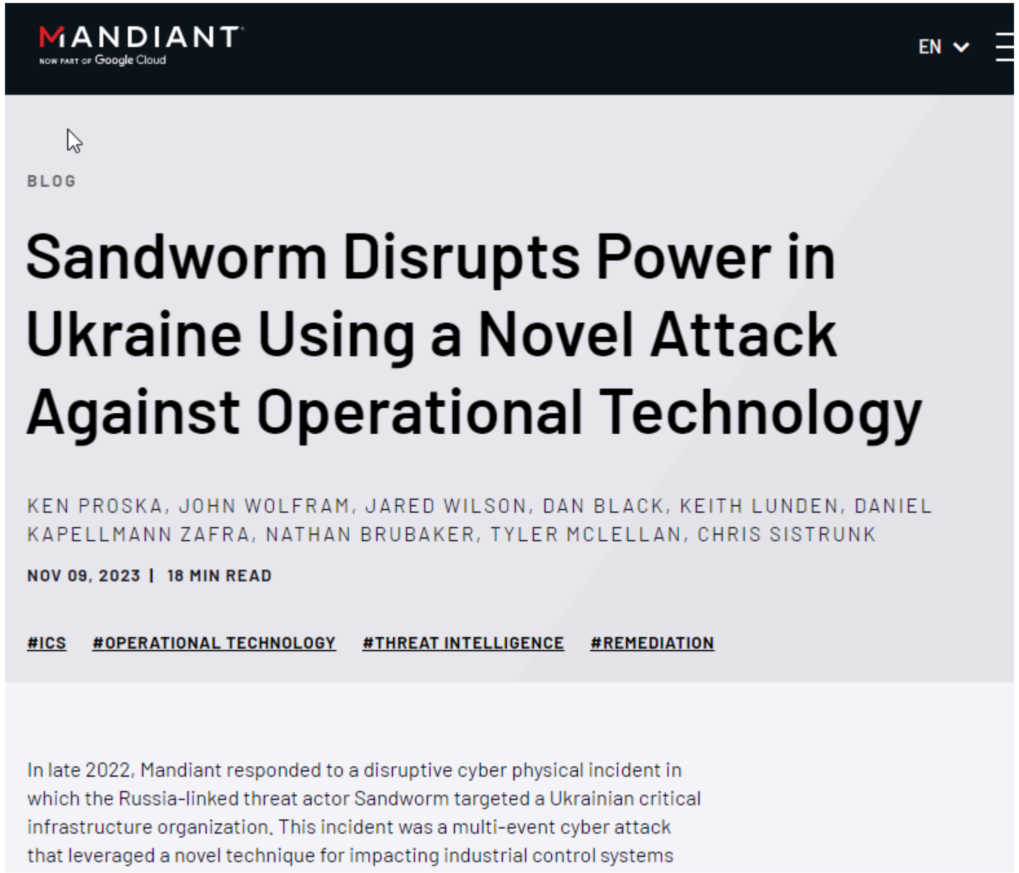


Not sure what … but SOMETHING is missing in this protocol design …

STORMSHIELD

Why is cybersecurity **at the heart of international challenges?**

Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology



BLOG

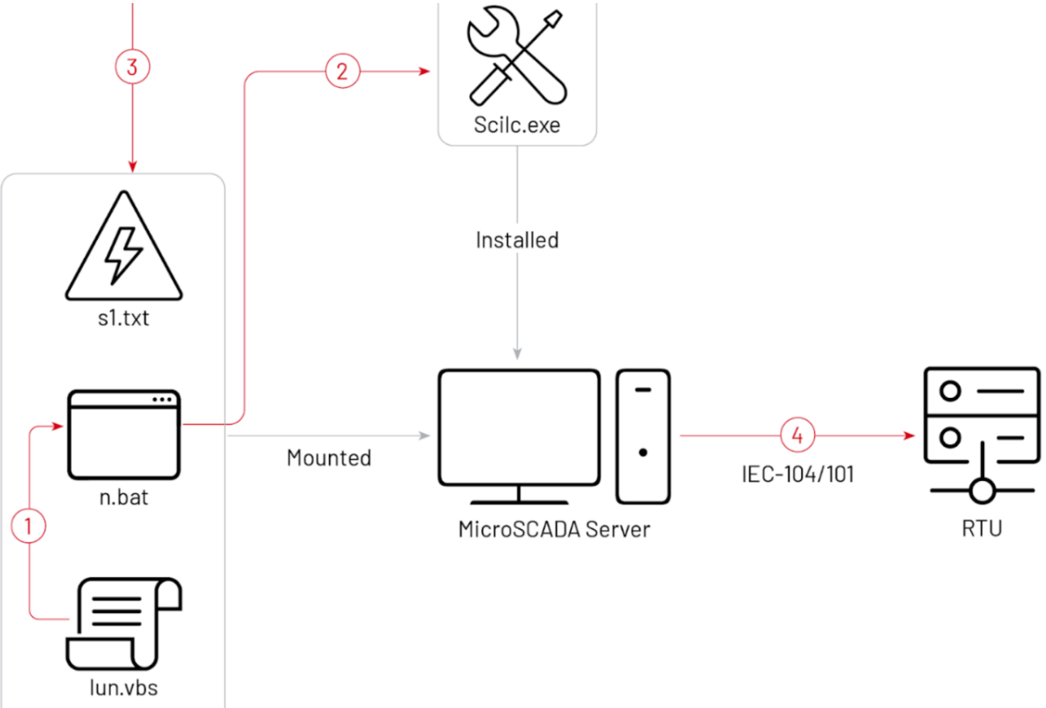
Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology

KEN PROSKA, JOHN WOLFRAM, JARED WILSON, DAN BLACK, KEITH LUNDEN, DANIEL KAPELLMANN ZAFRA, NATHAN BRUBAKER, TYLER MCLELLAN, CHRIS SISTRUNK

NOV 09, 2023 | 18 MIN READ

#ICS #OPERATIONAL TECHNOLOGY #THREAT INTELLIGENCE #REMEDIATION

In late 2022, Mandiant responded to a disruptive cyber physical incident in which the Russia-linked threat actor Sandworm targeted a Ukrainian critical infrastructure organization. This incident was a multi-event cyber attack that leveraged a novel technique for impacting industrial control systems



Thank you

Contacts

🏢 22, rue du Gouverneur Général Éboué
92130 Issy-les-Moulineaux FRANCE

☎ +33 (0) 9 69 32 96 29

✉ sales@stormshield.eu

STORMSHIELD