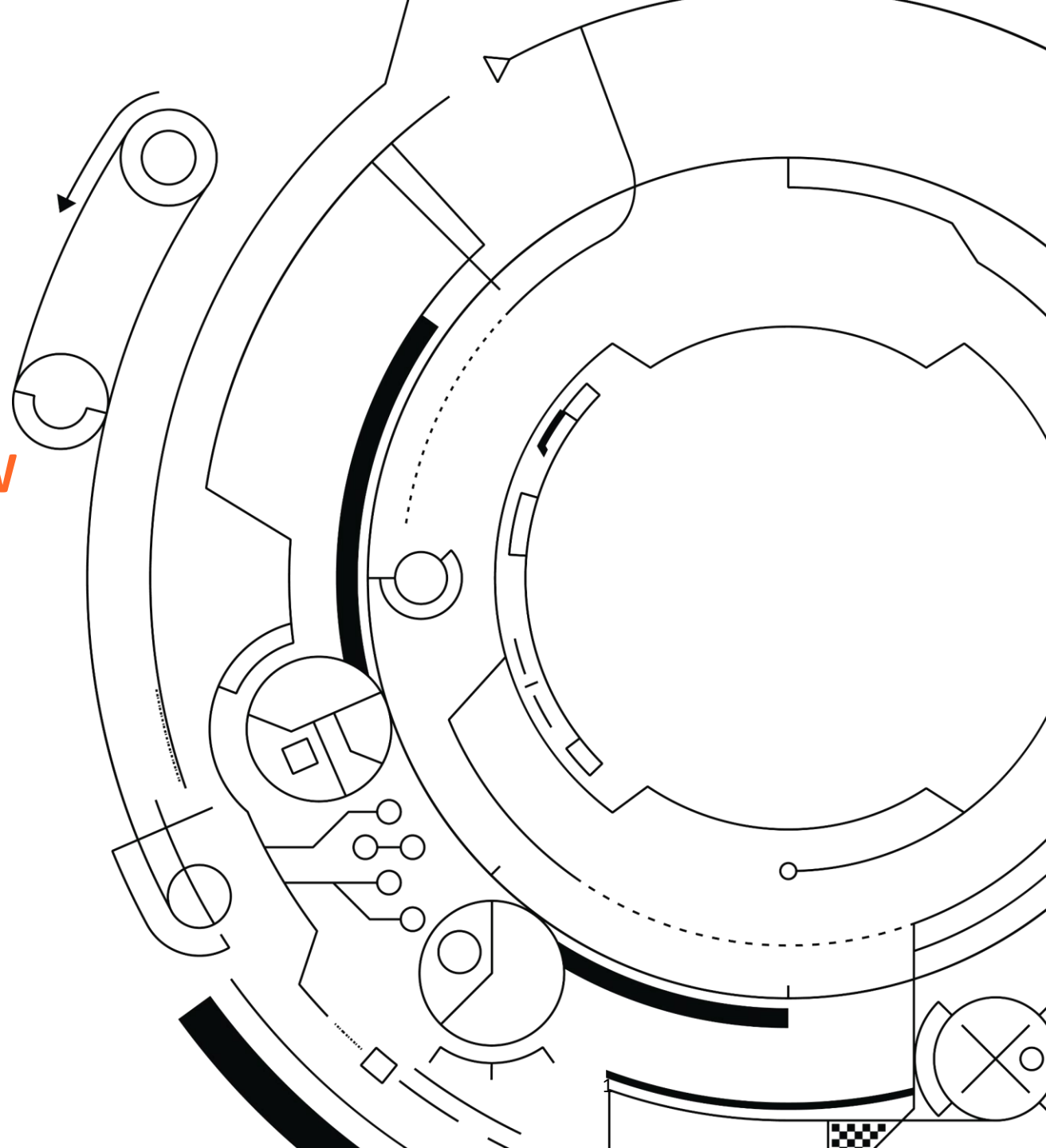


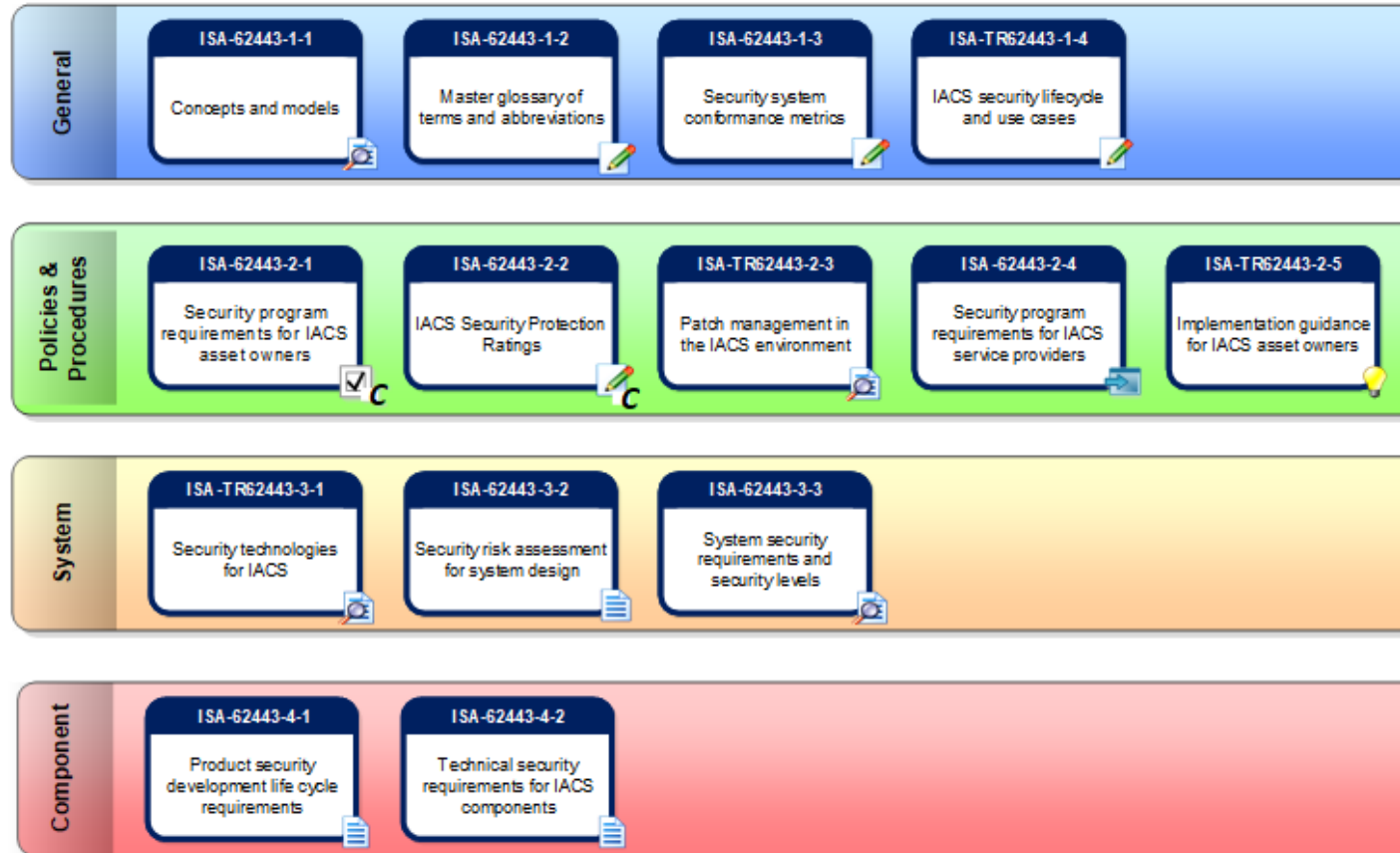
# UNIWERSALNA BRAMA DOSTĘPOWA DLA OBIEKTÓW ENERGETYCZNYCH

13/03/2024

Krzysztof Kawecki  
Menedżer Projektów Energetyki i Automatyki

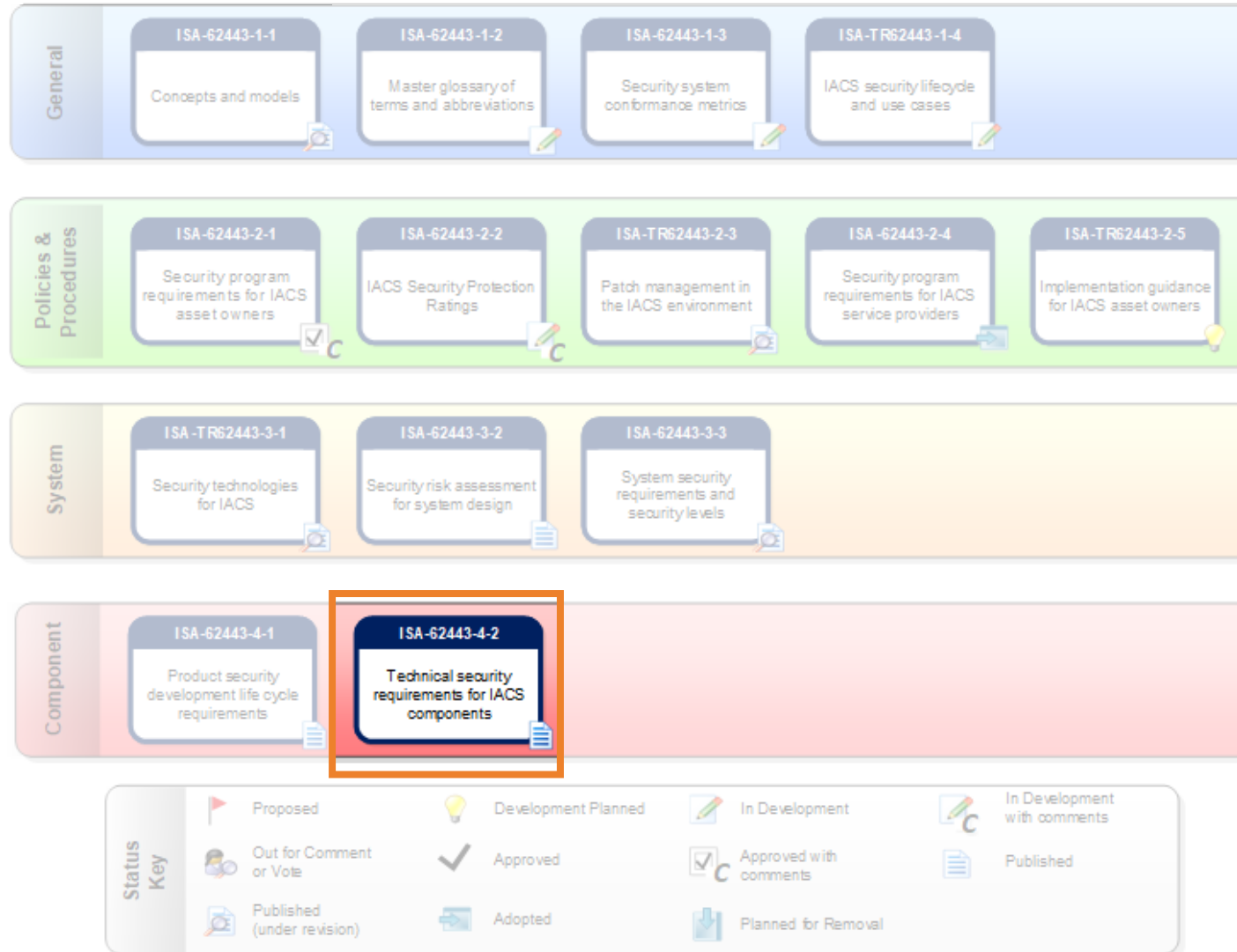


# IEC-62443



Status Key	Icon	Description
	🚩	Proposed
	💡	Development Planned
	✍️	In Development
	✍️ C	In Development with comments
	👤	Out for Comment or Vote
	✅	Approved
	✅ C	Approved with comments
	📄	Published
	📄	Published (under revision)
	📁	Adopted
	🗑️	Planned for Removal

# IEC-62443-4-2



## IEC 61850



### System Aspects

Part 1: Introduction and overview

Part 2: Glossary

Part 3: General Requirements

Part 4: System and Project Management

Part 5: Com. requirements for functions and device models

### Configuration

Part 6: Configuration language for communication in electrical substations related to IEDs

## IEC 61850-3

System Aspects
Part 1: Introduction and overview
Part 2: Glossary
<b>Part 3: General Requirements</b>
Part 4: System and Project Management
Part 5: Com. requirements for functions and device models
Configuration
Part 6: Configuration language for communication in electrical substations related to IEDs



**pojedynczy punkt awarii  
nie może spowodować  
braku operacyjności  
stacji elektroenergetycznej**

## Okoliczności w odniesieniu do bramy dostępowej



zmieniająca się infrastruktura komunikacyjna



zachowanie obsługi dla tzw.  
„legacy”



bezpieczeństwo



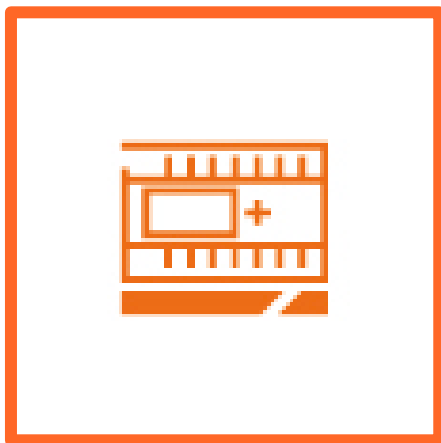
instytucje regulacyjne oczekujące  
większej kontroli  
i udostępniania danych

## Komponent #1 w łączności do obiektu – modem LTE



- Światłowód nie dociera jeszcze wszędzie (ale warto mieć tę opcję!)
- łącza dzierżawione | 2G/3G | ISDN - to już przeszłość...
- LTE:
  - Cat 4
  - Cat-M1/NB1 (mniejsze pasmo większy zasięg)
  - LTE 450
- Sieci publiczne i prywatne

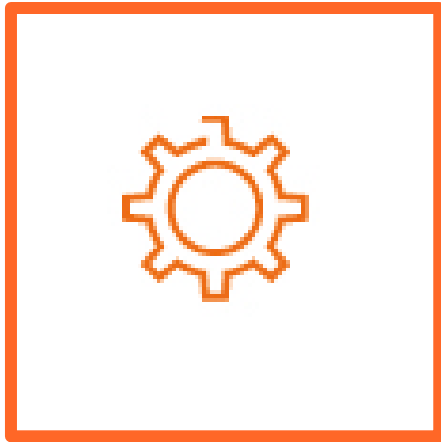
## Komponent #2 w łączności do obiektu – RS over ETH



- Nie tylko Ethernet ;-)
- Wiele urządzeń nadal posiada interfejs szeregowy
- Najczęściej spotykany:
  - RS-232
  - RS-485



## Komponent #3 w łączności do obiektu – konwerter protokołów SCADA



- Wiele urządzeń i protokołów po stronie obiektowej (stacyjnej)
- Jeden protokół SCADA dla gromadzenia danych i kontroli
- Na przykład:
  - IEC 101
  - IEC 104
  - Modbus RTU
  - Modbus IP
  - DNP3

## Komponent #4 w łączności do obiektu – Firewall + DPI



- Coraz częściej wymagany w torze komunikacyjnym i między urządzeniami obiektowymi
- DPI = Deep Packet Inspection
  - Rozwinięcie standardowej funkcji FW
  - Filtrowanie danych na poziomie pól przemysłowych protokołów komunikacyjnych

modem LTE

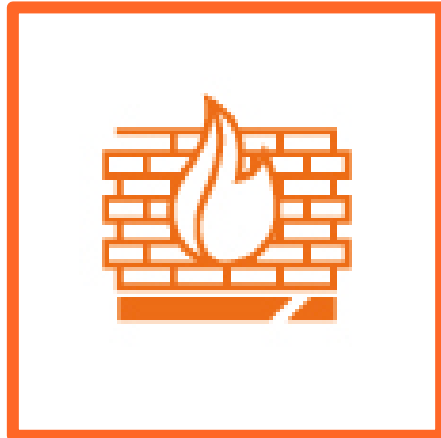
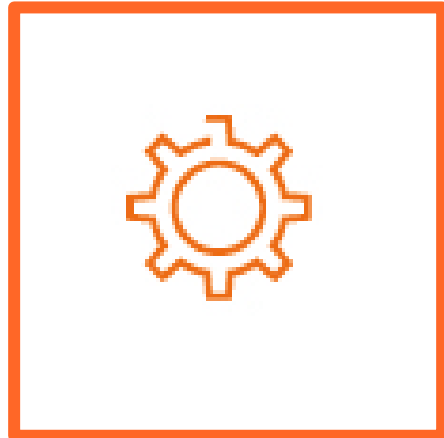
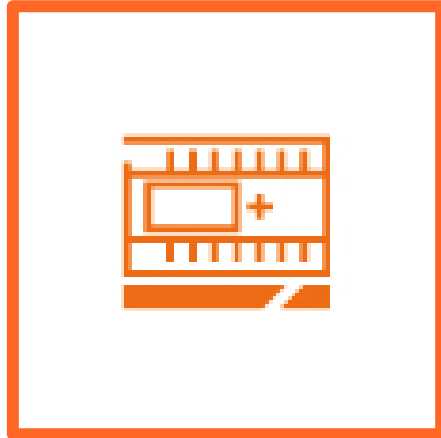
RS over ETH

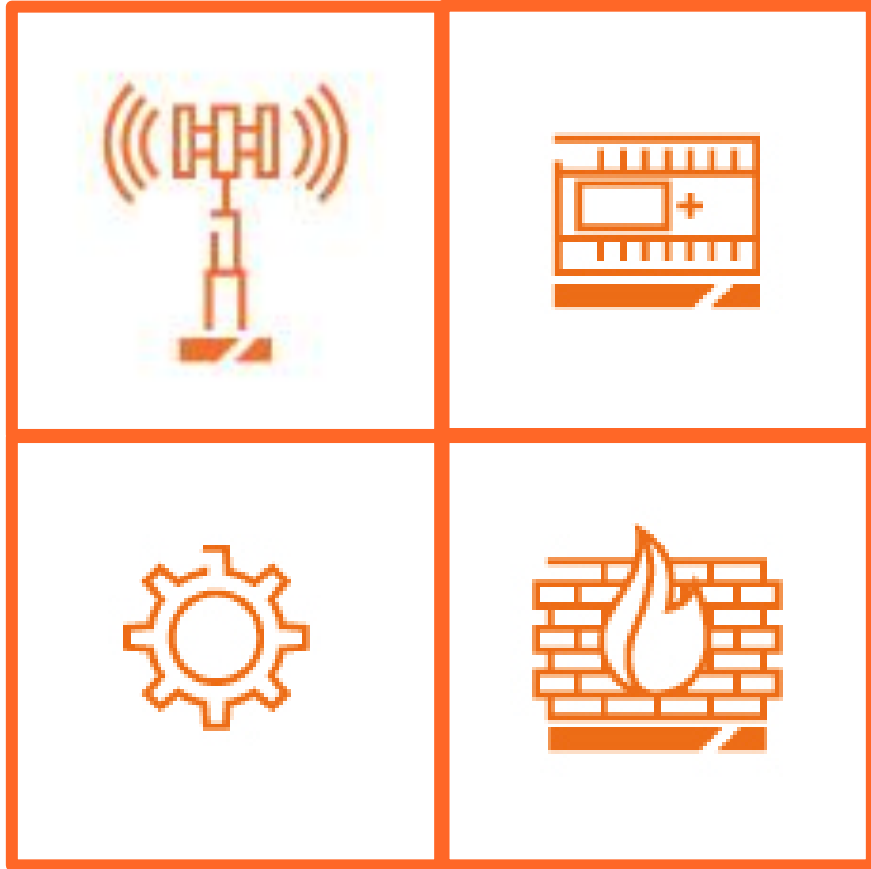


konwerter  
protokołów SCADA

firewall  
+ DPI

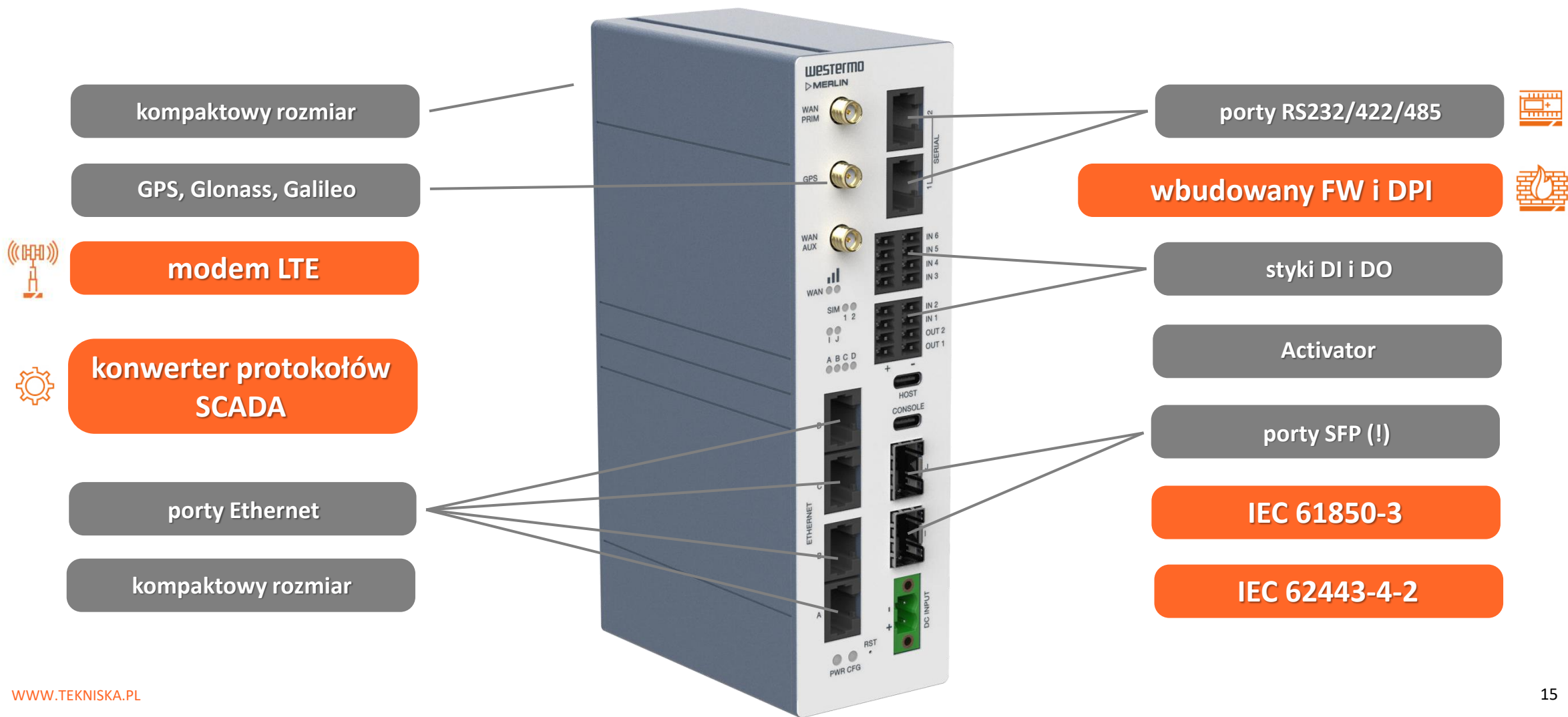








## Przemysłowa brama dostępowa „Merlin”



## Scenariusz zastosowania – 62443-4-2 „toolbox”

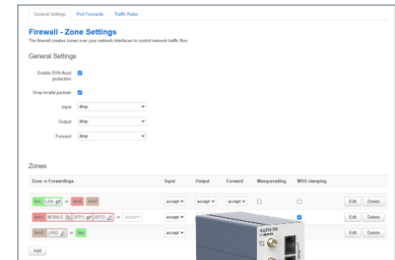
„Cybersecurity should be part of the design from the start”

- Secure boot
- TPM = Trusted Platform Module
- VPNs [Conduits]
- VLANs & Firewall [ZONES]
- Authentication (lokalna i zdalna)
- Różnorodne role



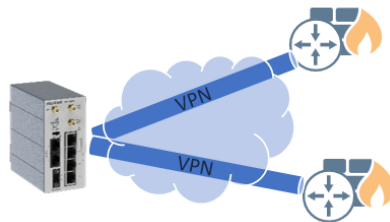
## Scenariusz zastosowania – Firewall i DPI („Defence In Depth”)

- Reguły mogą być stosowane do dowolnego interfejsu
- nie tylko WAN do LAN
- można skonfigurować między wszystkimi interfejsami
- NAT
- DPI dla protokołów przemysłowych
- IEC 104
- DNP3
- MODBUS
- W trakcie certyfikacji na zgodność z IEC-62443



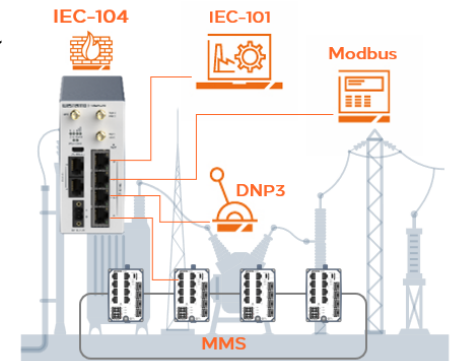
## Scenariusz zastosowania – VPN

- Wymiana kluczy IKE V1 i V2
- Wiele typów VPN
  - IPSec
  - DMVPN
  - SSL (OPENvpn)
  - WeConnect
  - FlexVPN (CISCO)
  - GRE
  - L2TP V2/3 (tryb mostu L2) i ABB ARM600
- PSK (Pre Shared Key) lub X.509
- SCEP (Secure Certificate Enrolment Process)



## Scenariusz zastosowania – konwerter protokołów SCADA

- Uwzględnienie „stanu obecnego”
- SCADA zazwyczaj wykorzystuje jeden protokół
- Urządzenia obiektowe często korzystają z różnych protokołów
- Merlin jako „Master” dla urządzeń na obiekcie
- Przychodzące żądania mapowane do lokalnych protokołów
- Lista obsługiwanych protokołów otwarta
- **Ekonomiczne rozwiązanie do integracji istniejących zasobów ze wspólnym systemem SCADA**





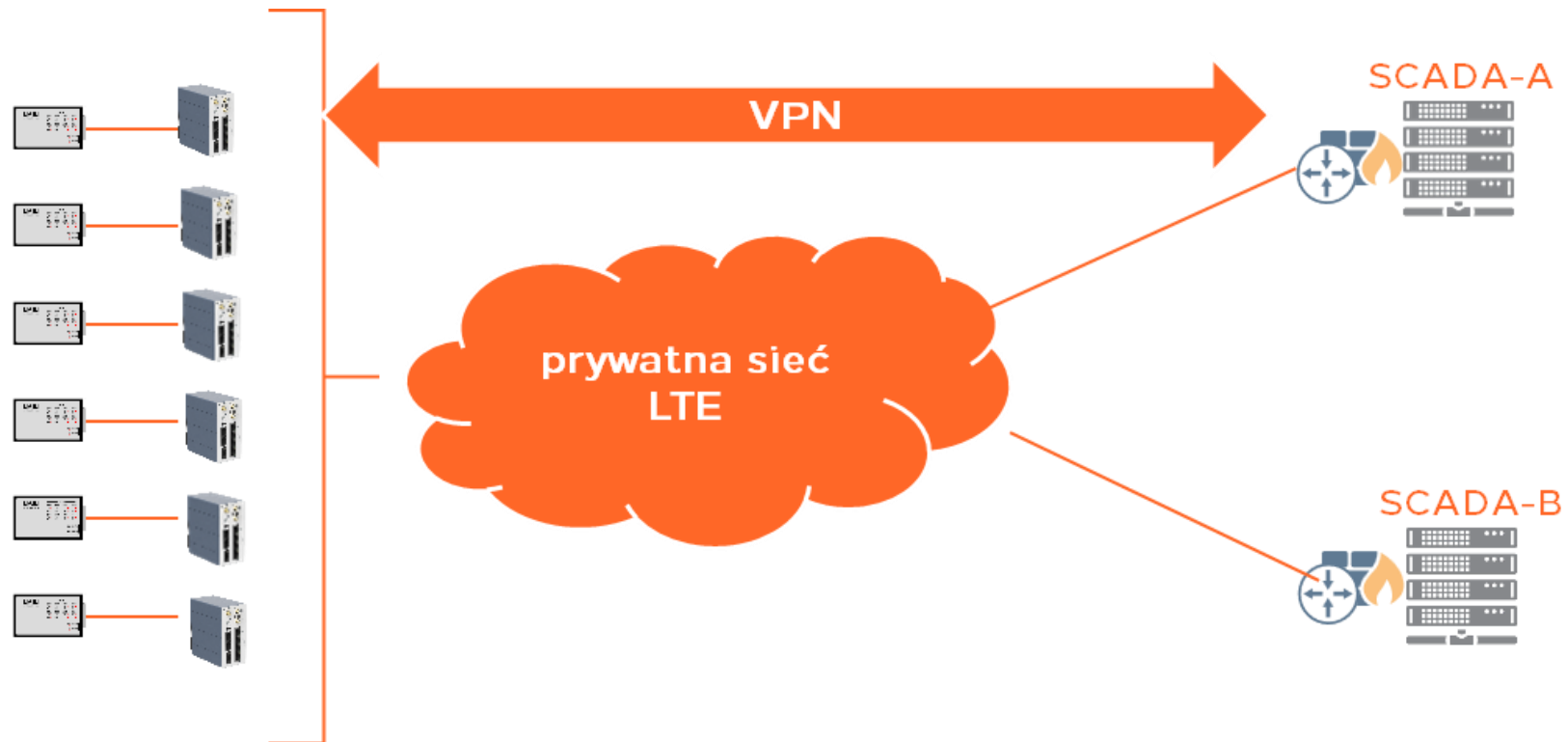


## Scentralizowane zarządzanie „Activator”

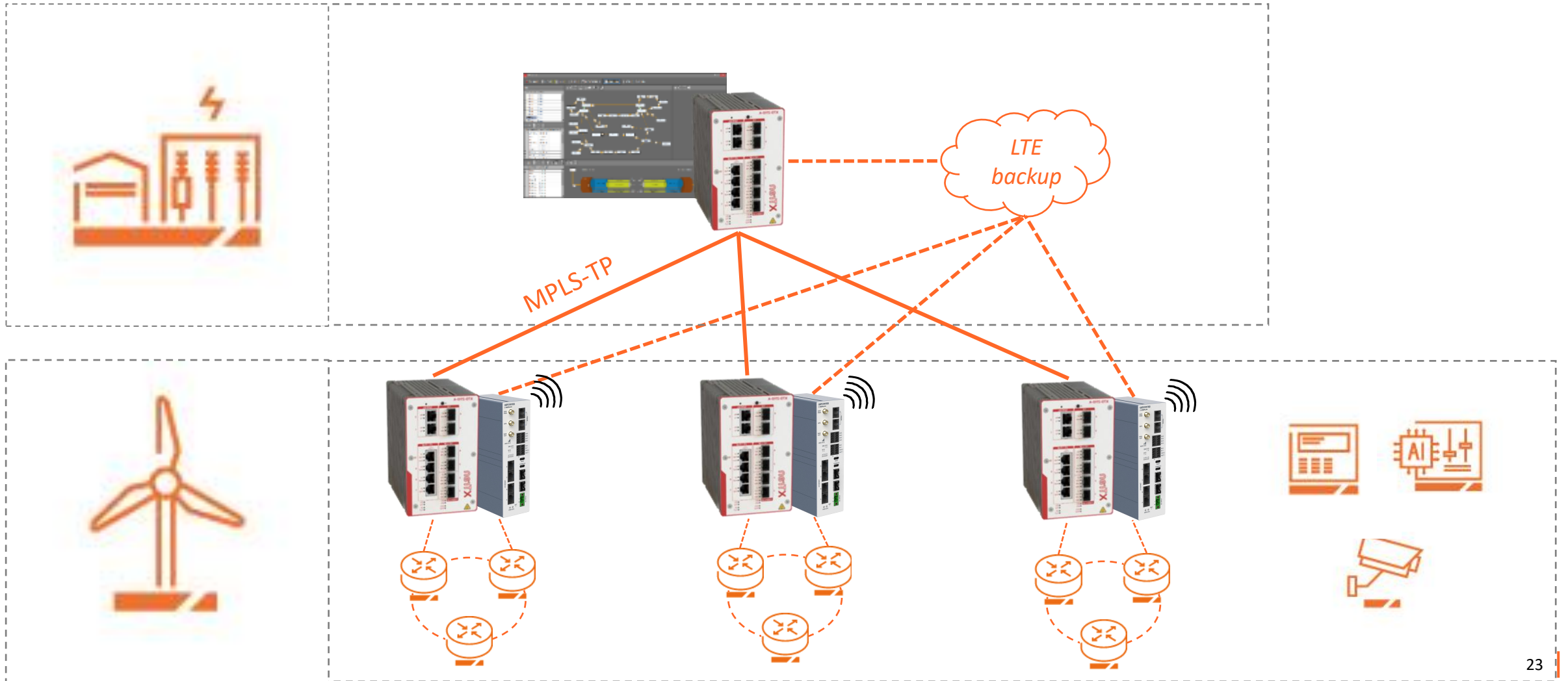


- Bez laptopa
- Bez zaawansowanego szkolenia
- Bez specjalnych narzędzi lub oprogramowania

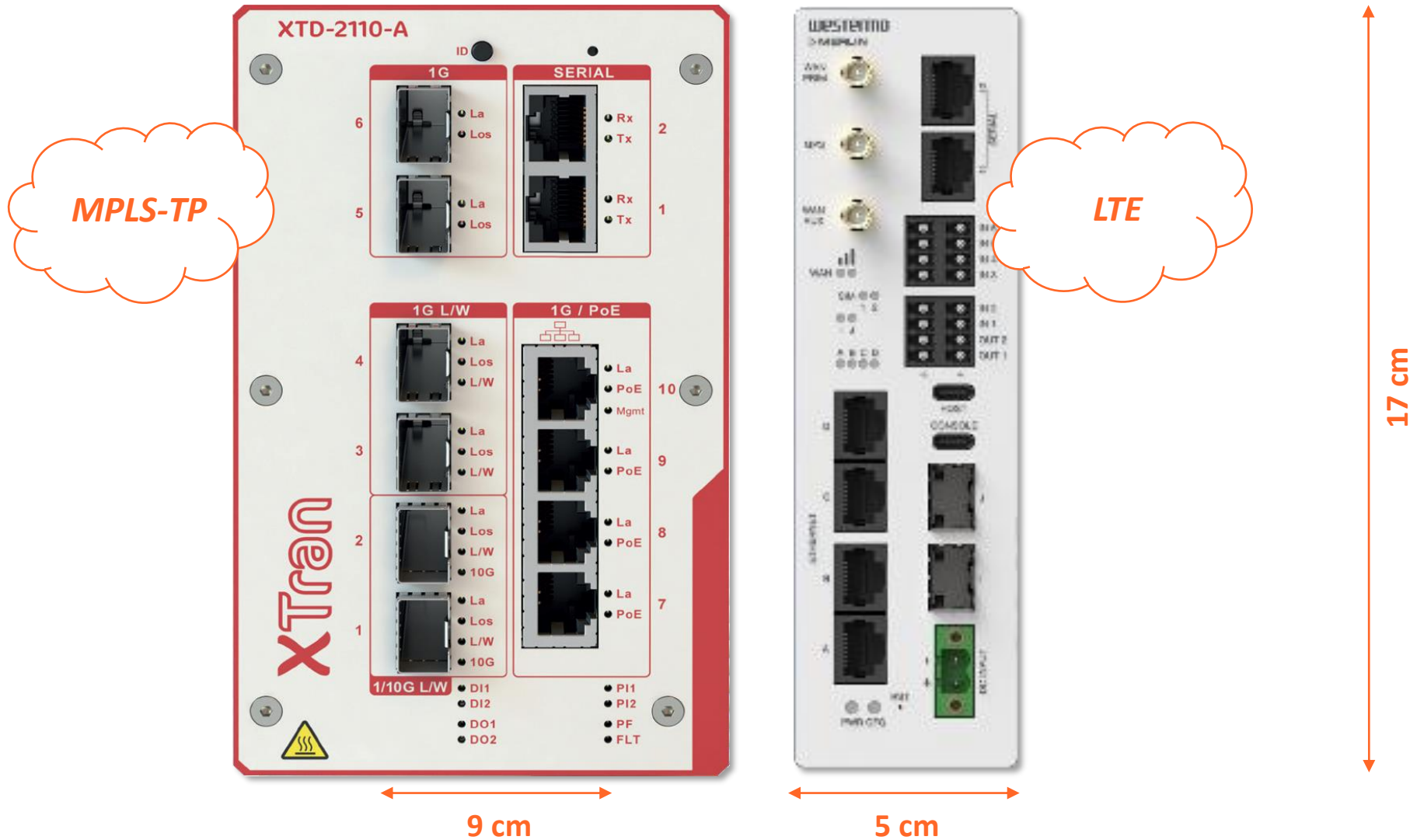
## Analiza przypadku – migracja do infrastruktury IP




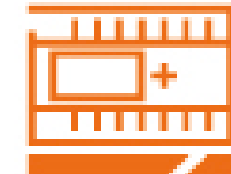


## Analiza przypadku - Off-shore MPLS-TP + LTE



## Analiza przypadku - Off-shore MPLS-TP + LTE





 modem LTE	 RS over ETH
 konwerter protokołów SCADA	 firewall + DPI



Krzysztof Kawecki

Menedżer projektów energetyki i automatyki

+48 32 33 111 06-09 (wew. 103)

+48 538 977 300

krzysztof.kawecki@tekniska.pl

Zapraszam!

TEKNISKA POLSKA  
Przemysłowe Systemy  
Transmisji Danych Sp. z o. o.

ul. Łabędzka 9-9A,  
44-121 Gliwice

+48 32 33 111 06 ÷ 09  
tekniska@tekniska.pl

NIP 6312631825  
KRS 0000383694

ODWIEDŹ NAS NA  
[WWW.TEKNISKA.PL](http://WWW.TEKNISKA.PL)





 **TEKNISKA®** | Everything connects