PTPiREE

SIWE 24

XXIII Konferencja

Systemy Informatyczne w Energetyce

5-7 listopada 2024 r., Wisła

ORGANIZATOR

PTPiREE

PARTNER MERYTORYCZNY

ESMETRIC

SPONSOR GENERALNY

APATOR

SPONSORZY

techinova

HITACHI
Inspire the Next

Hewlett Packard Enterprise

ZESKANUJ MNIE

Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej
ul. Wołyńska 22, 60-637 Poznań, tel. +48 61 846-02-00, fax: +48 61 846-02-09
e-mail: ptpiree@ptpiree.pl http://ptpiree.pl

PATRONI MEDIALNI

ENERGIA Elektryczna

nowa Energia

XXIII Konferencja

Systemy Informatyczne w Energetyce SIwE'24

5-7 listopada 2024 r., Wisła

Organizator

PTPiREE

Partner Merytoryczny

ESMETRIC

Sponsor Generalny

APATOR

Sponsorzy

techinova

HITACHI
Inspire the Next

Hewlett Packard Enterprise

SPIS TREŚCI

Referaty zostały umieszczone w materiałach zgodnie z kolejnością nadsyłania

PARTNER MERYTORYCZNY

ESMETRIC GROUP sp. z o.o.
ul. Kolejowa 5/7, 01-217 Warszawa
info@esmetric.pl
https://www.esmetric.pl/

SPONSOR GENERALNY

Apator SA
ul. Gdańska 4a lok. C4, 87-100 Toruń
apator@apator.com
https://www.apator.com/

SPONSORZY

Techinova AB
Intagsvägen 3, SE-371 46 Karlskrona
tel. +46 (0)455 655 530
info@techinova.net

Hitachi Europe Ltd. (Sp. z o.o.) Oddział w Polsce
ul. Złota 59, 00-120 Warszawa
tel. +48 22 112 02 02
https://www.hitachi.eu/pl-pl/

HITACHI ENERGY POLAND (Sp. z o.o.)
ul. Żegańska 1, 04-713 Warszawa
tel. +48 12 396 68 33
https://www.hitachienergy.com/pl/pl/

Hewlett Packard Enterprise
https://www.hpe.com/pl/en/home.html

Apius Technologies S.A.
ul. Moniuszki 50
31-523 Kraków
tel. +48 12 357 60 40
fax +48 12 378 39 30
https://apius.pl/

Atende S.A.
plac Konesera 10a, 03-736 Warszawa
https://atende.pl/

CERT Polska
ul. Kolska 12, 01-045 Warszawa
tel. +48 22 380 82 74
fax +48 22 380 83 99
info@cert.pl
https://cert.pl/

Elmark Automatyka S.A.
ul. Bukowińska 22 lokal 1B, 02-703 Warszawa
tel. +48 22 773 79 37
elmark@elmark.com.pl
https://www.elmark.com.pl/

ENERGA-OPERATOR SA
ul. Marynarki Polskiej 130, 80-557 Gdańsk
tel. +48 58 778 82 00
fax +48 58 732 60 69
operator.centrala@energa.pl
https://energa-operator.pl/

Enea Operator Sp. z o.o.
ul. Strzeszyńska 58, 60-479 Poznań
tel. +48 61 850 40 00
fax +48 61 884 59 57
https://www.operator.enea.pl/

envelio GmbH
Hildegard-von-Bingen-Allee 2, 50933 Cologne, Germany
https://envelio.com/

Esri Polska Sp. z o.o.
Plac Konesera 9, 03-736 Warszawa
tel. +48 22 749 87 00
esri@esri.pl
https://www.esri.pl/

FORTINET
909 Kifer Road, Sunnyvale, CA 94086 USA
tel. +1 408 235 7700
fax +1 408 235 7737
https://www.fortinet.com/

Globema Sp. z o.o.
ul. Wita Stwosza 22, 02-661 Warszawa
tel. +48 22 848 73 13
https://www.globema.pl/

Innsoft Sp. z o.o.
ul. Murmańska 25, 04-203 Warszawa
tel. +48 22 610 77 50
fax +48 22 870 36 59
poczta@innsoft.pl
https://www.innsoft.pl/

IPC Sp. z o.o.
ul. Młyńska 4 bud. B, 44-100 Gliwice
tel. +48 32 270 02 74
ipc@ipc.biz.pl
https://ipc.biz.pl/

Motorola Solutions Systems Polska Sp. z o.o.
ul. Czerwone Maki 82, 30-392 Kraków
ul. Wołoska 5, 02-675 Warszawa
https://www.motorolasolutions.com/

Nokia Solutions and Networks Sp. z o.o.
ul. Rodziny Hiszpańskich 8, 02-685 Warszawa
tel. +48 22 263 95 07
https://www.nokia.com/

PGE Systemy S.A.
ul. Sienna 39, 00-121 Warszawa
https://pgesystemy.pl/

Pirios S.A.
ul. Josepha Conrada 20, 31-357 Kraków
tel. +48 12 211 92 01
fax +48 12 211 92 10
http://www.pirios.com

POLIXEL Sp. z o.o.
ul. Taborowa 10, 02-699 Warszawa
tel. +48 22 511 19 99
fax +48 22 511 19 10
polixel@polixel.pl
https://www.polixel.pl/

Polcom Sp. z o.o.
ul. Krakowska 43, 32-050 Skawina
tel. 12 420 53 00
office@polcom.com.pl
http://www.polcom.com.pl

Polkomtel Sp. z o.o.
ul. Konstruktorska 4, 02-673 Warszawa
tel. +48 22 426 10 00, +48 22 426 56 00
fax +48 22 426 01 03
https://www.plus.pl/

Schneider Electric Polska Sp. z o.o.
ul. Konstruktorska 12, 02-673 Warszawa
tel. +48 22 584 43 77
poland.helpdesk@se.com
https://www.se.com/pl

Stoen Operator Sp. z o.o.
ul. Piękna 46, 00-672 Warszawa
https://stoen.pl/

Sygnity S.A.
Biurowiec Adgar Plaza B
ul. Postępu 17B, 02-676 Warszawa
tel. +48 22 290 88 00
fax +48 22 290 88 01
biuro@sygnity.pl
https://www.sygnity.pl/

TAURON Dystrybucja S.A.
ul. Podgórska 25A, 31-035 Kraków
https://www.tauron-dystrybucja.pl/

Tekniska Polska
Przemysłowe Systemy Transmisji Danych Sp. z o.o.
ul. Łabędzka 9-9A, 44-121 Gliwice
tel. +48 32 331 11 06 ÷ 09
tekniska@tekniska.pl
https://tekniska.pl/

Transition Technologies-Control Solutions Sp. z o.o.
Grunwaldzki Center
Plac Grunwaldzki 23-27, 50-365 Wrocław
tel. +48 71 77 10 050
sekretariat@tt-cs.com.pl
https://www.tt-cs.com.pl/

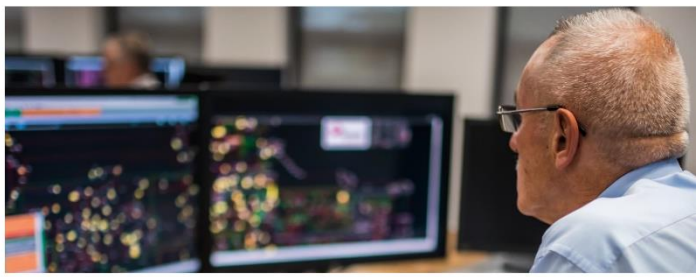
Transition Technologies-Systems Sp. z o.o.
ul. Pawia 55, 01-030 Warszawa
tel. +48 603 602 459
https://ttst.com.pl/tt-systems/

ZPAS S.A.
Przygórze 209, 57-431 Wolibórz
tel. 74 872 01 00, 74 872 01 01
fax 74 872 40 74
info@zpas.pl
https://zpasgroup.pl/

PROJEKT B+R „OPRACOWANIE INNOWACYJNEGO SYSTEMU SKUTECZNEGO MONITOROWANIA I WSPIERANIA URZĄDZEŃ ZABEZPIECZENIOWYCH SPEŁNIAJĄCYCH ZAŁOŻENIA DMS (DISTRIBUTION MANAGEMENT SYSTEM) WRAZ Z OPRACOWANIEM PROTOTYPU STEROWNIKÓW ZABEZPIECZEŃ (W TYM SYGNALIZATORÓW) NA SIECI SN" (SMIWUZ)

Grzegorz Kopacz (Tauron Dystrybucja S.A.)
Zbigniew Grzeszczuk (Mikronika sp. z o.o.)

Projekt B+R „Opracowanie innowacyjnego systemu skutecznego monitorowania i wspierania urządzeń zabezpieczeniowych spełniających założenia DMS (Distribution Management System) wraz z opracowaniem prototypu sterowników zabezpieczeń (w tym sygnalizatorów) na sieci SN"
(SMiWUZ)



Opracowali:

Mikronika Sp. z o.o. — Zbigniew Grzeszczuk

TAURON Dystrybucja S.A. — Grzegorz Kopacz

Fundusze Europejskie Inteligentny Rozwój | Rzeczpospolita Polska | NCBR Narodowe Centrum Badań i Rozwoju | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Konferencja SIwE, Wisła 5-7 listopada 2024r. Projekt „SMiWUZ" 1

Dlaczego SMiWUZ?

Skuteczne **M**onitorowanie i **W**spieranie **U**rządzeń **Z**abezpieczeniowych

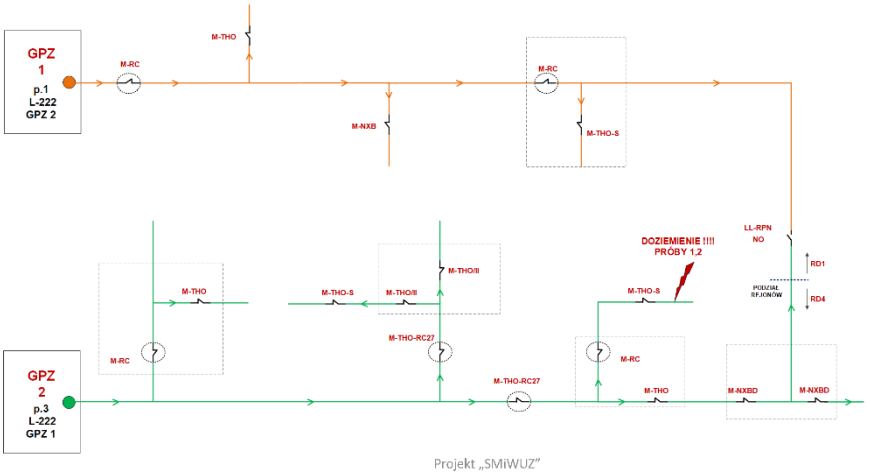
- Wprowadzenie w ostatnich latach na dużą skalę automatyki w głębi sieci dystrybucyjnych SN, spowodowało pojawienie się w tej sieci bardzo dużej ilości urządzeń zdalnie sterowanych (reklozery, wyłączniki wnętrzowe oraz rozłączniki napowietrzne/wnętrzowe z zabudowanymi układami detekcji prądów zwarciowych).
- Ilość tych urządzeń liczona jest już w tysiącach sztuk.
- Wszystkie te urządzenia są klasy zabezpieczeniowej, gdyż wykorzystują do detekcji zwarć pełny układ pomiarowy (3xU, 3xI)
- Zapanowanie nad taką ilością urządzeń (wyliczanie nastaw dla różnych układów pracy sieci) jest, dla specjalistów z wydziałów zabezpieczeń, bardzo uciążliwe i czasochłonne.
- Brak nastaw dostosowanych do bieżącego układu pracy sieci SN, może spowodować nieprawidłowe działanie EAZ oraz systemu FDIR i w konsekwencji wpływ na wzrost wskaźników CTP, CP (SAIDI i SAIFI)
- Dodatkowo sieć SN ciągle „żyje" (jest modernizowana i rozbudowywana).

Rozwiązaniem powyższego problemu jest stworzenie automatycznego systemu, który wspierałby pracę urządzeń zabezpieczeniowych w głębi sieci SN tzn. wyliczałby w sposób on-line nastawy zabezpieczeń dla rzeczywistego układu sieci i wysyłał je zdalnie (GPRS-APN) do urządzeń

Projekt „SMiWUZ" 2

Dlaczego SMiWUZ?

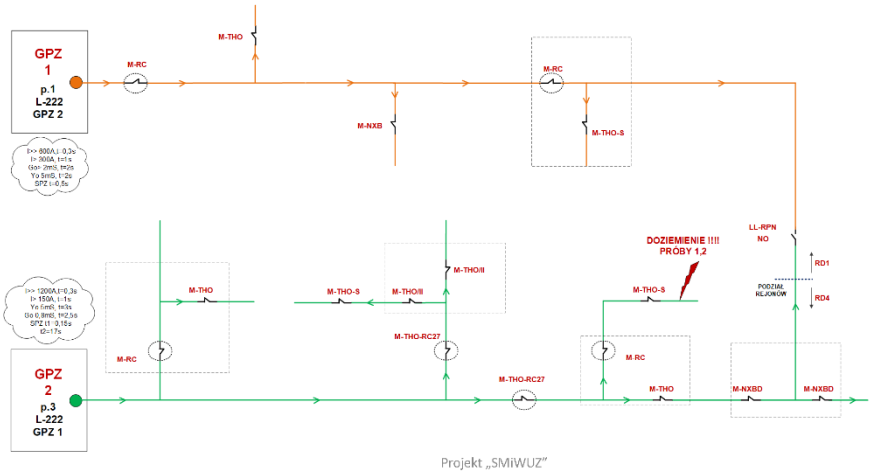
Przykładowy schemat sieci SN – 2 linie SN z 2 GPZ-ów



Projekt „SMiWUZ" 4

Dlaczego SMiWUZ?

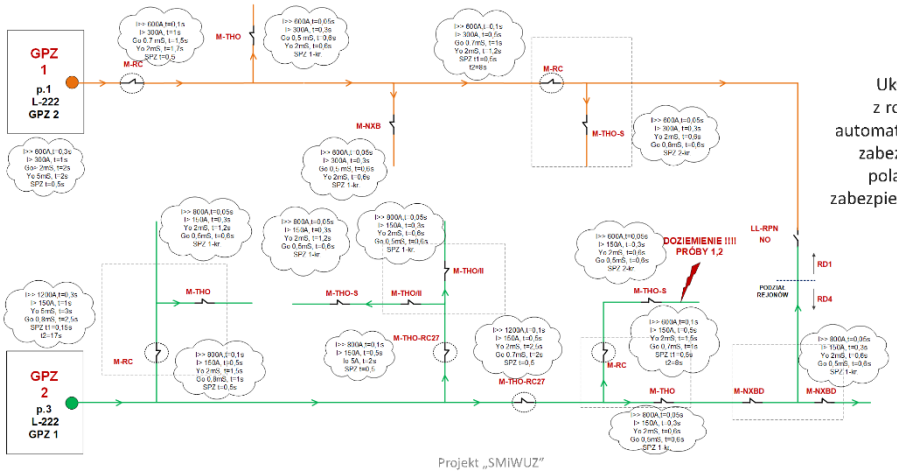
Przykładowy schemat z nastawami zabezpieczeń dla GPZ-ów



Projekt „SMiWUZ" 5

Dlaczego SMiWUZ?

Przykładowy schemat z nastawami zabezpieczeń dla wszystkich obiektów w głębi sieci SN



Układ sieci SN z rozbudowaną automatyką w głębi sieci zabezpieczenia w 2 polach GPZ + 17 zabezpieczeń w głębi sieci

Cel projektu SMiWUZ

Główne cele projektu:

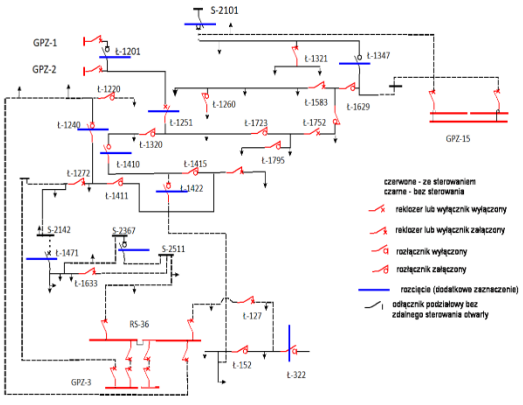
- przeprowadzenie prac badawczo-rozwojowych, które rozwiążą wcześniej omówione problemy,
- stworzony system będzie mógł na bieżąco analizować aktualny stan sieci SN i jej parametry,
- w sposób automatyczny (zdalny) zmieniać nastawy urządzeń w głębi sieci SN (przesyłać do nich wyliczone bieżące nastawy),
- ograniczać skutki zakłóceń.

Smart Grid w sieciach SN
SMiWUZ - realizacja

- W skład systemu **SMiWUZ** wchodzą:
  - Algorytm obliczeniowy wyznaczenia nastaw zabezpieczeń zintegrowany z systemem SCADA SYNDIS RV
  - Moduł zdalnej zmiany nastaw zabezpieczeń i sygnalizatorów poprzez protokół komunikacyjny
  - Prototypy urządzeń zabezpieczeniowych:
    - dla reklozera (pełne zabezpieczenie dla wyłącznika napowietrznego)
    - dla rozłącznika (sygnalizator przepływu prądów zwarciowych)
  - Przygotowany przez TAURON Dystrybucja S.A. obszar badawczo-testowy sieci SN
  - Zainstalowany i uruchomiony dla obszaru badawczo-testowego moduł FDIR.

Projekt „SMiWUZ" 8

Smart Grid w sieciach SN
SMiWUZ - realizacja



Kryteria wyboru obszaru:
- awaryjność sieci,
- potencjalna zmienność układów zasilania,
- zmienność warunków zwarciowych,
- różnorodność sposobów pracy punktu neutralnego sieci SN w obszarze,
- dotychczasowe nasycenie w reklozery, rozłączniki sterowane zdalnie oraz wskaźniki przepływu prądu zwarciowego.

Projekt „SMiWUZ" 9

Smart Grid w sieciach SN
SMiWUZ – realizacja – Ustalenie parametrów urządzeń

- Przyjęto nazwy dla dwóch urządzeń, które maja być wynikiem projektu:
- Sterownik z funkcjami EAZ (w zasadzie zabezpieczenie reklozera)
- Sterownik z funkcjami WPPZ (wskaźnika przepływu prądu zwarciowego)
- Zdefiniowano zakres stosowania nastawy korygowanej (nastawa wielkości kryterialnej, czasowej lub innej, która jest zmieniana przez SMIWUZ po rekonfiguracji sieci)
- Określono wymagane wyposażenie w/w urządzeń ich cechy, funkcje, parametry techniczne

Fragment tabeli definiującej zabezpieczenia sterownika reklozera (sieci ze źródłami lokalnymi):

L.p.	Nazwa zabezpieczenia	Nastawa	Zakres nastawczy	Nastawa korygowana/ stała	Typ sieci - ogólnie	Typ sieci - zalecany	Uwagi
1	-----	napięcie nominalne sieci	6-30 kV	stała	każda	każda	
2	Nadprądowe od skutków zwarć międzyfazowych $I_2>$	prąd I>	20 - 1200 A	korygowana	każda	każda	
		czas t>	0 - 6 s	korygowana			
		blokada od 2. harmonicznej	tak, nie	stała			
		blokada kierunkowa	dodatni ujemny brak	korygowana			

Smart Grid w sieciach SN
SMiWUZ – realizacja
– lista nastaw reklozera i ich zakresy

- System SMIWUZ **wylicza on-line 33 parametry** (wyróżnione na szaro) z listy 95 nastaw zabezpieczeń.
- Pozostałe 62 parametry są konfigurowalne ręcznie przez użytkownika w systemie SMIWUZ
- Do obiektu wysyłany jest cały komplet nastaw zabezpieczeń tzn. 95

Nazwa zabezpieczenia	Numer nastawy	Nazwa nastawy	Zakres nastawy	Uwagi
Nadprądowe zwarciowe I1>>	1	**Tryb działania**	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	2	**Prąd [A]**	20,0 - 8000,0	
	3	**Czas opóźnienia [s]**	0,000 - 6,000	
	4	**Kierunek działania**	Brak / Przód / Tył	Nastawa binarna
	5	**Kąt**	- / 0 / 180	
	6	Blokada 2. harmoniczną	Tak / Nie	Nastawa binarna
Nadprądowe zwarciowe I2>>	7	Tryb działania	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	8	Prąd [A]	20,0 - 8000,0	
	9	Czas opóźnienia [s]	0,000 - 6,000	
	10	**Kierunek działania**	Brak / Przód / Tył	Nastawa binarna
	11	**Kąt**	- / 0 / 180	
	12	Blokada 2. harmoniczną	Tak / Nie	Nastawa binarna
Nadprądowe zwłoczne I1>	13	**Tryb działania**	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	14	**Prąd [A]**	10,0 - 1200,0	
	15	**Czas opóźnienia [s]**	0,00 - 60,00	
	16	**Kierunek działania**	Brak / Przód / Tył	Nastawa binarna
	17	**Kąt**	- / 0 / 180	
	18	Blokada 2. harmoniczną	Tak / Nie	Nastawa binarna
Nadprądowe zwłoczne I2>	19	Tryb działania	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	20	Prąd [A]	10,0 - 1200,0	
	21	Czas opóźnienia [s]	0,00 - 60,00	
	22	**Kierunek działania**	Brak / Przód / Tył	Nastawa binarna
	23	**Kąt**	- / 0 / 180	
	24	Blokada 2. harmoniczną	Tak / Nie	Nastawa binarna
Od asymetrii prądowej Iasym>	25	Tryb działania	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	26	Kryterium detekcji	Składowa przeciwna I2 / Stosunek składowych symetrycznych I2/I1	Nastawa binarna
	27	Prąd [A]	20,0 - 600,0	
	28	Prąd [%]	0 - 500	
	29	Czas opóźnienia [s]	0,00 - 60,00	
	30	Prąd minimalny I1 [A]	0,0 - 500,0	
	31	Blokada 2. harmoniczną	Tak / Nie	Nastawa binarna

Smart Grid w sieciach SN
SMiWUZ – realizacja
– lista nastaw reklozera i ich zakresy – c.d.

Nazwa zabezpieczenia	Numer nastawy	Nazwa nastawy	Zakres nastawy	Uwagi
Zerowoprądowe I0>>	32	Tryb działania	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	33	Prąd 3I0 [A]	1,00 - 300,00	
	34	Czas opóźnienia [s]	0,00 - 20,00	
Zerowoprądowe I0>	35	**Tryb działania**	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	36	**Prąd 3I0 [A]**	1,00 - 300,00	
	37	**Czas opóźnienia [s]**	0,00 - 20,00	
Zerowoprądowe kierunkowe I0k>	38	Tryb działania	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	39	**Kierunek działania**	Czynnomocowe - przód / Czynnomocowe - tył /Biernomocowe - przód / Biernomocowe - tył	Nastawa służy tylko do określenia typu charakterystyki - determinuje nastawę "Kąt"
	40	**Kąt**	0 / 180 / 90 / 270	
	41	Prąd 3I0 [A]	1,00 - 100,00	
	42	Czas opóźnienia [s]	0,00 - 20,00	
Konduktancyjne G0>	43	**Tryb działania**	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	44	**Kierunek działania**	Brak / Przód / Tył	Nastawa binarna
	45	**Kąt**	- / 0 / 180	
	46	**Konduktancja [mS]**	0,10 - 50,00	
	47	**Czas opóźnienia [s]**	0,00 - 20,00	
Susceptancyjne kierunkowe B0k>	48	**Tryb działania**	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	49	**Kierunek działania**	Przód / Tył	Nastawa binarna
	50	**Kąt**	90 / 270	
	51	**Susceptancja [mS]**	0,10 - 50,00	
	52	**Czas opóźnienia [s]**	0,00 - 20,00	
Admitancyjne Y0>	53	**Tryb działania**	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	54	**Admitancja [mS]**	0,10 - 50,00	
	55	**Czas opóźnienia [s]**	0,00 - 20,00	
Człon rozruchowy zerowonapięciowy U0r>	56	**Napięcie 3U0 [%]**	2 - 50	
Nadnapięciowe U>	57	Tryb działania	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	58	Napięcie [V]	6000 - 38000	
	59	Czas opóźnienia [s]	0,00 - 60,00	
Podnapięciowe U<<	60	Tryb działania	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	61	Napięcie [V]	3000 - 30000	
	62	Czas opóźnienia [s]	0,00 - 60,00	

Smart Grid w sieciach SN
SMiWUZ – realizacja
– lista nastaw reklozera i ich zakresy – c.d.

Nazwa zabezpieczenia	Numer nastawy	Nazwa nastawy	Zakres nastawy	Uwagi
Podnapięciowe U<	63	Tryb działania	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	64	Napięcie [V]	3000 - 30000	
	65	Czas opóźnienia [s]	0,00 - 60,00	
Zerowonapięciowe U0>	66	Tryb działania	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	67	Napięcie 3U0 [%]	2 - 50	
	68	Czas opóźnienia [s]	0,00 - 60,00	
Nadczęstotliwościowe f>	69	Tryb działania	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	70	Częstotliwość [Hz]	49,00 - 54,00	
	71	Czas opóźnienia [s]	0,0 - 300,0	
Podczęstotliwościowe f<	72	Tryb działania	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	73	Częstotliwość [Hz]	46,00 - 51,00	
	74	Czas opóźnienia [s]	0,0 - 300,0	
df/dt	75	Tryb działania	NIEAKTYWNE / SYGNALIZACJA / WYŁĄCZ	Nastawa binarna
	76	Szybkość zmian częstotliwości [Hz/s]	0,00 - 10,00	
	77	Czas opóźnienia [s]	0,0 - 300,0	
Automatyka SPZ - zabezpieczenia nadprądowe zwarciowe	78	Tryb działania	Odstawiona / 1 cykl / 2 cykle / 3 cykle	
	79	Czas 1 przerwy w cyklu SPZ [s]	0,10 - 180,00	
	80	Czas 2 przerwy w cyklu SPZ [s]	0,10 - 180,00	
	81	Czas 3 przerwy w cyklu SPZ [s]	0,10 - 180,00	
Automatyka SPZ - zabezpieczenia nadprądowe zwłoczne	82	Tryb działania	Odstawiona / 1 cykl / 2 cykle / 3 cykle	
	83	Czas 1 przerwy w cyklu SPZ [s]	0,10 - 180,00	
	84	Czas 2 przerwy w cyklu SPZ [s]	0,10 - 180,00	
	85	Czas 3 przerwy w cyklu SPZ [s]	0,10 - 180,00	
Automatyka SPZ - zabezpieczenia ziemnozwarciowe	86	Tryb działania	Odstawiona / 1 cykl / 2 cykle / 3 cykle	
	87	Czas 1 przerwy w cyklu SPZ [s]	0,10 - 180,00	
	88	Czas 2 przerwy w cyklu SPZ [s]	0,10 - 180,00	
	89	Czas 3 przerwy w cyklu SPZ [s]	0,10 - 180,00	
Parametry dodatkowe	90	Czas akceptacji SPZ [s]	1,50 - 180,00	
	91	Czas blokady SPZ po operacyjnym załączeniu [s]	1,00 - 30,00	
Blokada 2. harmoniczną	92	Udział 2. harmonicznej w prądzie roboczym [%]	5 - 50	
	93	Minimalna suma modułów prądów fazowych [A]	10,0 - 2000,0	
	94	Maksymalna suma modułów prądów fazowych [A]	50,0 - 3000,0	
	95	Maksymalny czas trwania blokady [s]	0,10 - 30,00	

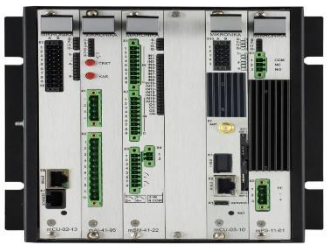
Smart Grid w sieciach SN
SMiWUZ – realizacja – urządzenia

W ramach projektu opracowano i wyprodukowano 2 prototypy urządzeń pod roboczymi nazwami:

1. **Sterownik SO-52v21-SMRE** - prototypowy sterownik reklozera z funkcjami zabezpieczeń SN
2. **Sterownik SO-52v21-SMRO** - prototypowy sterownik rozłącznika z funkcjami sygnalizatora zwarć SN

Sterownik SO-52v21-SMRE

Sterownik SO-52v21-SMRO



Projekt „SMiWUZ" 15

Smart Grid w sieciach SN
SMiWUZ – realizacja – parametry urządzeń

Parametry urządzeń

W warunkach laboratoryjnych potwierdzono parametry prototypów m.in.:

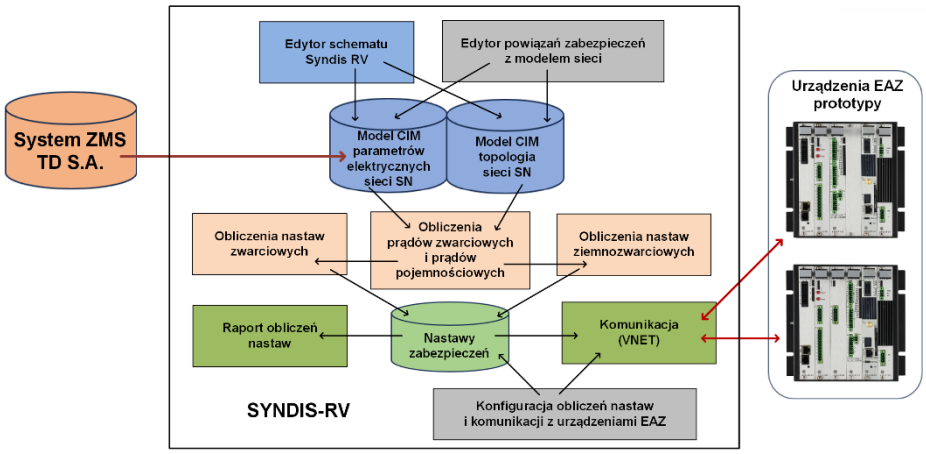
- szybkość procesora min. 300MHz
- rozmiar pamięci wewnętrznej min.256MB
- porty komunikacyjne: min. 1xRS232, 1xRS485, Ethernet,
- rodzaje mediów komunikacyjnych: skrętka, światłowód, GSM/2G/4G, TETRA.
- wymagane protokoły komunikacyjne: DNP3, IEC 60870-5-103, IEC 60870-5-104, IEC 61850
- zakresy temp. pracy min.: -5°C ÷ 50°C
- parametry kompatybilności środowiskowej: IEC 60255-26, IEC 61850-3
- poziom bezpieczeństwa cybernetycznego IT: IEC 62351
- Moc pobierana ze źródła zasilania: < 20W

Urządzenia prototypowe spełniają ponadto poniższe wymagania:

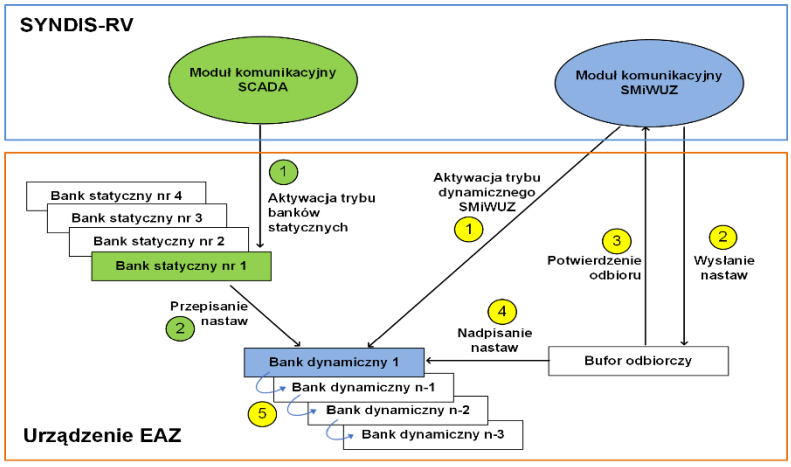
- realizują odbiór, przetworzenie i aktywacja obliczonych nastaw w czasie poniżej 30 sekund
- obsługują następujące protokoły komunikacyjne: DNP3, IEC 60870-5-103, IEC 60870-5-104, IEC61850.

Projekt „SMiWUZ" 16

Smart Grid w sieciach SN
SMiWUZ – realizacja – konfiguracja systemu



Smart Grid w sieciach SN
SMiWUZ – realizacja – konfiguracja systemu



Smart Grid w sieciach SN
SMiWUZ – realizacja – obliczenia

- Wybrany fragment sieci SN tzw. obszar badawczo-testowy został wprowadzony do systemu SYNDIS-SMiWUZ.
- Parametry elektryczne i stan sieci zostały wprowadzone w opracowanym modelu zgodnym z normami CIM - IEC 61970, IEC61968.
- Proces importu i mapowania na model CIM był połączony z weryfikacją spójności danych z bazami systemu SCADA SYNDIS RV oraz systemu majątkowego ZMS.
- Dla modelu obszaru badawczo-testowy zbudowanego w systemie SYNDIS RV uruchomiono następujące obliczenia inżynierskie:
  - prądów zwarciowych
  - rozpływowych,
  - estymatora obciążeń,
  - optymalizacji punktów podziału.

Powyższe moduły były niezbędne dla uzyskania przez system badawczy cech systemu SCADA DMS.

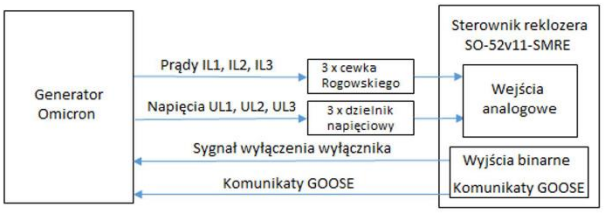
Projekt „SMiWUZ" 19

Smart Grid w sieciach SN
SMiWUZ – realizacja – obliczenia

- Moduły obliczeniowe zostały uruchomione w środowisku laboratoryjnym Mikroniki.
- Moduły obliczeniowe współpracowały z systemem SYNDIS RV, korzystając z jego baz danych i modułów komunikacyjnych.
- Wyniki obliczeń modułów programowych porównane były z wynikami obliczeń inżynierów-specjalistów ds. EAZ TAURON Dystrybucja S.A.
- Dla 15 układów pracy sieci osiągnięto deklarowaną we wniosku zgodność.

Projekt „SMiWUZ" 20

Smart Grid w sieciach SN
SMiWUZ – realizacja – schemat układu testowego

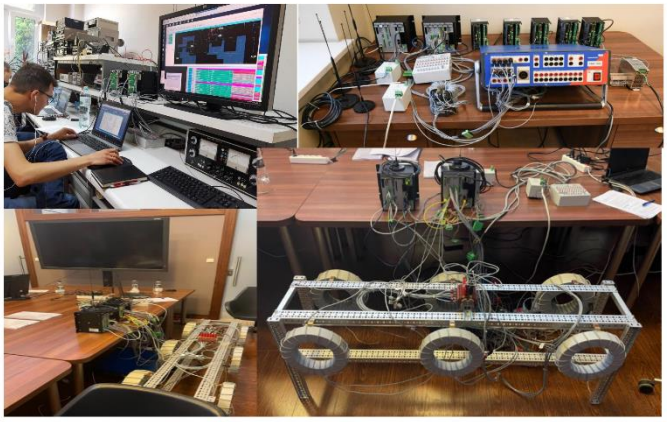


Podczas testów integracyjnych przeprowadzono szereg prób potwierdzających skuteczność systemu SMiWUZ w zakresie:

- obliczania nastaw funkcji zabezpieczeniowych,
- przesyłania nastaw do urządzeń prototypowych (SO-52v21-SMRE oraz SO-52v21-SMRO)
- przeładowania nastaw w urządzeniach prototypowych
- sprawdzenie poprawności działania modułów zabezpieczeniowych

Projekt „SMiWUZ" 21

Smart Grid w sieciach SN
SMiWUZ – realizacja – testy laboratoryjne



Projekt „SMiWUZ" 22

Smart Grid w sieciach SN
SMiWUZ – realizacja – testy terenowe

TESTY SYSTEMU w konfiguracji docelowej z urządzeniami w głębi sieci SN

Na obiektach w terenie na obszarze badawczo-testowym zainstalowano:

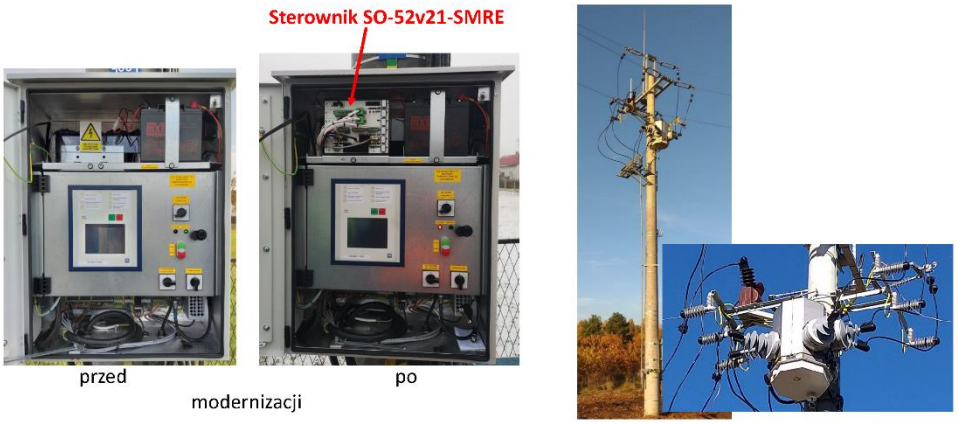
- 6 szt. **Sterownik SO-52v21-SMRO** - sterownik rozłącznika z funkcjonalnością sygnalizatora zwarć - obiekty zmodernizowane były już pod względem układów pomiarowych, wymieniono istniejące sterowniki na prototypy
- 2 szt. **Sterownik SO-52v21-SMRE** - sterownik reklozera z funkcjami zabezpieczeń SN - obiekty nowo zainstalowane dostosowane do sterowników prototypowych

Przeprowadzano testy na wybranych 4 z 15 wariantów układu pracy sieci.

Projekt „SMiWUZ" 23

Smart Grid w sieciach SN
SMiWUZ – realizacja – testy terenowe

Reklozer THO-RC27 dostosowany do wymogów SMIWUZ



Projekt „SMiWUZ" 24

Smart Grid w sieciach SN
SMiWUZ – realizacja – testy terenowe

Rozłącznik THO-24 dostosowany do wymogów SMIWUZ

przed

Sterownik SO-52v21-SMRO

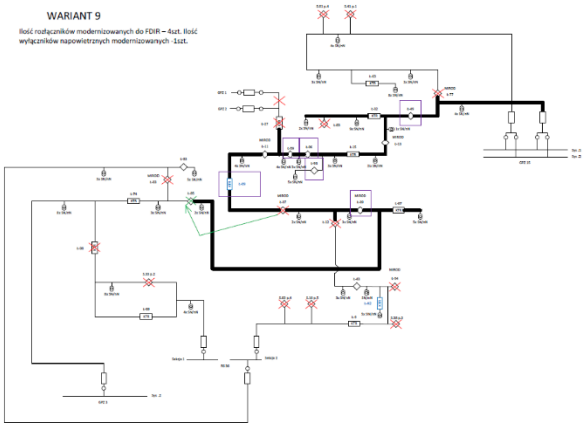
po

modernizacji

Projekt „SMiWUZ" 25

Smart Grid w sieciach SN
SMiWUZ – realizacja – testy terenowe

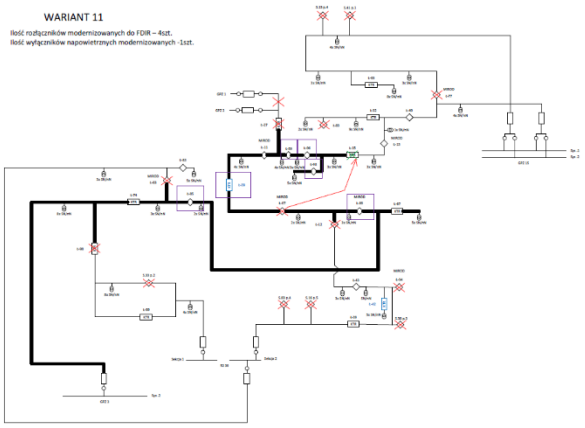
Przykładowy wariant 9 układu pracy sieci SN (jeden z 15)



Projekt „SMiWUZ" 26

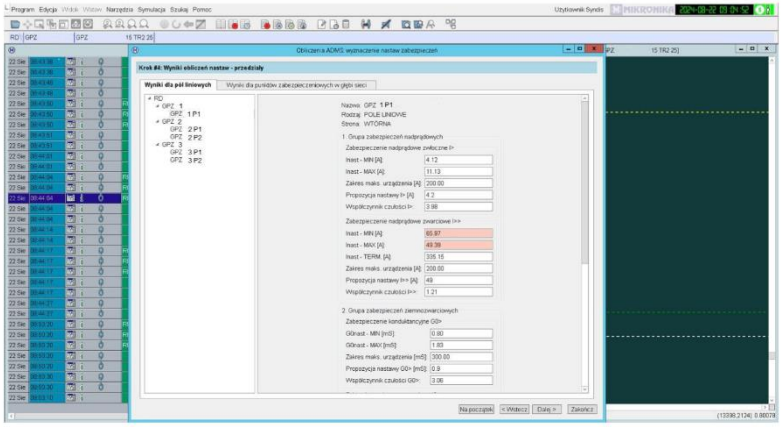
Smart Grid w sieciach SN
SMiWUZ – realizacja – testy terenowe

Przykładowy wariant 11 układu pracy sieci SN (jeden z 15)



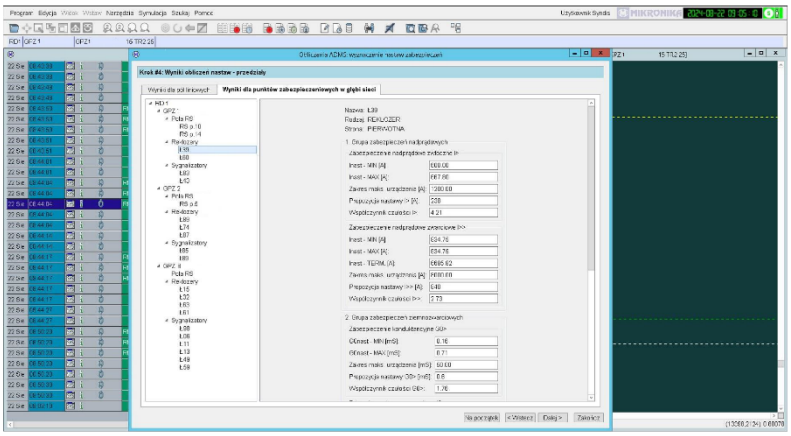
Projekt „SMiWUZ" 27

Smart Grid w sieciach SN
SMiWUZ – przykładowe wyniki obliczeń – pole liniowe



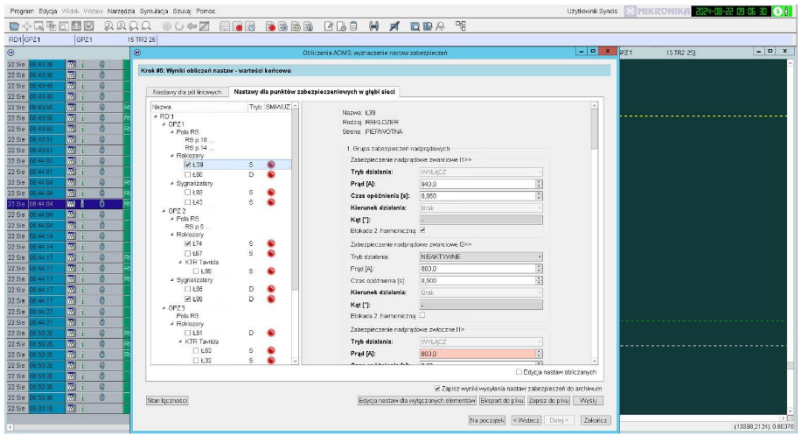
Projekt „SMiWUZ" 28

Smart Grid w sieciach SN
SMiWUZ – przykładowe wyniki obliczeń - reklozer



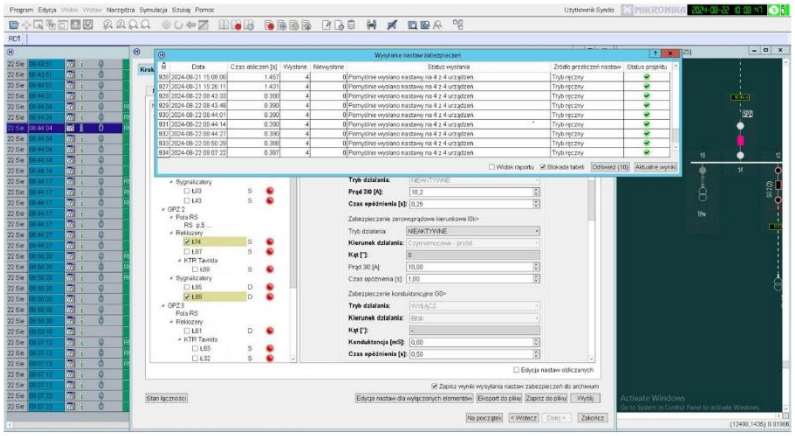
Projekt „SMiWUZ" 29

Smart Grid w sieciach SN
SMiWUZ – przykładowe wyniki obliczeń - reklozer



Projekt „SMiWUZ" 30

Smart Grid w sieciach SN
SMiWUZ – przykładowe wyniki obliczeń i przesyłania nastaw



Projekt „SMiWUZ" 31

Smart Grid w sieciach SN
SMiWUZ – podsumowanie

Projekt B&R zakończył się pomyślnie w czerwcu 2022 roku !!!

WNIOSKI:

- **Podczas testów potwierdzono przyjęte założenia**
  - System prawidłowo wylicza i przesyła nastawy zarówno przy wyzwoleniu ręcznym jak i przy zdarzeniach z sieci SN (wyłączenie wyłączników z automatyki zabezpieczeniowej)
  - System SMiWUZ poprawnie współpracuje z systemem FDIR
  - Urządzenia prototypowe spełniają przyjęte założenia pod względem komunikacyjnym i funkcjonalnym
  - Realny czas obliczenia nastaw dla 8 obiektów na obszarze badawczo-testowym łącznie z ich wysłaniem do obiektów wynosił: 12-15 sek.

Projekt „SMiWUZ" 32

Smart Grid w sieciach SN
SMiWUZ – dalsze prace rozwojowe i wdrożeniowe

DALSZE PRACE ROZWOJOWE po zakończeniu projektu B+R:

Zakończone:

- Pełna integracja systemu SMiWUZ z systemem produkcyjnym SCADA SYNDIS-RV
- Optymalizacja w zakresie współpracy z modułem FDIR (nie wszystkie pobudzenia będą wymuszać obliczenia i wysyłania nastaw np. „znieczulenie" na zdarzenia SPZ oraz przełączenia modułu FDIR)
- Optymalizacja w sposobie wysyłania wyliczonych nastaw (wysyłanie nastawy tylko do obiektów, w których nastąpiły zmiany nastaw o zadaną wartość)
- Uruchomienie drivera do urządzeń zabezpieczeniowych KTR firmy Tavrida – dla 8 szt.
- Optymalizacja obszarów obliczeń do obszaru zasilanego z danej sekcji GPZ, na której wystąpiło wymuszenie obliczeń (zmieniła się topologia sieci SN)

W trakcie realizacji:

- Rozwinięcie interfejsu komunikacji z użytkownikami **- w trakcie realizacji (w 2024 r.)**
- Uwzględnienie źródeł wytwórczych w głębi sieci w algorytmach wyznaczania rozpływów prądów zwarciowych oraz nastawy zabezpieczeń **- do realizacji (w 2025/2026 r.)**

Projekt „SMiWUZ" 33

Smart Grid w sieciach SN
SMiWUZ – podsumowanie

1. **Model CIM**
   a. Model topologiczny w SCADA SYNDIS
   b. Model parametrów elektrycznych (typy przewodów/kabli, ich długość, przekrój, moce trafo, itp.)
2. **Podstawowy obszar obliczeń dla SMiWUZ**
   a. **Sekcja GPZ** – system SCADA „śledzi" na bieżąco, które obiekty należą do danej sekcji GPZ. Po zmianie układu sieci następuje migracja obiektów pomiędzy sekcjami GPZ-ów
   b. Obliczenia wykonywane są dla danej sekcji GPZ lub kilku sekcji różnych GPZ-ów, w których nastąpiła zmiana układu.
   c. Umożliwia to etapowe wdrażanie systemu SMIWUZ
3. **Wiele konfigurowalnych typów obiektów uwzględnianych w obliczeniach**
   a. Reklozery – stopniowanie czasowe z GPZ i innymi reklozerami/wyłącznikami
   b. Rozłączniki z sygnalizatorami p.p.z.
   c. Łączniki podziałowe
   d. Obiekty przy generacjach (zazwyczaj reklozery) – konfiguracja stała, ale wpływająca na obliczenia i parametry innych obiektów

Projekt „SMiWUZ" 34

Smart Grid w sieciach SN
SMiWUZ – podsumowanie

4. Urządzenia w głębi sieci SN współpracujące z SMiWUZ (odbierające zdalnie nastawy)

a. Urządzenia firmy Mikronika
   i. Zabezpieczenia współpracujące z reklozerami i wyłącznikami SN
   ii. Zabezpieczenia współpracujące z rozłącznikami z sygnalizatorami p.p.z.

b. Urządzenia/zabezpieczenia firmy Tavrida dla reklozera KTR – oddzielny driver
   i. Nastawy przesyłane protokołem IEC 60870-5-104 do odpowiednich statycznych banków nastaw i potem banki są przełączane

c. Urządzenia/zabezpieczenia innych firm~~y~~ – do napisania oddzielny/odpowiedni driver
   i. Warunek konieczny to możliwość przesyłania nastaw do zabezpieczenia protokołem komunikacyjnym IEC 60870-5-104 lub DNP3 (nie programem fabrycznym !!!)

Projekt „SMiWUZ" 35

Smart Grid w sieciach SN
SMiWUZ – podsumowanie

5. Wyzwolenie systemu SMIWUZ poprzez zmianę układu sieci

a. Start obliczeń SMIWUZ po zakończeniu rekonfiguracji sieci SN przez moduł FDIR
b. Start obliczeń SMIWUZ po każdym przełączeniu sieci przez Operatora lub wyzwolenie przez operatora po zakończeniu operacji łączeniowych
   i. Prace planowe
   ii. Zmiana układu normalnego
   iii. itp.
c. Start obliczeń SMIWUZ poprzez niezależne (w dowolnym momencie) wyzwolenie przez Operatora (np. w celu sprawdzenia poprawności działania systemu)

6. Praca systemu SMIWUZ w trybie symulacji (off-line)

a. Możliwość wyliczenia nastaw dla różnych symulowanych układów sieci SN i ich weryfikacja przez Wydziały Zabezpieczeń

Projekt „SMiWUZ" 36

Smart Grid w sieciach SN
SMiWUZ – podsumowanie

7. Walidacja wyników obliczeń

a. Jeśli jakiś parametr nie mieści się we wcześniej zadeklarowanych przedziałach to dla tej sekcji przerywany jest dalszy proces, następuje ALARM (co i gdzie jest źle) i SMIWUZ zostaje zatrzymany

8. Automatyczne wysyłanie nastaw do obiektów w głębi sieci SN (konfigurowane)

a. Do wszystkich obiektów niezależnie od zmian parametrów
b. Tylko do tych, w których nastąpiła zmiana wartości nastawy o skonfigurowany wcześniej przedział (procentowy lub wartościowy)

9. Prezentacja wyników obliczeń i transmisji

a. Na ekranach/oknach z poziomu systemu SCADA
b. Eksport do Excela lub PDF

10. Archiwizacja wyników obliczeń

Projekt „SMiWUZ" 37

Referat stanowi rozpowszechnienie rezultatów projektu „Opracowanie innowacyjnego systemu skutecznego monitorowania i wspierania urządzeń zabezpieczeniowych spełniających założenia DMS (Distribution Management System) wraz z opracowaniem prototypu sterowników zabezpieczeń (w tym sygnalizatorów) na sieci SN" współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Inteligentny Rozwój, Działanie 1.2. Sektorowe programy B+R.

Termin realizacji projektu: 2018-08-01 do 2022-06-30

Całkowity koszt realizacji projektu netto: 7 013 100,00 zł

Wkład Funduszy Europejskich: 4 026 587,50 zł

Fundusze Europejskie Inteligentny Rozwój | Rzeczpospolita Polska | NCBR Narodowe Centrum Badań i Rozwoju | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Projekt „SMiWUZ" 38

Dziękujemy za uwagę

Projekt „SMiWUZ" 39

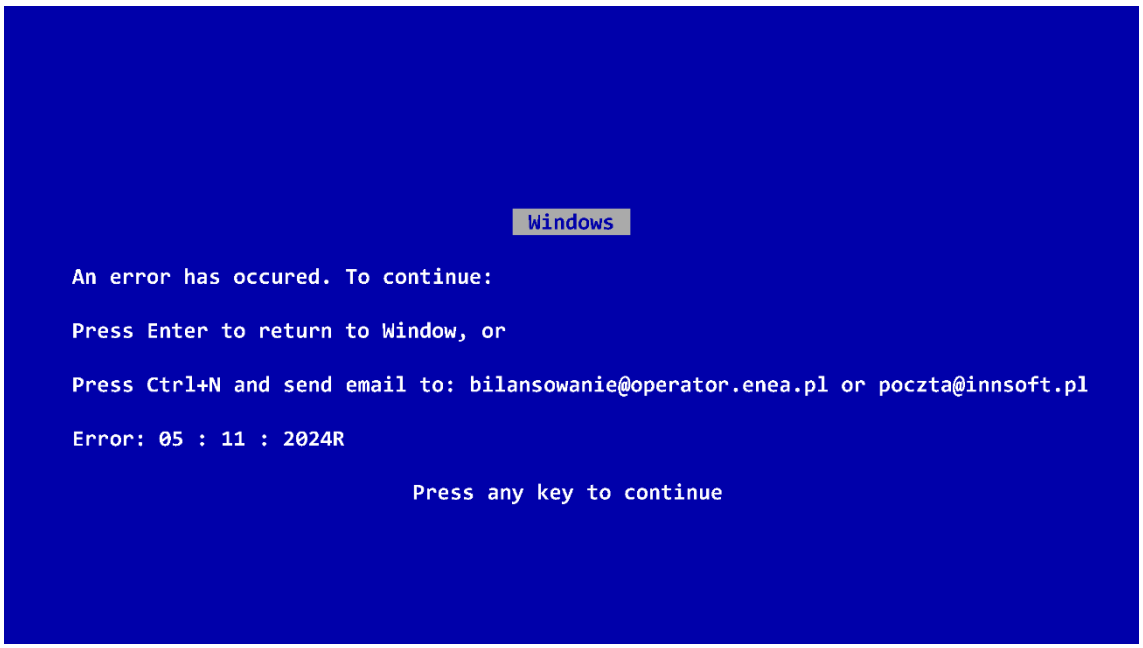
AUTOMATYZACJA MASOWYCH PROCESÓW UŻYTKOWNIKA NA PRZYKŁADZIE WDROŻENIA W ENEA OPERATOR

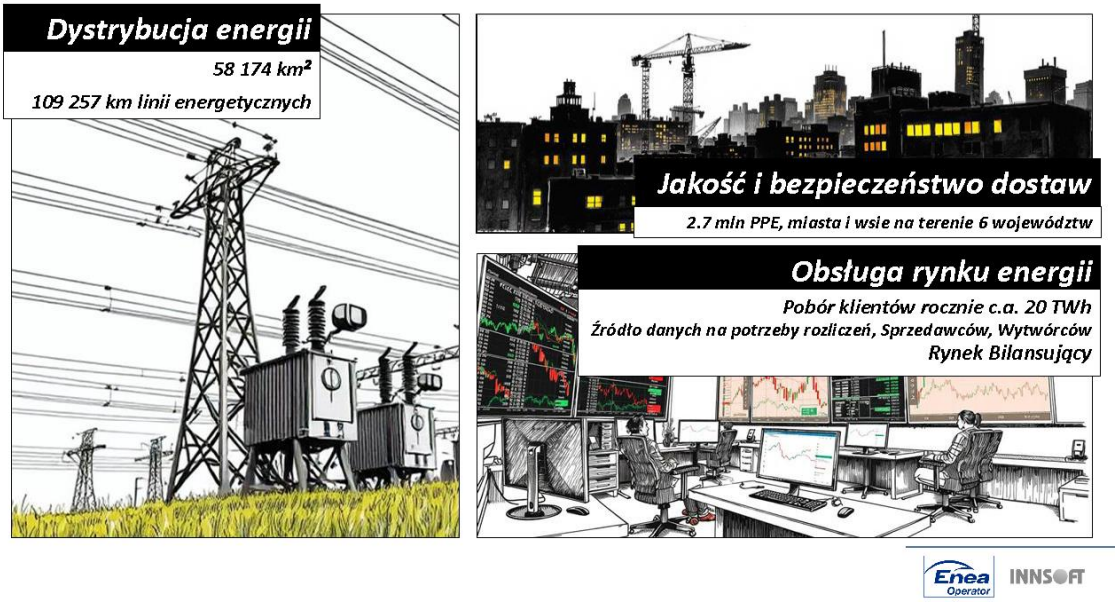
Tomasz Leskier (Innsoft Sp. z o.o.)
dr inż. Jakub Dąbrowski (Enea Operator Sp. z o.o.)

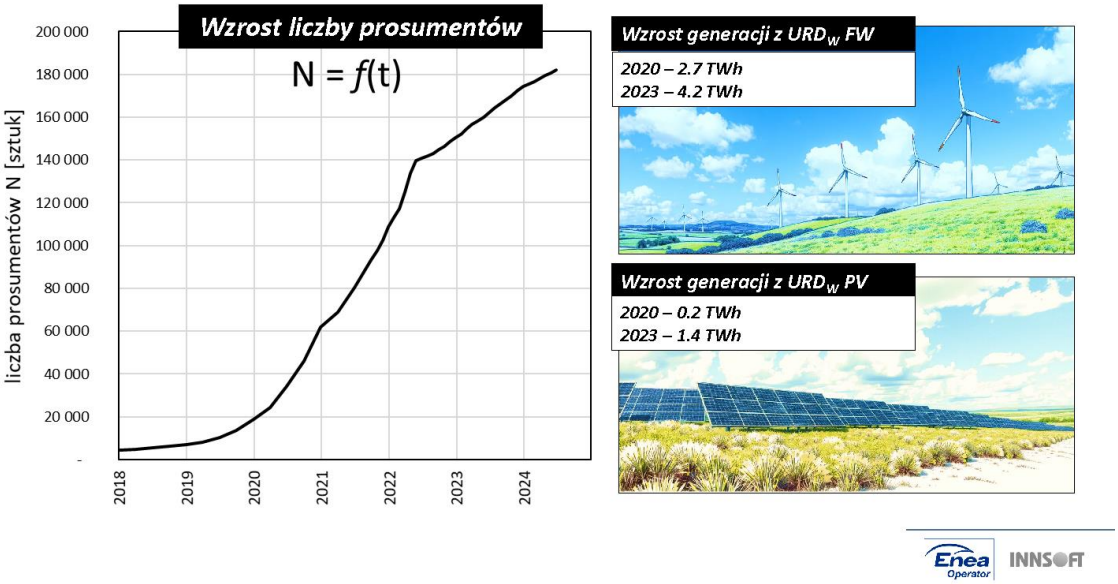
Automatyzacja masowych procesów użytkownika na przykładzie wdrożenia w ENEA Operator

Enea Operator
dr inż. Jakub Dąbrowski

INNSOFT
mgr inż. Tomasz Leskier




Dystrybucja energii
58 174 km²
109 257 km linii energetycznych
Jakość i bezpieczeństwo dostaw
2.7 mln PPE, miasta i wsie na terenie 6 województw
Obsługa rynku energii
Pobór klientów rocznie c.a. 20 TWh
Źródło danych na potrzeby rozliczeń, Sprzedawców, Wytwórców
Rynek Bilansujący
Enea Operator
INNSOFT

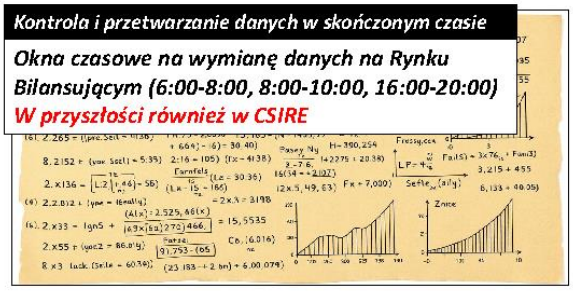

Wzrost liczby prosumentów
N = f(t)
liczba prosumentów N [sztuk]
200 000
180 000
160 000
140 000
120 000
100 000
80 000
60 000
40 000
20 000
-
2018
2019
2020
2021
2022
2023
2024
Wzrost generacji z URD$_W$ FW
2020 – 2.7 TWh
2023 – 4.2 TWh
Wzrost generacji z URD$_W$ PV
2020 – 0.2 TWh
2023 – 1.4 TWh
Enea Operator
INNSOFT

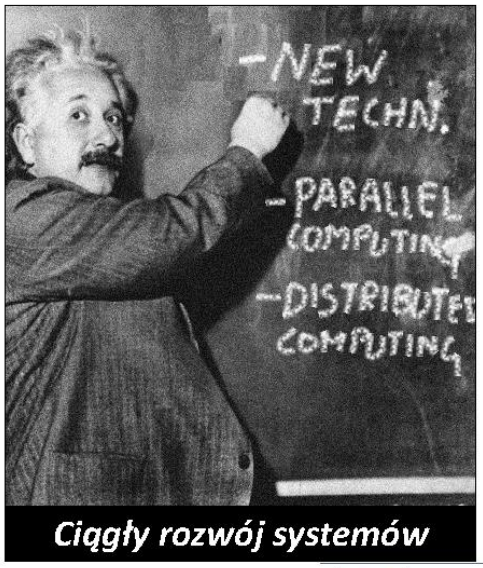
Pozyskiwanie coraz większych ilości danych

Interfejs z systemem AMI:
10.2020 – kilkaset MB i c.a. 25k xml-i / dobę (format 1h)
10.2024 – 80 GB i c.a. 500k xml-i /dobę (format 15min)

Kontrola i przetwarzanie danych w skończonym czasie

Okna czasowe na wymianę danych na Rynku Bilansującym (6:00-8:00, 8:00-10:00, 16:00-20:00)
W przyszłości również w CSIRE



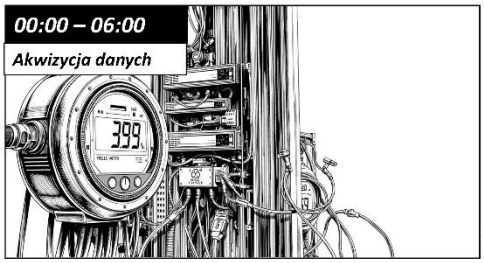


Ciągły rozwój systemów

Enea Operator INNSOFT

00:00 – 06:00

Akwizycja danych

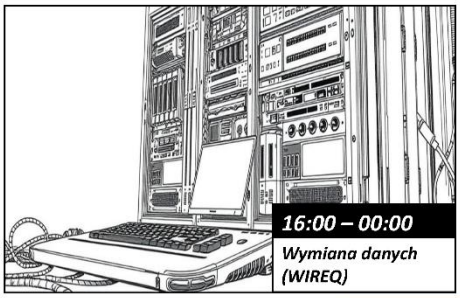


06:00 – 10:00

Agregacja, weryfikacja i wymiana danych (sFTP, WIREQ)

10:00 – 16:00

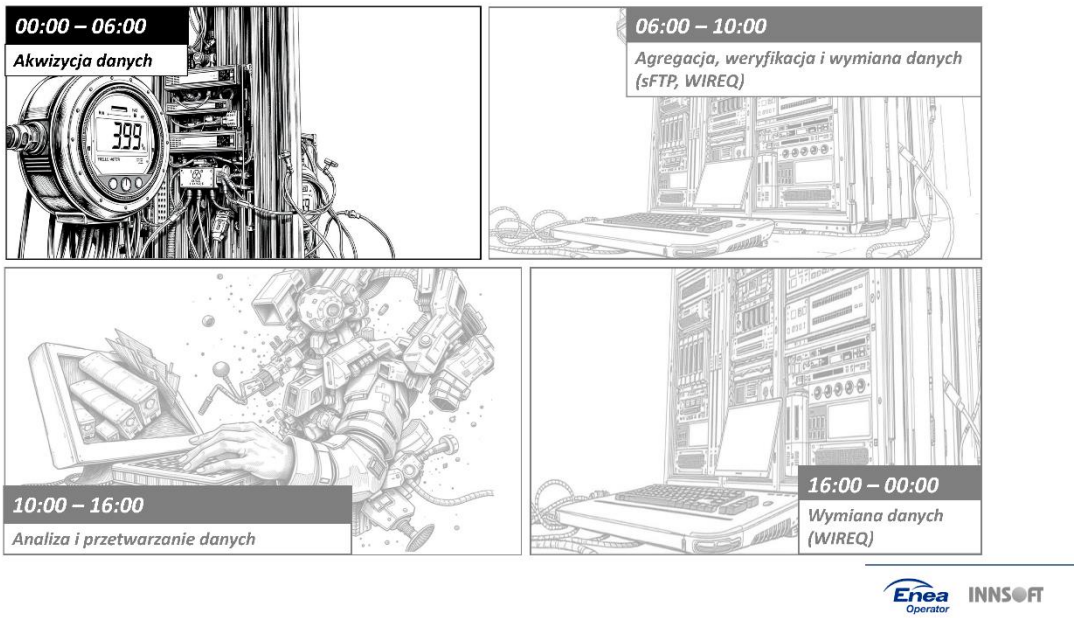
Analiza i przetwarzanie danych

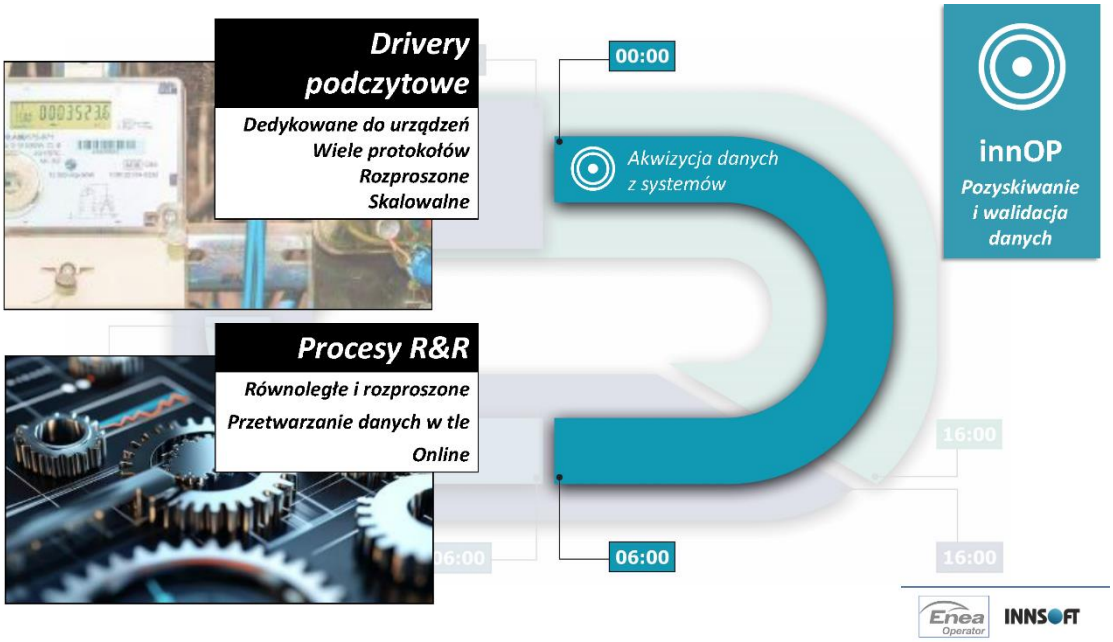


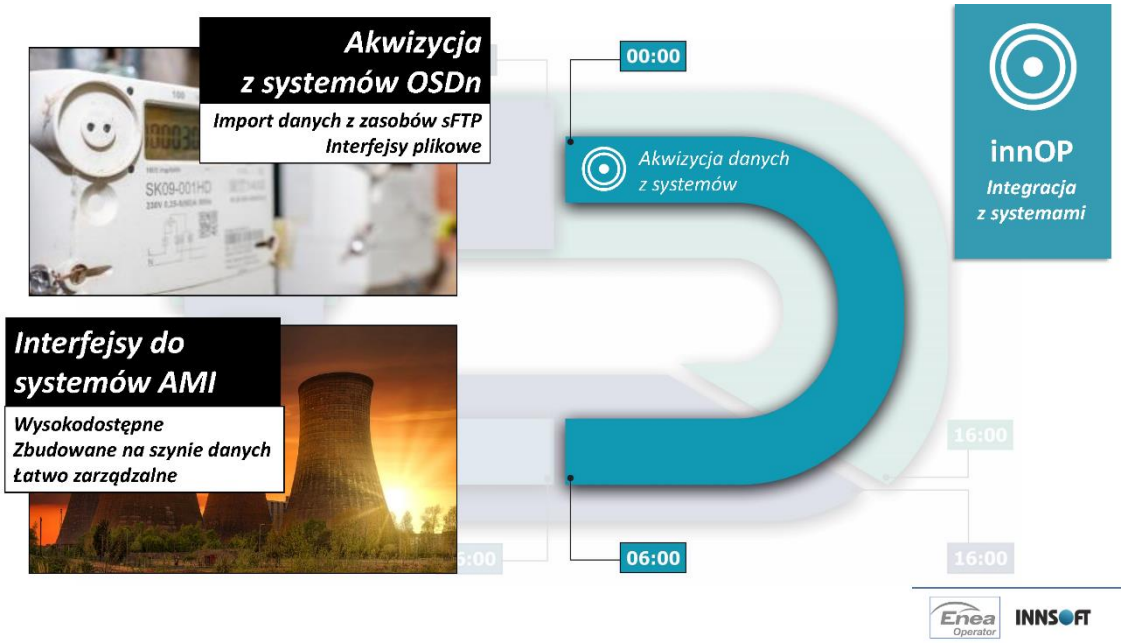
16:00 – 00:00

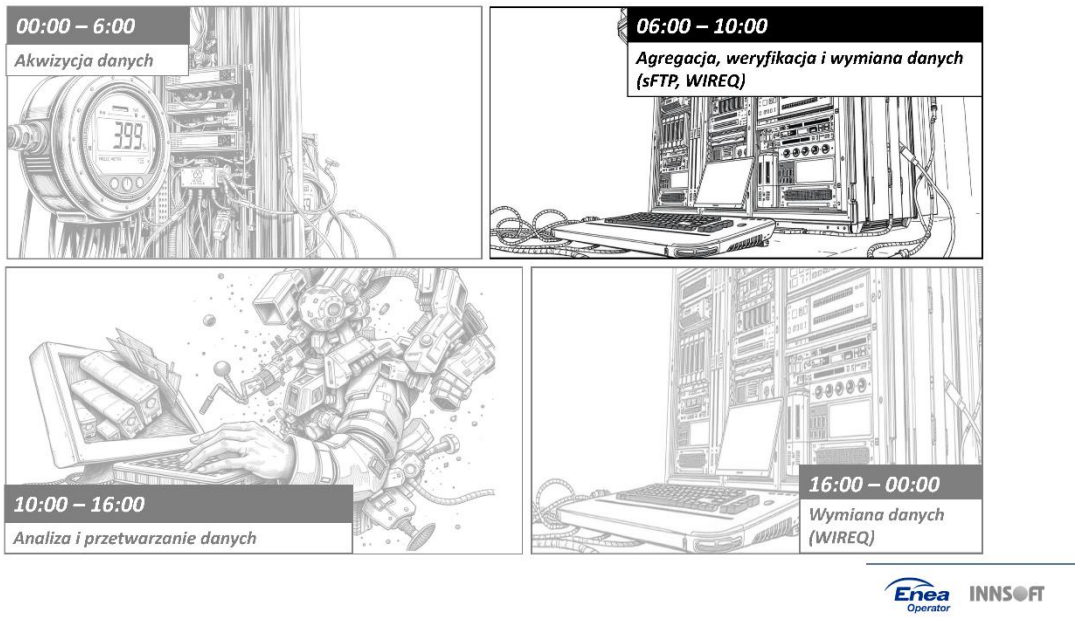
Wymiana danych (WIREQ)

Enea Operator INNSOFT

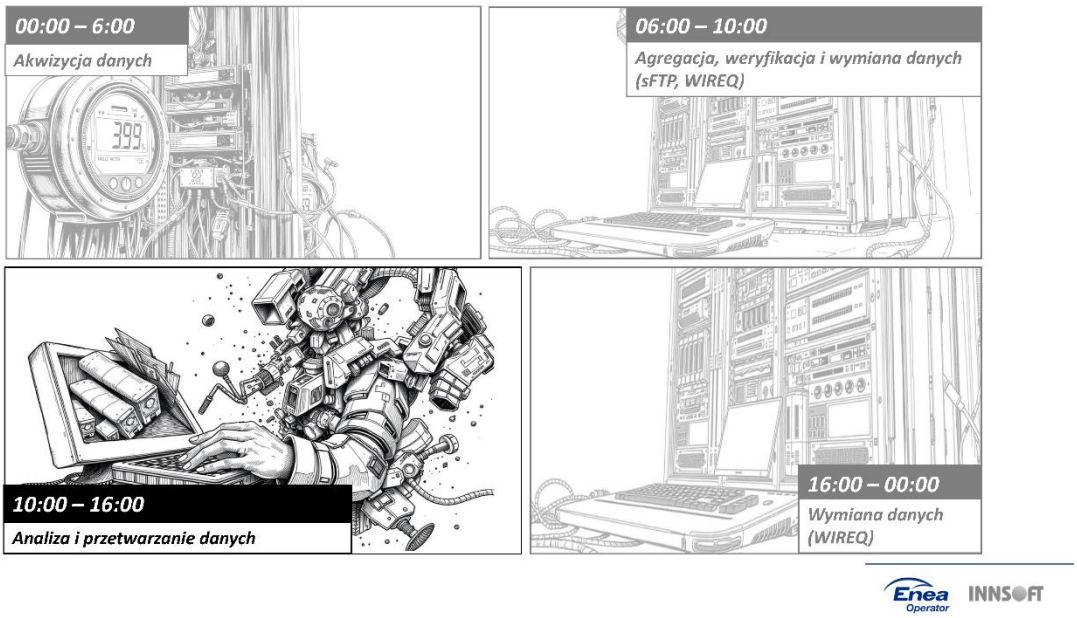

00:00 – 06:00
Akwizycja danych
06:00 – 10:00
Agregacja, weryfikacja i wymiana danych (sFTP, WIREQ)
10:00 – 16:00
Analiza i przetwarzanie danych
16:00 – 00:00
Wymiana danych (WIREQ)
Enea Operator
INNSOFT


Drivery podczytowe
Dedykowane do urządzeń
Wiele protokołów
Rozproszone
Skalowalne
Procesy R&R
Równoległe i rozproszone
Przetwarzanie danych w tle
Online
00:00
Akwizycja danych z systemów
06:00
16:00
16:00
innOP
Pozyskiwanie i walidacja danych
Enea Operator
INNSOFT

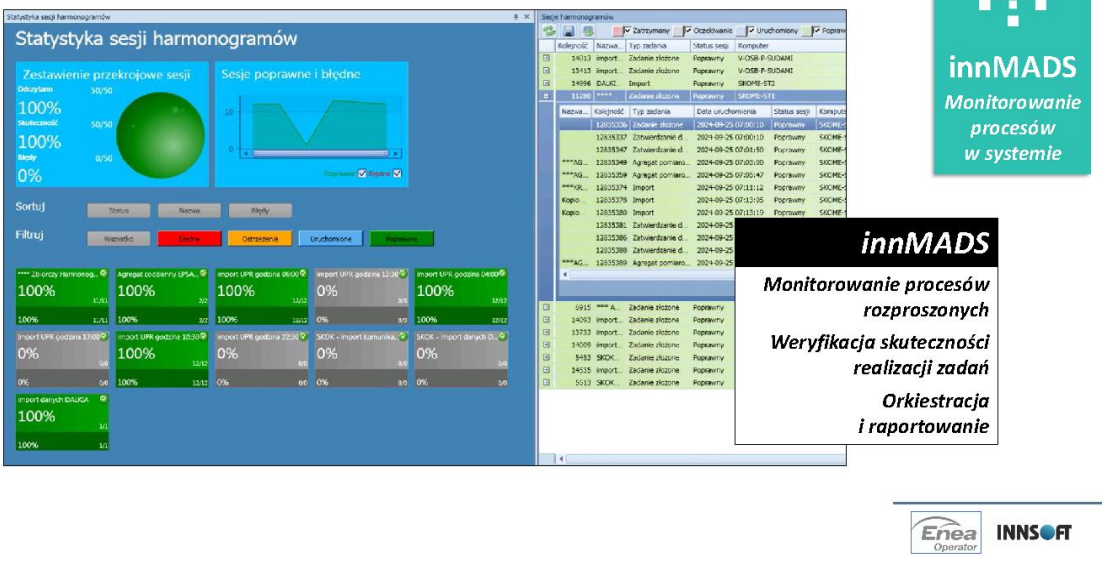

Akwizycja
z systemów OSDn
Import danych z zasobów sFTP
Interfejsy plikowe
Interfejsy do
systemów AMI
Wysokodostępne
Zbudowane na szynie danych
Łatwo zarządzalne
00:00
Akwizycja danych
z systemów
06:00
innOP
Integracja
z systemami
16:00
16:00
Enea Operator
INNSOFT

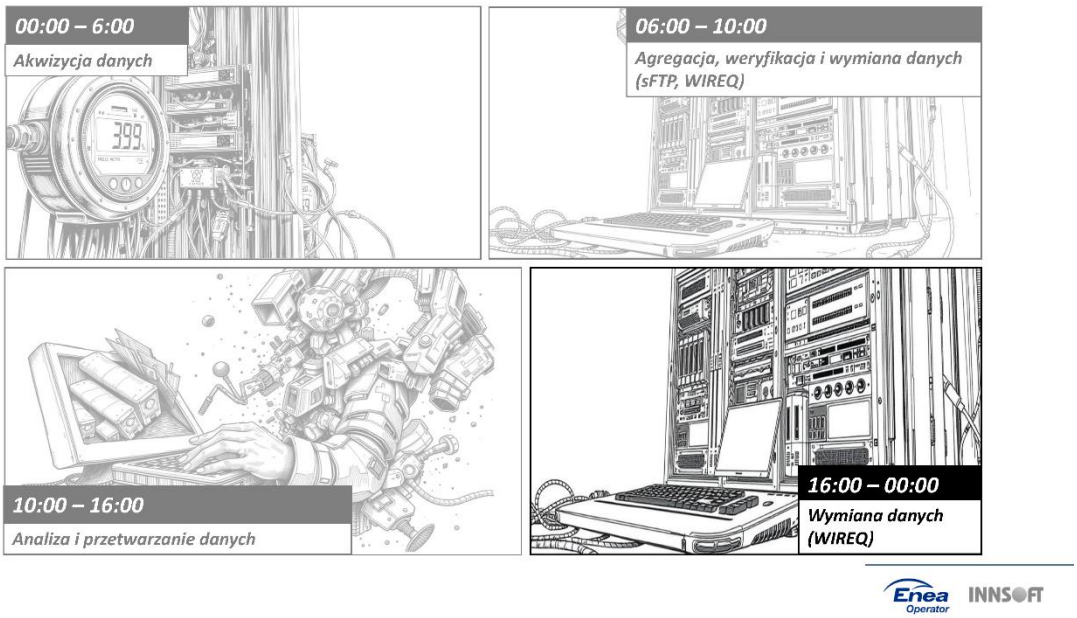

00:00 – 6:00
Akwizycja danych
06:00 – 10:00
Agregacja, weryfikacja i wymiana danych
(sFTP, WIREQ)
10:00 – 16:00
Analiza i przetwarzanie danych
16:00 – 00:00
Wymiana danych
(WIREQ)
Enea Operator
INNSOFT

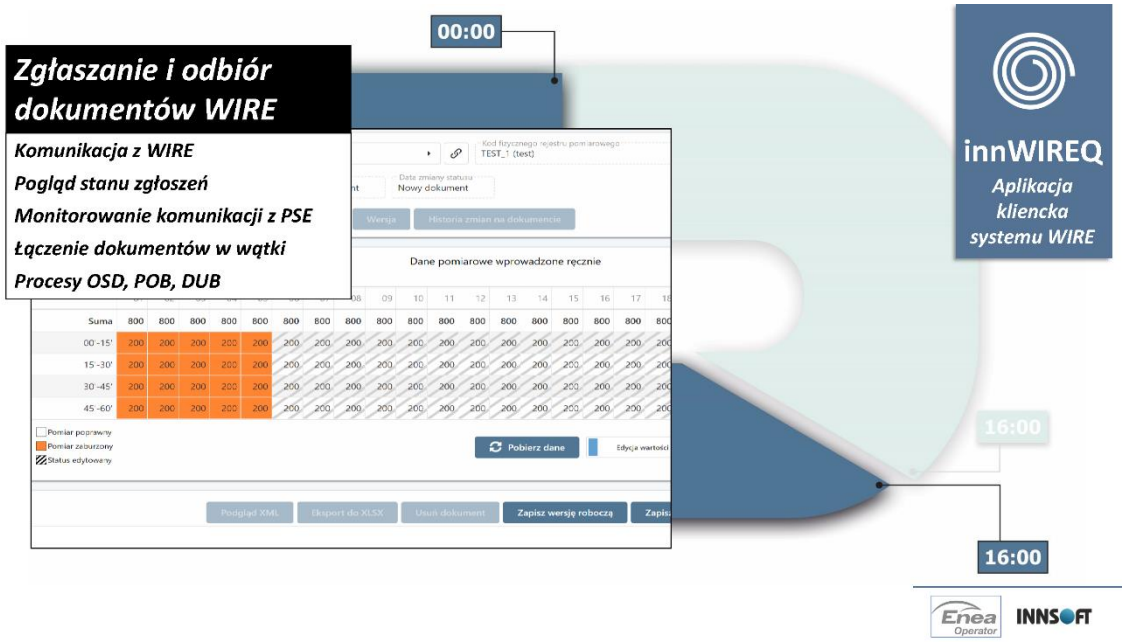

00:00
00:00
10:00
Przekazywanie danych
Interfejsy plikowe
Przesyłanie danych na
Zasoby sieciowe sFTP
CSIRE ready
innOP
Analiza
i udostępnianie
danych
10:00
Wymiana danych
16:00
06:00
06:00
16:00
Enea Operator
INNSOFT

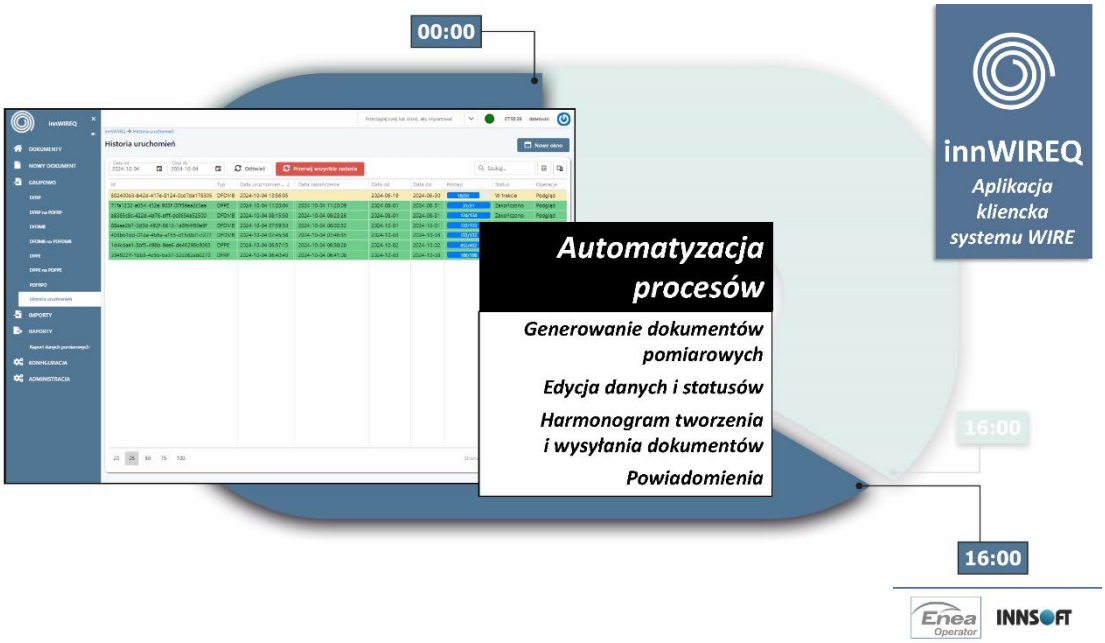

00:00 – 6:00
Akwizycja danych
06:00 – 10:00
Agregacja, weryfikacja i wymiana danych
(sFTP, WIREQ)
10:00 – 16:00
Analiza i przetwarzanie danych
16:00 – 00:00
Wymiana danych
(WIREQ)
Enea Operator
INNSOFT

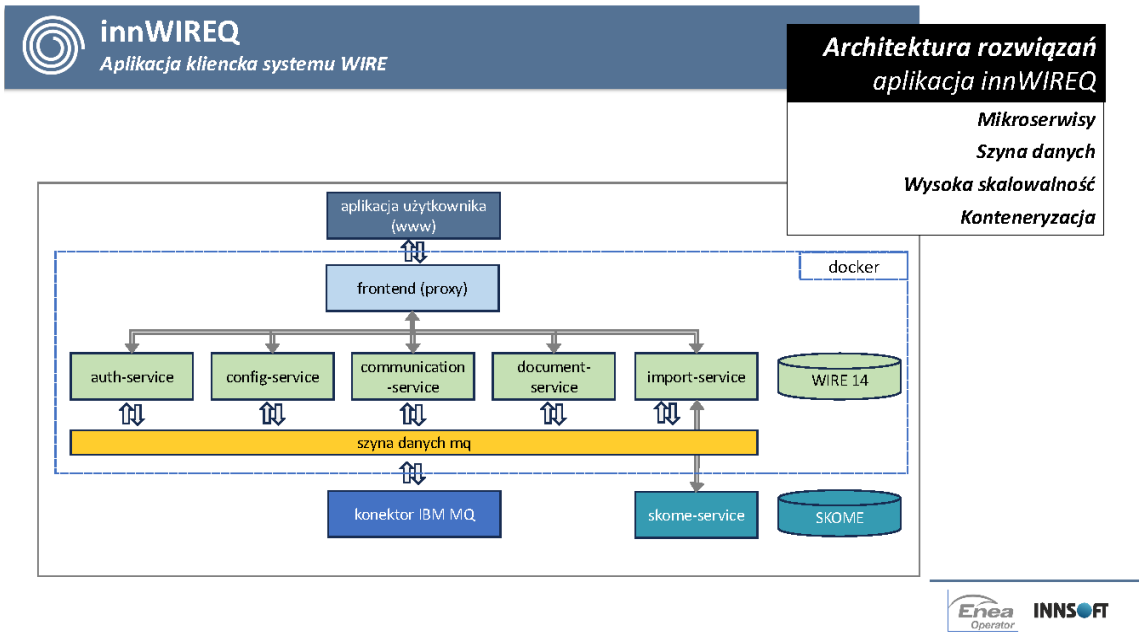

00:00
00:00
10:00
Analiza i przetwarzanie danych
Agregacja danych
Obliczanie agregatów pomiarowych
Procesy automatyczne i rozproszone
10:00
Weryfikacja i zatwierdzanie
Weryfikacja poprawności danych
Wprowadzanie korekt
Procesy automatyczne i rozproszone
16:00
06:00
16:00
R & R
Mechanizmy równoległe i rozproszone
Enea Operator
INNSOFT


Statystyka sesji harmonogramów
Zestawienie przekrojowe sesji
Sesje poprawne i błędne
Sortuj
Filtruj
innMADS
Monitorowanie procesów w systemie
innMADS
Monitorowanie procesów rozproszonych
Weryfikacja skuteczności realizacji zadań
Orkiestracja i raportowanie
Enea Operator
INNSOFT

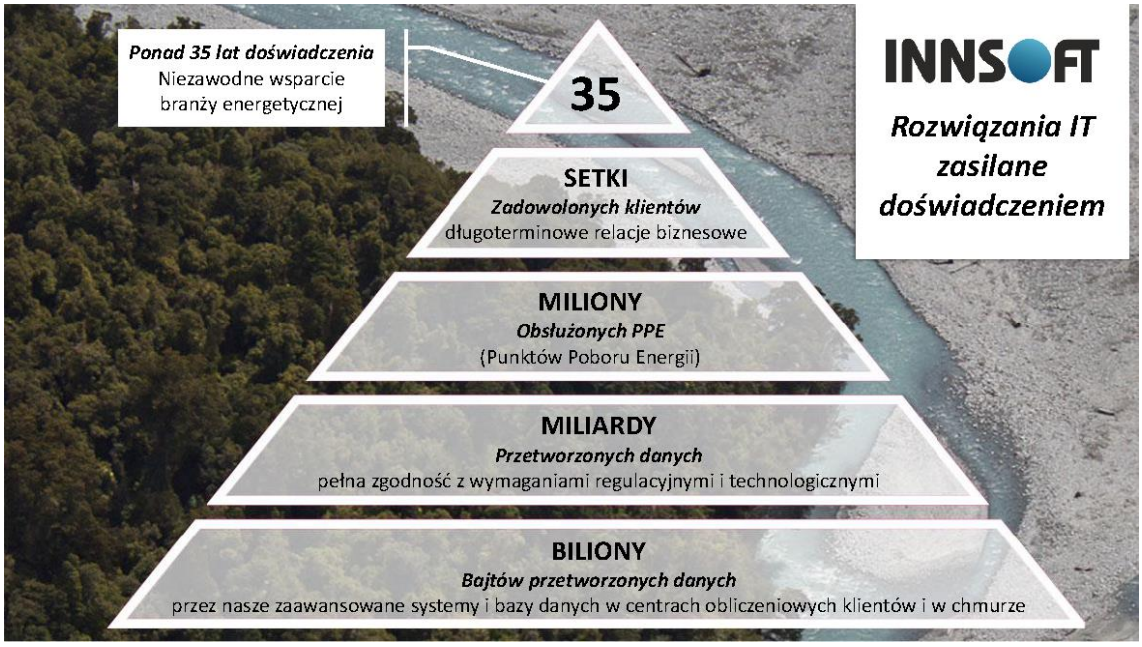

00:00 – 6:00
Akwizycja danych
06:00 – 10:00
Agregacja, weryfikacja i wymiana danych (sFTP, WIREQ)
10:00 – 16:00
Analiza i przetwarzanie danych
16:00 – 00:00
Wymiana danych (WIREQ)
Enea Operator
INNSOFT


Zgłaszanie i odbiór dokumentów WIRE
Komunikacja z WIRE
Pogląd stanu zgłoszeń
Monitorowanie komunikacji z PSE
Łączenie dokumentów w wątki
Procesy OSD, POB, DUB
00:00
innWIREQ
Aplikacja kliencka systemu WIRE
Dane pomiarowe wprowadzone ręcznie
Pobierz dane
16:00
16:00
Enea Operator
INNSOFT


00:00
innWIREQ
Aplikacja kliencka systemu WIRE
Automatyzacja procesów
Generowanie dokumentów pomiarowych
Edycja danych i statusów
Harmonogram tworzenia i wysyłania dokumentów
Powiadomienia
16:00
16:00
Enea Operator
INNSOFT


innWIREQ
Aplikacja kliencka systemu WIRE
Architektura rozwiązań
aplikacja innWIREQ
Mikroserwisy
Szyna danych
Wysoka skalowalność
Konteneryzacja
aplikacja użytkownika (www)
docker
frontend (proxy)
auth-service
config-service
communication -service
document-service
import-service
WIRE 14
szyna danych mq
konektor IBM MQ
skome-service
SKOME
Enea Operator
INNSOFT


infiniHUB
Koncentrator usług IT
Wymiana informacji pomiędzy uczestnikami rynku energii a CSIRE
Komunikacja z CSIRE
Integracja systemów dziedzinowych
Rejestr kartotek
Analityka przetworzonych danych
Monitorowanie komunikacji
Wsparcie migracji
CSIRE
INNSOFT


Ponad 35 lat doświadczenia
Niezawodne wsparcie branży energetycznej
35
SETKI
Zadowolonych klientów
długoterminowe relacje biznesowe
MILIONY
Obsłużonych PPE
(Punktów Poboru Energii)
MILIARDY
Przetworzonych danych
pełna zgodność z wymaganiami regulacyjnymi i technologicznymi
BILIONY
Bajtów przetworzonych danych
przez nasze zaawansowane systemy i bazy danych w centrach obliczeniowych klientów i w chmurze
INNSOFT
Rozwiązania IT zasilane doświadczeniem

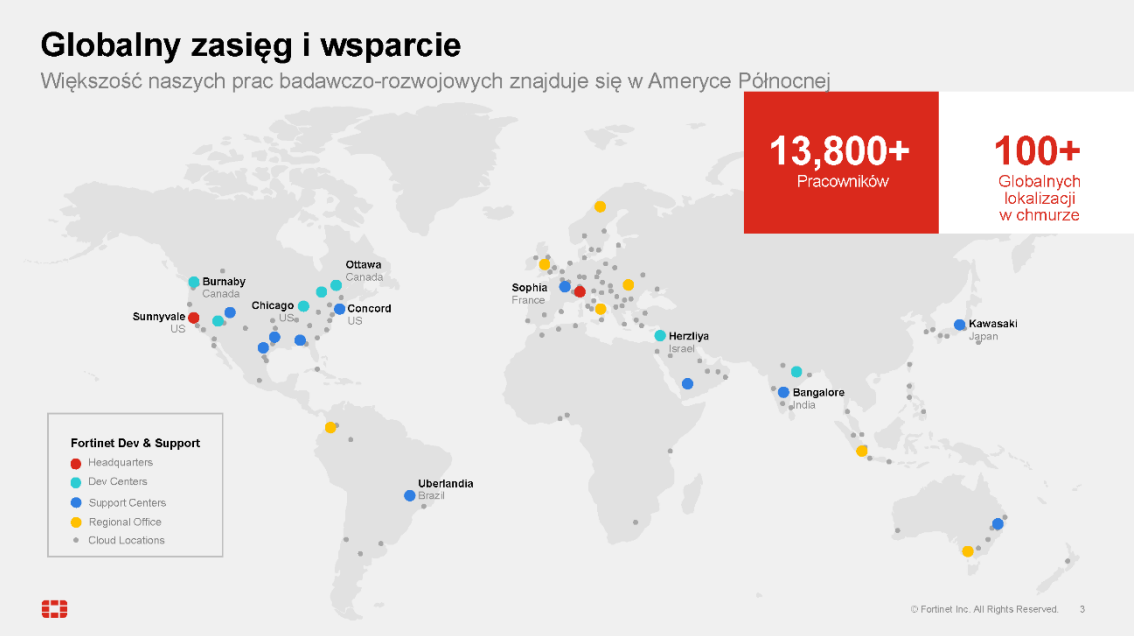
Automatyzacja masowych procesów użytkownika na przykładzie wdrożenia w ENEA Operator

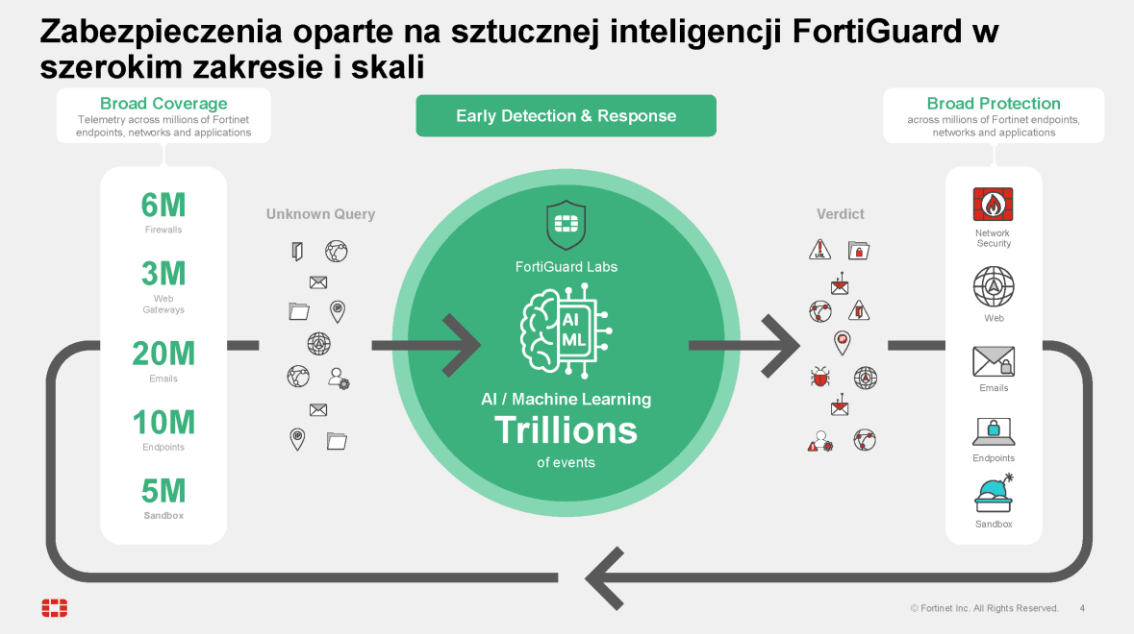
dr inż. Jakub Dąbrowski (ENEA Operator)
mgr inż. Tomasz Leskier (INNSOFT)

SIWE 2024

OCHRONA INFRASTRUKTURY ENERGETYCZNEJ WG FORTINET SECURITY FABRIC

Szymon Poliński (Fortinet)
Sebastian Kulczycki (Atende S.A.)


Globalny zasięg i wsparcie
Większość naszych prac badawczo-rozwojowych znajduje się w Ameryce Północnej
13,800+
Pracowników
100+
Globalnych lokalizacji w chmurze
Burnaby
Canada
Ottawa
Canada
Chicago
US
Concord
US
Sunnyvale
US
Sophia
France
Herzliya
Israel
Kawasaki
Japan
Bangalore
India
Uberlandia
Brazil
Fortinet Dev & Support
Headquarters
Dev Centers
Support Centers
Regional Office
Cloud Locations
© Fortinet Inc. All Rights Reserved. 3


Zabezpieczenia oparte na sztucznej inteligencji FortiGuard w szerokim zakresie i skali
Broad Coverage
Telemetry across millions of Fortinet endpoints, networks and applications
Early Detection & Response
Broad Protection
across millions of Fortinet endpoints, networks and applications
6M
Firewalls
3M
Web Gateways
20M
Emails
10M
Endpoints
5M
Sandbox
Unknown Query
FortiGuard Labs
AI
ML
AI / Machine Learning
Trillions
of events
Verdict
Network Security
Web
Emails
Endpoints
Sandbox
© Fortinet Inc. All Rights Reserved. 4

Kluczowe technologie umożliwiające konwergencję

Uprość i zautomatyzuj zarządzanie bezpieczeństwem dzięki FortiOS, integrując 30+ funkcji bezpieczeństwa i sieciowych, wykorzystując FortiASIC w celu poprawy wydajności, obniżenia kosztów i zmniejszenia zużycia energii

FortiOS

OS

Integracja 30+ funkcji bezpieczeństwa oraz sieciowych

ASIC

ASIC

Wiodąca w branży cena/wydajność i zużycie energii

 5

FortiOS – 30+ funkcji cyberbezpieczeństwa oraz sieciowych

FortiOS organicznie opracowywany system operacyjny

 6

Kontynuacja inwestycji w rozwój układów ASIC

Wraz z dodawaniem kolejnych aplikacji do systemu operacyjnego wymagana jest większa moc obliczeniowa. Podobnie jak procesor graficzny jest niezbędny do przetwarzania graficznego, a TPU do przetwarzania AI, układ zabezpieczeń ASIC przyspiesza funkcje bezpieczeństwa sieci poza procesory ogólnego przeznaczenia.

Security Processor 5 (SPU 5)

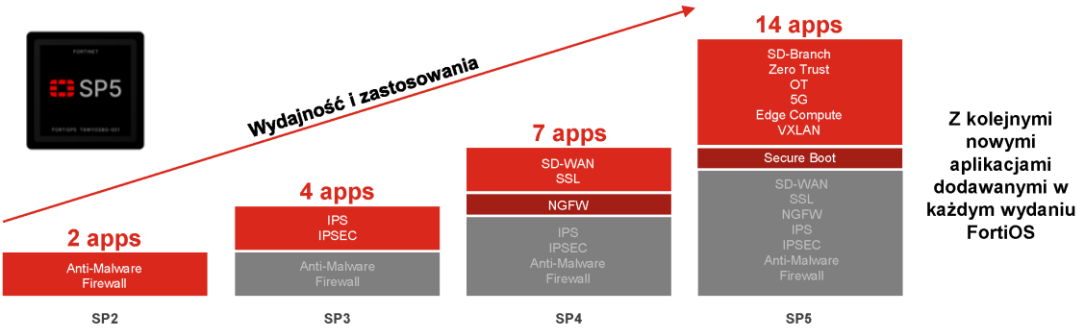
Kompleksowa konstrukcja ASIC, obejmująca procesor, przetwarzanie treści i przetwarzanie sieciowe

Network Processor 7 (NP7)

Architektura NP7 zapewnia funkcje bezpieczeństwa sieci w czasie rzeczywistym o niskich opóźnieniach i lepszej wydajności

FortiASIC przyspiesza działanie funkcji FortiOS

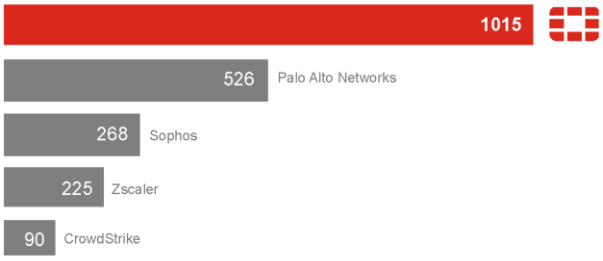
FortiSP5 obsługuje jednocześnie 2 razy więcej aplikacji niż poprzednia generacja



#1 Innowator w dziedzinie cyberbezpieczeństwa

Dwa razy większa liczba patentów niż porównywalne firmy zajmujące się cyberbezpieczeństwem

US Patents



Source: U.S. Patent Office, as of June 30, 2024

1354
Global Patents

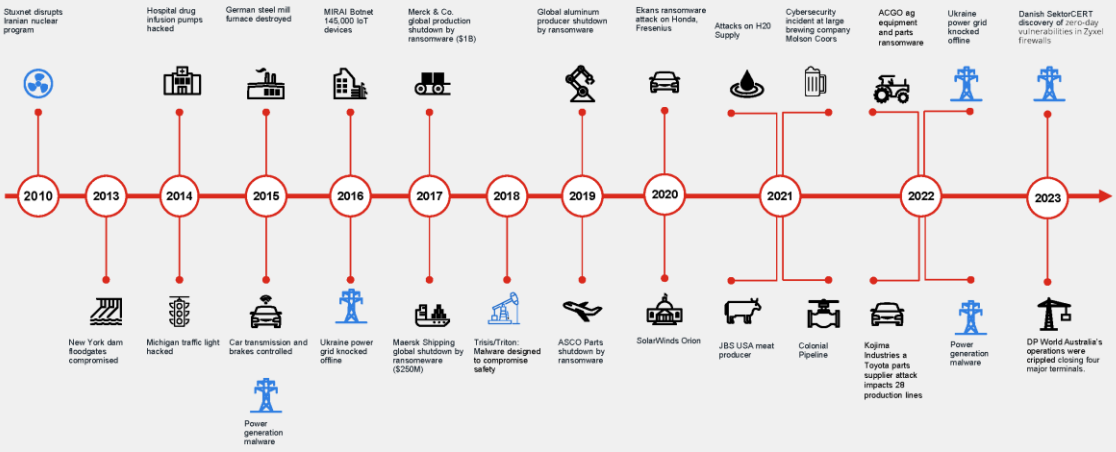
1,015 U.S. Patents
340 International Patents
454 Pending Patents

Includes patents from Lacework and Next DLP acquisitions

 9

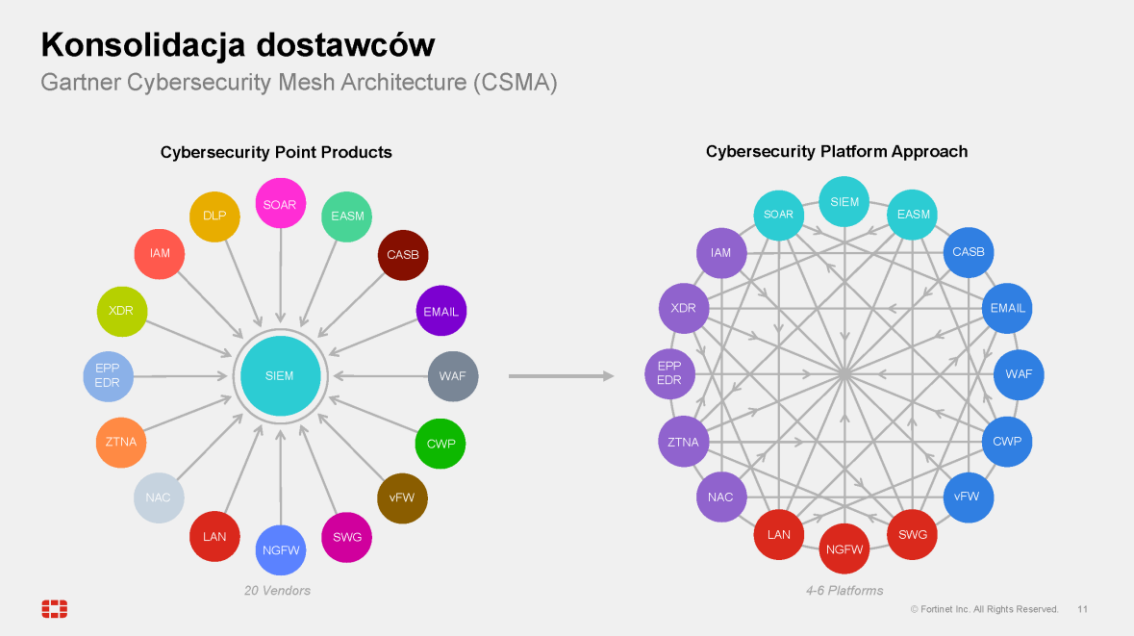
Ataki na infrastrukturę OT nasilają się

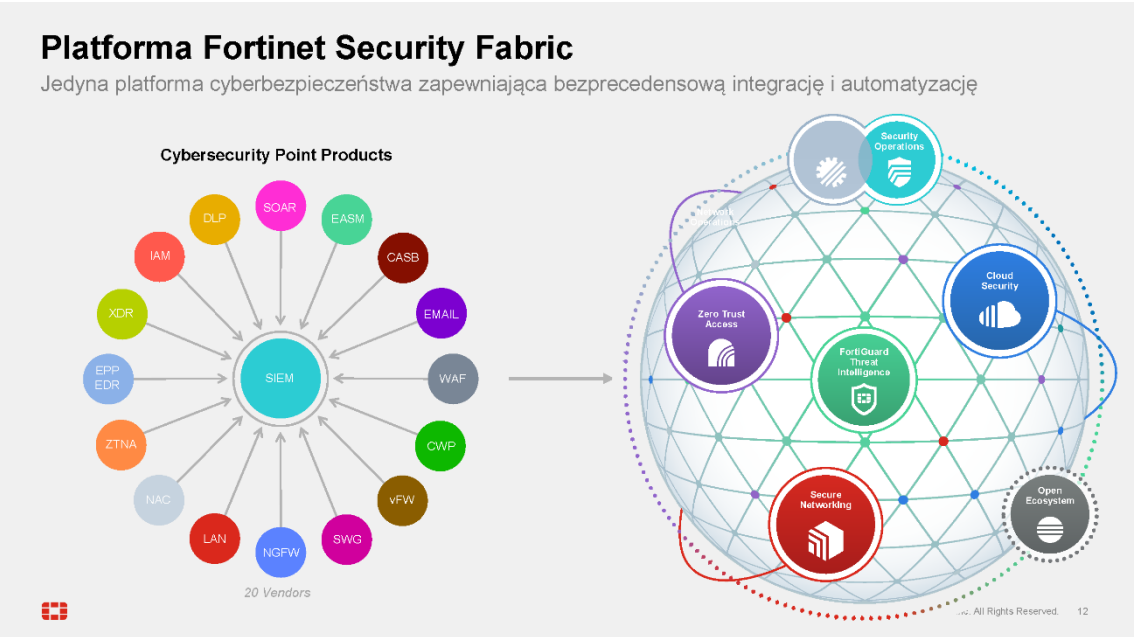
Ataki stają się coraz częstsze i mają coraz większy wpływ



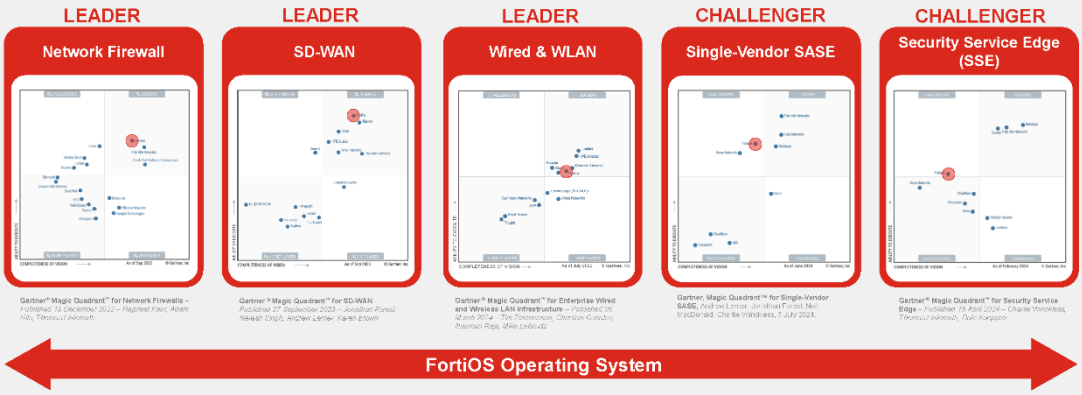
OT targeted attacks

 10

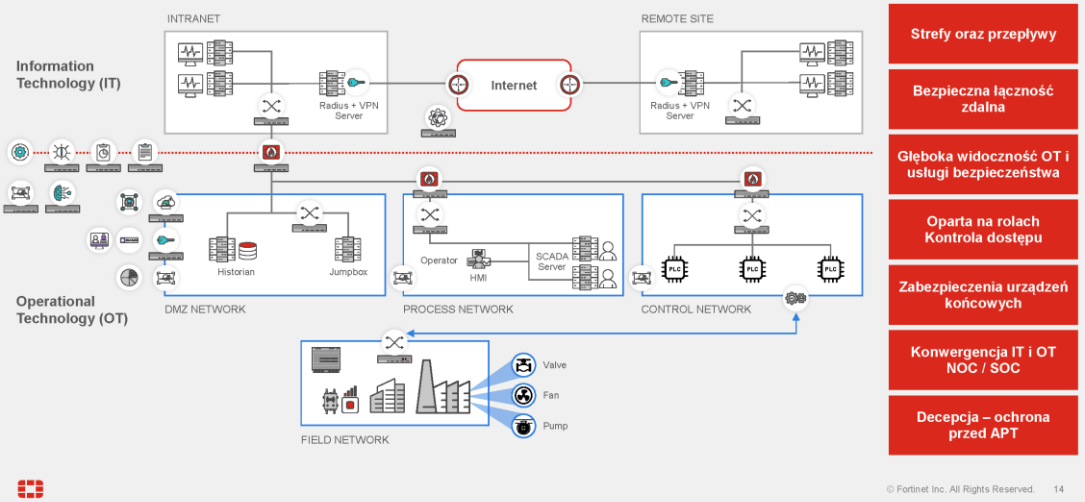

Konsolidacja dostawców
Gartner Cybersecurity Mesh Architecture (CSMA)
Cybersecurity Point Products
SIEM
SOAR
EASM
CASB
EMAIL
WAF
CWP
vFW
SWG
NGFW
LAN
NAC
ZTNA
EPP EDR
XDR
IAM
DLP
20 Vendors
Cybersecurity Platform Approach
4-6 Platforms
© Fortinet Inc. All Rights Reserved. 11


Platforma Fortinet Security Fabric
Jedyna platforma cyberbezpieczeństwa zapewniająca bezprecedensową integrację i automatyzację
Cybersecurity Point Products
SIEM
SOAR
EASM
CASB
EMAIL
WAF
CWP
vFW
SWG
NGFW
LAN
NAC
ZTNA
EPP EDR
XDR
IAM
DLP
20 Vendors
Security Operations
Cloud Security
Zero Trust Access
FortiGuard Threat Intelligence
Secure Networking
Open Ecosystem
All Rights Reserved. 12

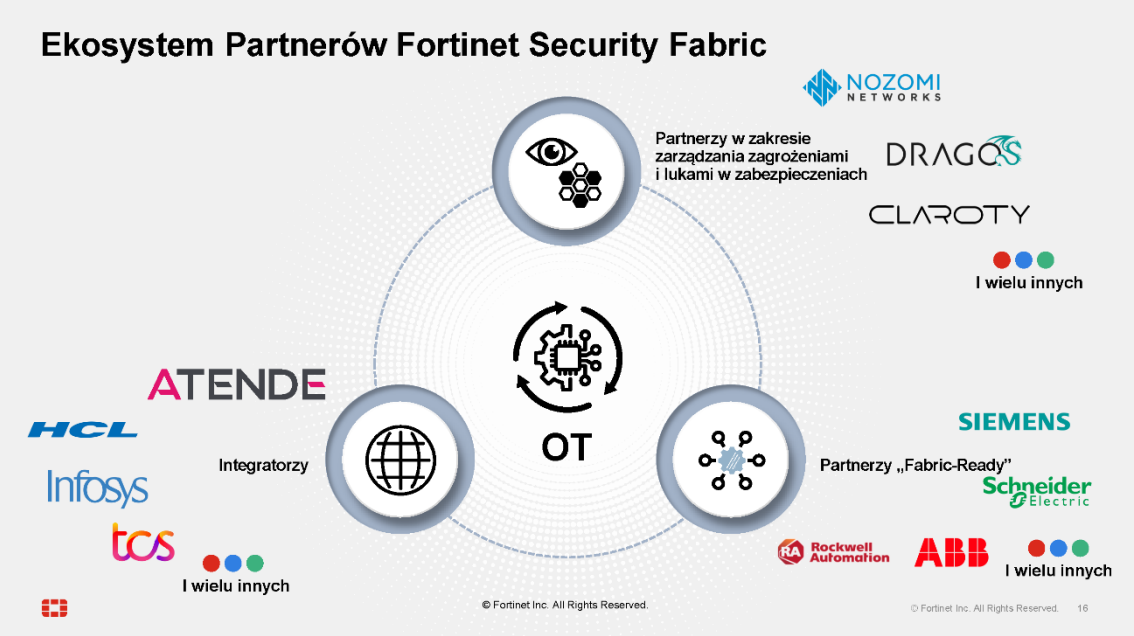
Fortinet wyróżniony w pięciu raportach Magic Quadrant firmy Gartner, oparty na tym samym systemie operacyjnym



Mechanizmy kontroli integrujące OT oraz IT




Oferta rozwiązań Fortinet dla sieci ICS/OT
Portfolio urządzeń „Rugged"
IEC 61850-3 IEEE 1613
Wytrzymała konstrukcja
Brak wentylatora i zastosowanie wytrzymałych komponentów zapewniają niezawodną pracę w trudnych warunkach przemysłowych.
Skonsolidowana architektura bezpieczeństwa
FortiGate ze skonsolidowanymi zabezpieczeniami FortiOS zapewnia lepszą ochronę i niższy koszt posiadania niż rozwiązania oparte o wielu dostawców.
Łatwość zarządzania
Umożliwia szybkie wdrażanie, monitorowanie stanu urządzeń i zagrożeń przy jednoczesnym raportowaniu.
FortiGate Rugged Series
FortiSwitch Rugged, FortiAP Outdoor Series
FGR-70F 3G/4G
Oparta na SoC4, brama bezpieczeństwa i VPN o kompaktowej, bezwentylatorowej konstrukcji i wbudowanej sieci 3G/4G/LTE
FGR-70F
Zasilana przez SoC4, brama bezpieczeństwa i VPN o kompaktowej, bezwentylatorowej konstrukcji
FGR-60F 3G/4G
Zasilany przez SoC-4, brama bezpieczeństwa i VPN z wbudowanym 3G/4G/LTE
FGR-60F
Oparty na SoC4, zabezpieczenia i brama VPN
FSR-112D-POE and FSR-424F
Pasywne chłodzenie bez wentylatora z możliwością montażu na szynie DIN lub na ścianie. Obsługa zasilania przez sieć Ethernet, w tym PoE+. Redundantne zasilanie. MTBF dłuższy niż 25 lat.
FortiAP Outdoor 234F
Anteny wewnętrzne, obudowa IP67, do użytku wewnątrz/na zewnątrz
Zasilanie PoE
Możliwość montażu na ścianie i słupie
Certyfikat Wi-Fi Alliance
FortiAP Outdoor 432F
Anteny zewnętrzne
IP67, do użytku wewnątrz/na zewnątrz
Zasilanie PoE
Możliwość montażu na ścianie i słupie
Certyfikat Wi-Fi Alliance
Funkcje FortiGate
Security (IPS, FW, OT traffic monitor)
Encryption (GRE, VXLAN, IPSEC)
Connectivity (Proxy, VLANs, IPv6.)
Advance features (SD-WAN)
Central authentication (LDAP, RADIUS, etc.)
DLP
Wi-Fi
Antivirus
DNS Filter
Web Filtering
IPSEC VPN
SSL VPN – Client/Clientless
SSL Inspection
Packet capture triggered by IPS
Virtual Domains (VDOM)
Transparent or Proxy (Man in the middle)
© Fortinet Inc. All Rights Reserved. 15


Ekosystem Partnerów Fortinet Security Fabric
NOZOMI NETWORKS
Partnerzy w zakresie zarządzania zagrożeniami i lukami w zabezpieczeniach
DRAGOS
CLAROTY
I wielu innych
ATENDE
HCL
Infosys
tcs
I wielu innych
Integratorzy
OT
SIEMENS
Partnerzy „Fabric-Ready"
Schneider Electric
Rockwell Automation
ABB
I wielu innych
© Fortinet Inc. All Rights Reserved.
© Fortinet Inc. All Rights Reserved. 16


FORTINET

INTEGRACJA UCZESTNIKÓW RYNKU Z CSIRE - WYZWANIA, CELE, RYZYKA - PERSPEKTYWA DOSTAWCY IT

Przemysław Chojnicki, Piotr Karwaczyński (Sygnity SA)

Integracja uczestników rynku z CSIRE - wyzwania, cele, ryzyka

Perspektywa dostawcy IT

Przemysław Chojnicki

Piotr Karwaczyński

Sygnity

Agenda

Uczestniku Rynku Energii Elektrycznej:

- Kim jesteś?
- Czego potrzebujesz?
- Masz wybór!
- Jak możemy pomóc?

Uczestniku Rynku Energii Elektrycznej: KIM JESTEŚ?

- Liczba i rodzaj PP
- Rola pełniona na rynku
- Liczba i rodzaj zawartych umów
- Oprogramowanie dziedzinowe
- Złożoność organizacyjna
- Dojrzałość procesów biznesowych

Uczestniku Rynku Energii Elektrycznej: CZEGO POTRZEBUJESZ?

- „Wszystkiego"?
- Wiesz, czy się domyślasz?
- Jaki jest Twój „próg bólu"?
- Co musisz, a co możesz?
- Wszystko naraz, czy etapami?
- Jakiego narzędzia użyć?

Uczestniku Rynku Energii Elektrycznej: MASZ WYBÓR!

- Portal Użytkownika Profesjonalnego
- Nadawca Fizyczny
- Automatyzacja (ETL, RPA)
- Wprowadzenie świadomości CSIRE do systemów dziedzinowych
- Uruchomienie pośrednika łączącego CSIRE i systemy dziedzinowe

Uczestniku Rynku Energii Elektrycznej: JAK MOŻEMY POMÓC?

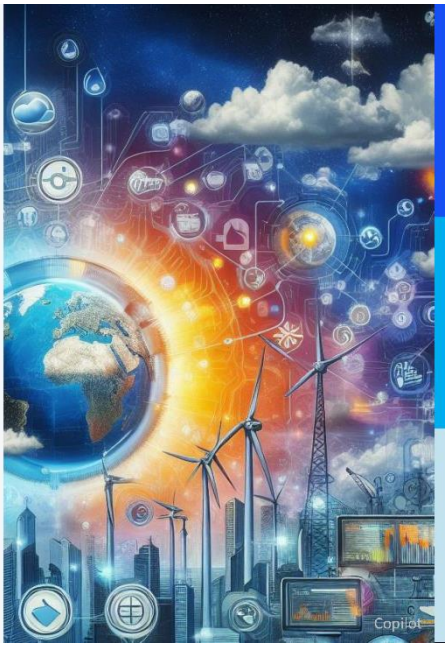
- Projekt analityczny
- Zmiany w systemach dziedzinowych
- Przeprowadzenie *Proof of Concept*
- Rozwiązanie do komunikacji AS4
- Rozwiązanie do integracji systemów dziedzinowych z CSIRE
- Wsparcie w Pilotażach rynkowych
- Wsparcie w Certyfikacji

Sygnity

AStral

- Moduł komunikacyjny wg protokołu AS4
- Obsługa wzorców komunikacji (MEP): *One-Way/Push, Two-Way/Sync*
- Kompresja, szyfrowanie i podpisywanie wiadomości
- Kolejkowanie komunikatów i ponawianie wysyłki

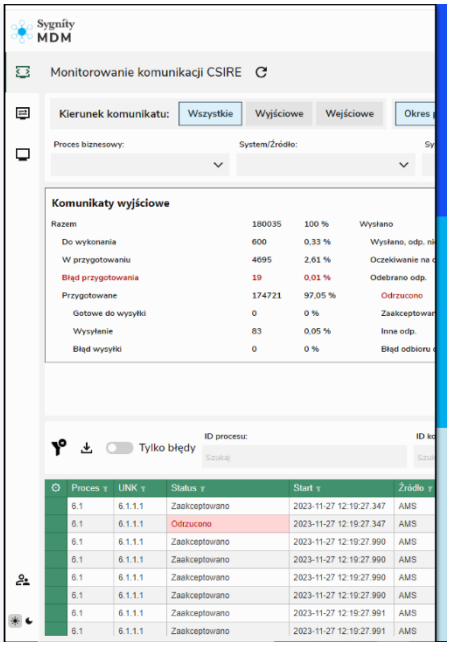
- Testy techniczne integracji z CSIRE zakończone w maju 2024 r.



Sygnity

DH4CSIRE

- Identyfikacja zdarzeń inicjujących komunikację z CSIRE
- Integracja z systemami dziedzinowymi
- Przygotowanie komunikatów TSKB
- Współpraca z modułem komunikacji AS4
- Obsługa archiwum komunikatów
- Monitorowanie stanu komunikacji
- Diagnostyka błędów technicznych i biznesowych



Fundusze Europejskie Inteligentny Rozwój | Rzeczpospolita Polska | NCBR Narodowe Centrum Badań i Rozwoju | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

SPECTRA

Opracowanie optymalnej pod względem kosztowym i wydajnościowym architektury chmurowej (szczególnie poprzez badania dostępnych usług chmurowych), niezbędnej do przygotowania rozwiązania pomiarowego przeznaczonego do integracji z Centralnym Systemem Informacji Rynku Energii, realizującego procesy biznesowe oparte na standardzie ebIX.

https://www.sygnity.pl/dotacje/ 2021-10-01 – 2023-12-31 Sygnity

5G W ENERGETYCE – CZY JUŻ CZAS?

Paweł Niedzielski (Nokia Solutions and Networks Sp. z o.o.)

Prywatne sieci 5G w energetyce – Czy to już czas?
TAK, to NAJWYŻSZY czas!

Energetyka, podobnie jak inne branże gospodarki, stoi na progu rewolucji technologicznej związanej z możliwościami wykorzystania prywatnych sieci 5G. Dzięki cechom sieci Priv-5G, takim jak szybkość, niezawodność, bezpieczeństwo oraz elastyczność, przedsiębiorstwa energetyczne mogą usprawnić operacje, poprawić komunikację i wprowadzać innowacyjne rozwiązania, takie jak rzeczywistość rozszerzona, AI, wykorzystanie dronów, rozwój IoT. Sieci 5G pozwalają również na wdrażanie zaawansowanych systemów zarządzania energią oraz monitorowania infrastruktury w czasie rzeczywistym, co pozwala na szybsze reakcje na potencjalne problemy i minimalizację przestojów.

Dziś, kiedy pasmo n77 (3800-4200 MHz) jest dostępne w Polsce i koszty uruchomienia sieci nie są wysokie, pojawia się możliwość wdrażania rozwiązań 5G i tworzenia prywatnych sieci dostosowanych do specyficznych potrzeb branży energetycznej.

Dlaczego warto inwestować w prywatne sieci 5G? Jest kilka oczywistych powodów: większa efektywność, obniżone koszty, lepsza kontrola nad operacjami i bezpieczeństwem. Prywatne sieci 5G dają możliwość pełnej kontroli nad infrastrukturą komunikacyjną i jej rozwoju stosownie do potrzeb. Rewolucja 5G wiąże się bardzo dobrze z koncepcją Przemysłu 4.0, który stawia na cyfryzację, robotyzację oraz wykorzystanie sztucznej inteligencji i IoT w celu zwiększenia wydajności produkcji i komunikacji w całym sektorze. Dzięki możliwościom, jakie daje 5G, możliwe jest również wdrożenie zaawansowanych systemów analizy danych, co umożliwia lepsze przewidywanie zapotrzebowania na energię oraz optymalizację procesów produkcyjnych. W efekcie, przedsiębiorstwa energetyczne mogą nie tylko poprawić swoją konkurencyjność, ale także przyczynić się do bardziej zrównoważonego wykorzystania zasobów energetycznych.

2


Prywatne sieci 5G
czy to już właściwy czas?
To już NAJWYŻSZY czas!
3 © 2024 Nokia
NOKIA


5G
Prywatne sieci 5G
To już NAJWYŻSZY czas!
5G
~800
instalacji Nokia
Private Wireless na świecie
5G
n77
pasmo 3.8-4.2GHz dostępne w Polsce
do zastosowań prywatnych
4 © 2024 Nokia
NOKIA

n77 w Polsce – nowa jakość komunikacji

- Pasmo N77 to część pasma C sieci 5G o zakresie częstotliwości 3800-4200 MHz pracujące w trybie TDD
- zakres 3800-3900 wyłącznie dla Jednostek Samorządu Terytorialnego
- zakres 3900-4200 MHz przeznaczony jest dla innych podmiotów (przedsiębiorstw)
- użytkowanie pasma na zasadzie „first come, first served"
- pozwolenia będą wydawane na wykorzystywanie urządzeń małej lub średniej mocy
- pozwolenie kosztować będzie jednorazowo 82 zł

5 © 2024 Nokia

NOKIA

n77 w Polsce – nowa jakość komunikacji

Proste 3 kroki do własnej i sieci 5G

1. Złożenie wniosku o pasmo
2. Zaplanowanie sieci 5G
3. Zgłoszenie pozwoleń radiowych

Pasmo 3800-4200 MHz – opłaty roczne:

	gmina wiejska	gmina miejsko-wiejska	gmina miejska	miasto na prawach powiatu
10 MHz	100 zł	250 zł	1 250 zł	2 500 zł
20 MHz	200 zł	500 zł	2 500 zł	5 000 zł
30 MHz	300 zł	750 zł	3 750 zł	7 500 zł
40 MHz	400 zł	1 000 zł	5 000 zł	10 000 zł
50 MHz	500 zł	1 250 zł	6 250 zł	12 500 zł
60 MHz	600 zł	1 500 zł	7 500 zł	15 000 zł
70 MHz	700 zł	1 750 zł	8 750 zł	17 500 zł
80 MHz	800 zł	2 000 zł	10 000 zł	20 000 zł
90 MHz	900 zł	2 250 zł	11 250 zł	22 500 zł
100 MHz	1 000 zł	2 500 zł	12 500 zł	25 000 zł

6 © 2024 Nokia

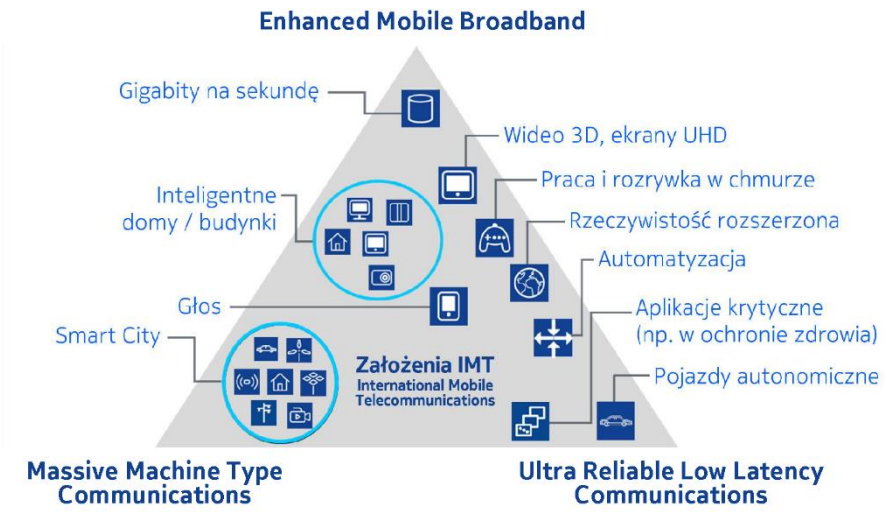
NOKIA


5G
Prywatne sieci 5G
To już NAJWYŻSZY czas!
5G
~800
instalacji Nokia
Private Wireless na świecie
5G
n77
pasmo 3.8-4.2GHz dostępne w Polsce
do zastosowań prywatnych
5G
rozwiązania Priv-5G stają się ekonomicznie
uzasadnione, opłacalne i rozwojowe
7 © 2024 Nokia
NOKIA


Szybkość, wydajność, niezawodność, bezpieczeństwo
we własnej sieci bezprzewodowej
5G
Ale przecież
budujemy LTE 450
8 © 2024 Nokia
NOKIA

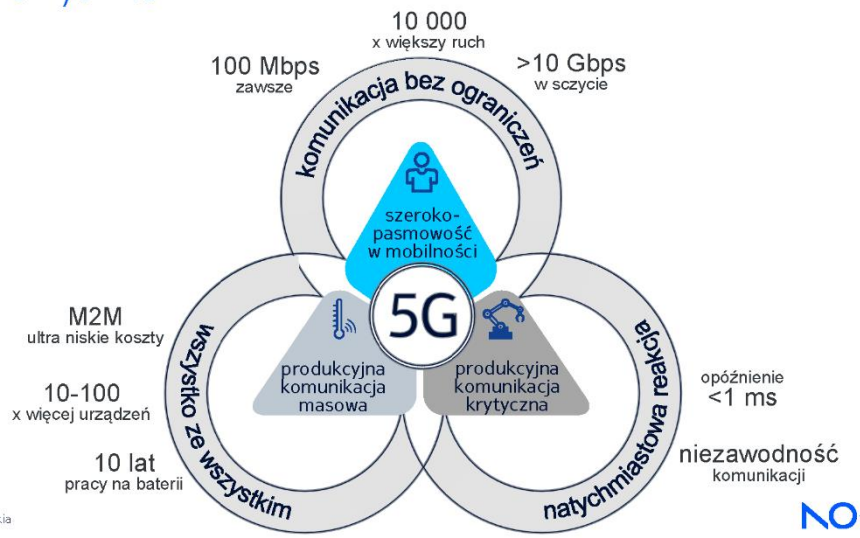

LTE 450
5G
Ogólnopolska sieć LTE 450 do komunikacji dyspozytorskiej i krytycznej
Lokalna, uniwersalna sieć bezprzewodowa przedsiębiorstwa energetycznego
pasmo
5 MHz
2 x 100 MHz (+2 x 100 MHz)
zasięg
~30 km (rural)
~4 km (rural)
szerokość kanału
1.4 - 3.0 - 5.0 MHz
10 . . . 100 MHz
przesyłanie danych
DL: <32 Mb/s
UL: <10 Mb/s
DL: <1600 Mb/s
UL: <350 Mb/s
przesyłanie obrazu
DL: 4 UHD; 8 FHD
UL: 1 UHD; 2 FHD
DL: 200 UHD; 400 FHD
UL: 42 UHD; 86 FHD
drony – nadzór i dane
tak
tak
9
© 2024 Nokia
NOKIA


LTE 450
5G
Zastosowania 5G niedostępne w LTE
5 MHz
2 x 100 MHz (+2 x 100 MHz)
~30 km (rural)
~4 km (rural)
1.4 - 3.0 - 5.0 MHz
10 . . . 100 MHz
DL: <32 Mb/s
UL: <10 Mb/s
DL: <1600 Mb/s
UL: <350 Mb/s
DL: 4 UHD; 8 FHD
UL: 1 UHD; 2 FHD
DL: 200 UHD; 400 FHD
UL: 42 UHD; 86 FHD
tak
tak
aplikacje eMBB (Enhanced Mobile Broadband): VR, XR (wirtualna i rozszerzona rzeczywistość)
transmisja strumieni wideo UHD
aplikacje wymagające bardzo niskich opóźnień (<3ms)
Ultra Reliable Low Latency Communications
URLLC: 99,9999%
10
© 2024 Nokia
NOKIA



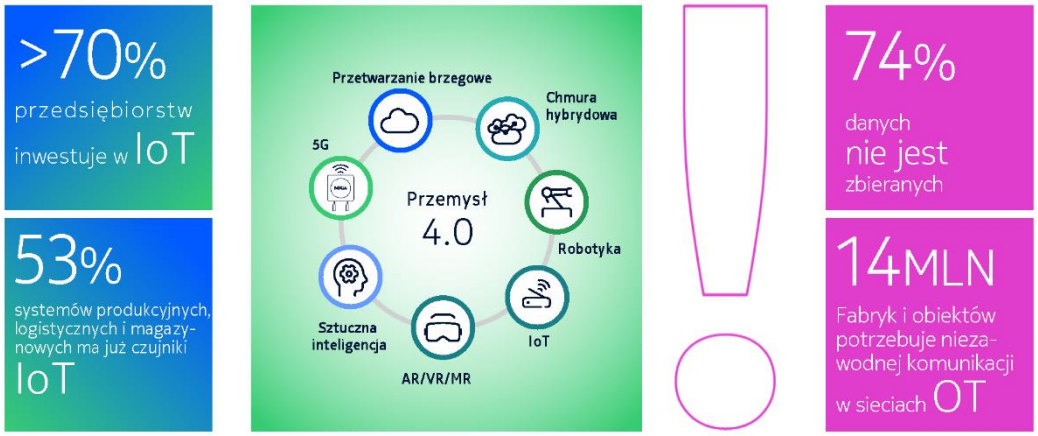
NOKIA

5G i Przemysł 4.0



NOKIA

Cyfryzacja jest drogą do zwiększenia efektywności produkcji

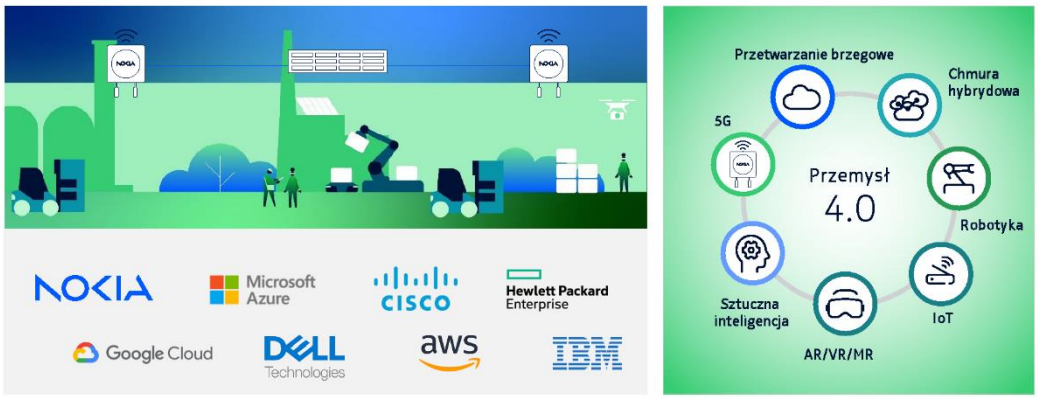


13 © 2024 Nokia

NOKIA

Motorem transformacji cyfrowej jest Przemysł 4.0

Globalni dostawcy i integratorzy współpracują przy cyfryzacji gospodarki

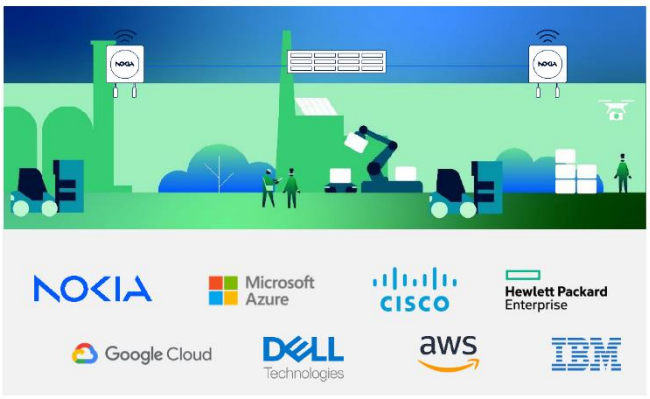


14 © 2024 Nokia

NOKIA

Motorem transformacji cyfrowej jest Przemysł 4.0

Globalni dostawcy i integratorzy współpracują przy cyfryzacji gospodarki



NOKIA Microsoft Azure cisco Hewlett Packard Enterprise Google Cloud DELL Technologies aws IBM

15 © 2024 Nokia

NOKIA

Prywatne i publiczne sieci 5G

Private wireless networks

Public/non-public network slicing or Secure MVNO

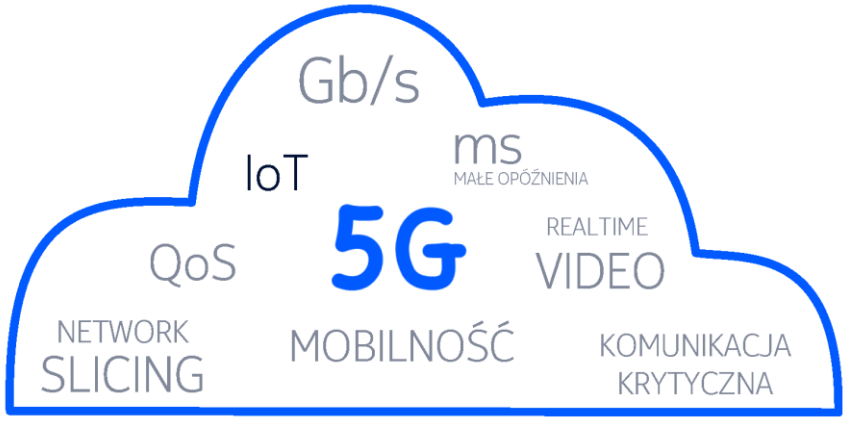
- Dedykowanie pojemności i dopasowany zasięg
- Maksymalna dostępność i niezawodność
- Pełna prywatność danych (control channel traffic)
- **Pełna kontrola**

- Duży zasięg
- Wsparcie dla wszystkich RAT i LPWAN
- Roaming międzynarodowy
- **Niższe koszty początkowe**

16 © 2024 Nokia

NOKIA

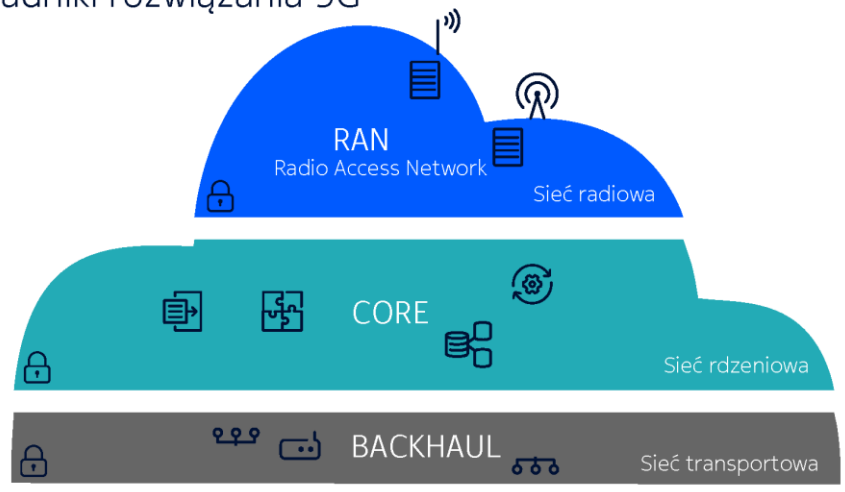
Własności sieci 5G



17 © 2024 Nokia

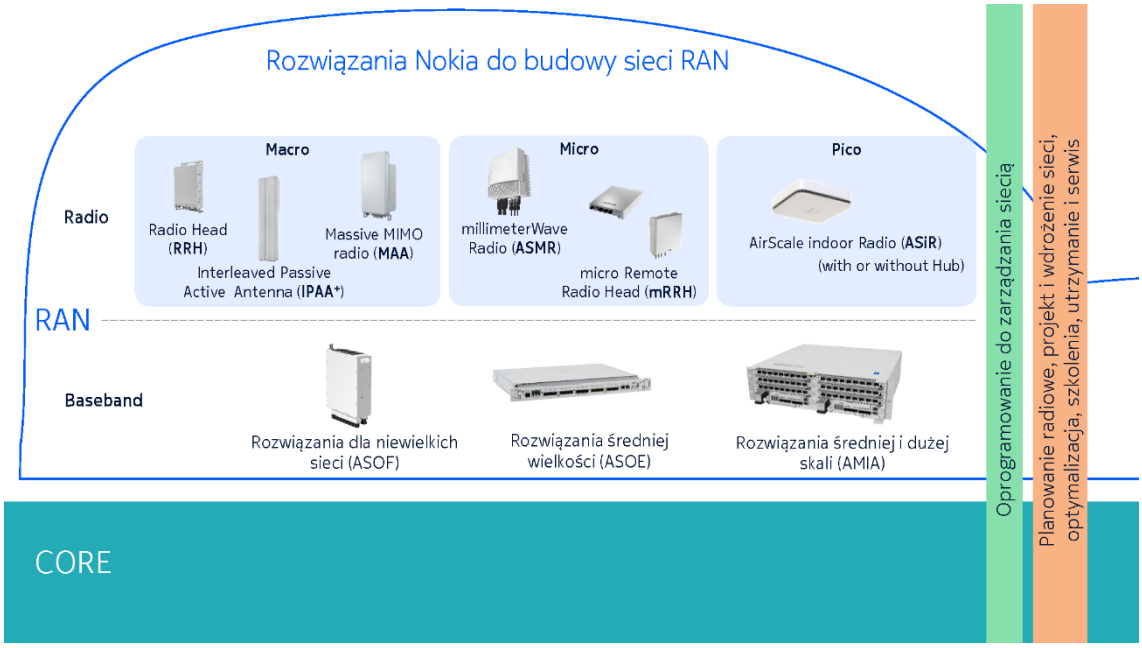
NOKIA

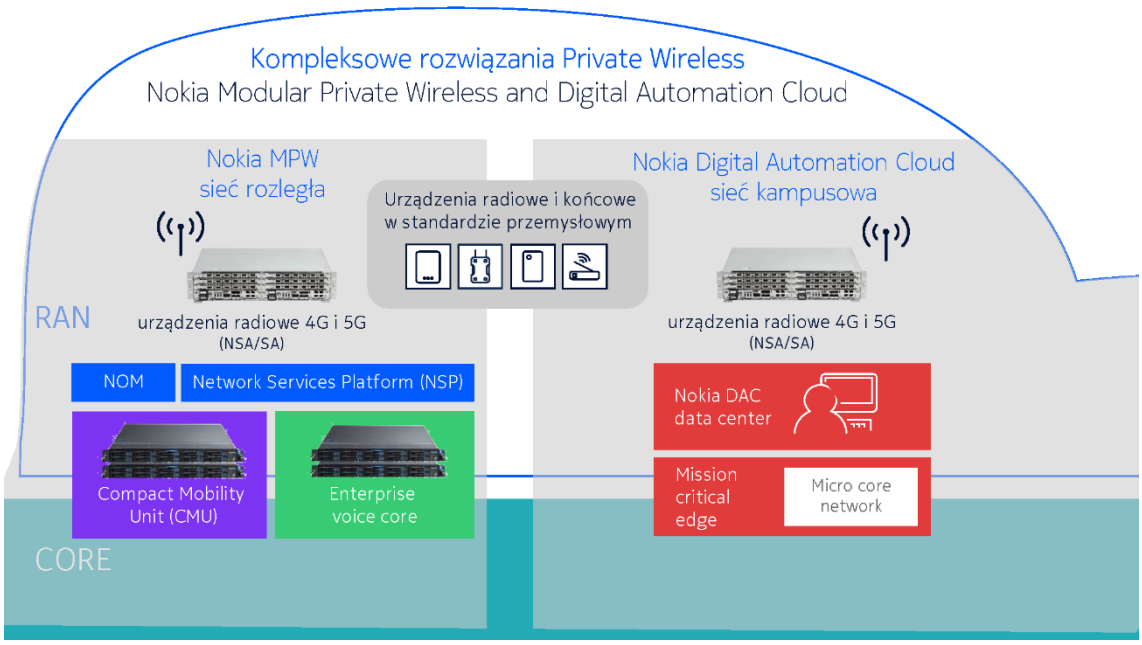
Składniki rozwiązania 5G



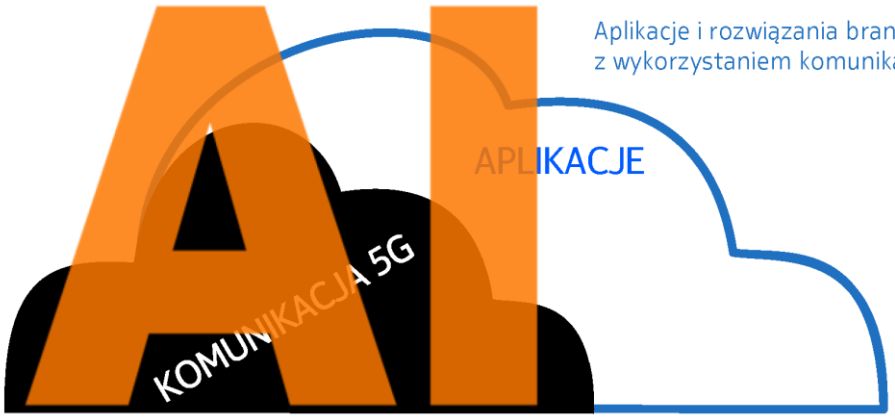
18 © 2024 Nokia

NOKIA


Rozwiązania Nokia do budowy sieci RAN
Macro
Micro
Pico
Radio
Radio Head (RRH)
Massive MIMO radio (MAA)
Interleaved Passive Active Antenna (IPAA*)
millimeterWave Radio (ASMR)
micro Remote Radio Head (mRRH)
AirScale indoor Radio (ASiR) (with or without Hub)
RAN
Baseband
Rozwiązania dla niewielkich sieci (ASOF)
Rozwiązania średniej wielkości (ASOE)
Rozwiązania średniej i dużej skali (AMIA)
CORE
Oprogramowanie do zarządzania siecią
Planowanie radiowe, projekt i wdrożenie sieci, optymalizacja, szkolenia, utrzymanie i serwis

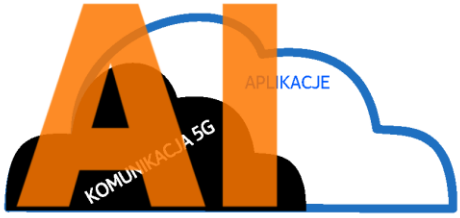

Kompleksowe rozwiązania Private Wireless
Nokia Modular Private Wireless and Digital Automation Cloud
Nokia MPW sieć rozległa
Urządzenia radiowe i końcowe w standardzie przemysłowym
Nokia Digital Automation Cloud sieć kampusowa
RAN
urządzenia radiowe 4G i 5G (NSA/SA)
urządzenia radiowe 4G i 5G (NSA/SA)
NOM
Network Services Platform (NSP)
Nokia DAC data center
Compact Mobility Unit (CMU)
Enterprise voice core
Mission critical edge
Micro core network
CORE

Zastosowania rozwiązań 5G



NOKIA

Czy rynek jest na to gotowy?



Przegląd informacji z raportu:

Private Mobile Networks | September 2024

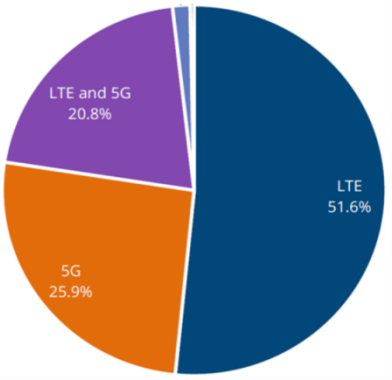
GSA
Global mobile Suppliers Association

NOKIA

Instalacje P-LTE i 5G na świecie

GSA
Global mobile Suppliers Association

RAPORT
Private Mobile Networks | September 2024



technologie

23 © 2024 Nokia

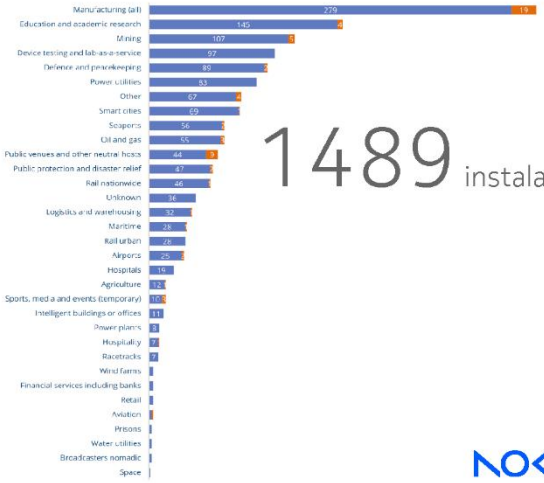
NOKIA

Instalacje P-LTE i 5G na świecie

GSA
Global mobile Suppliers Association

RAPORT
Private Mobile Networks | September 2024

branże



1489 instalacji

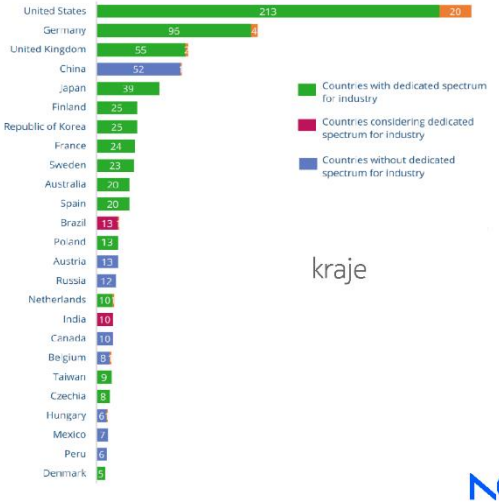
24 © 2024 Nokia

NOKIA

Instalacje P-LTE i 5G na świecie

GSA
Global mobile Suppliers Association

RAPORT
Private Mobile Networks | September 2024



NOKIA

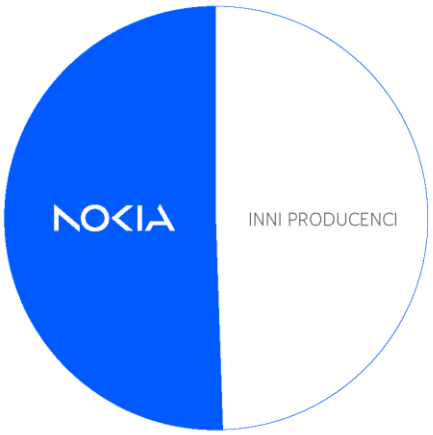
Instalacje P-LTE i 5G na świecie

GSA
Global mobile Suppliers Association

RAPORT
Private Mobile Networks | September 2024

NOKIA

Instalacje P-LTE i 5G na świecie



27 © 2024 Nokia

NOKIA

Prywatne sieci bezprzewodowe Nokia znajdują zastosowanie w komunikacji krytycznej we wszystkich branżach na całym świecie

795+
instalacji prywatnych sieci bezprzewodowych NOKIA

176 Energetyka

158 Produkcja i łańcuchy dostaw

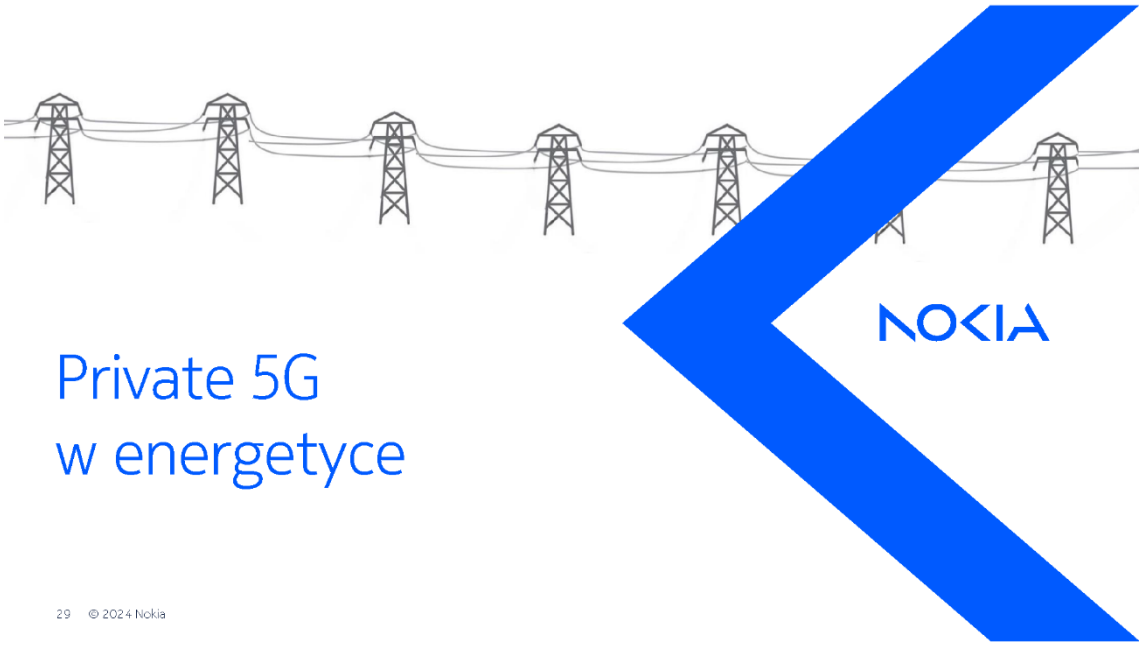
>100 Inne

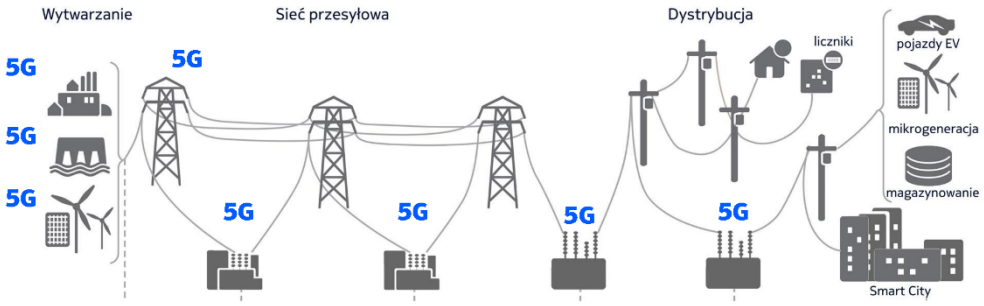
204 Sektor publiczny i miasta

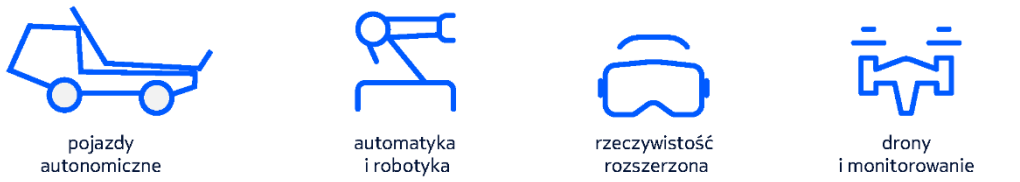
124 Transport

28 © 2024 Nokia |

NOKIA

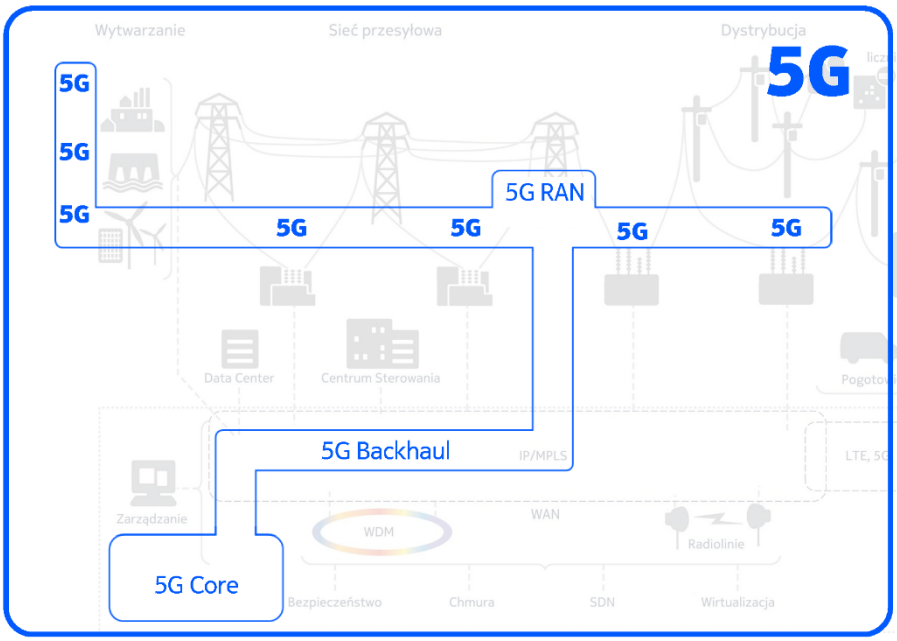

Private 5G
w energetyce
29 © 2024 Nokia


Wytwarzanie
Sieć przesyłowa
Dystrybucja
5G
liczniki
pojazdy EV
mikrogeneracja
magazynowanie
Smart City

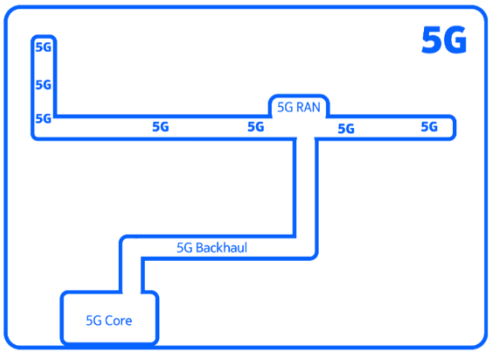

pojazdy autonomiczne
automatyka i robotyka
rzeczywistość rozszerzona
drony i monitorowanie


monitorowanie infrastruktury
wspomaganie obsługi urządzeń
zdalna diagnostyka
szkolenia
. . .

NOKIA


Wytwarzanie
Sieć przesyłowa
Dystrybucja
5G
5G
5G
5G
5G RAN
5G
5G
5G
5G
pojazdy EV
mikrogeneracja
magazynowanie
Smart City
Data Center
Centrum Sterowania
5G Backhaul
IP/MPLS
Zarządzanie
WAN
WDM
Radiolinie
FAN
5G Core
Bezpieczeństwo
Chmura
SDN
Wirtualizacja

NOKIA

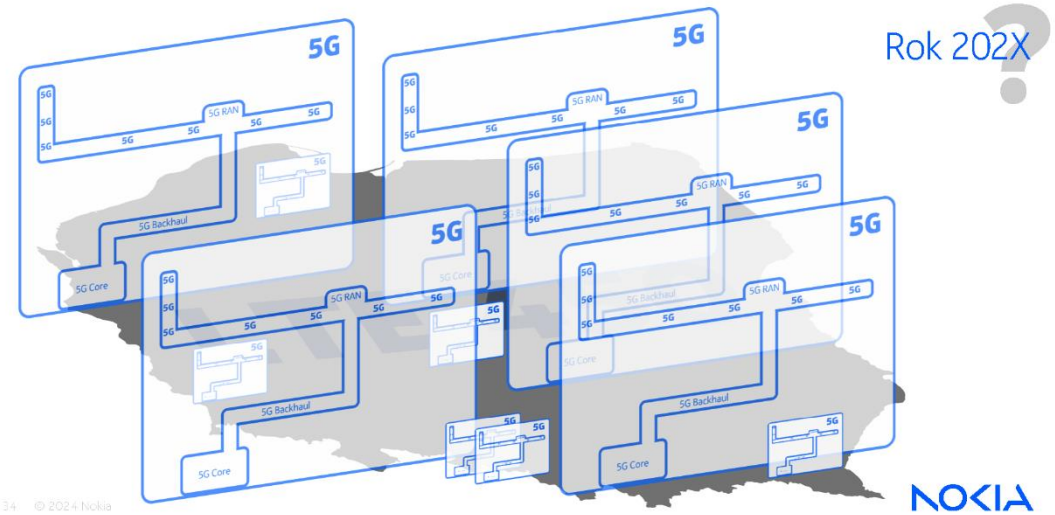


Prywatna sieć 5G operatora energetycznego, elektrowni, kopalni, fabryki, . . .

Ogólnopolska sieć LTE 450

NOKIA

Krajobraz prywatnych sieci bezprzewodowych w energetyce



NOKIA


5G w energetyce: Czy już czas?
TAK
To już NAJWYŻSZY czas
5G
35 © 2024 Nokia
NOKIA


NOKIA

Copyright and confidentiality

PROGNOZOWANIE PRODUKCJI OZE I BILANSOWANIE LOKALNE

Krzysztof Kołodziejczyk (Globema Sp. z o.o.)

globema
EXPERIENCE. INNOVATIONS. SMART SOLUTIONS.

Prognozowanie produkcji OZE i bilansowanie lokalne

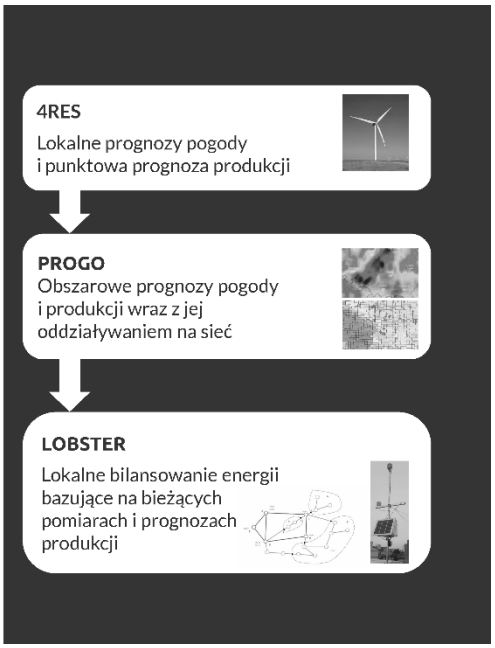
Systemy Informatyczne
w Energetyce – Wisła 2024

6.11.2024 • Dr inż. Krzysztof Kołodziejczyk

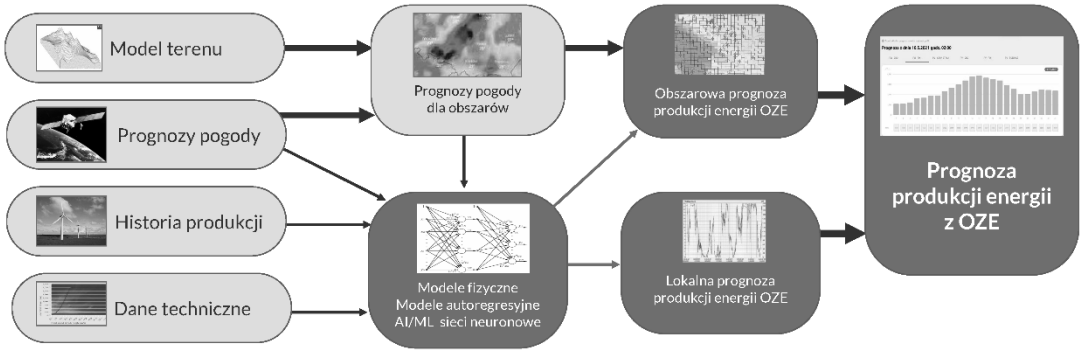
Od prognoz lokalnych do bilansowania

- Ponad **20 lat współpracy** z energetyką zawodową
- Doświadczenie w zakresie **predykcji**
- Dedykowany **zespół ekspertów** w ramach CRO
- Bieżąca współpraca ze specjalistami z **IEn PW** i zespołem prognoz **ICM UW**

www.globema.pl



Wiele modeli prognostycznych i indywidualizacja



www.globema.pl

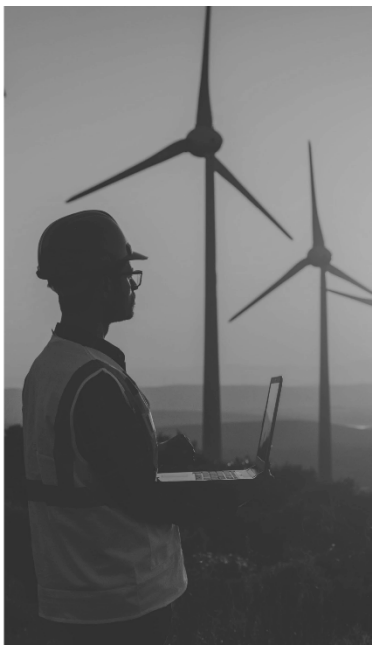
Zakres usługi prognozowania D+1

Prognozowanie produkcji dla farm wiatrowych

- Model uczenia maszynowego, uczony na historycznych pomiarach
- Optymalizacja wieloparametrowa
- Wielopunktowe prognozy pogody
- W razie braku danych pomiarowych – krzywe mocy

Prognozowanie produkcji dla farm słonecznych

- Metoda analityczna średniogodzinowego potencjału mocy
- Indywidualne współczynniki korekcji dobrane na danych pomiarowych lub ekspercko
- Obszarowe prognozy pogody



www.globema.pl

Prognozy uzupełniające

Prognozy w horyzoncie D+9

- Na potrzeby raportowania do OSD
- Wysyłka do godz. 7:30
- Zakres prognozy: od D+1 do D+9 co godzinę
- Mniejsza dokładność

Prognozy na dzień bieżący

- Dwie wysyłki: około 8:00 i około 14:00
- Prognozy 15 minutowe lub godzinowe
- Zakres prognozy: godz. 1..24 dnia bieżącego
- Błąd mniejszy o ok. 10% względem prognoz na dzień następny

www.globema.pl

Dokładność prognoz – miara błędu

$$\text{nMAE} = \frac{\sum_{i=1}^{n} \left| E_{pred_i} - E_{real_i} \right|}{n * P_{nom}}$$

E_{pred_i} – energia godzinowa prognozowana

E_{real_i} – energia godzinowa rzeczywista

P_{nom} – znamionowa moc farmy

n – liczba próbek godzinowych w mierzonym okresie

www.globema.pl

Dokładność prognoz

Dla farm słonecznych

Rodzaj farmy	Błąd całodobowy		Błąd dzienny	
	Zima	Lato	Zima	Lato
Pojedyncza PV	2,0%	7,5%	5,5%	11%
Elektrownia witrualna	1%	3,5%	3%	5,5%

Dla farm wiatrowych

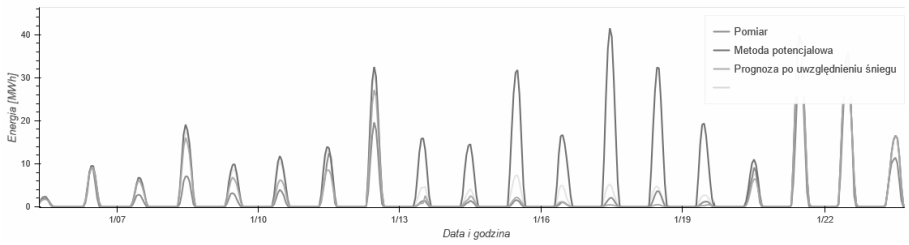
Modele fizyczne	błąd 12-15%
Modele AI/ML	błąd 7-9%

www.globema.pl

Dokładność prognoz dla farm wiatrowych

Wpływ śniegu na prognozę produkcji
- bezpośredni opad
- zaleganie pokrywy śnieżnej

nMAE na okresie 12.2020-01.2021
- bez korekty śniegowej: **1,62%**
- z korektą śniegową: **1,23%**



www.globema.pl

4RES API – dla usługobiorców

Pozwala na określenie redukcji

- addytywnie, np. do potrzeb własnych farmy
- proporcjonalnie, np. do odstawienia części (lub całości) farmy do konserwacji lub naprawy
- pułapowo, np. do ograniczeń systemowych

Pozwala na samodzielne kształtowanie listy farm do prognozowania

- w zakresie modeli opartych na krzywych mocy

Technologia:

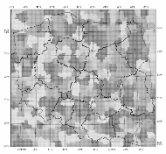
- https z uwierzytelnieniem
- REST (GET, POST)

www.globema.pl

Prognozowanie bilansu energii dla prosumentów w oparciu o AI/ML

Wykorzystanie modelu obszarowego prognozowania

obszarowe prognozy **pogody**



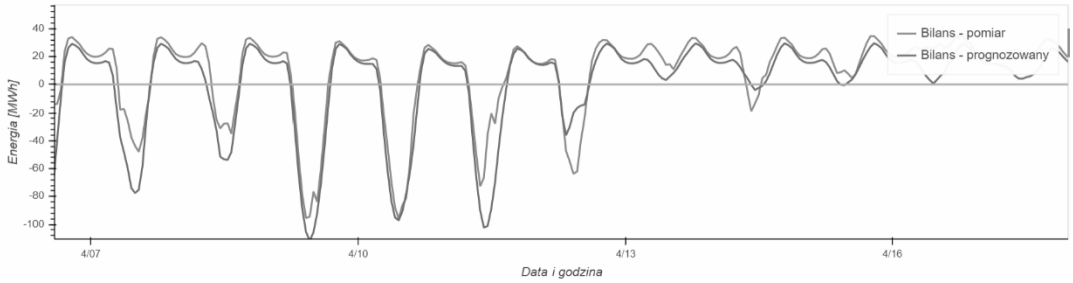
obszarowe prognozy **produkcji**

Błąd nMAE

- dla małych prosumentów (do 10 kW peak) – **4,6%**
- dla dużych prosumentów (do 50 kW peak) – **6,7%**

www.globema.pl

Wyniki prognozowania prosumentów



Fragment przebiegu czasowego bilansu pomierzonego i prognozowanego

www.globema.pl

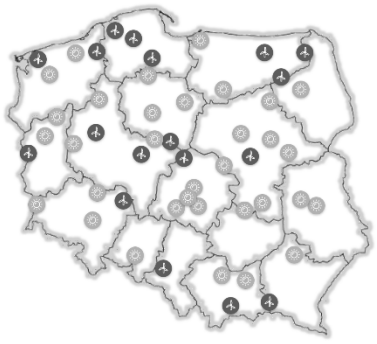
Zakres prognoz produkcji OZE w Polsce

Prognozy Punktowe

- Kilkaset OZE o mocy 1,5 GW

Prognozy obszarowe obejmujące:

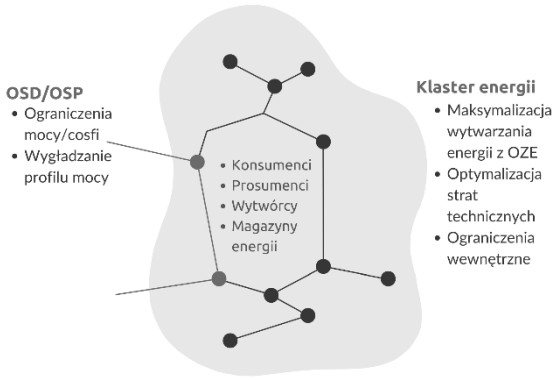
- 9,5 GW farm wiatrowych
- 5,2 GW farm słonecznych
- 11 GW prosumentów



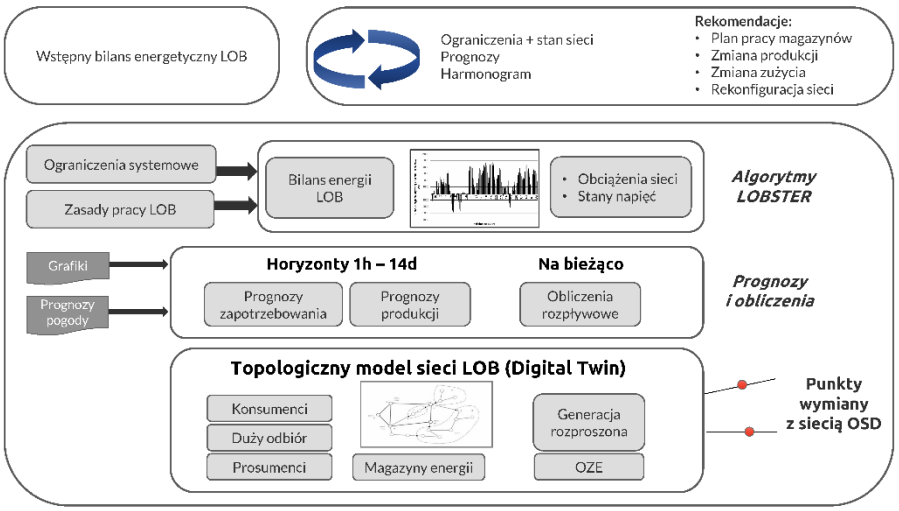
www.globema.pl

LOBSTER – wsparcie lokalnych obszarów bilansowania

- **LOBSTER** umożliwia prowadzenie **bilansowania energii na poziomie sieci dystrybucyjnych** w dowolnie zdefiniowanym Lokalnym Obszarze Bilansowania (**LOB**).
- Utworzony w systemie **Cyfrowy Bliźniak LOB** jest miejscem wykonywania obliczeń rozpływowych z **analizą prądowo-napięciową** oraz **predykcją zmian zapotrzebowania i produkcji** w horyzoncie czasowym od 1 godziny do 14 dni.



www.globema.pl

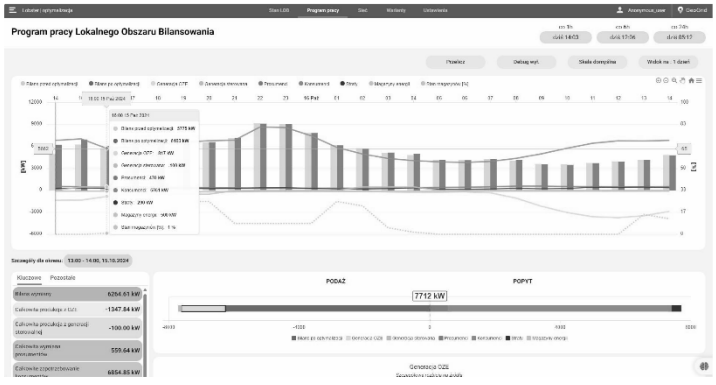


www.globema.pl

LOBSTER – topologiczny model sieci

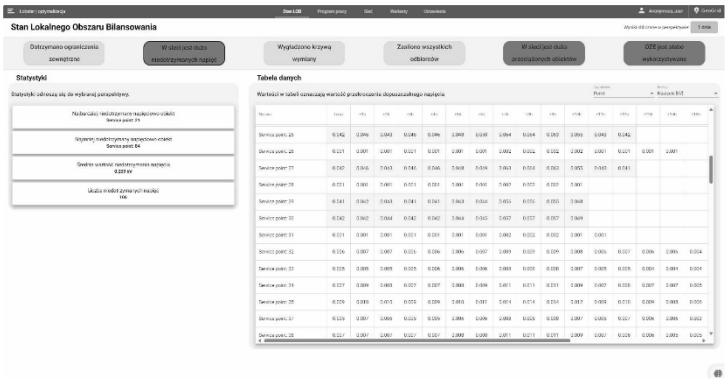
www.globema.pl

LOBSTER – bilans energii



www.globema.pl

LOBSTER – aktualny stan napięć



www.globema.pl

Wspierane serwisy społecznościowe

prognOZEr

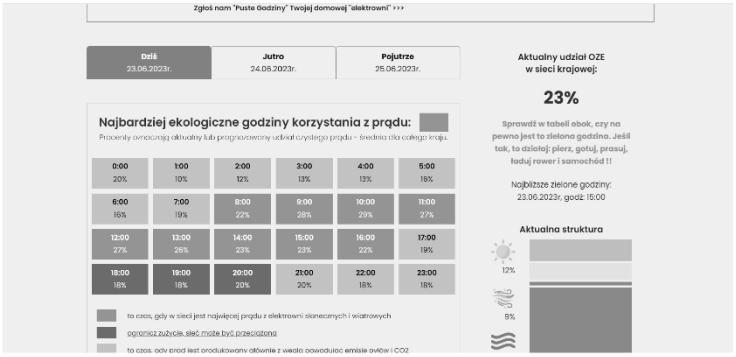
- Serwis prezentujący **intensywność dobowej produkcji energii w źródłach słonecznych i wiatrowych** w horyzoncie trzech dni i podziale na województwa lub powiaty.
- Dane źródłowe dotyczące lokalizacji i mocy poszczególnych źródeł pochodzą z **URE**, a prognozy obszarowe są generowane na naszej platformie prognostycznej **4RES** we współpracy z **ICM**.

https://prognozer.globema.pl/

www.globema.pl

Wspierane serwisy społecznościowe

Zielone Godziny



www.globema.pl

Globema w pigułce

7 oddziałów w 5 krajach

- **Globema PL** • Polska (3 oddziały)
- **Globema CS** • Czechy
- **Globema RO** • Rumunia
- **Globema US** • USA
- **Globema Adria** • Serbia

Prywatna spółka założona w 1997 roku.
Zatrudnia **wysoko wykwalifikowanych specjalistów IT** – w sumie ponad **200** osób.

Geoprzestrzenne rozwiązania IT oraz rozwiązania mobilne przeznaczone do szerokiej gamy zastosowań.
Zbudowane z wykorzystaniem **wiodących technologii** i platform.
Innowacyjne projekty **R&D**.

800+ klientów biznesowych w **50+** krajach.
Referencje od klientów z branży **teleco, utilities** i innych
Solidne **partnerstwa**.

www.globema.pl

Wybrani klienci – utilities

PERN · TAURON POLSKA ENERGIA · STOEN OPERATOR powered by E.ON · Energa operator · POLENERGIA · pes s.a. Polskie Elektrownie Słoneczne S.A.
PGE · ORLEN · umeme · ENEXIS · Manitoba Hydro · UE UNITED ENERGY
TURKCELL · VEOLIA · yedaş · DELGAZ grid · Xcel Energy · EWII
STEDIN · AMERICAN ELECTRIC POWER · TREDAŞ · NamPower · Exelon · alliander

www.globema.pl

globema

Dziękuję!

Dr inż. Krzysztof Kołodziejczyk

Dyrektor Rozwoju Biznesu Utilities

- krzysztof.kolodziejczyk@globema.pl
- www.globema.pl

www.globema.pl

globema

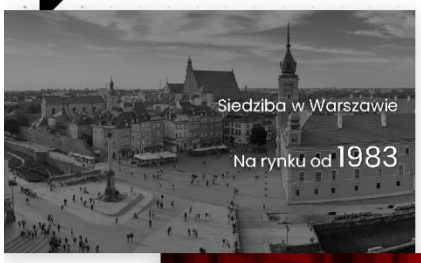
SYSTEM MONITORINGU INSTALACJI OZE – OD POZYSKANIA DANYCH PO WIZUALIZACJĘ I SERWIS

Przemysław Strzała (Elmark Automatyka S.A.)

System monitoringu instalacji OZE – od pozyskania danych po wizualizację i serwis

Przemysław Strzała
IIoT & ICG Product Sales Manager
e-mail: Przemyslaw.Strzala@elmark.com.pl
telefon: +48 607-197-727

Elmark Automatyka w pigułce



Jeden z największych dystrybutorów w Europie producentów:
Advantech, Getac, Moxa, Unitronics

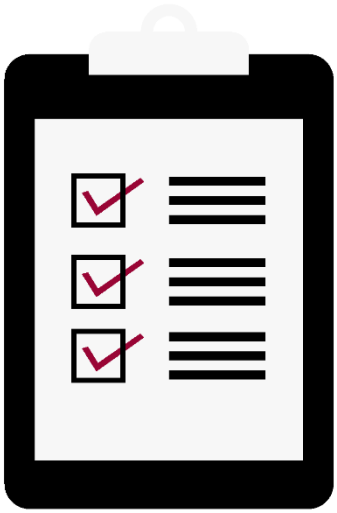
Lider wśród dostawców produktów automatyki przemysłowej w Polsce


Czym się zajmujemy?
Wizualizacja
Analiza
Agregacja
Transmisja
Pomiary
HTML5 MOBILEHMI
SQL OPC UA PROFINET MODBUS DNP3 IEC101 IEC61850
ETHERNET WIFI 4G 5G LTE450
RS-232/485 ETHERNET WIFI LoRaWAN USB
SYGNAŁY ANALOGOWE/CYFROWE


Podejście projektowe - etapy
Analiza problemu
Klient zgłasza się do nas z problemem występującym w jego organizacji
Przygotowanie koncepcji
Przedstawiamy koncepcję software'ową oraz hardware'ową rozwiązującą problem
Pełnoskalowe wdrożenie
Po wdrożeniu PoC i uporaniu się z „problemami życia dziecięcego" aplikacji przechodzimy do pełnego wdrożenia
Projekt rozwiązania (PoC)
Po zaakceptowaniu koncepcji przygotowujemy projekt w małej skali

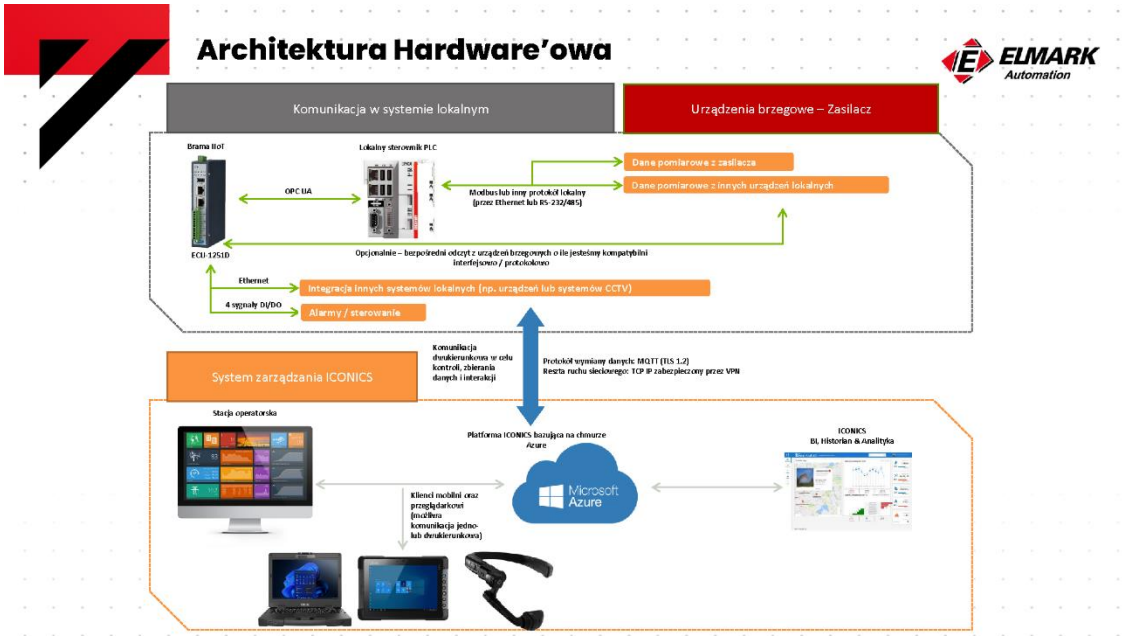
System monitoringu instalacji OZE

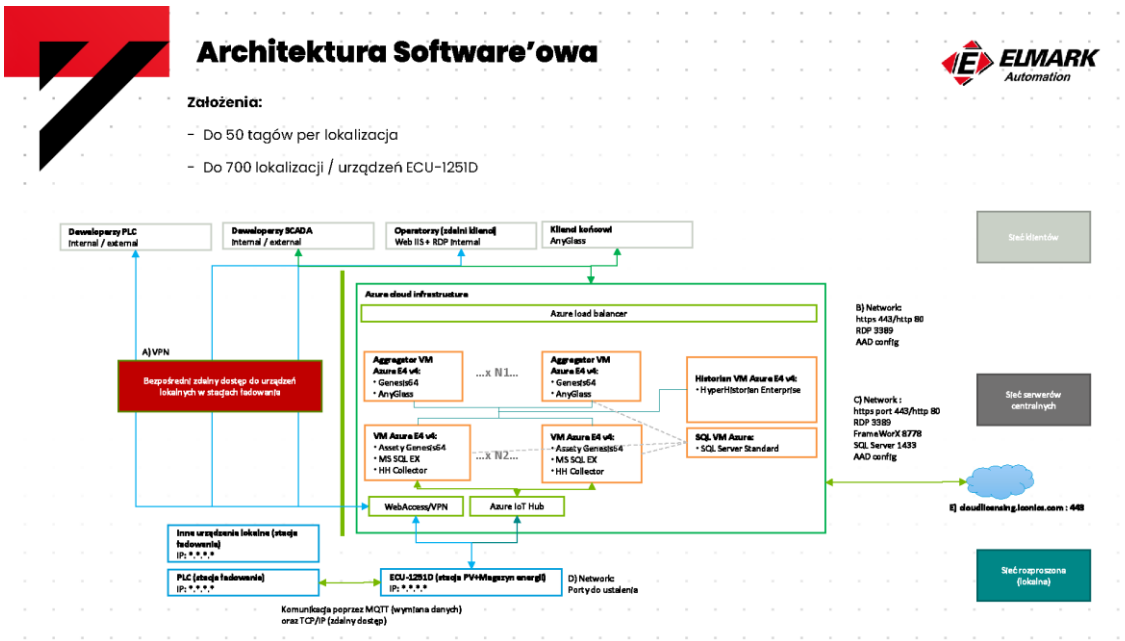
Analiza problemu



Analiza problemu

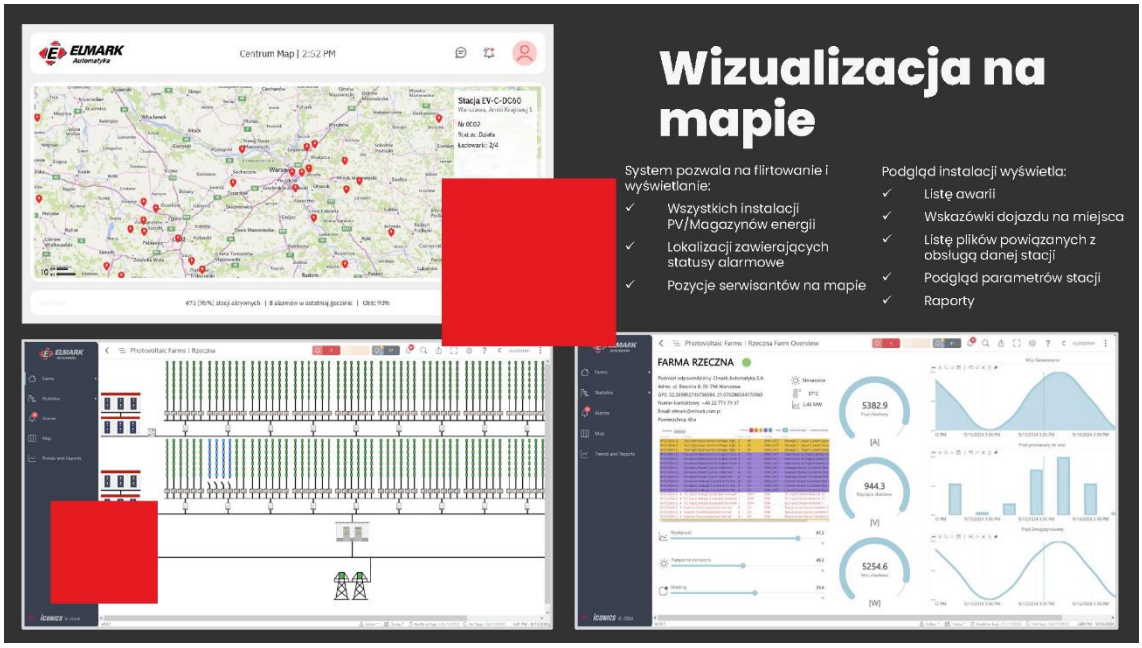

System monitoringu instalacji OZE
Przygotowanie koncepcji

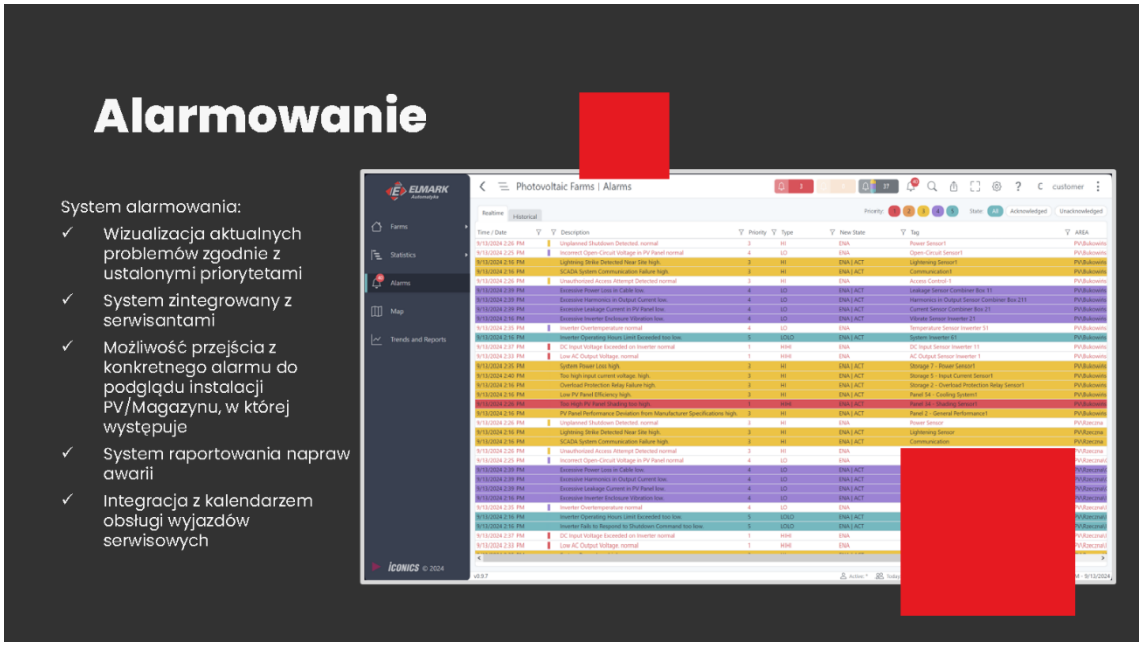

Architektura Hardware'owa
ELMARK Automation
Komunikacja w systemie lokalnym
Urządzenia brzegowe – Zasilacz
Brama IIoT
Lokalny sterownik PLC
OPC UA
Modbus lub inny protokół lokalny (przez Ethernet lub RS-232/485)
Dane pomiarowe z zasilacza
Dane pomiarowe z innych urządzeń lokalnych
ECU-1251D
Opcjonalnie – bezpośredni odczyt z urządzeń brzegowych o ile jesteśmy kompatybilni interfejsowo / protokołowo
Ethernet
4 sygnały DI/DO
Integracja innych systemów lokalnych (np. urządzeń lub systemów CCTV)
Alarmy / sterowanie
System zarządzania ICONICS
Komunikacja dwukierunkowa w celu kontroli, zbierania danych i interakcji
Protokół wymiany danych: MQTT (TLS 1.2)
Reszta ruchu sieciowego: TCP IP zabezpieczony przez VPN
Stacja operatorska
Platforma ICONICS bazująca na chmurze Azure
Microsoft Azure
ICONICS BI, Historian & Analityka
Klienci mobilni oraz przeglądarkowi (możliwa komunikacja jedno- lub dwukierunkowa)



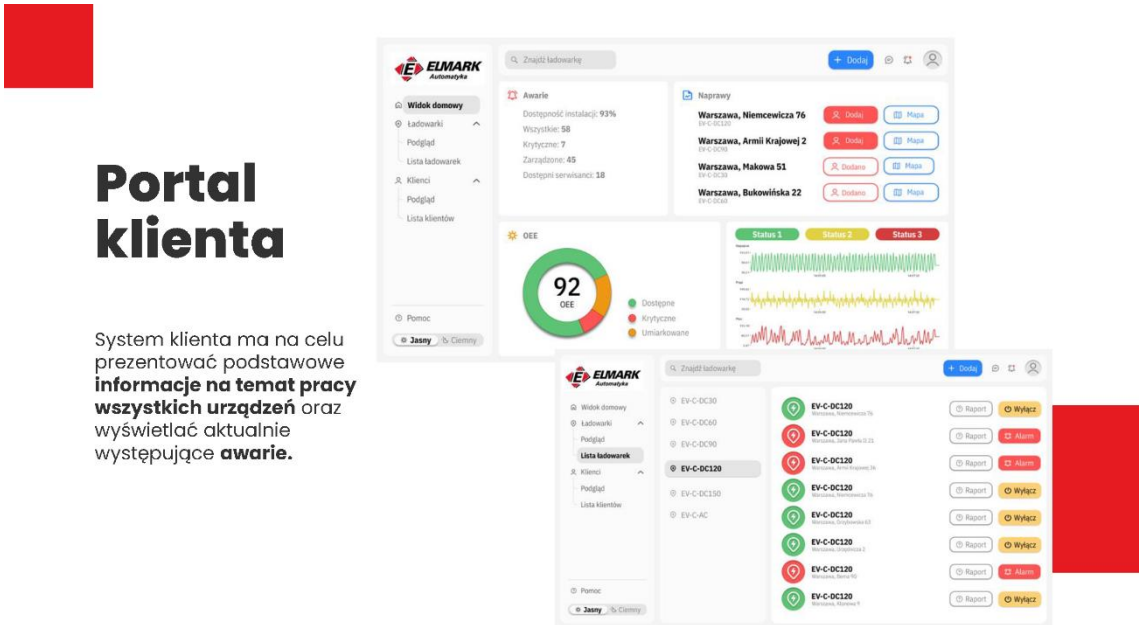
System monitoringu instalacji OZE

Projekt rozwiązania (PoC)


Wizualizacja na mapie
System pozwala na flirtowanie i wyświetlanie:
Wszystkich instalacji PV/Magazynów energii
Lokalizacji zawierających statusy alarmowe
Pozycje serwisantów na mapie
Podgląd instalacji wyświetla:
Listę awarii
Wskazówki dojazdu na miejsca
Listę plików powiązanych z obsługą danej stacji
Podgląd parametrów stacji
Raporty
FARMA RZECZNA


Alarmowanie
System alarmowania:
Wizualizacja aktualnych problemów zgodnie z ustalonymi priorytetami
System zintegrowany z serwisantami
Możliwość przejścia z konkretnego alarmu do podglądu instalacji PV/Magazynu, w której występuje
System raportowania napraw awarii
Integracja z kalendarzem obsługi wyjazdów serwisowych


System serwisowy
Wymagania:
✓ Wizualizacja danych niezbędnych dla serwisanta (użytkownicy i ich role)
✓ Dostosowanie do różnych systemów przenośnych
✓ Możliwość interakcji serwisant – control room
INFORMACJE
INSTRUKCJA
ALARMY
94.1 V
81.18 mA
78.56 W
Demo technologiczne | Elmark Automatyka
STATYSTYKI
INSTRUKCJA
ALARMY
NR SERYJNY:
ELM-2023-SN-777
TYP:
ROZDZIELNICA SN ZASILACZ X STEROWNIK Y
ZADANIA DO WYKONANIA:
1. ZNALEŹĆ ZWARCIE
2. WYMIENIĆ ZASILACZ
3. WGRAĆ NOWY PROGRAM NA PLC
Demo technologiczne | Elmark Automatyka
STATYSTYKI
INSTRUKCJA
INFORMACJE
OBECNE ALARMY W STACJI:
Pojemność baterii awaryjnego zasilania jest prawidłowa.
Napięcie na module zasilania jest wysokie.
Temperatura otoczenia jest zbyt niska.
Zabezpieczenia przeciwporażeniowe nie działają poprawnie!
Demo technologiczne | Elmark Automatyka


Portal klienta
System klienta ma na celu prezentować podstawowe **informacje na temat pracy wszystkich urządzeń** oraz wyświetlać aktualnie występujące **awarie.**
ELMARK Automatyka
Widok domowy
Ładowarki
Podgląd
Lista ładowarek
Klienci
Podgląd
Lista klientów
Pomoc
Jasny
Ciemny
Awarie
Naprawy
Warszawa, Niemcewicza 76
Warszawa, Armii Krajowej 2
Warszawa, Makowa 51
Warszawa, Bukowińska 22
OEE
92
Dostępne
Krytyczne
Umiarkowane
Status 1
Status 2
Status 3
EV-C-DC30
EV-C-DC60
EV-C-DC90
EV-C-DC120
EV-C-DC150
EV-C-AC

System monitoringu instalacji OZE

Kluczowe podzespoły

Pozyskiwanie danych ECU-1251D

Urządzenie łączy jednocześnie funkcje:

- Serwera portów szeregowych
- Konwertera protokołów
- Lokalnego back-upu danych
- Zdalnego dostępu
- Komunikacji LTE
- Alarmowania SMS, E-mail
- Komunikacji z SCADA/chmurą
- Sterownika PLC

Rozwiązywane problemy:

1. Zapewnienie stabilnej komunikacji z infrastrukturą brzegową
2. Lokalny backup danych
3. Szyfrowanie komunikacji
4. Zdalny dostęp do urządzeń brzegowych
5. Scentralizowane zarządzanie urządzeniami brzegowymi
6. Możliwość wymiany urządzenia pośredniego (sterownika PLC)
7. Łatwa skalowalność systemu

System serwisanta – komputery wzmocnione

Laptopy przemysłowe, to urządzenia świetnie sprawdzające się w terenie. Na tę przydatność składają się:

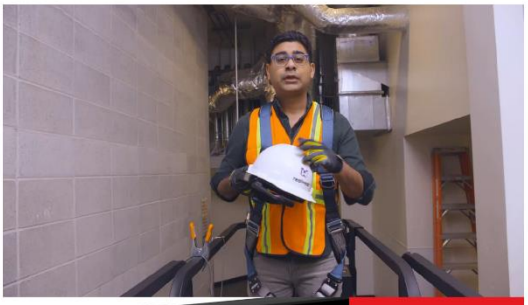
- Szer. zakres temp. pracy (-20-60)
- Certyfikat MIL-STD-810G
- Odporność na śnieg i wodę (IP66)
- Bezpieczeństwo – TPM2.0
- Bateria hot swap
- Najwyższa wydajność – i7 11Gen
- Ekran o jasności do 1000 nitów
- Mnogość interfejsów:
  - LTE/LTE450/GPS
  - Bluetooth 5.2
  - RFID/Czytnik odcisku palca/IR
  - Czytnik kodów kreskowych/QR
  - USB 3.2/Thunderbolt
  - Docking Connector

System serwisanta – tablety wzmocnione

Tablety wzmocnione to produkty cechujące się tymi samymi parametrami, co komputery ale stawiające na większą mobilność. Głównymi różnicami w stosunku do laptopów są:

- Nieco mniejsza bateria, ale wciąż hot swapowa
- Darmowa wymiana ekranu raz w roku
- Stacja dokująca zmieniająca tablet w laptopa

System serwisowy - Komputery nasobne



RealWeare to komputer nasobny wyposażony w system Android, który pozwala na obsługę zgłoszeń serwisowych z wolnymi rękoma.

- Symulacja ekranu 10" (1280x720px)
- Obsługa głosowa
- Wysokiej rozdz. kamera (48Mpx)
- Dodatkowa kamera termowizyjna
- Bateria hot swap
- IP66 i MIL-STD-810H
- Snapdragon 662 + Android

Mnogość zastosowań:
- Zdalne wsparcie techniczne
- Inspekcje i instruktaże
- Przegląd dokumentów
- Wizualizacja danych

realwear

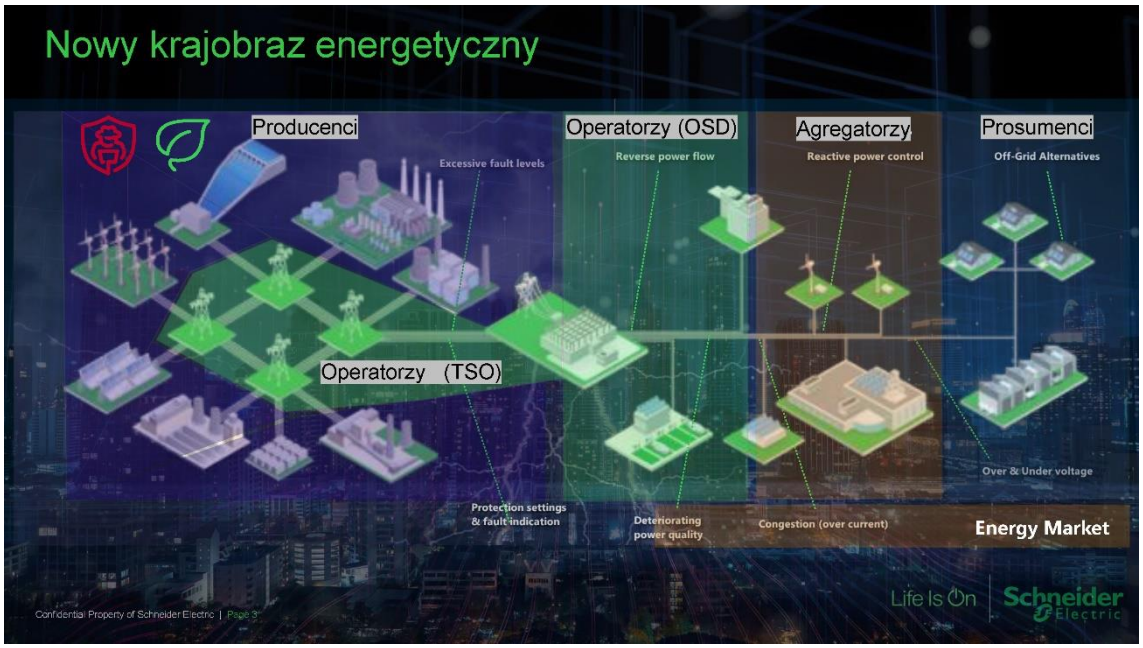
Dziękujemy za uwagę

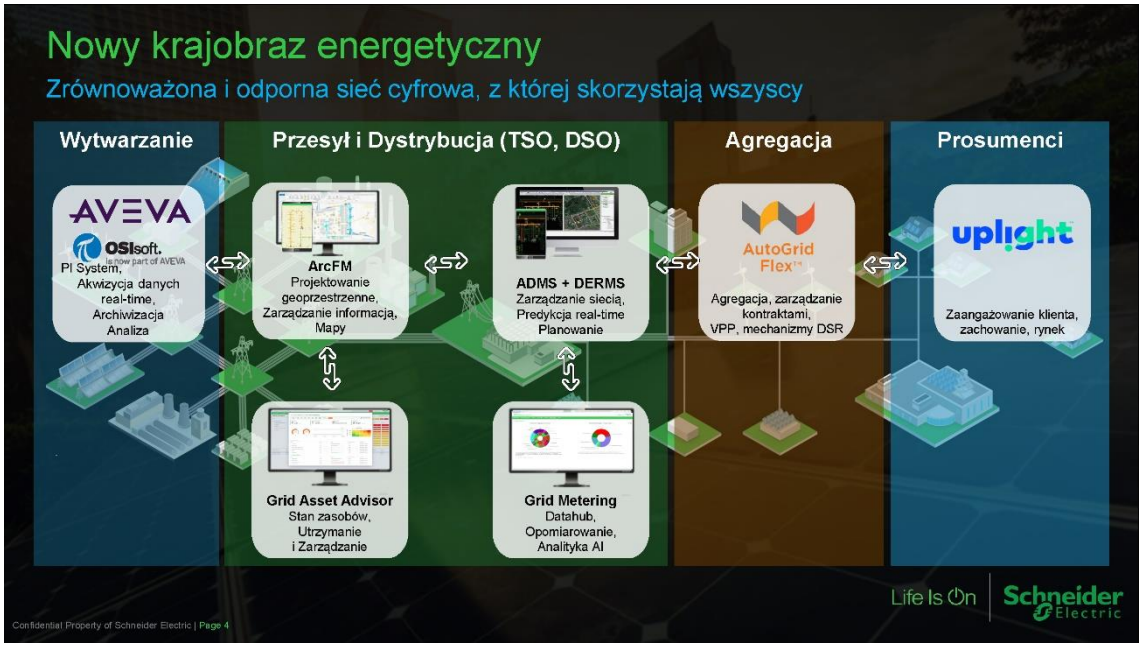
Sprawdź:

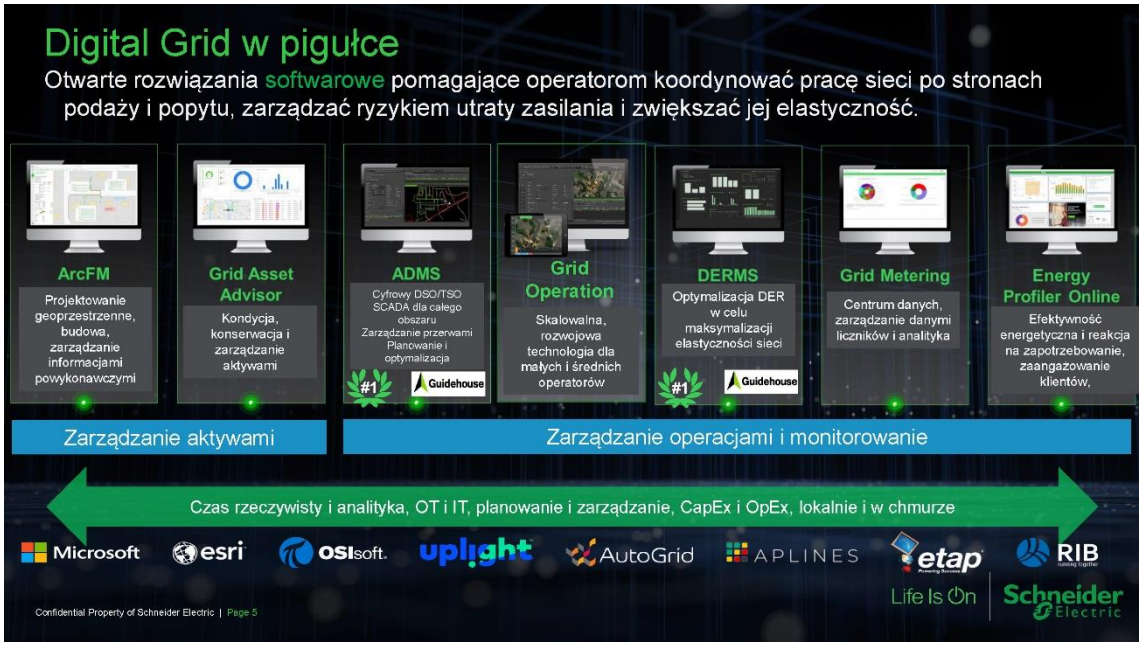
www.elmark.com.pl www.elmark-automation.com www.elmark.com.ro

CYFROWE ZARZĄDZANIE ZASOBAMI I PORTFELEM AKTYWÓW PRZEDSIĘBIORSTWA. PRZEGLĄD APLIKACJI I ROZWIĄZAŃ WSPIERAJĄCYCH PROJEKTOWANIE ORAZ ANALIZUJĄCYCH RYZYKA

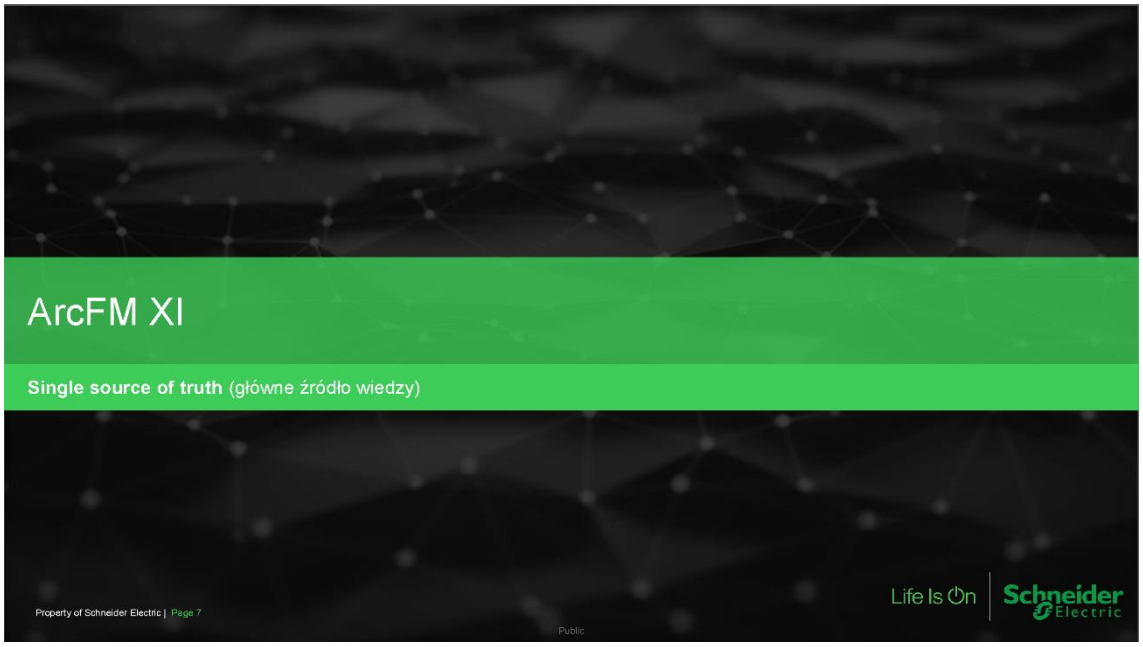
Przemysław Liman (Schneider Electric)

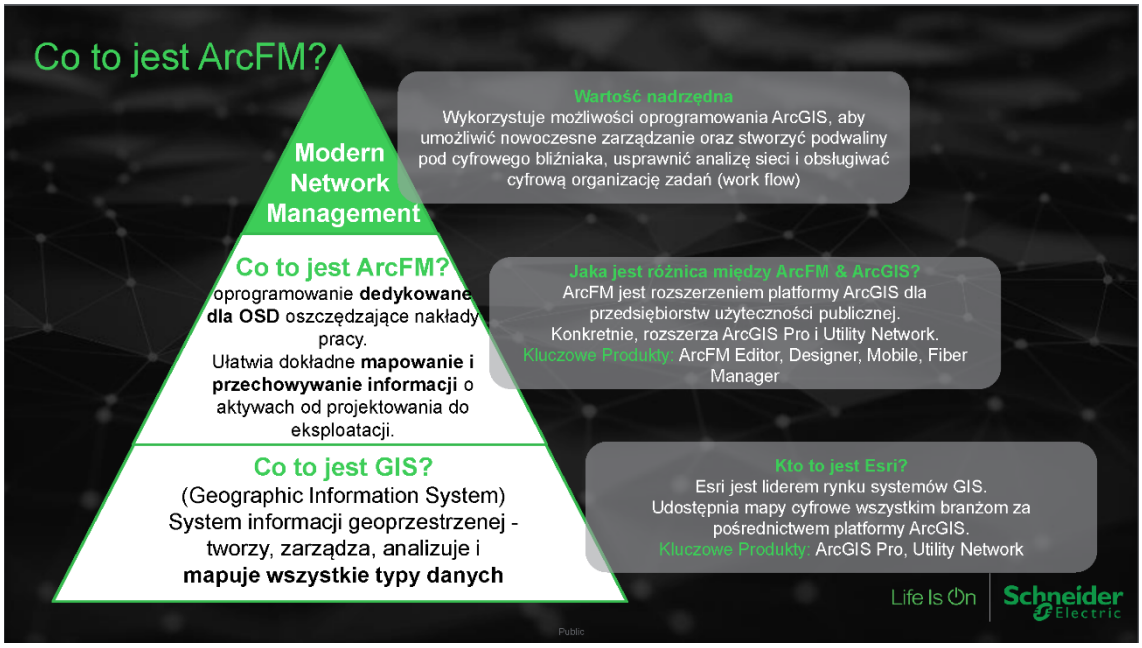


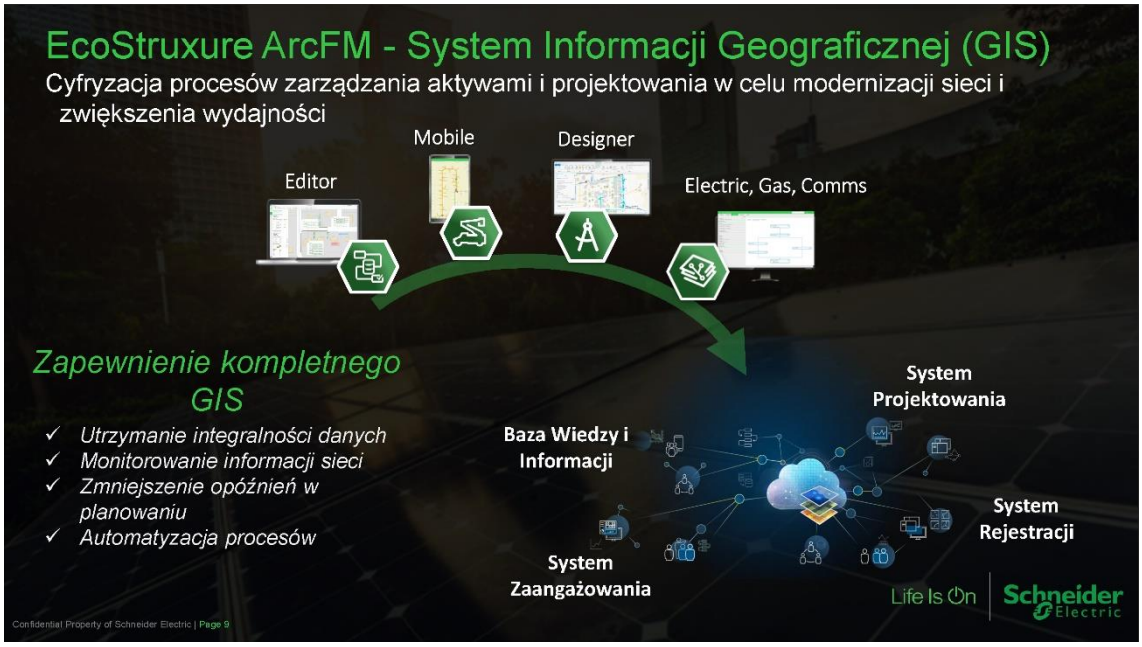

Nowy krajobraz energetyczny
Zrównoważona i odporna sieć cyfrowa, z której skorzystają wszyscy
Wytwarzanie
Przesył i Dystrybucja (TSO, DSO)
Agregacja
Prosumenci
AVEVA
OSIsoft.
PI System,
Akwizycja danych real-time,
Archiwizacja
Analiza
ArcFM
Projektowanie geoprzestrzenne,
Zarządzanie informacją,
Mapy
ADMS + DERMS
Zarządzanie siecią,
Predykcja real-time
Planowanie
AutoGrid Flex™
Agregacja, zarządzanie kontraktami,
VPP, mechanizmy DSR
uplight
Zaangażowanie klienta, zachowanie, rynek
Grid Asset Advisor
Stan zasobów,
Utrzymanie
i Zarządzanie
Grid Metering
Datahub,
Opomiarowanie,
Analityka AI
Life Is On
Schneider Electric
Confidential Property of Schneider Electric | Page 4

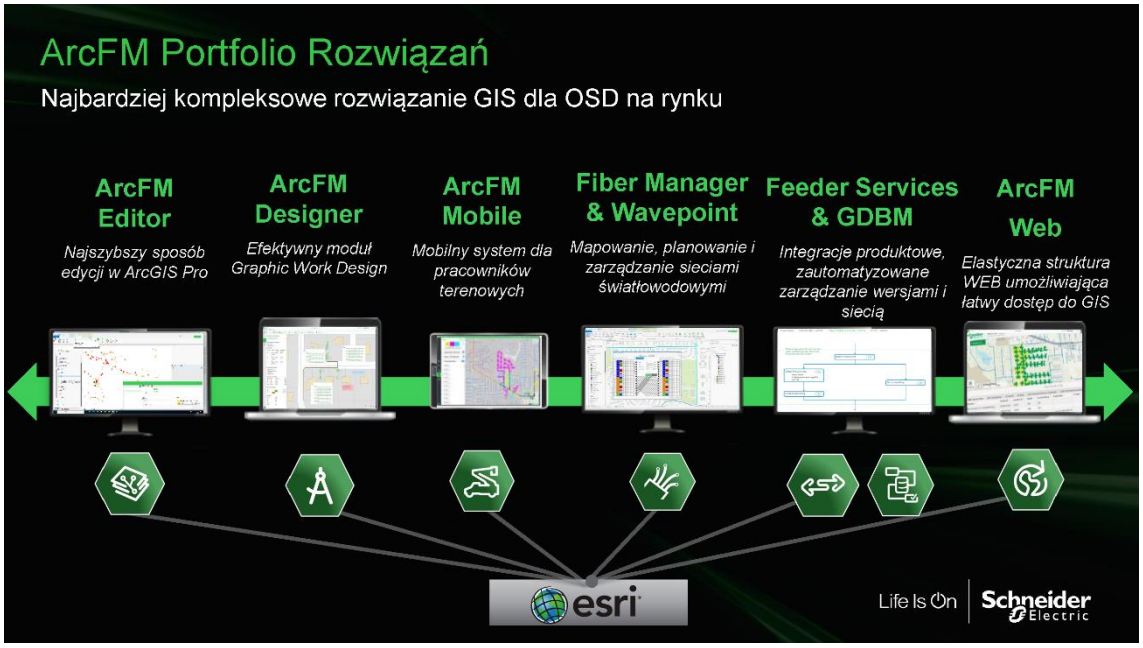

Digital Grid w pigułce
Otwarte rozwiązania softwarowe pomagające operatorom koordynować pracę sieci po stronach podaży i popytu, zarządzać ryzykiem utraty zasilania i zwiększać jej elastyczność.
ArcFM
Projektowanie geoprzestrzenne, budowa, zarządzanie informacjami powykonawczymi
Grid Asset Advisor
Kondycja, konserwacja i zarządzanie aktywami
ADMS
Cyfrowy DSO/TSO SCADA dla całego obszaru
Zarządzanie przerwami
Planowanie i optymalizacja
#1
Guidehouse
Grid Operation
Skalowalna, rozwojowa technologia dla małych i średnich operatorów
DERMS
Optymalizacja DER w celu maksymalizacji elastyczności sieci
#1
Guidehouse
Grid Metering
Centrum danych, zarządzanie danymi liczników i analityka
Energy Profiler Online
Efektywność energetyczna i reakcja na zapotrzebowanie, zaangażowanie klientów,
Zarządzanie aktywami
Zarządzanie operacjami i monitorowanie
Czas rzeczywisty i analityka, OT i IT, planowanie i zarządzanie, CapEx i OpEx, lokalnie i w chmurze
Microsoft
esri
OSIsoft.
uplight
AutoGrid
APLINES
etap
RIB
Life Is On
Schneider Electric
Confidential Property of Schneider Electric | Page 5


Zarządzanie cyklem życia sieci
Stopniowa, cyberbezpieczna transformacja cyfrowa oraz zarządzanie danymi sieci
Planowanie
Planowanie sieci
analiza OZE Planowanie inwestycji
Projektowanie
Projektowanie graficzne
Współpraca
Współpraca z klientami i zarządzanie popytem
Budowa
Geoprzestrzenne
Zarządzanie zasobami
Zarządzanie pracą w terenie
Utrzymanie
Kondycja majątku trwałego i konserwacja
Monitorowanie
Centrum danych i zarządzanie urządzeniami
Zarządzanie danymi z liczników
Analityka nN
Optymalizacja
Elastyczność sieci
Zarządzanie DER
Obsługa
Zaawansowane zarządzanie dystrybucją i przesyłem
Life Is On
Schneider Electric
Confidential Property of Schneider Electric | Page 6

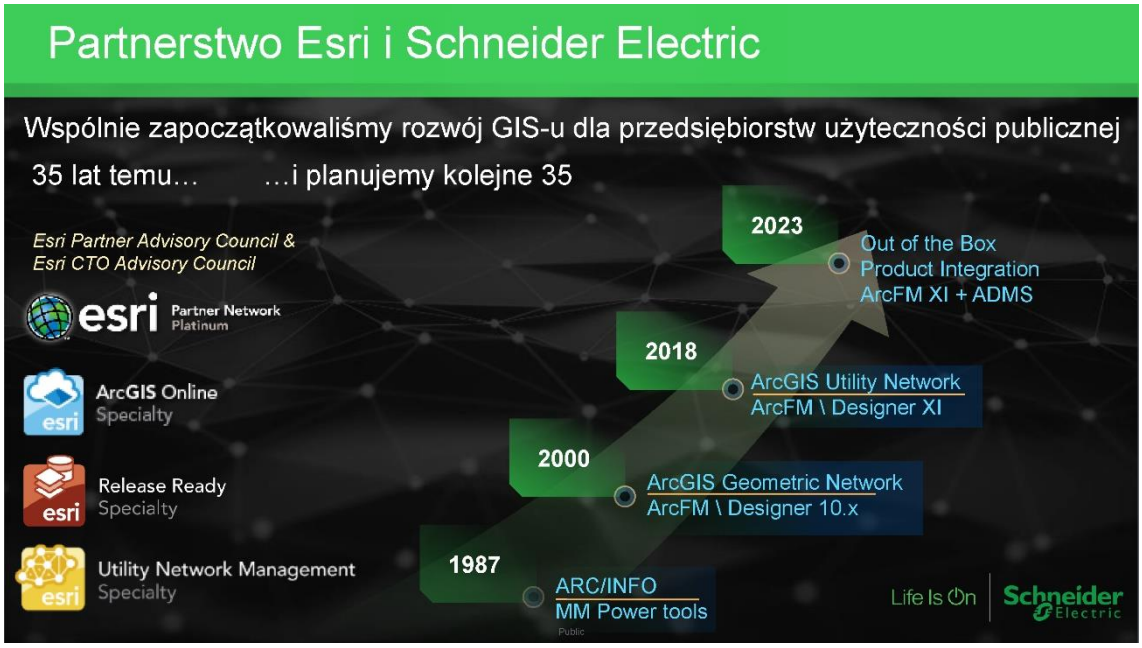

ArcFM XI
Single source of truth (główne źródło wiedzy)
Life Is On
Schneider Electric
Property of Schneider Electric | Page 7
Public


Co to jest ArcFM?
Modern Network Management
Wartość nadrzędna
Wykorzystuje możliwości oprogramowania ArcGIS, aby umożliwić nowoczesne zarządzanie oraz stworzyć podwaliny pod cyfrowego bliźniaka, usprawnić analizę sieci i obsługiwać cyfrową organizację zadań (work flow)
Co to jest ArcFM?
oprogramowanie dedykowane dla OSD oszczędzające nakłady pracy.
Ułatwia dokładne mapowanie i przechowywanie informacji o aktywach od projektowania do eksploatacji.
Jaka jest różnica między ArcFM & ArcGIS?
ArcFM jest rozszerzeniem platformy ArcGIS dla przedsiębiorstw użyteczności publicznej.
Konkretnie, rozszerza ArcGIS Pro i Utility Network.
Kluczowe Produkty: ArcFM Editor, Designer, Mobile, Fiber Manager
Co to jest GIS?
(Geographic Information System)
System informacji geoprzestrzenej - tworzy, zarządza, analizuje i mapuje wszystkie typy danych
Kto to jest Esri?
Esri jest liderem rynku systemów GIS.
Udostępnia mapy cyfrowe wszystkim branżom za pośrednictwem platformy ArcGIS.
Kluczowe Produkty: ArcGIS Pro, Utility Network
Life Is On
Schneider Electric
Public

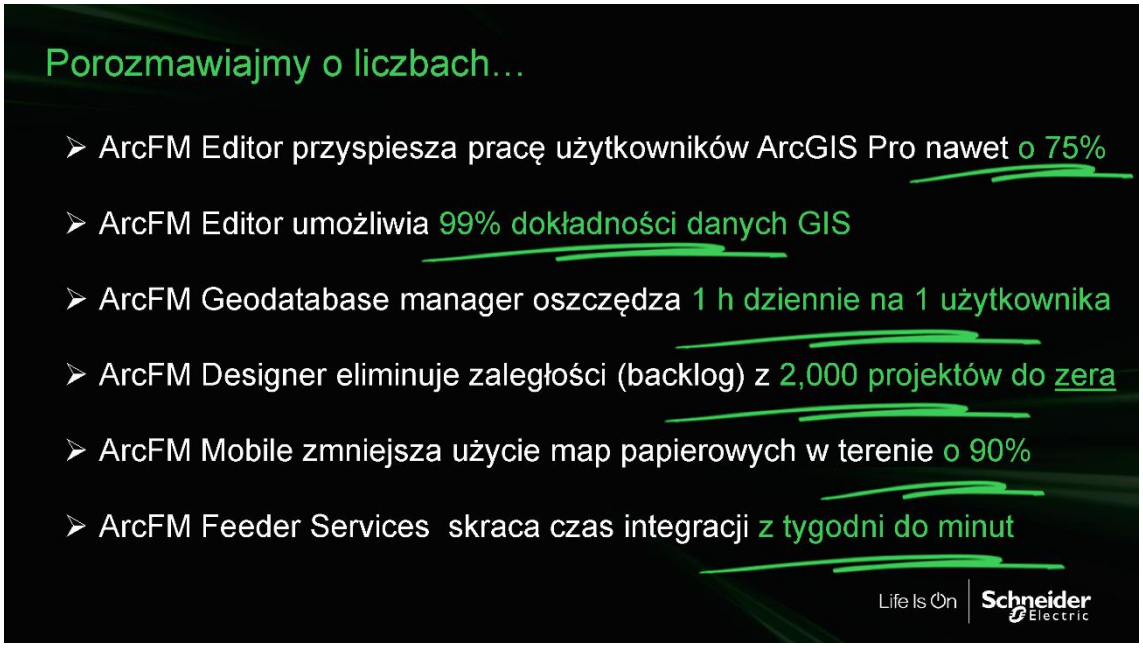

EcoStruxure ArcFM - System Informacji Geograficznej (GIS)
Cyfryzacja procesów zarządzania aktywami i projektowania w celu modernizacji sieci i zwiększenia wydajności
Editor
Mobile
Designer
Electric, Gas, Comms
Zapewnienie kompletnego GIS
✓ Utrzymanie integralności danych
✓ Monitorowanie informacji sieci
✓ Zmniejszenie opóźnień w planowaniu
✓ Automatyzacja procesów
Baza Wiedzy i Informacji
System Projektowania
System Rejestracji
System Zaangażowania
Life Is On
Schneider Electric
Confidential Property of Schneider Electric | Page 9

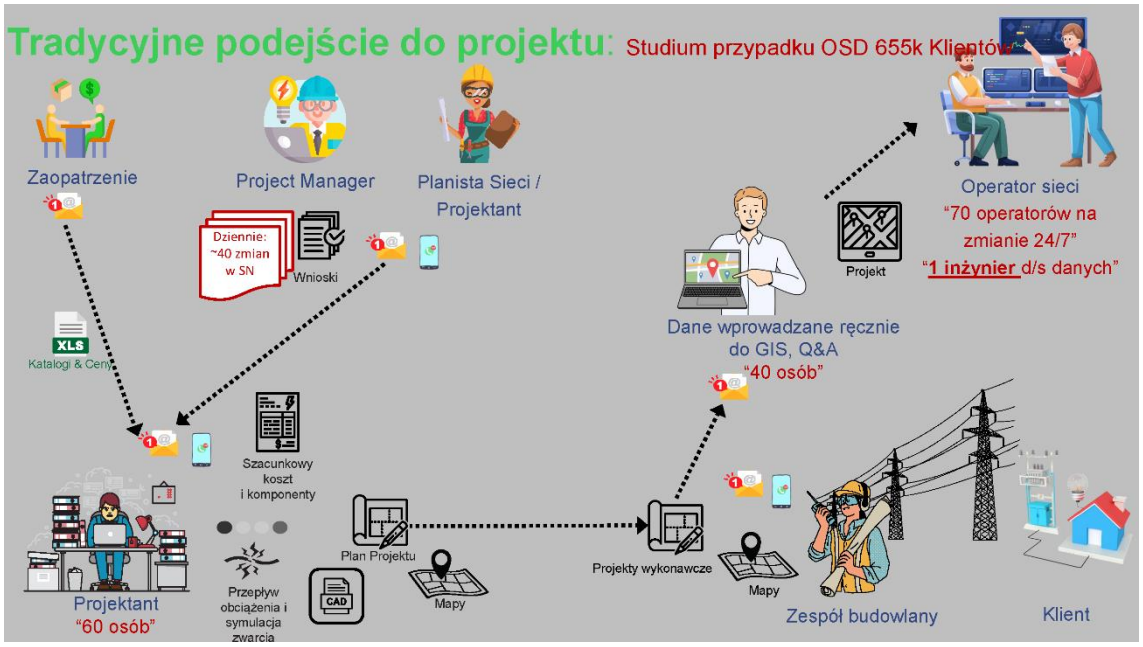

ArcFM Portfolio Rozwiązań
Najbardziej kompleksowe rozwiązanie GIS dla OSD na rynku
ArcFM Editor
Najszybszy sposób edycji w ArcGIS Pro
ArcFM Designer
Efektywny moduł Graphic Work Design
ArcFM Mobile
Mobilny system dla pracowników terenowych
Fiber Manager & Wavepoint
Mapowanie, planowanie i zarządzanie sieciami światłowodowymi
Feeder Services & GDBM
Integracje produktowe, zautomatyzowane zarządzanie wersjami i siecią
ArcFM Web
Elastyczna struktura WEB umożliwiająca łatwy dostęp do GIS
esri
Life Is On
Schneider Electric

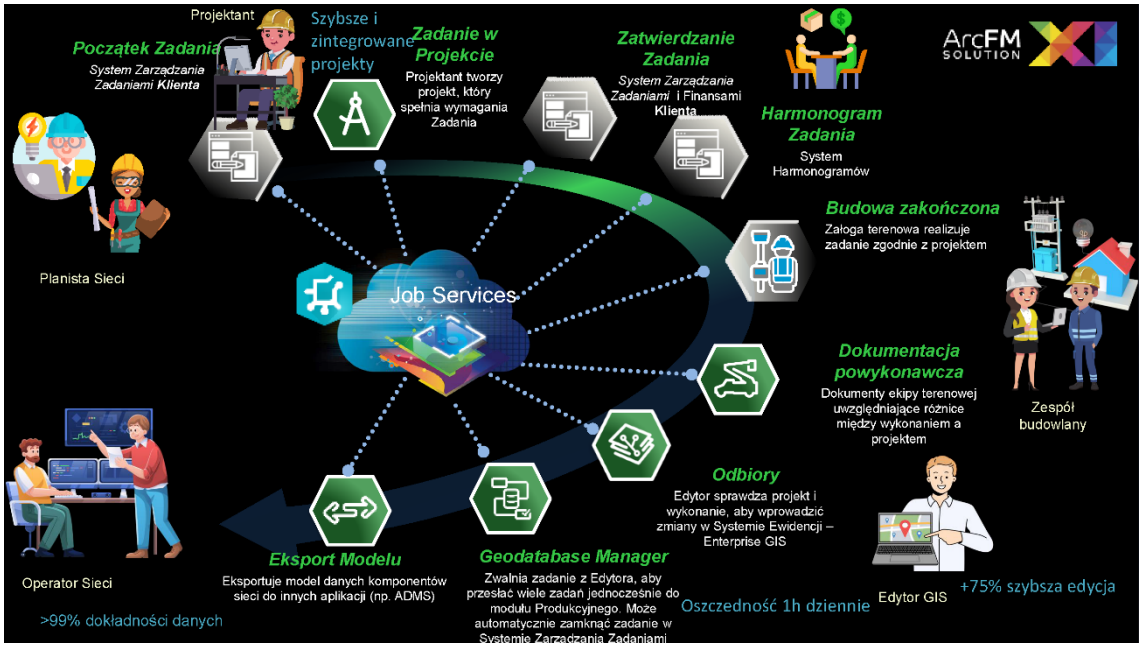

Ponad 500 globalnych użytkowników ArcFM
XL Customers (>5,000,000 opomiarowanych Klientów)
Large Customers (>1,000,000 opomiarowanych Klientów)
Medium Customers (>500,000 opomiarowanych Klientów)
Small Customers (>100,000 opomiarowanych Klientów)
V. Small Customers (<100,000 opomiarowanych Klientów)

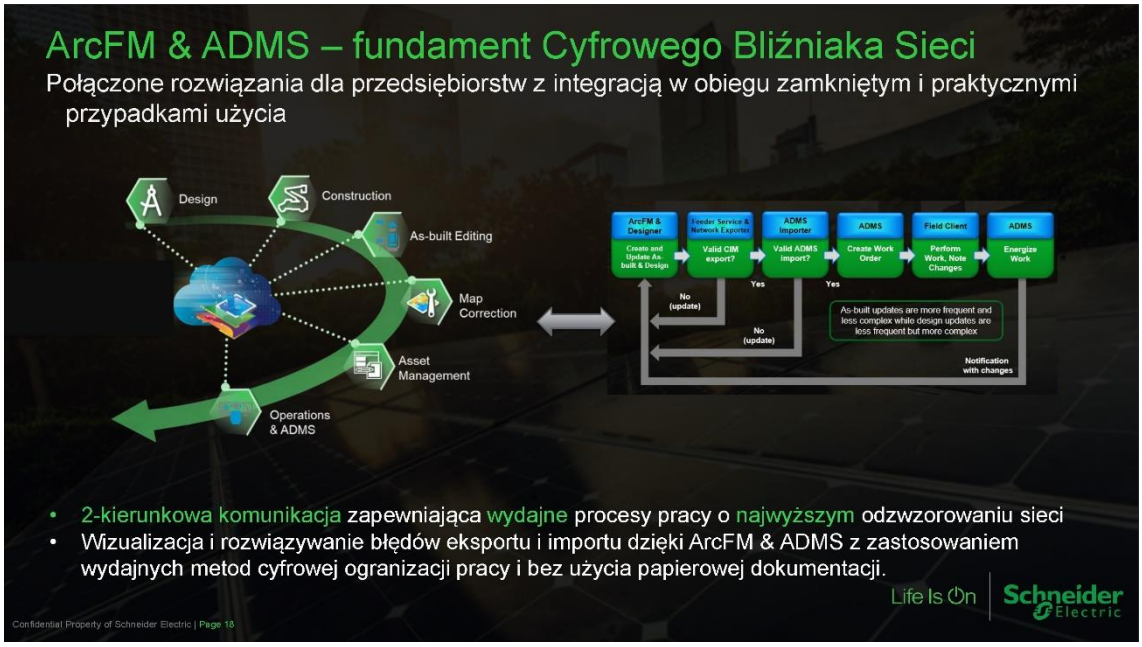

Partnerstwo Esri i Schneider Electric
Wspólnie zapoczątkowaliśmy rozwój GIS-u dla przedsiębiorstw użyteczności publicznej
35 lat temu…
…i planujemy kolejne 35
Esri Partner Advisory Council &
Esri CTO Advisory Council
esri Partner Network Platinum
ArcGIS Online Specialty
Release Ready Specialty
Utility Network Management Specialty
2023
Out of the Box Product Integration ArcFM XI + ADMS
2018
ArcGIS Utility Network ArcFM \ Designer XI
2000
ArcGIS Geometric Network ArcFM \ Designer 10.x
1987
ARC/INFO MM Power tools
Life Is On Schneider Electric

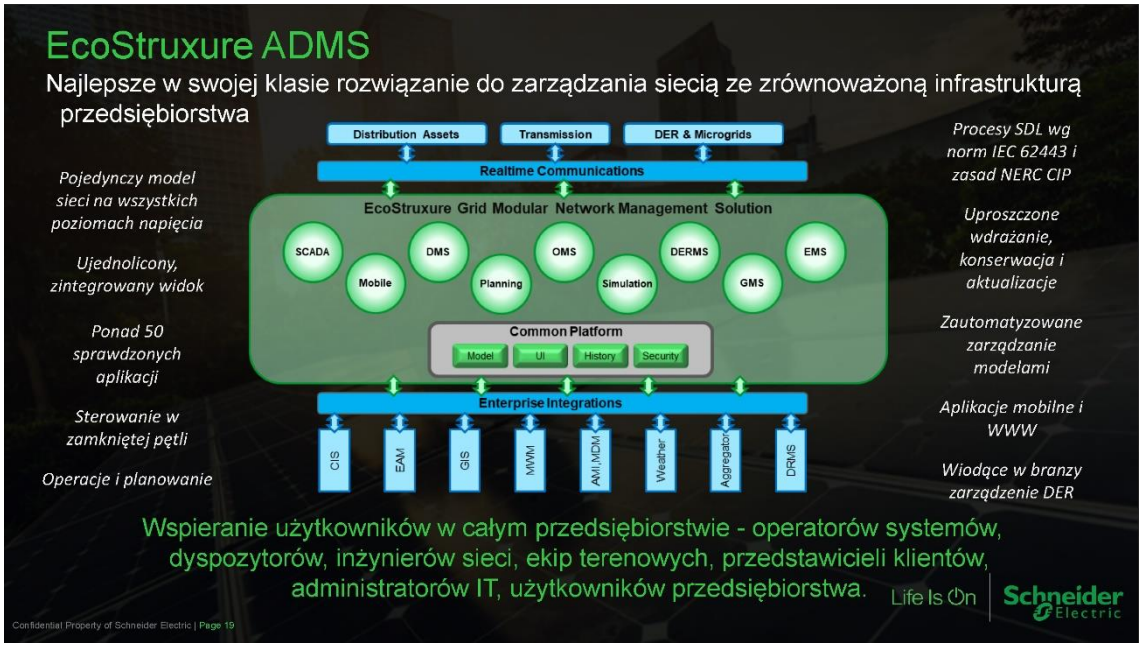

Zaawansowane rozwiązania GIS przekształcą Twoją organizację
Zwiększ produktywność i bezpieczeństwo
Go Digital & Redukuj papier
Eliminuj Duplikaty
Redukuj Zaległości
Przyspiesz Realizację
Przy użyciu ArcGIS i ArcFM, możesz mieć...
IMPACT
ArcGIS Platform
ArcFM SOLUTION
... na transformację energetyczną
Life Is On Schneider Electric

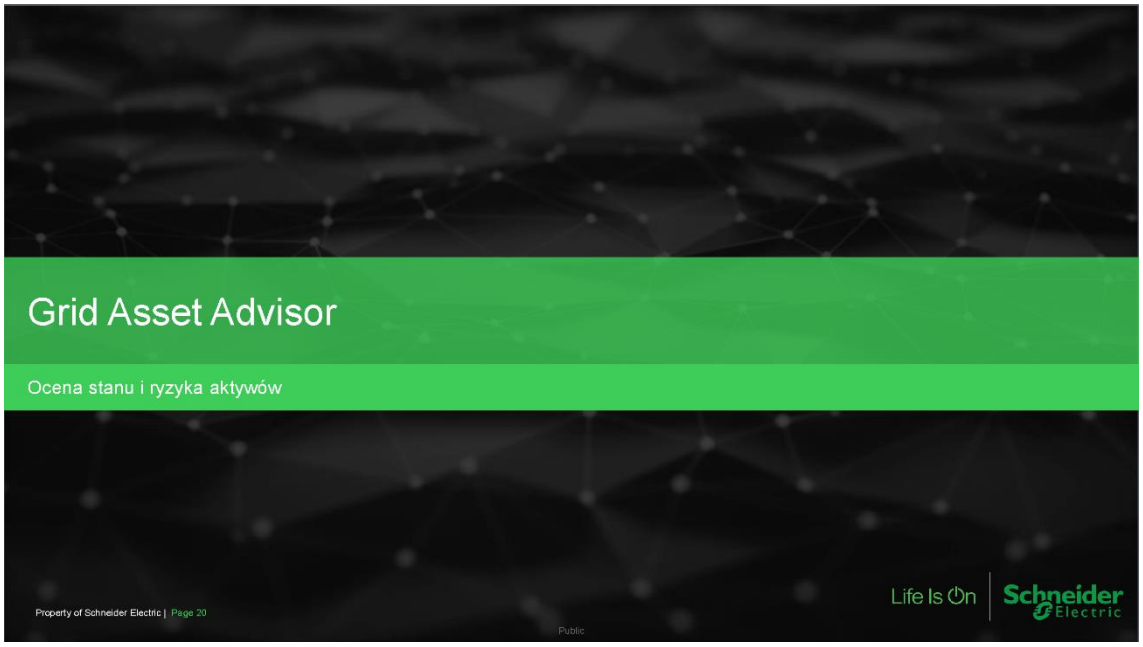

Porozmawiajmy o liczbach…
ArcFM Editor przyspiesza pracę użytkowników ArcGIS Pro nawet o 75%
ArcFM Editor umożliwia 99% dokładności danych GIS
ArcFM Geodatabase manager oszczędza 1 h dziennie na 1 użytkownika
ArcFM Designer eliminuje zaległości (backlog) z 2,000 projektów do zera
ArcFM Mobile zmniejsza użycie map papierowych w terenie o 90%
ArcFM Feeder Services skraca czas integracji z tygodni do minut
Life Is On
Schneider Electric


Tradycyjne podejście do projektu: Studium przypadku OSD 655k Klientów
Zaopatrzenie
Project Manager
Planista Sieci / Projektant
Dziennie: ~40 zmian w SN
Wnioski
XLS
Katalogi & Cen
Operator sieci
"70 operatorów na zmianie 24/7"
"1 inżynier d/s danych"
Projekt
Dane wprowadzane ręcznie do GIS, Q&A
"40 osób"
Szacunkowy koszt i komponenty
Projektant
"60 osób"
Przepływ obciążenia i symulacja zwarcia
Plan Projektu
CAD
Mapy
Projekty wykonawcze
Mapy
Zespół budowlany
Klient


Początek Zadania
System Zarządzania Zadaniami Klienta
Projektant
Szybsze i zintegrowane projekty
Zadanie w Projekcie
Projektant tworzy projekt, który spełnia wymagania Zadania
Zatwierdzanie Zadania
System Zarządzania Zadaniami i Finansami Klienta
Harmonogram Zadania
System Harmonogramów
ArcFM SOLUTION
Budowa zakończona
Załoga terenowa realizuje zadanie zgodnie z projektem
Planista Sieci
Job Services
Dokumentacja powykonawcza
Dokumenty ekipy terenowej uwzględniające różnice między wykonaniem a projektem
Zespół budowlany
Odbiory
Edytor sprawdza projekt i wykonanie, aby wprowadzić zmiany w Systemie Ewidencji – Enterprise GIS
Operator Sieci
Eksport Modelu
Eksportuje model danych komponentów sieci do innych aplikacji (np. ADMS)
Geodatabase Manager
Zwalnia zadanie z Edytora, aby przesłać wiele zadań jednocześnie do modułu Produkcyjnego. Może automatycznie zamknąć zadanie w Systemie Zarządzania Zadaniami
Edytor GIS
+75% szybsza edycja
>99% dokładności danych
Oszczędność 1h dziennie


ArcFM & ADMS – fundament Cyfrowego Bliźniaka Sieci
Połączone rozwiązania dla przedsiębiorstw z integracją w obiegu zamkniętym i praktycznymi przypadkami użycia
Design
Construction
As-built Editing
Map Correction
Asset Management
Operations & ADMS
ArcFM & Designer
Create and Update As-built & Design
Feeder Service & Network Exporter
Valid CIM export?
ADMS Importer
Valid ADMS import?
ADMS
Create Work Order
Field Client
Perform Work, Note Changes
ADMS
Energize Work
No (update)
Yes
No (update)
Yes
As-built updates are more frequent and less complex while design updates are less frequent but more complex
Notification with changes
2-kierunkowa komunikacja zapewniająca wydajne procesy pracy o najwyższym odzwzorowaniu sieci
Wizualizacja i rozwiązywanie błędów eksportu i importu dzięki ArcFM & ADMS z zastosowaniem wydajnych metod cyfrowej ogranizacji pracy i bez użycia papierowej dokumentacji.
Life Is On
Schneider Electric
Confidential Property of Schneider Electric | Page 18

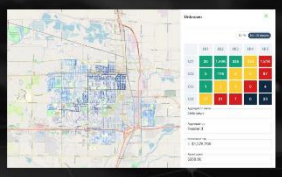

EcoStruxure ADMS
Najlepsze w swojej klasie rozwiązanie do zarządzania siecią ze zrównoważoną infrastrukturą przedsiębiorstwa
Pojedynczy model sieci na wszystkich poziomach napięcia
Ujednolicony, zintegrowany widok
Ponad 50 sprawdzonych aplikacji
Sterowanie w zamkniętej pętli
Operacje i planowanie
Distribution Assets
Transmission
DER & Microgrids
Realtime Communications
EcoStruxure Grid Modular Network Management Solution
SCADA
DMS
OMS
DERMS
EMS
Mobile
Planning
Simulation
GMS
Common Platform
Model
UI
History
Security
Enterprise Integrations
CIS
EAM
GIS
MWM
AMI,MDM
Weather
Aggregator
DRMS
Procesy SDL wg norm IEC 62443 i zasad NERC CIP
Uproszczone wdrażanie, konserwacja i aktualizacje
Zautomatyzowane zarządzanie modelami
Aplikacje mobilne i WWW
Wiodące w branży zarządzenie DER
Wspieranie użytkowników w całym przedsiębiorstwie - operatorów systemów, dyspozytorów, inżynierów sieci, ekip terenowych, przedstawicieli klientów, administratorów IT, użytkowników przedsiębiorstwa.
Life Is On
Schneider Electric
Confidential Property of Schneider Electric | Page 19


Grid Asset Advisor
Ocena stanu i ryzyka aktywów
Life Is On
Schneider Electric
Property of Schneider Electric | Page 20
Public

Wprowadzenie

Funkcjonalności

- zarządzania aktywami dedykowane OSD przez moduły:
  - Asset Performance Management
  - wycena Ryzyka
  - Asset Investment & Maintenance Planning
    (planowanie inwestycji i konserwacji zasobów)
- Elastyczne modele oparte na indeksach CNAIM
- Biblioteki firmy Schneider dla analityki aktywów
- Podejście do monetyzacji ryzyka, które pomaga ustalić priorytety w zakresie konserwacji i inwestycji
- Współpraca z zespołami Schneider Electric d/s Predictive Services
- Uzupełnia istniejące rozwiązania EAM/CMMS



Property of Schneider Electric | Page 21

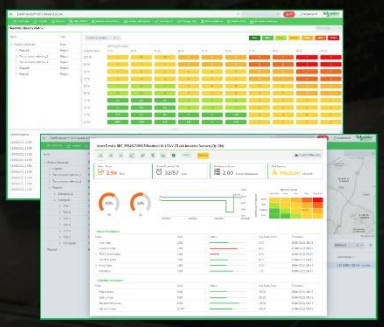
Public

Life Is On Schneider Electric

EcoStruxure Grid Asset Advisor

Ocena stanu i ryzyka aktywów oparte na topologii na potrzeby strategii utrzymania aktywów

- **Zbiera i analizuje dane o zasobach sieci**
- **Dostosowuje ocenę wydajności zasobów sieci**
- **Zaleca i ustala priorytety działań dla aktywów**
- **Łączy dane o aktywach z ludźmi, procesami i systemami**




Asset Health Analysis


Asset Risk Analysis


Future / Predictive Analysis

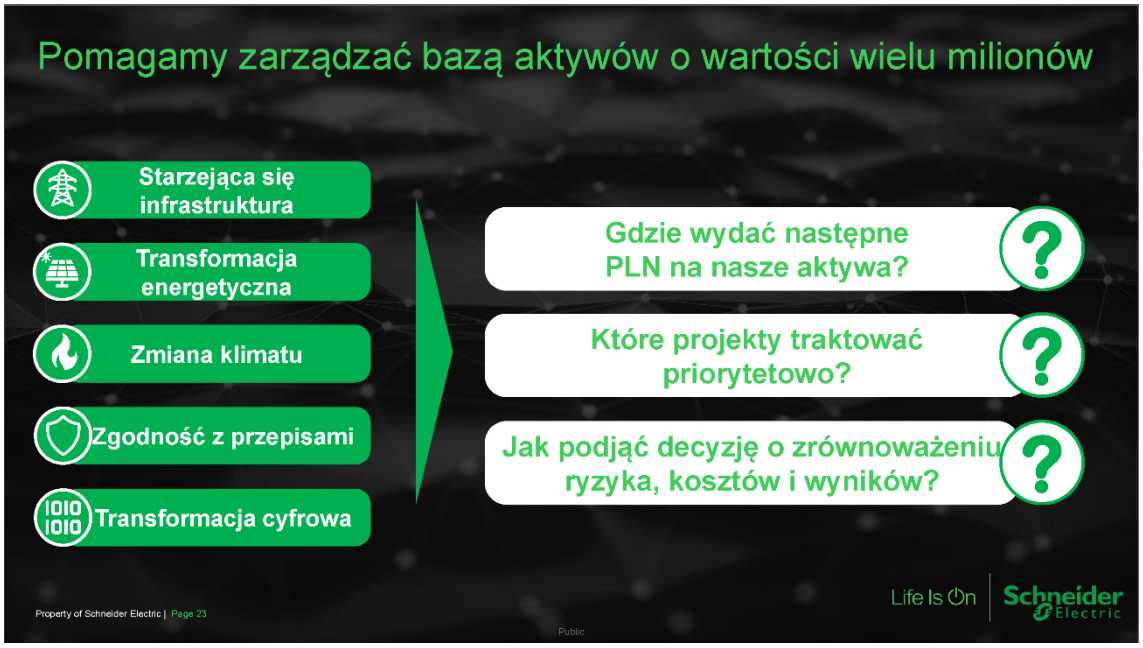

Geo-location of Assets at Risk


Alerts & Notifications

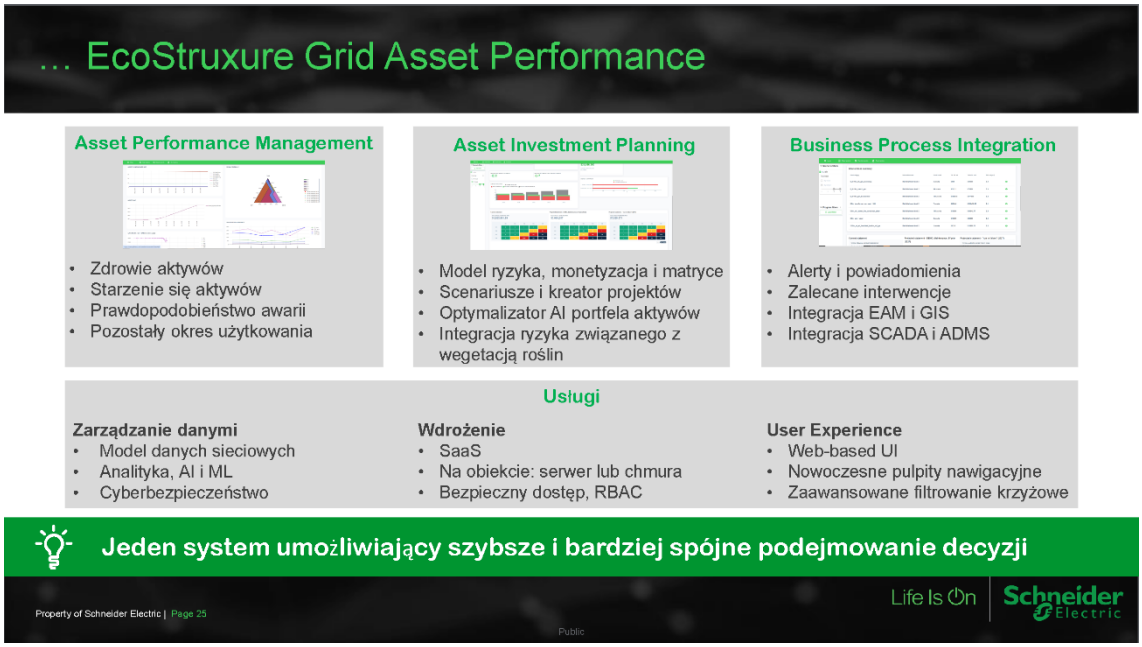

Actions Recommendations

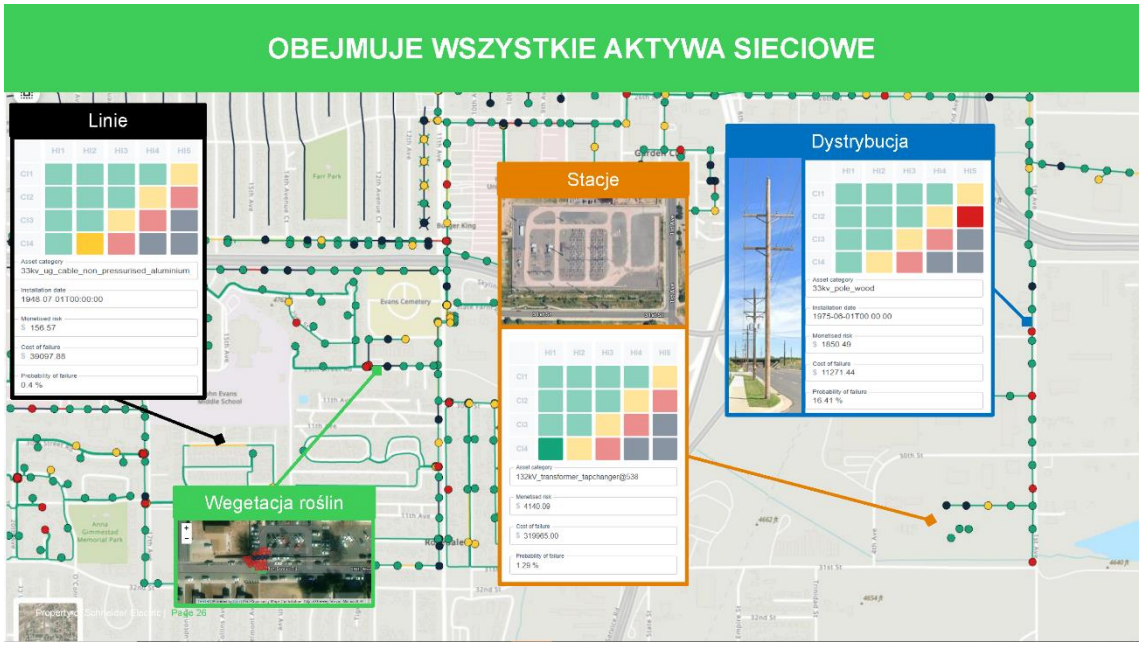
Confidential Property of Schneider Electric | Page 22

Life Is On Schneider Electric


Pomagamy zarządzać bazą aktywów o wartości wielu milionów
Starzejąca się infrastruktura
Transformacja energetyczna
Zmiana klimatu
Zgodność z przepisami
Transformacja cyfrowa
Gdzie wydać następne PLN na nasze aktywa?
Które projekty traktować priorytetowo?
Jak podjąć decyzję o zrównoważeniu ryzyka, kosztów i wyników?
Property of Schneider Electric | Page 23
Public
Life Is On Schneider Electric


… dla lepszej efektywności operacyjnej i odporności sieci…
Wydajność operacyjna
Odporność sieci
Do 20% oszczędności OpEx na kosztach konserwacji
Do 10% odroczonych wydatków kapitałowych utrzymujących
Do 80% redukcji ryzyka awarii aktywów
Do 5% Ulepszenia w SAIDI/SAIFI
Property of Schneider Electric | Page 24
Public
Life Is On Schneider Electric


… EcoStruxure Grid Asset Performance
Asset Performance Management
• Zdrowie aktywów
• Starzenie się aktywów
• Prawdopodobieństwo awarii
• Pozostały okres użytkowania
Asset Investment Planning
• Model ryzyka, monetyzacja i matryce
• Scenariusze i kreator projektów
• Optymalizator AI portfela aktywów
• Integracja ryzyka związanego z wegetacją roślin
Business Process Integration
• Alerty i powiadomienia
• Zalecane interwencje
• Integracja EAM i GIS
• Integracja SCADA i ADMS
Usługi
Zarządzanie danymi
• Model danych sieciowych
• Analityka, AI i ML
• Cyberbezpieczeństwo
Wdrożenie
• SaaS
• Na obiekcie: serwer lub chmura
• Bezpieczny dostęp, RBAC
User Experience
• Web-based UI
• Nowoczesne pulpity nawigacyjne
• Zaawansowane filtrowanie krzyżowe
Jeden system umożliwiający szybsze i bardziej spójne podejmowanie decyzji
Property of Schneider Electric | Page 25
Life Is On Schneider Electric
Public


OBEJMUJE WSZYSTKIE AKTYWA SIECIOWE
Linie
Stacje
Dystrybucja
Wegetacja roślin

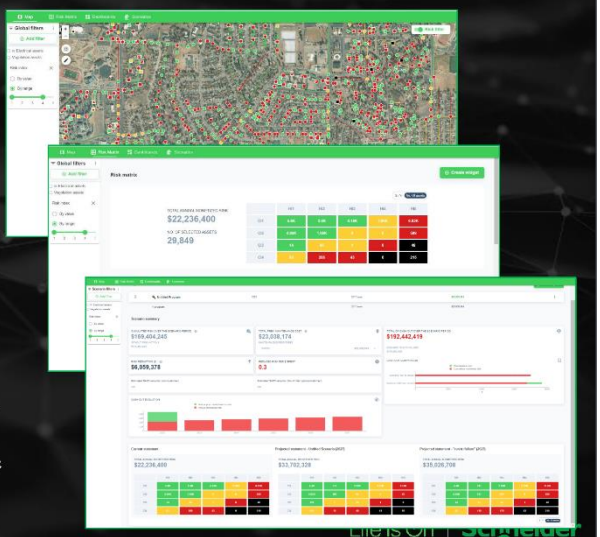
Asset Investment Planning

Optymalizacja planów inwestycyjnych

Profil użytkownika: Manager d/s zasobów sieciowych

Studium przypadku:

- **Ocena ryzyka** i monetyzacja w całym portfolio
- Optymalizacja i **planowanie konserwacji** i wymian w oparciu o ograniczenia budżetowe i zasobowe
- Scenariusze CAPEX/OPEX
- Decyzje dotyczące **okresów taryfowych** i długoterminowych symulacji
- **Uzasadnianie planów inwestycyjnych** interesariuszom: kierownictwu, organowi regulacyjnemu, udziałowcom.
- Wegetacja: integruje ryzyko ponoszone przez roślinność na liniach napowietrznych w celu tworzenia zoptymalizowanych **planów usuwania roślinności**



Page 27

Public

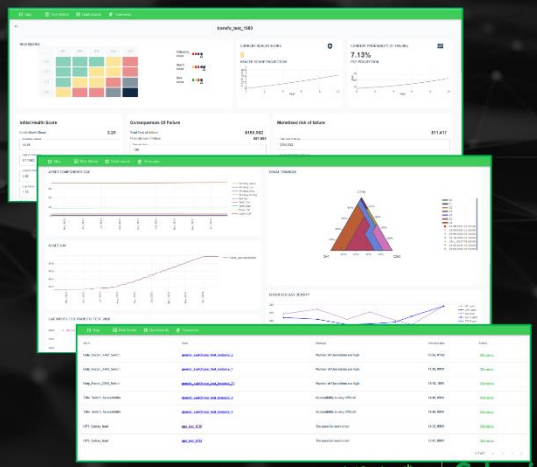
Asset Performance Management & Analytics

Rekomendacje - moduł *Asset Insights & Maintenance*

Profil użytkownika : Zespół Utrzymania

Studium przypadku:

- **Oceń stan aktywów, ich kondycję**, starzenie się i prawdopodobieństwo awarii w czasie
- Wykryj początkowe awarie na wczesnym etapie i unikaj awarii aktywów (**konserwacja proaktywna**)
- **Wyślij alerty** i powiadomienia
- **Identyfikuj** odpowiednie **działania** konserwacyjne



Page 28

Public


Cyberbezpieczeństwo w centrum wszystkiego, co robimy
Cyberbezpieczeństwo jest najwyższym priorytetem
SE 1st to achieve SL4 maturity
TÜV Rhineland (IEC 62443-4-1)
Vulnerability Handling & Disclosure Process
ISO/IEC 30111:2019 & ISO/IEC 29147:2018
Certified Secure Dev Environment
Novi Sad & Seville ISO 27001
Moving NAM DG Infrastructure
SOC 2 Type 2 Compliant Datacenter
TÜVRheinland CERTIFIED
ISO 27001
AICPA SOC
Cloud Security Model
Zero Trust security
Micro segmentation
Privileged access mgmt
Resiliency and scalability
Microsoft Azure
Cybersecurity Services
Security Operations Center (SOC)
System Security Verification Services
Risk Management & Security Consulting
Industry standards alignment
GDPR
IEC
NERC
NIST
Life Is On Schneider Electric
Confidential Property of Schneider Electric | Page 30


Life Is On Schneider Electric

UTRZYMANIE I BEZPIECZEŃSTWO SYSTEMÓW AUTOMATYKI PRZEMYSŁOWEJ A MONITORING ZASOBÓW I REAKCJA NA INCYDENT

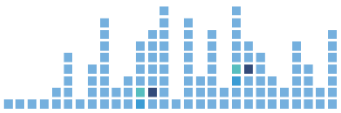
Andrzej Bocheński, Bartosz Piechaczek (Polcom)

Polcom

Czwartek, 7.11.2024, godz. 11:30
Sesja 6 – Cyberbezpieczeństwo (sala 6/1)

Utrzymanie i bezpieczeństwo systemów automatyki przemysłowej a monitoring zasobów i reakcja na incydent

Andrzej Bocheński, Dyrektor Techniczny Data Center, Polcom
Bartosz Piechaczek, Ekspert ds. Cyberbezpieczeństwa, Polcom

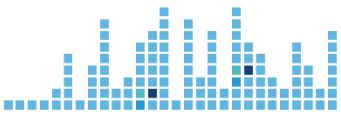


Polcom

2

Data Center III generacji - Polcom IIMS

Intelligent Infrastructure Management System



Polcom

3

Data Center III generacji

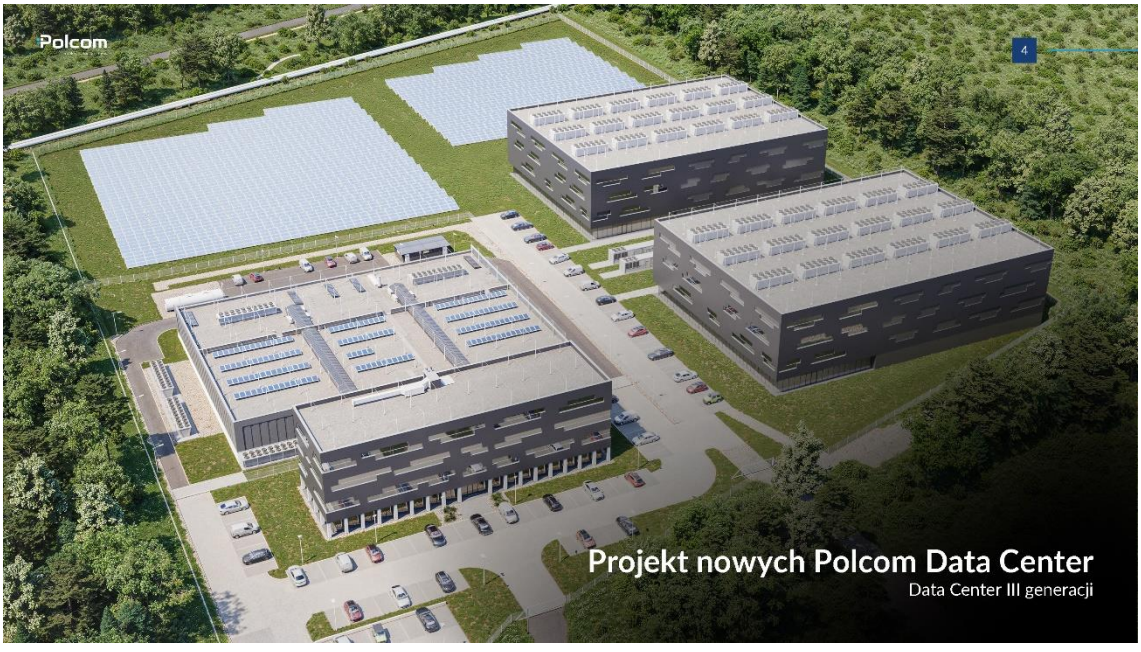
Intelligent Infrastructure Management System

15 lat doświadczenia na rynku Data Center

Bezpieczeństwo

Wydajność

Elastyczność



Polcom

5

Data Center III generacji

Zaprojektowanie szeregu tak rozbudowanych instalacji wymagało nowego podejścia do każdej gałęzi technologicznej i zadbania o odpowiednie parametry całej infrastruktury.

- Realizacja dwóch serweroni
- 20 000 m2 powierzchni
- 44 MW mocy przyłączeniowej
- 12 komór serwerowych
- Wydzielone strefy chłodu

Polcom

6

Systemy energetyczne w DC

Data Center III generacji

III generacja Data Center to rozwiązania wysokiej gęstości obciążenia energetycznego. Nowe ośrodki zaprojektowaliśmy tak, aby zapewnić platformę sprzętową dla naszych klientów w każdym aspekcie ich działania.

- 100 KW per szafa rack
- 2,4 MW per komora serwerowa
- 22 MW globalna moc 1 obiektu

Polcom

7

Autorskie rozwiązanie chłodzenia

Data Center III generacji

Wierzymy, że systemy obliczeniowe, w tym te związane z AI, będą ciągle i dynamicznie się rozwijać. Dlatego dostosowujemy nasze rozwiązania, aby zapewniać większą elastyczność, bezpieczeństwo i możliwości rozwoju nowych projektów, bez kompromisów w dotychczasowym poziomie bezpieczeństwa.

- 8 MW energii cieplnej
- Water cooling
- Hybrid Air cooling
- Systemy detekcji dymu i gaszenia


Polcom
9
Przemysł 4.0, 5.0 i pochodne technologie
Korzyści
Rozwiązania oparte na chmurze hybrydowej, konteneryzacji i wirtualizacji stają się standardem, umożliwiając szybkie dostosowanie infrastruktury do bieżących potrzeb.
Systemy IoT
Przemysł 4.0 i 5.0
Cloud, konteneryzacja i wirtualizacja
Optymalizacja wydajności


Polcom
10
POLCOM IIMS
Intelligent Infrastructure Management System
Polcom IIMS to więcej niż tylko zbiór narzędzi technologicznych — to oprogramowanie zapewniające najwyższy poziom bezpieczeństwa i efektywności operacyjnej.
3 lata prac rozwojowych
Magistrala DataLinkPLC
Analiza zgłoszonych ticketów
Analityka predykcyjna

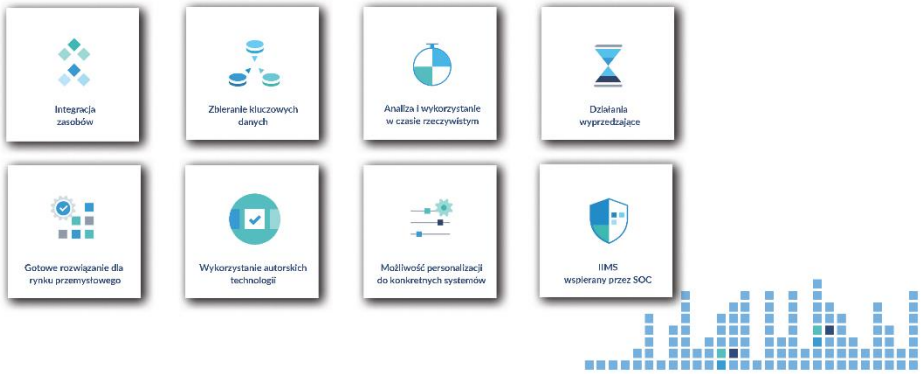
Polcom

11

Polcom IIMS

Intelligent Infrastructure Management System

Polcom IIMS to rozwiązanie gotowe do wdrożenia w systemach przemysłowych jako rozwiązanie kompletne i kompleksowe z możliwością personalizacji i rozwoju konkretnego systemu.

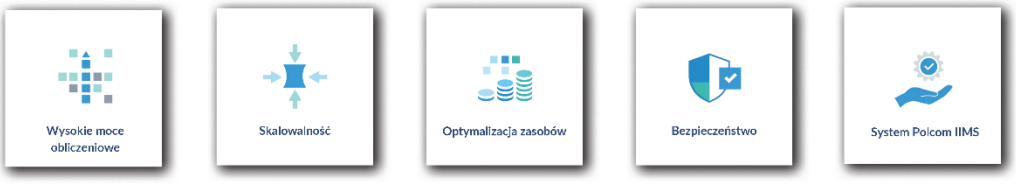


Polcom

12

Data Center III generacji

Data Center III generacji w połączeniu z naszym systemem IIMS, który oferuje integrację, optymalizację i efektywność w zarządzaniu, jesteśmy gotowi sprostać wyzwaniom przyszłości.

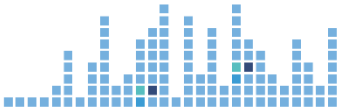


Polcom

13

Security Operations Center

Skuteczna reakcja na incydent bezpieczeństwa



Polcom

14

Security Operations Center

Wykorzystanie usługi Security Operations Center w firmie zwiększa efektywność procesu zarządzania bezpieczeństwem oraz ułatwia spełnienie wymagań prawa i standardów bezpieczeństwa m.in. KNF, PCI-DSS, RODO i ustawy o cyberbezpieczeństwie.

Usługa Polcom SOC składa się z dwóch warstw:

Polcom SOC

Polcom SIEM

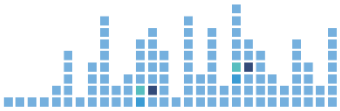
Polcom

15

Proces wdrożenia usługi SOC

Proces wdrożenia usługi SOC, dzielimy na 5 kluczowych etapów:

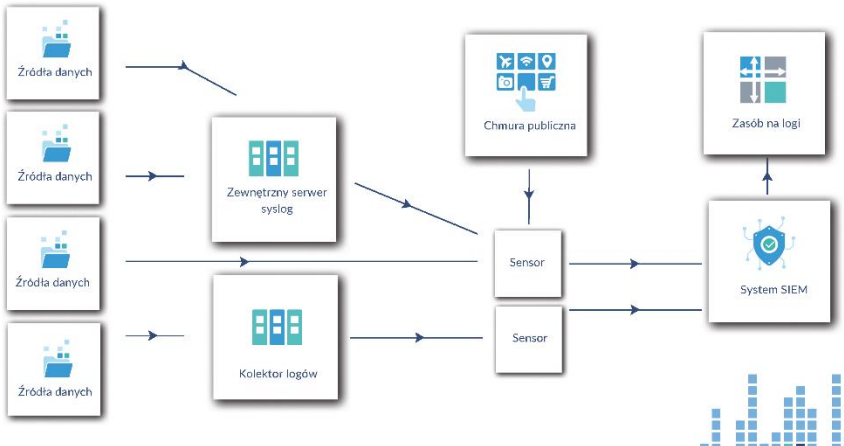
I	II	III	IV	V
Określenie planu działania	Infrastruktura	Analiza zebranych danych	Przygotowanie scenariuszy szybkiej reakcji	Utrzymanie i monitoring infrastruktury



Polcom

16

Architektura usługi SOC



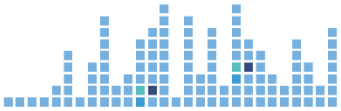
Polcom

17

Zapraszamy do kontaktu!

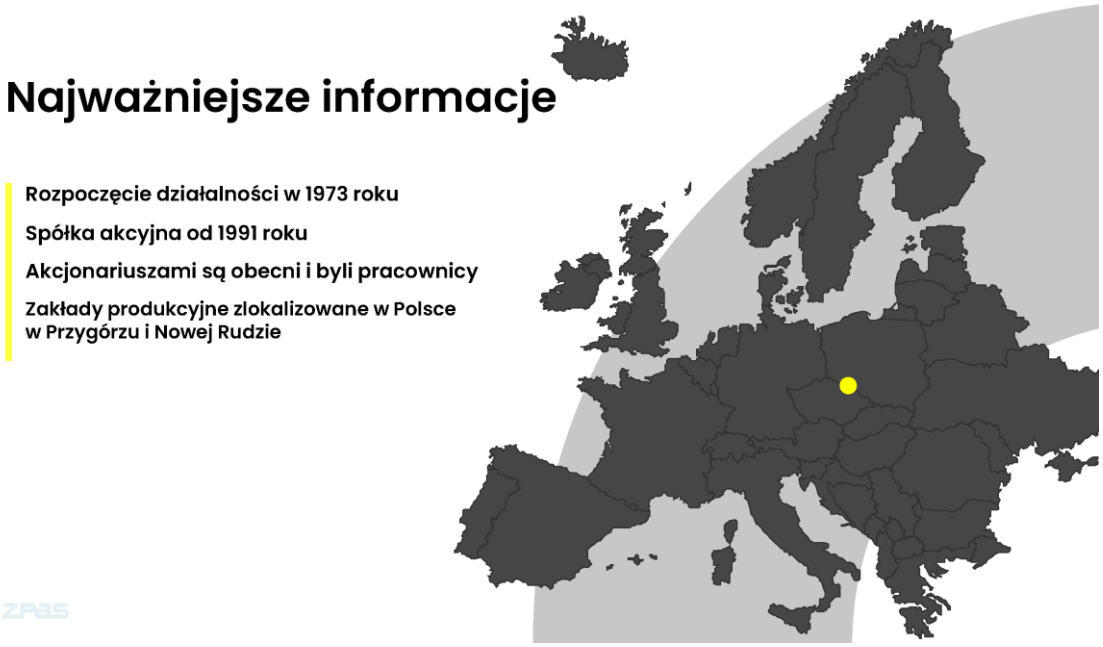
Dziękujemy za uwagę

Andrzej Bocheński, Dyrektor Techniczny Data Center, Polcom
Bartosz Piechaczek, Ekspert ds. Cyberbezpieczeństwa, Polcom



INWERTEROWE POMPY CIEPŁA W SŁUŻBIE ZAPEWNIENIA WARUNKÓW KLIMATYCZNYCH W SZAFACH DOSTĘPOWYCH I KONTENERACH ENERGETYCZNYCH

Andrzej Kupiec (ZPAS)



Struktura zatrudnienia, grudzień 2023

671 wszystkich pracowników
315 pracowników produkcyjnych
61 pracowników w działach kontroli jakości
80 inżynierów ze specjalizacjami:
- 44 – konstruktorów mechaników
- 27 – inżynierów elektryków
- 9 – osób w dziale badań i rozwoju

Dział techniczny projektuje na podstawie dokumentacji dostarczonej przez klienta lub zapewnia samodzielne projektowanie w zakresie mechaniki, elektryki i automatyki.
Dodatkowo w 2022: 71 pracowników (przeszkolonych i z aktualnym pozwoleniem na pracę) z agencji pracy tymczasowej lub na podstawie umowy zlecenia.

ZPAS 3

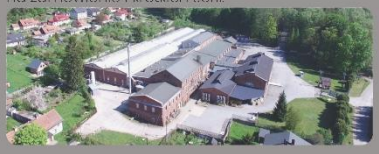
Eksport do 37 państw świata

Austria
Azerbejdżan
Belgia
Bułgaria
Chorwacja
Czechy
Dania
Estonia
Finlandia
Francja
Gruzja
Hiszpania
Holandia
Irlandia
Islandia
Izrael
Kanada
Litwa
Łotwa
Malta
Mołdawia
Niemcy
Norwegia
Rumunia
Singapur
Słowacja
Szwajcaria
Szwecja
Ukraina
USA
Węgry
Wielka Brytania
Wielka Brytania
Włochy

ZPAS 4

Zakłady produkcyjne (powierzchnia ok. 36 000 m²)

Przygórze – 14 000 m²
Siedziba główna, administracja, produkcja wyrobów na zamówienie i krótkich serii.



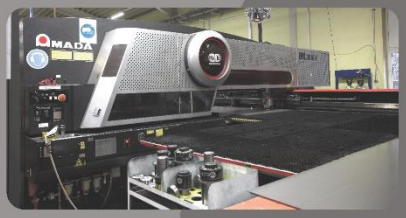
Nowa Ruda, Słupiec – 10 000 m²
Zakład specjalizujący się w produkcji wyrobów seryjnych, magazyn wyrobów gotowych

Nowa Ruda, Górnicza – 3 500 m²
Zakład specjalizujący się w produkcji szaf zewnętrznych.

Nowa Ruda, Piłsudskiego – 9 000 m²
Zakład specjalizujący się w montażu elektrycznym i FAT.

ZPAS 5

Zdolności produkcyjne



ZPAS

Produkty i rozwiązania

Teleinformatyka i IT
Szafy serwerowe, serwerownie, kontenerowe data center

Tekomunikacja
Szafy zewnętrzne, szafy IT, systemy klimatyzacji dla szaf zewnętrznych

Energetyka
Szafy systemowe, pulpity dyspozytorskie

Automatyka i sterowanie
Szafy sterownicze i automatyki, prefabrykacja szaf

Sektor publiczny i ITS
Infokioski, totemy, informacja pasażerska, pulpity dyspozytorskie

Odnawialne Źródła Energii
Magazyny energii

Kompleksowe realizacje obiektowe

ZPAS 7

Produkty i rozwiązania

Teleinformatyka i IT
Szafy serwerowe, serwerownie, kontenerowe data center

ZPAS 8


Produkty i rozwiązania
Teleinformatyka i IT
Szafy serwerowe, serwerownie, kontenerowe data center
ZPAS

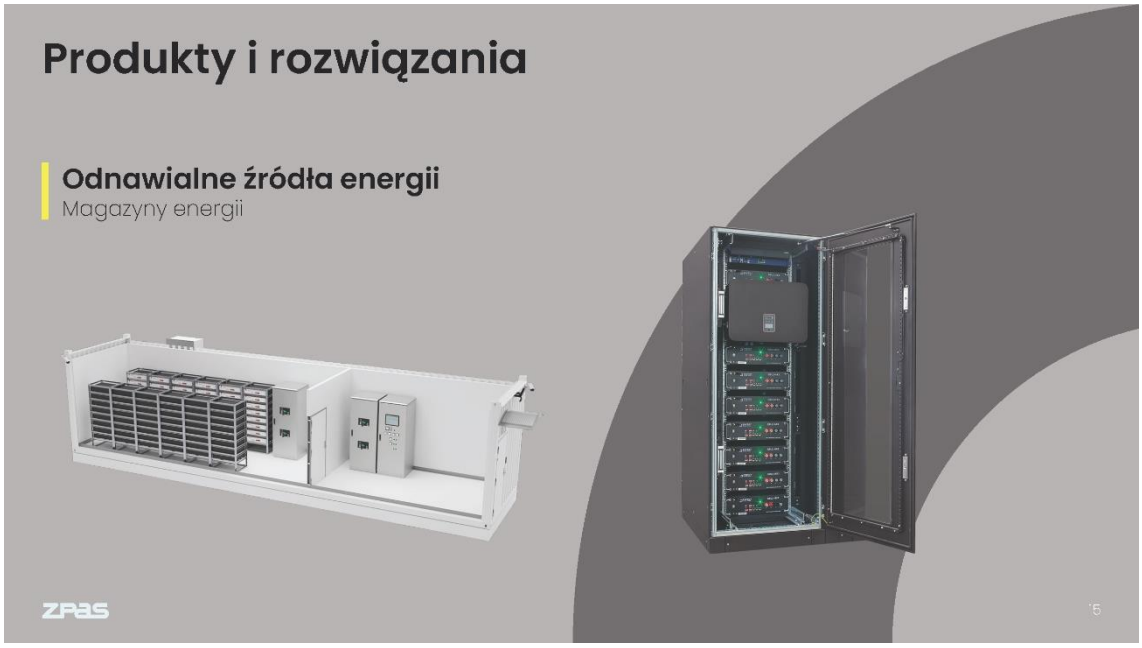

Produkty i rozwiązania
Telekomunikacja
Szafy zewnętrzne, szafy IT, systemy klimatyzacji szaf zewnętrznych
ZPAS


Produkty i rozwiązania
Energetyka
Szafy systemowe, pulpity sterownicze
ZPAS
11

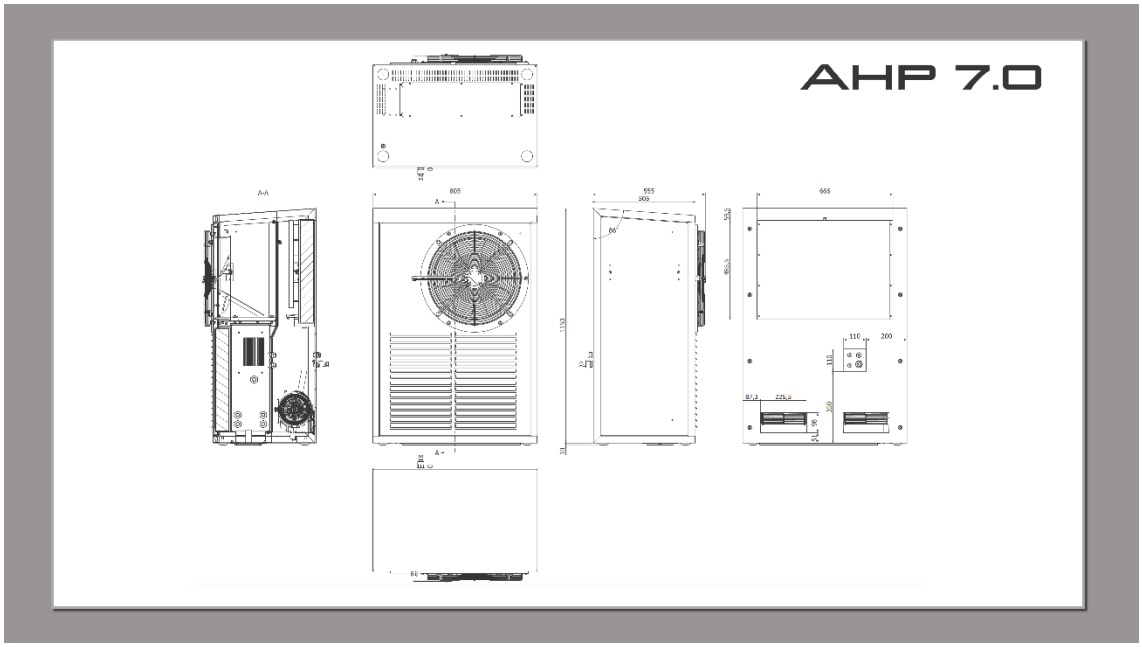

Produkty i rozwiązania
Automatyka
Szafy sterownicze i automatyki, prefabrykacja szaf
ZPAS
12


Produkty i rozwiązania
Sektor publiczny, ITS
Infokioski, totemy, informacja pasażerska, pulpity
ZPAS
13

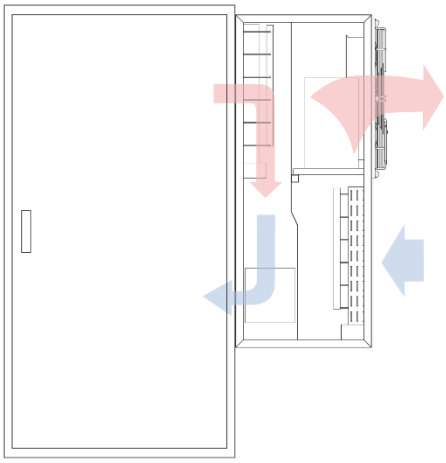

Produkty i rozwiązania
Wykonawstwo od projektu do realizacji na obiektach
ZPAS
14


Produkty i rozwiązania
Odnawialne źródła energii
Magazyny energii
ZPAS


AHP 7.0


AHP 7.0

Obieg chłodzenia szafy

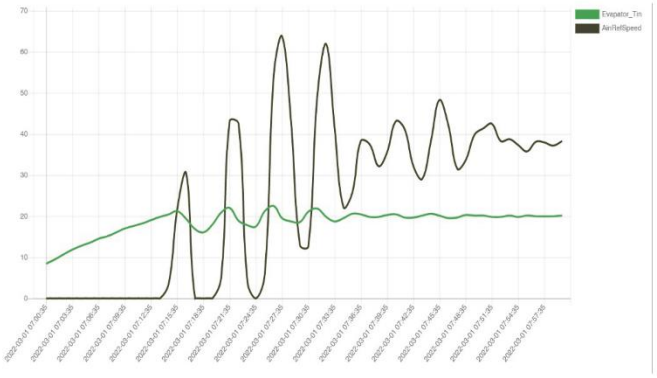


Dane techniczne

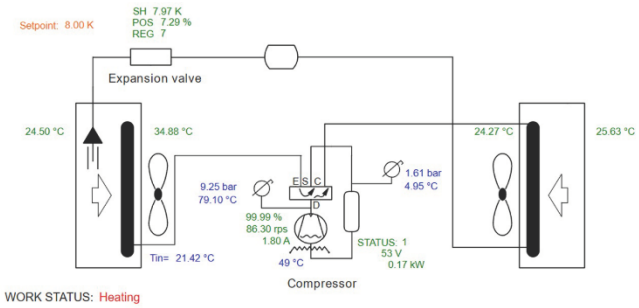
Wydajność chłodnicza A35A35	7 kW
Wydajność chłodnicza A35A50	6,5 kW
Zasilanie	230 V, 50 Hz
Maksymalny pobór prądu	14 A
Pobór mocy A35A35	3,5 kW
Czas pracy	24/7
Ilość czynnika R134	2,75 kg
Maksymalne ciśnienie	23 bar
Zewnętrzny wentylator	1200 m^3/h
Wewnętrzny wentylator	1200 m^3/h
Maksymalna głośność urządzenia	59 dB
Kolor	RAL 7035
Temperatura pracy	od -15 do +50 °C
Zakres temperatury zadanej	od +5 do +50 °C
Waga	90 kg
Stopień ochrony wg EN 60529	IP 21/55
Komunikacja	Ethernet (local) RJ45
Obsługiwane protokoły	HTTP, FTP, SNMP

Sterownik może być odpytywane za pomocą protokołu SNMP. Może także wysyłać komunikaty TRAP.

Sterowanie inwerterowe

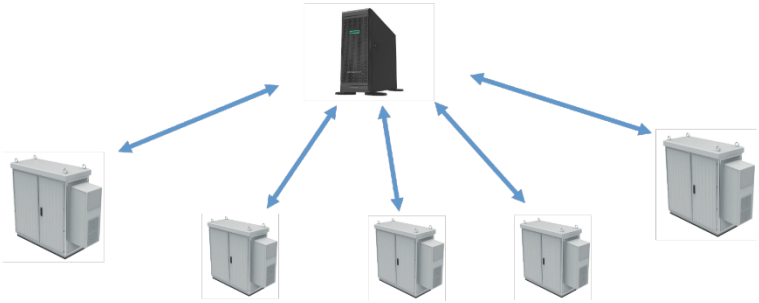


Sprężarka inwerterowa pozwala dostosować moc chłodniczą i grzewczą pompy do chwilowego zapotrzebowania. Zmniejsza ilość załączeń urządzenia i pozwala zaoszczędzić na energii rozruchowej (niższe prądy rozruchowe i mniejsze obciążenie sieci elektroenergetycznej). Urządzenie łatwo dostosowuje się do zmiennych warunków wewnętrznych i na zewnętrznych.



- płynne sterowanie pracą sprężarki
- elektroniczny zawór rozprężny
- regulacja obrotów wentylatorów
- algorytm sterowania PID

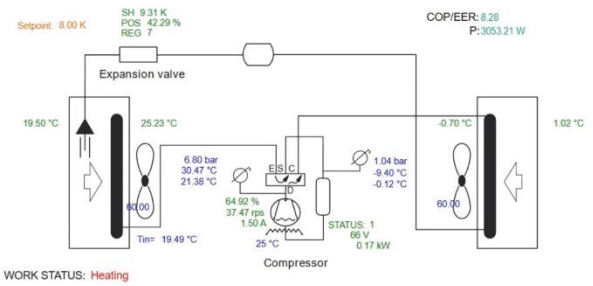
= niezawodność + niskie koszty eksploatacji



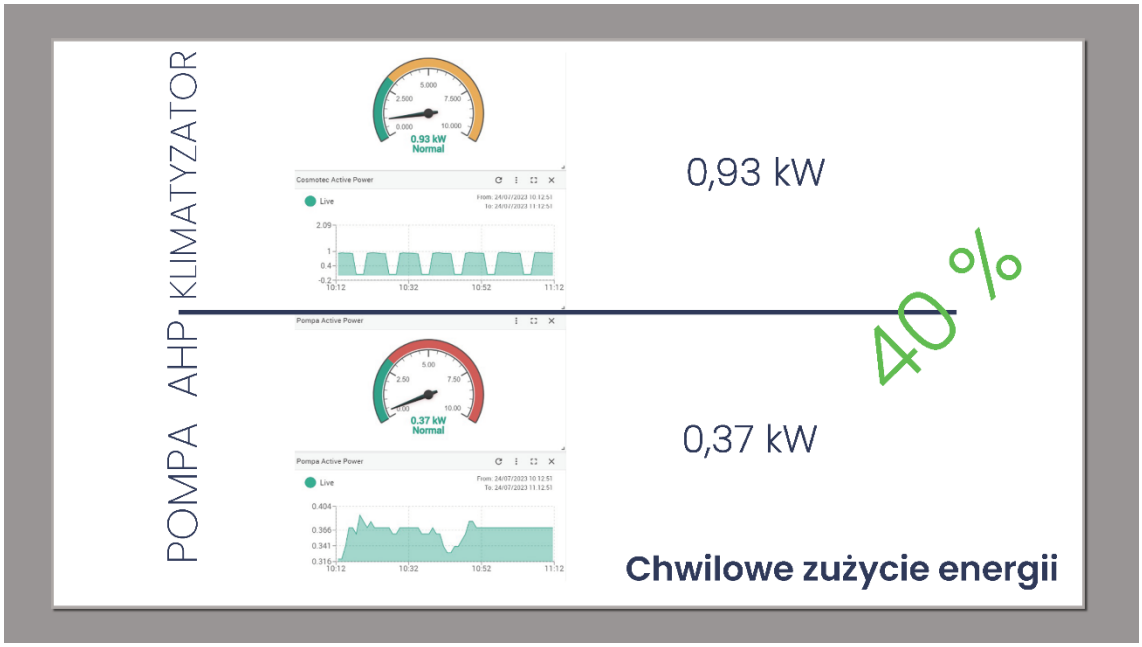
Pompa ciepła AHP 2.0 może stanowić element systemu nadzoru nad bezpieczeństwem infrastruktury sieciowej.

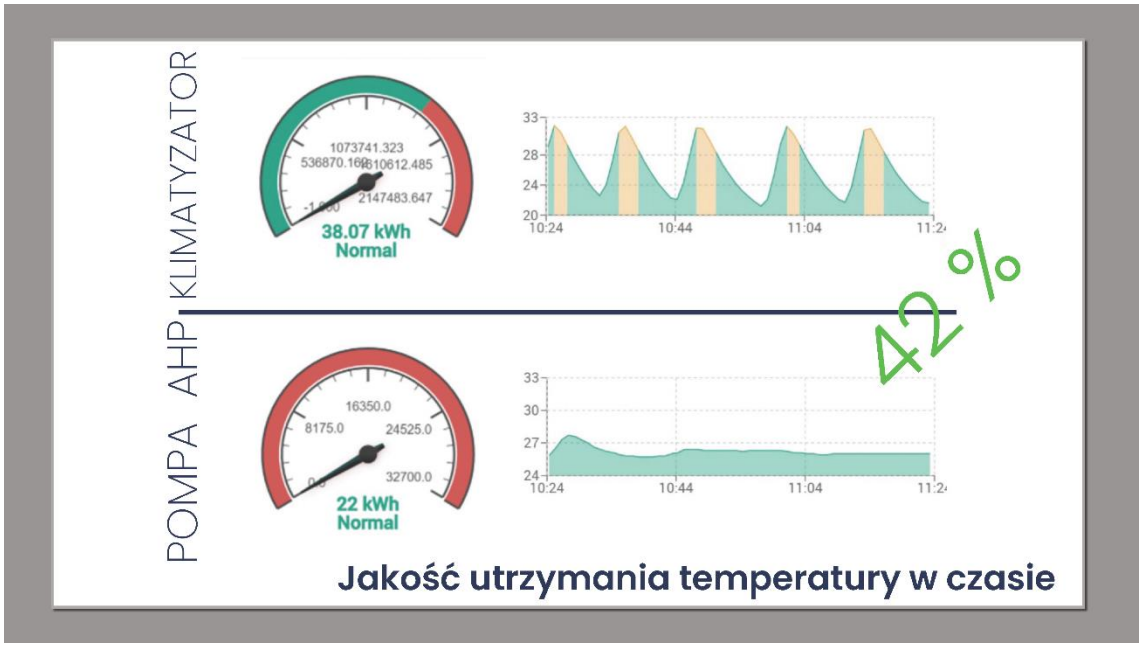
Sterownik urządzenia prowadzi ciągłą rejestracje najważniejszych parametrów i umożliwia ich przeglądanie za pomocą dowolnej przeglądarki internetowej. Pomiar zapisywany jest co 1 minutę w nieulotnej pamięci sterownika.

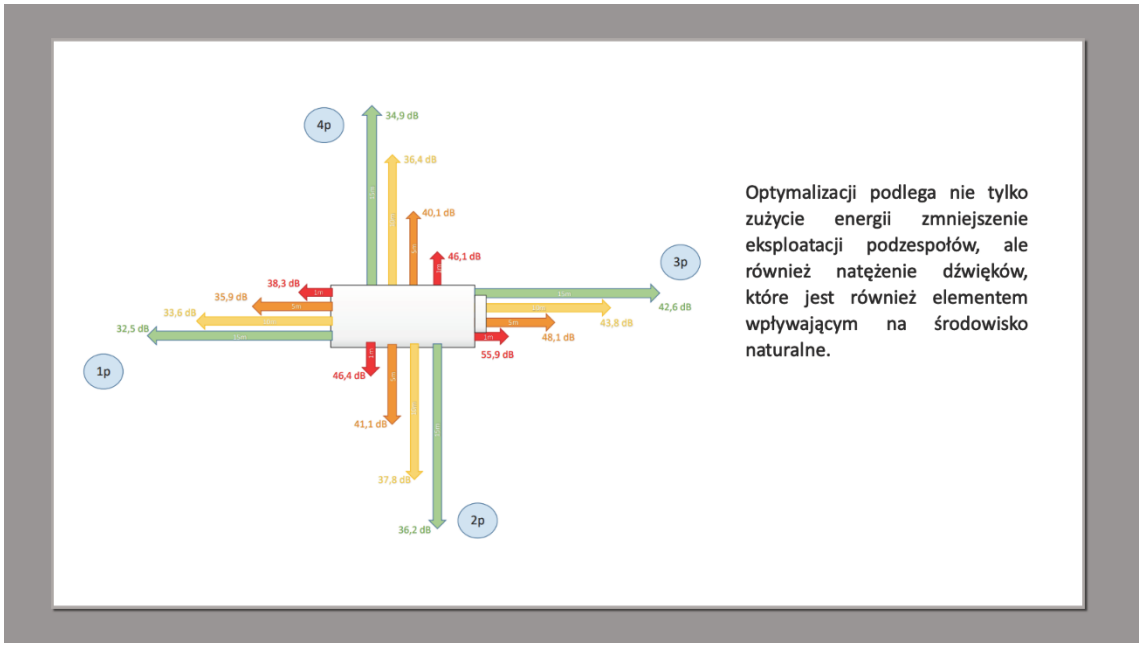
Wizualizacja do monitorowania pracy urządzenia podaje bieżące pomiary i wyliczenia. Między innym wyliczany jest współczynnik COP i EER. Podawana moc jest wyliczana na podstawie pomiarów temperatur i przepływu powietrza przez wymiennik wewnętrzny




POMPA AHP KLIMATYZATOR
Cosmotec Active Power
0.93 kW
Normal
Cosmotec Current
4.8 A
Normal
Cosmotec Total Active Energy
38.07 kWh
Normal
Pompa Active Power
0.37 kW
Normal
Pompa Current
1.88 A
Normal
Pompa Total Active Energy
22 kWh
Normal


POMPA AHP KLIMATYZATOR
0,93 kW
40 %
0,37 kW
Chwilowe zużycie energii


POMPA AHP
KLIMATYZATOR
1073741.323
536870.166
810612.485
2147483.647
38.07 kWh
Normal
33
28
24
20
10:24
10:44
11:04
42 %
16350.0
8175.0
24525.0
32700.0
22 kWh
Normal
33
30
27
24
10:24
10:44
11:04
Jakość utrzymania temperatury w czasie

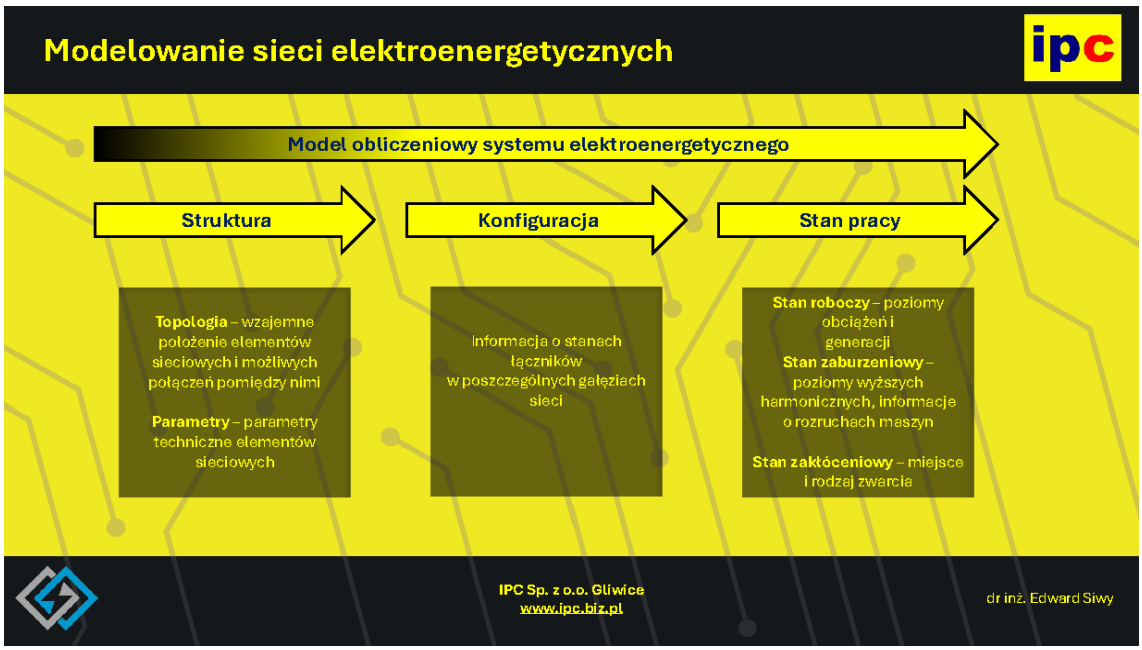

4p
34,9 dB
36,4 dB
40,1 dB
46,1 dB
3p
38,3 dB
35,9 dB
33,6 dB
32,5 dB
42,6 dB
43,8 dB
48,1 dB
55,9 dB
1p
46,4 dB
41,1 dB
37,8 dB
36,2 dB
2p
Optymalizacji podlega nie tylko zużycie energii zmniejszenie eksploatacji podzespołów, ale również natężenie dźwięków, które jest również elementem wpływającym na środowisko naturalne.

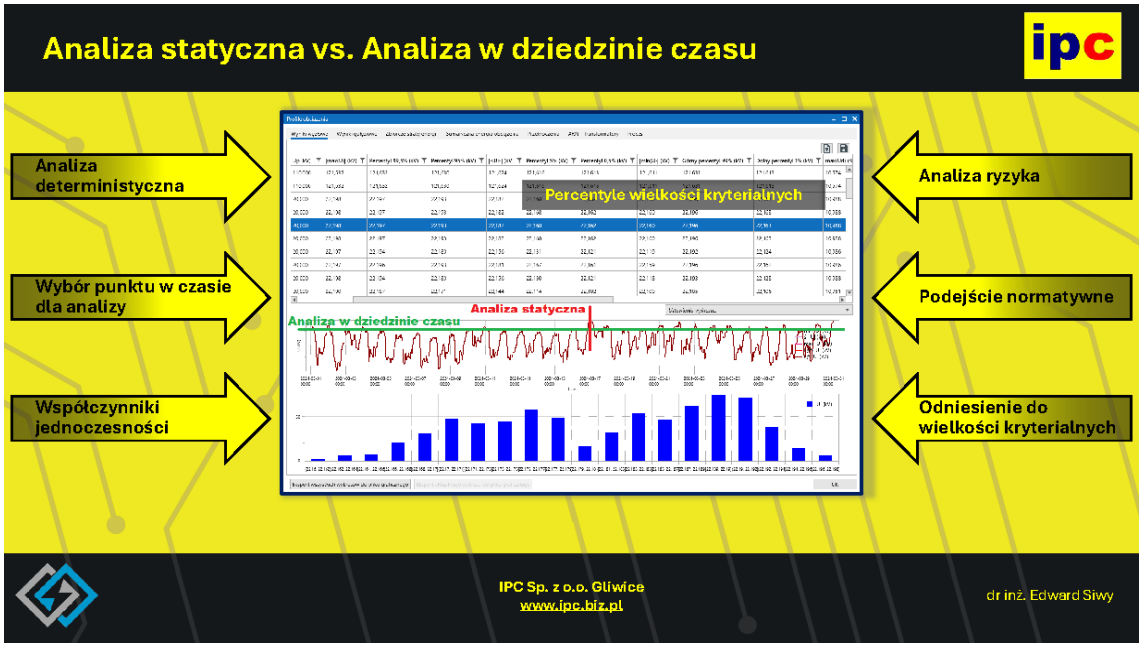

obniżenie hałasu o 5 dB


WWW.ZPAS.PL
ZPAS

WYKORZYSTANIE OBLICZEŃ GRAFIKOWYCH W OPROGRAMOWANIU OES OBLICZENIA SIECIOWE DO WYKONYWANIA EKSPERTYZ PRZYŁĄCZENIOWYCH NA PRZYKŁADZIE WDROŻENIA W TAURON DYSTRYBUCJA S.A.

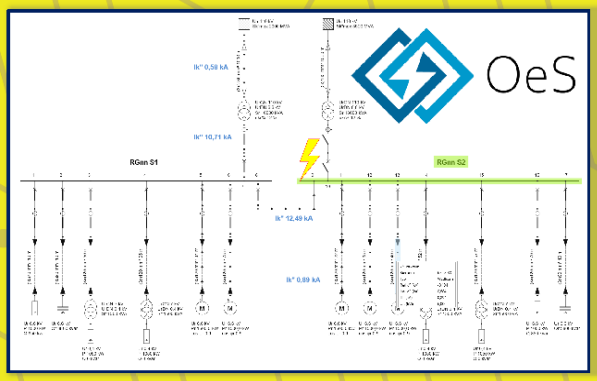
Edward Siwy (IPC Sp. z o.o.)


Modelowanie sieci elektroenergetycznych
ipc
Model obliczeniowy systemu elektroenergetycznego
Struktura
Konfiguracja
Stan pracy
Topologia – wzajemne położenie elementów sieciowych i możliwych połączeń pomiędzy nimi
Parametry – parametry techniczne elementów sieciowych
Informacja o stanach łączników w poszczególnych gałęziach sieci
Stan roboczy – poziomy obciążeń i generacji
Stan zaburzeniowy – poziomy wyższych harmonicznych, informacje o rozruchach maszyn
Stan zakłóceniowy – miejsce i rodzaj zwarcia
IPC Sp. z o.o. Gliwice
www.ipc.biz.pl
dr inż. Edward Siwy


Analiza statyczna vs. Analiza w dziedzinie czasu
ipc
Analiza deterministyczna
Wybór punktu w czasie dla analizy
Współczynniki jednoczesności
Analiza ryzyka
Podejście normatywne
Odniesienie do wielkości kryterialnych
Percentyle wielkości kryterialnych
Analiza statyczna
Analiza w dziedzinie czasu
IPC Sp. z o.o. Gliwice
www.ipc.biz.pl
dr inż. Edward Siwy

Smart-OeS – podstawowe funkcjonalności

- Digitalizacja modelu sieci
- Obliczenia rozpływowe
- Obliczenia zwarciowe
- Analiza pracy zabezpieczeń
- Obciążalność torów prądowych



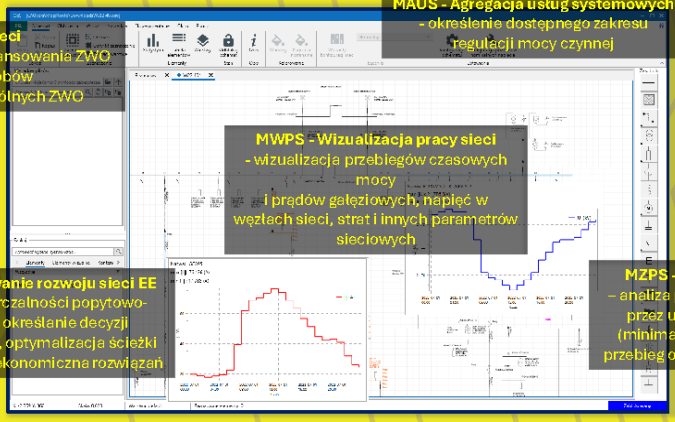
IPC Sp. z o.o. Gliwice
www.ipc.biz.pl

dr inż. Edward Siwy

Smart-OeS – obliczenia grafikowe

MBIL - Bilansowanie sieci
- analiza możliwości bilansowania ZWO przy uwzględnieniu zasobów regulacyjnych poszczególnych ZWO

MAUS - Agregacja usług systemowych
- określenie dostępnego zakresu regulacji mocy czynnej



MWPS - Wizualizacja pracy sieci
- wizualizacja przebiegów czasowych mocy i prądów gałęziowych, napięć w węzłach sieci, strat i innych parametrów sieciowych

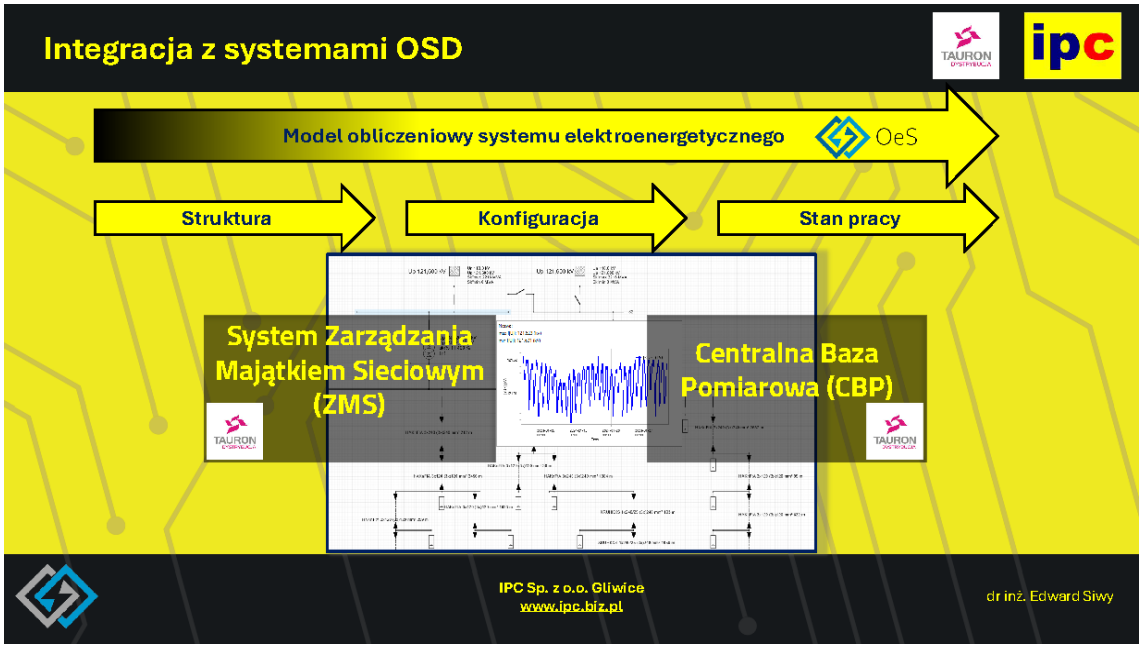
MPRS - Planowanie rozwoju sieci EE
- ocena wystarczalności popytowo-podażowej, określanie decyzji inwestycyjnych, optymalizacja ścieżki rozwoju, ocena ekonomiczna rozwiązań

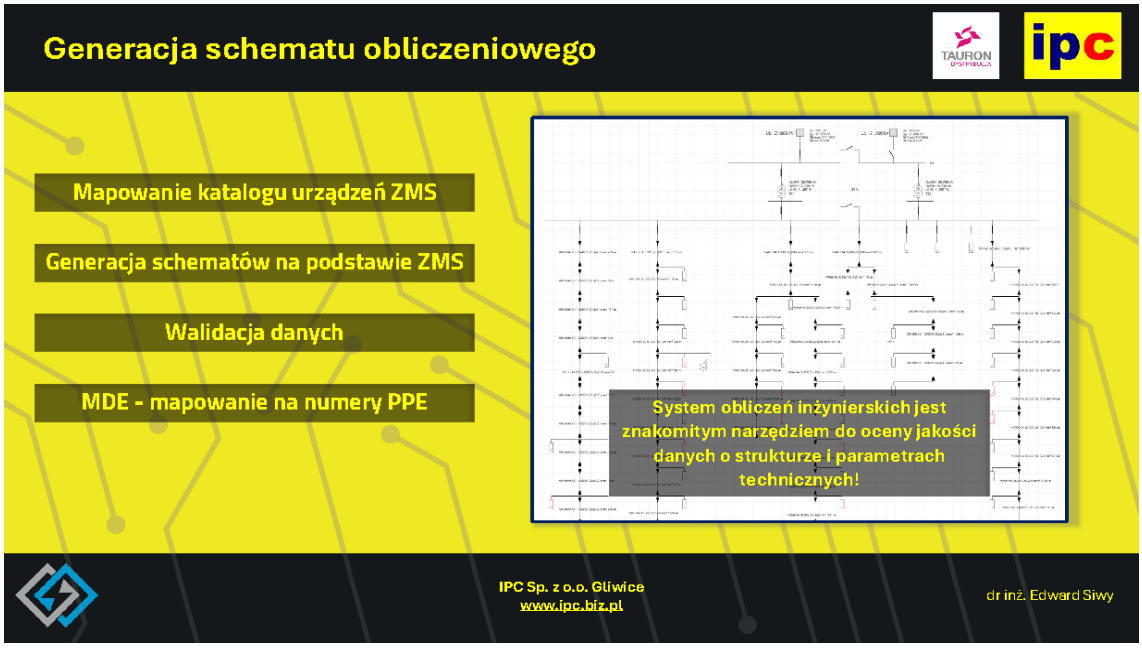
MZPS - Zarządzanie pracą sieci
– analiza pracy sieci przy zadawanym przez użytkownika celu regulacji (minimalizacja ograniczeń, zadany przebieg obciążenia w wybranej gałęzi)

Narodowe Centrum Badań i Rozwoju
POIR.01.01.01-00-0972/18

IPC Sp. z o.o. Gliwice
www.ipc.biz.pl

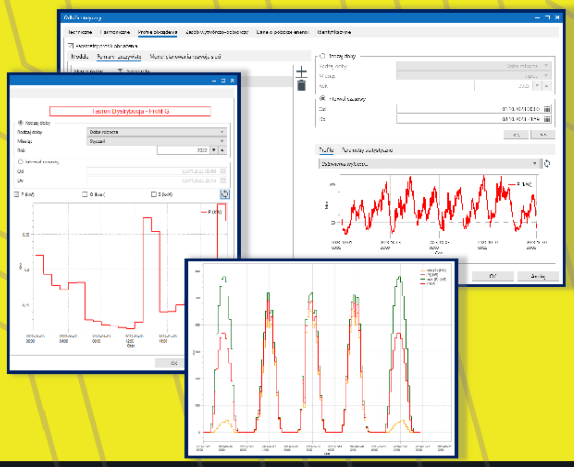
dr inż. Edward Siwy


Integracja z systemami OSD
Model obliczeniowy systemu elektroenergetycznego
OeS
Struktura
Konfiguracja
Stan pracy
System Zarządzania Majątkiem Sieciowym (ZMS)
Centralna Baza Pomiarowa (CBP)
IPC Sp. z o.o. Gliwice
www.ipc.biz.pl
dr inż. Edward Siwy


Generacja schematu obliczeniowego
Mapowanie katalogu urządzeń ZMS
Generacja schematów na podstawie ZMS
Walidacja danych
MDE - mapowanie na numery PPE
System obliczeń inżynierskich jest znakomitym narzędziem do oceny jakości danych o strukturze i parametrach technicznych!
IPC Sp. z o.o. Gliwice
www.ipc.biz.pl
dr inż. Edward Siwy

Modelowanie w dziedzinie czasu

- Wczytanie danych z CBP
- Identyfikacja brakujących danych
- Taryfy dla odbiorców końcowych
- Modele ENTSO dla farm wiatrowych
- Modele ENTSO dla farm fotowoltaicznych
- Modele biogazowni z magazynem
- Modele magazynu grafikowanego



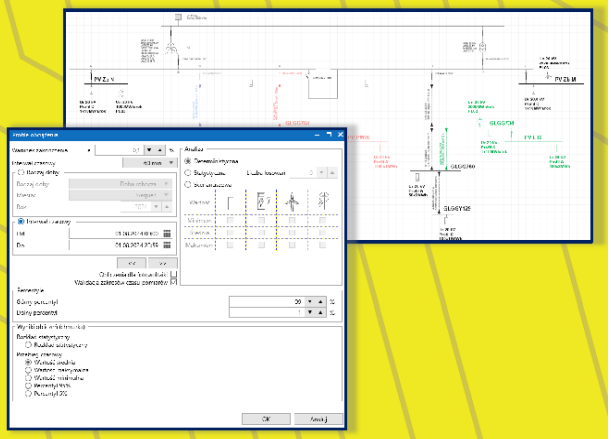
IPC Sp. z o.o. Gliwice
www.ipc.biz.pl

dr inż. Edward Siwy

Smart-OeS – metody obliczeniowe

Metody wykonywania analiz:

- **deterministyczne** – gdzie wykorzystywana jest wyłącznie wartość oczekiwana procesu losowego EX(k) – pojedynczy grafik, dla każdego obiektu w sieci,
- **stochastyczne** (metoda Monte Carlo) – są to analizy wielowariantowe, przy czym wykorzystywane są przebiegi losowe przy wykorzystaniu odpowiednio parametryzowanych generatorów liczb pseudolosowych,
- **scenariuszowe** – są to analizy wielowariantowe, użytkownik definiuje scenariusze wybierając, dla których rodzajów obiektów ma być wykorzystywana wartość oczekiwana, maksymalna lub minimalna.



IPC Sp. z o.o. Gliwice
www.ipc.biz.pl

dr inż. Edward Siwy

Przykład ekspertyzy przyłączeniowej

Analiza statystyczna danych wejściowych

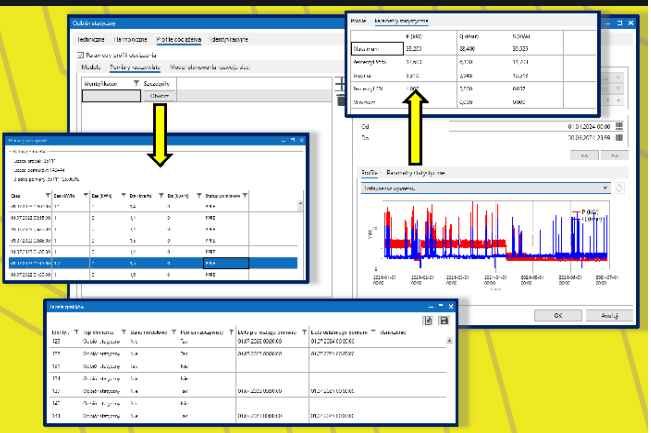
Weryfikacja kompletności modelu

Parametryzacja i wykonanie obliczeń

...

Mechanizmy wsparcia dla wykonywania ekspertyz:

- walidacja danych
- analiza na podstawie schematu i tabeli elementów
- wykorzystanie technologii warstw
- warianty konfiguracji sieci
- parametryzacja danych do obliczeń



IPC Sp. z o.o. Gliwice
www.ipc.biz.pl

dr inż. Edward Siwy

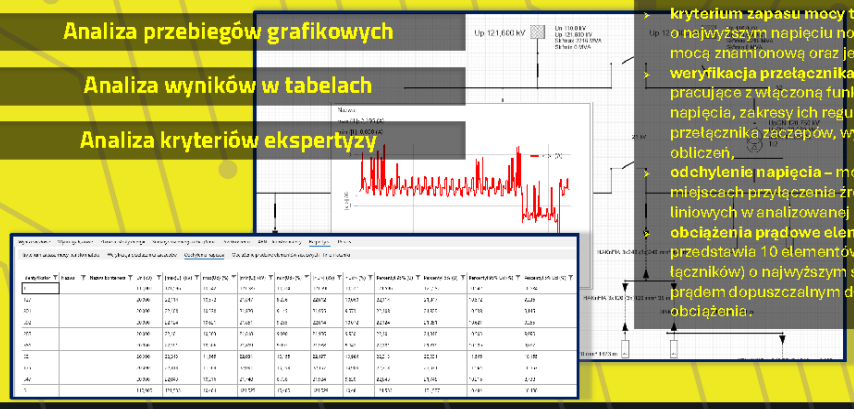
Przykład ekspertyzy przyłączeniowej

...

Analiza przebiegów grafikowych

Analiza wyników w tabelach

Analiza kryteriów ekspertyzy



Prezentacja wyników obliczeń na potrzeby ekspertyzy przyłączeniowej:

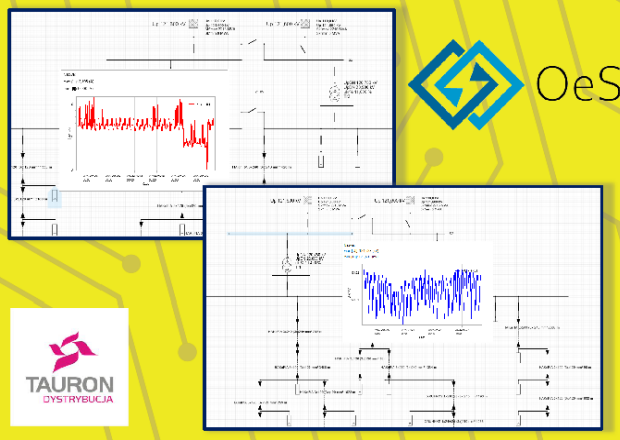
- **kryterium zapasu mocy transformatora** – transformatory o najwyższym napięciu nominalnym górnym wraz z jego mocą znamionową oraz jego obciążeniem,
- **weryfikacja przełącznika zaczepów** – transformatory pracujące z włączoną funkcją automatycznej regulacji napięcia, zakresy ich regulacji oraz ekstremalne stany przełącznika zaczepów, wynikające z przeprowadzonych obliczeń,
- **odchylenie napięcia** – moduły oraz odchylenia napięcia w miejscach przyłączenia źródeł i na końcach ciągów liniowych w analizowanej sieci,
- **obciążenia prądowe elementów sieciowych** – przedstawia 10 elementów (linii elektroenergetycznych lub łączników) o najwyższym stopniu obciążenia wraz z ich prądem dopuszczalnym długotrwale oraz prądem obciążenia.

IPC Sp. z o.o. Gliwice
www.ipc.biz.pl

dr inż. Edward Siwy

Podejście realizacyjne – wymierne korzyści dla OSD

- Wykorzystanie systemu ZMS i danych pomiarowych
- Budowa cyfrowego modelu obliczeniowego
- Możliwość rozszerzenia katalogu analiz
- Analiza w dziedzinie czasu – prawidłowa ocena ryzyka



OeS

TAURON DYSTRYBUCJA

IPC Sp. z o.o. Gliwice
www.ipc.biz.pl

dr inż. Edward Siwy

Dziękuję za uwagę!

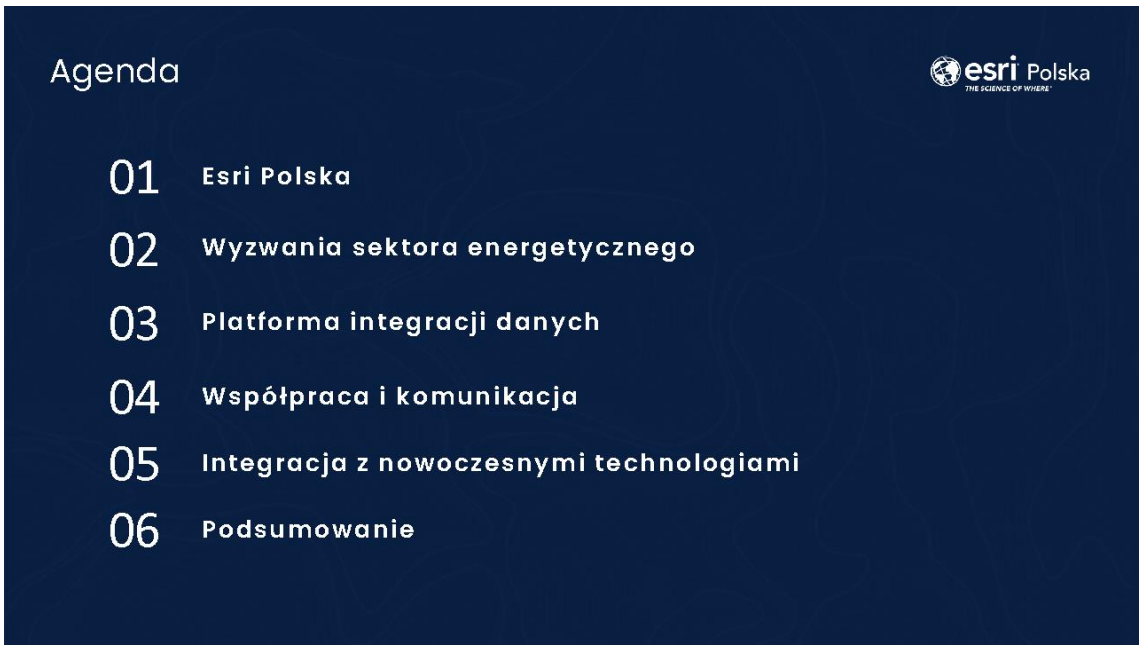
IPC Sp. z o.o.
ul. Młyńska 4 bud. B
44-100 Gliwice
www.ipc.biz.pl

NIP: 631-266-01-81
REGON: 363305534
KRS: 0000593731

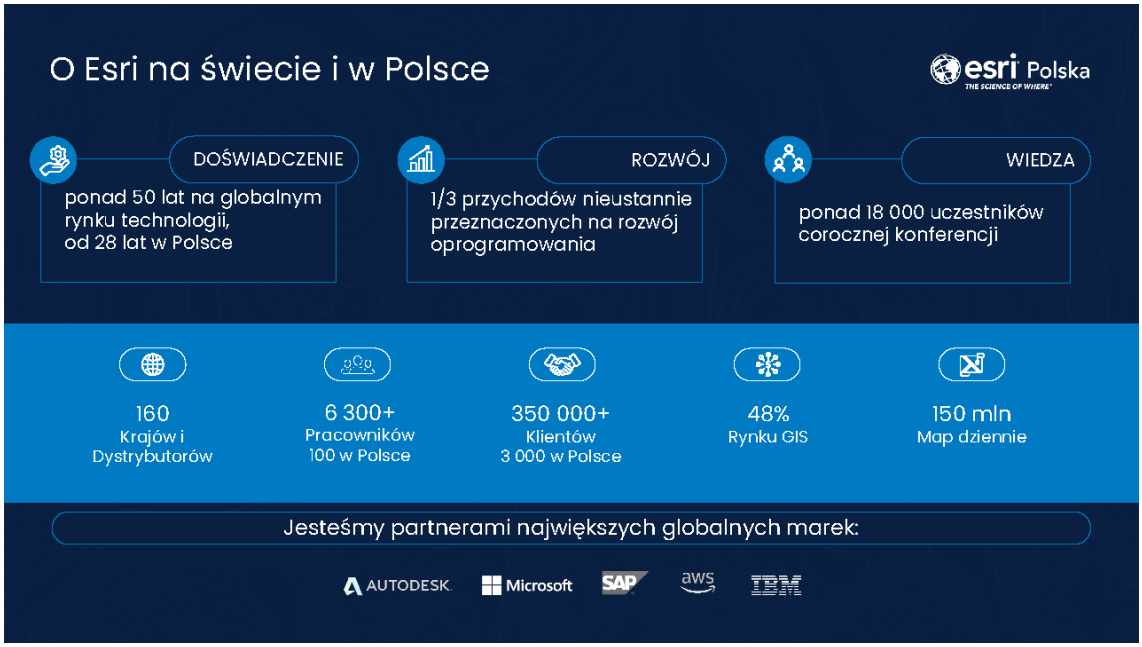
Zapraszam na stoisko wystawowe!

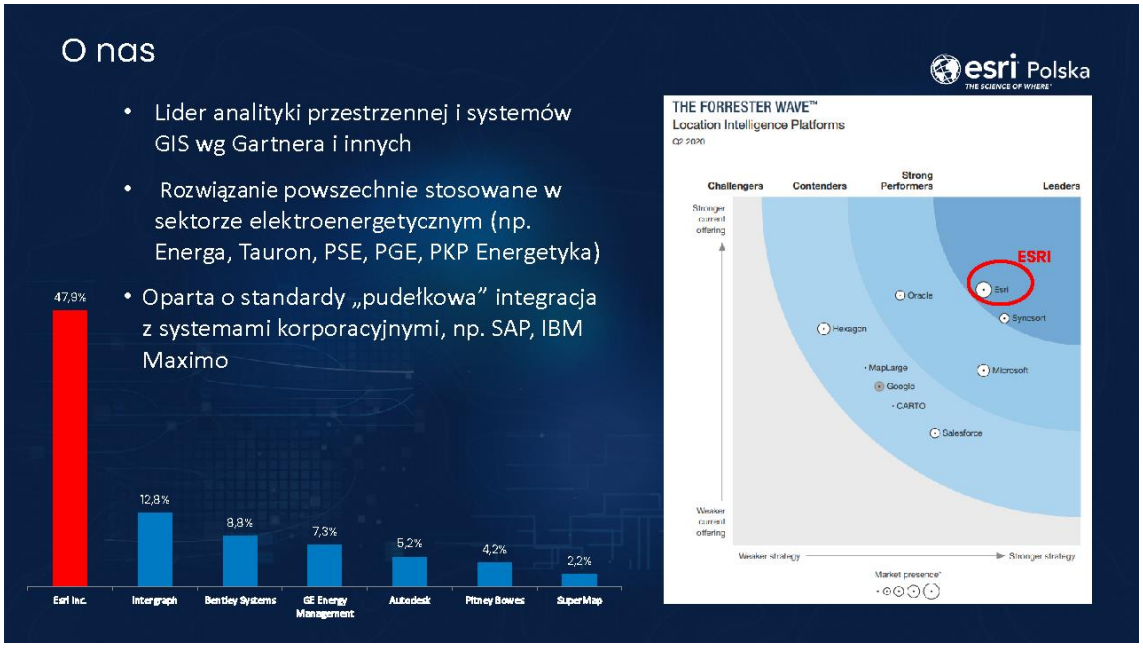
ARCGIS JAKO PLATFORMA INTEGRACJI DANYCH I KOMUNIKACJI INTERESARIUSZY W SEKTORZE ENERGETYKI

Grzegorz Bobola, Jerzy Kisiel (Esri Polska Sp. z o.o.)

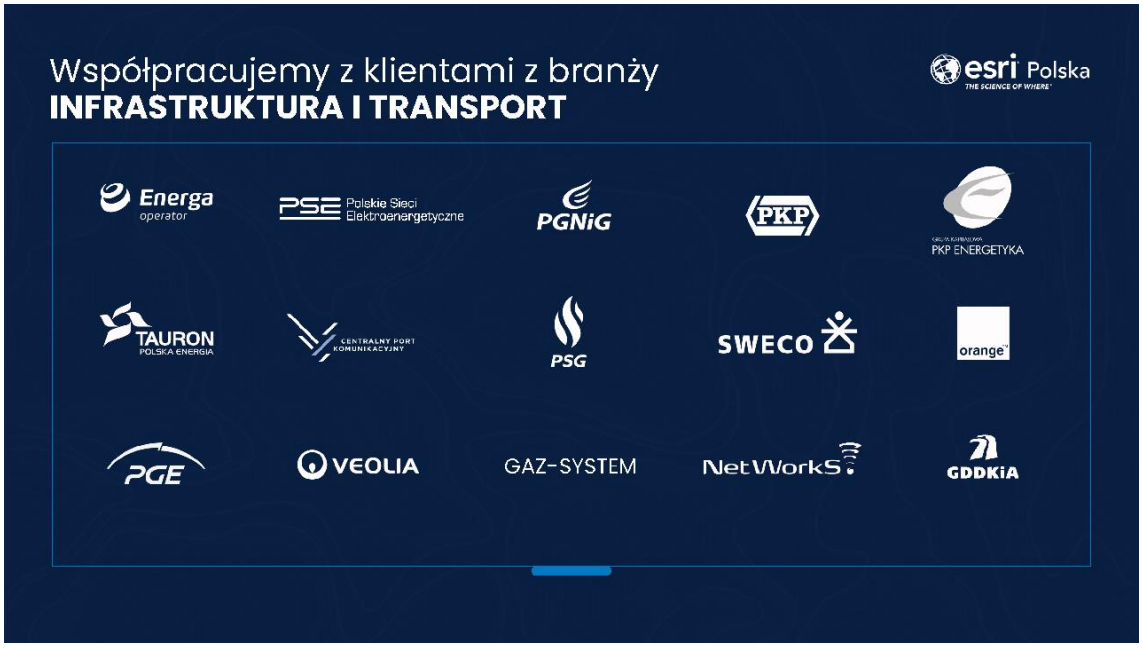



esri Polska
Esri Polska
Co i dla kogo robimy?


O Esri na świecie i w Polsce
esri Polska
DOŚWIADCZENIE
ponad 50 lat na globalnym rynku technologii, od 28 lat w Polsce
ROZWÓJ
1/3 przychodów nieustannie przeznaczonych na rozwój oprogramowania
WIEDZA
ponad 18 000 uczestników corocznej konferencji
160
Krajów i Dystrybutorów
6 300+
Pracowników 100 w Polsce
350 000+
Klientów 3 000 w Polsce
48%
Rynku GIS
150 mln
Map dziennie
Jesteśmy partnerami największych globalnych marek:
AUTODESK
Microsoft
SAP
aws
IBM


O nas
esri Polska
THE SCIENCE OF WHERE
• Lider analityki przestrzennej i systemów GIS wg Gartnera i innych
• Rozwiązanie powszechnie stosowane w sektorze elektroenergetycznym (np. Energa, Tauron, PSE, PGE, PKP Energetyka)
• Oparta o standardy „pudełkowa" integracja z systemami korporacyjnymi, np. SAP, IBM Maximo
47,9%
12,8%
8,8%
7,3%
5,2%
4,2%
2,2%
Esri Inc.
Intergraph
Bentley Systems
GE Energy Management
Autodesk
Pitney Bowes
SuperMap
THE FORRESTER WAVE™
Location Intelligence Platforms
Q2 2020
Challengers
Contenders
Strong Performers
Leaders
ESRI
Esri
Oracle
Syncsort
Hexagon
MapLarge
Microsoft
Google
CARTO
Salesforce
Weaker current offering
Stronger current offering
Weaker strategy
Stronger strategy
Market presence


Zaufało nam wielu klientów różnych branż
esri Polska
THE SCIENCE OF WHERE
ADMINISTRACJA SAMORZĄDOWA
POZnań
KATOWICE
Śląskie.
ADMINISTRACJA CENTRALNA
GUS
RCB
Ministerstwo Finansów
NFZ
BEZPIECZEŃSTWO
FRONTEX
POLICJA
ŚRODOWISKO
Państwowe Gospodarstwo Wodne Wody Polskie
BIZNES
AmRest
pwc
CUSHMAN & WAKEFIELD
Colliers
JLL
EDUKACJA
AGH


Współpracujemy z klientami z branży
INFRASTRUKTURA I TRANSPORT
esri Polska
Energa operator
PSE Polskie Sieci Elektroenergetyczne
PGNiG
PKP
PKP ENERGETYKA
TAURON POLSKA ENERGIA
CENTRALNY PORT KOMUNIKACYJNY
PSG
SWECO
orange
PGE
VEOLIA
GAZ-SYSTEM
NetWorkS
GDDKiA


Wdrażamy Platformę GIS
Jedno źródło „prawdy" dla procesów biznesowych
i ludzi w całym przedsiębiorstwie
esri Polska
Praca specjalistów
Integracje z innymi systemami
CIS
ERP
ADMS
PM
Praca w terenie
Pozyskiwanie i przetwarzanie
danych z dronów
Analityka i predykcja
Jedno źródło „prawdy"

esri Polska
THE SCIENCE OF WHERE

Wyzwania sektora energetycznego

Nasze obserwacje

Wyzwania sektora energetycznego w kontekście GIS

esri Polska
THE SCIENCE OF WHERE

1. Kompleksowość infrastruktury energetycznej

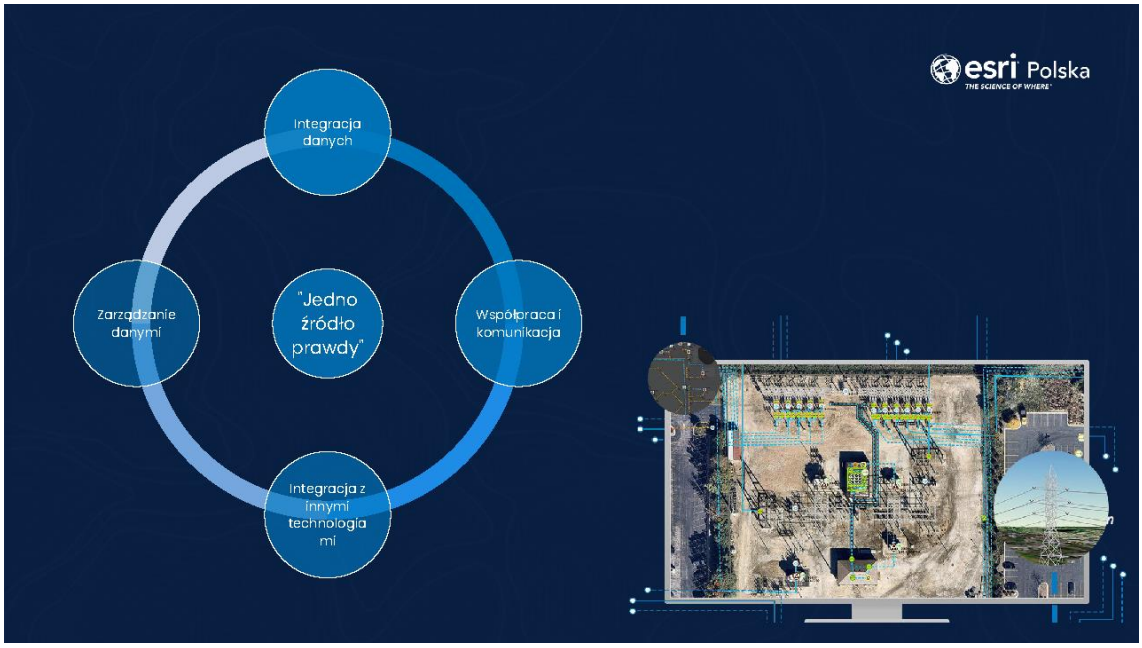
Zarządzanie rozległymi sieciami przesyłowymi i dystrybucyjnymi – wiele procesów do obsłużenia w zakresie wytwarzania, przesyłu i dystrybucji energii elektrycznej.

2. Różnorodność danych

Integracja danych z różnych źródeł oraz danych różnych typów (dziedzinowych, biznesowych, ogólnogeograficznych, środowiskowych, społecznych, planistycznych itd.)

3. Potrzeba aktualnych informacji dla różnych grup odbiorców

Szybkie reagowanie na awarie i efektywne planowanie konserwacji.


esri Polska
THE SCIENCE OF WHERE
Integracja danych
Współpraca i komunikacja
Integracja z innymi technologia mi
Zarządzanie danymi
"Jedno źródło prawdy"


esri Polska
THE SCIENCE OF WHERE
Integracja danych

ArcGIS jako zaawansowana platforma integracji danych

Integracja z systemami branżowymi

esri Polska

E.ON Group

Wyzwania:

- Rozproszone dane: Dane były przechowywane w różnych systemach, co utrudniało ich analizę i wykorzystanie w podejmowaniu decyzji.
- Brak spójnego obrazu sieci: Trudności w uzyskaniu całościowego widoku infrastruktury energetycznej.
- Potrzeba poprawy efektywności operacyjnej: Konieczność optymalizacji działań konserwacyjnych i szybkiego reagowania na awarie.

Rozwiązanie:

E.ON zdecydował się wdrożyć ArcGIS Enterprise, platformę GIS umożliwiającą integrację i analizę danych przestrzennych w czasie rzeczywistym. Wdrożenie obejmowało:

- Integrację z systemami SCADA i IoT: Połączenie danych z czujników i systemów monitorujących w jedną platformę.
- Centralizację danych: Stworzenie jednolitej bazy danych dostępnej dla różnych działów i lokalizacji.
- Udostępnienie narzędzi analitycznych: Wykorzystanie zaawansowanych funkcji analizy przestrzennej do predykcyjnej konserwacji i zarządzania aktywami.

ArcGIS jako zaawansowana platforma integracji danych

Integracja z systemami branżowymi

esri Polska

E.ON Group

Korzyści:

- Zwiększona efektywność operacyjna: Szybsze podejmowanie decyzji dzięki dostępowi do aktualnych i dokładnych danych.
- Redukcja kosztów utrzymania: Optymalizacja harmonogramów konserwacji i lepsze wykorzystanie zasobów.
- Poprawa niezawodności sieci: Szybsze wykrywanie i reagowanie na awarie, co przekłada się na mniejszą liczbę przerw w dostawie energii.
- Lepsza współpraca między działami: Ułatwienie komunikacji i wymiany informacji w organizacji.

Przykładowe zastosowania:

- Monitorowanie infrastruktury w czasie rzeczywistym: Pracownicy mogą śledzić stan sieci na interaktywnych mapach.
- Predykcyjna konserwacja: Analiza danych historycznych i bieżących pozwala przewidywać potencjalne awarie.
- Planowanie inwestycji: Lepsza ocena potrzeb i efektywniejsze planowanie rozbudowy sieci.

ArcGIS jako zaawansowana platforma integracji danych

Obsługa dużych zbiorów danych

esri Polska
THE SCIENCE OF WHERE

Dominion Energy

Wyzwania:

- Przetwarzanie dużych zbiorów danych: Konieczność zarządzania ogromną ilością danych generowanych w czasie rzeczywistym.
- Optymalizacja dystrybucji energii: Potrzeba lepszego zrozumienia wzorców zużycia energii i szybkiego reagowania na zmiany popytu.
- Poprawa obsługi klienta: Szybsze wykrywanie awarii i minimalizacja przerw w dostawie energii.

Rozwiązanie:

- Wdrożenie ArcGIS GeoEvent Server: Umożliwiło to przetwarzanie strumieni danych w czasie rzeczywistym i integrację z istniejącymi systemami.
- Analiza danych w czasie rzeczywistym: Monitorowanie zużycia energii, wykrywanie anomalii i predykcyjne modelowanie popytu.
- Interaktywne wizualizacje: Tworzenie map i dashboardów dla lepszego zrozumienia danych.

ArcGIS jako zaawansowana platforma integracji danych

Obsługa dużych zbiorów danych

esri Polska
THE SCIENCE OF WHERE

Dominion Energy

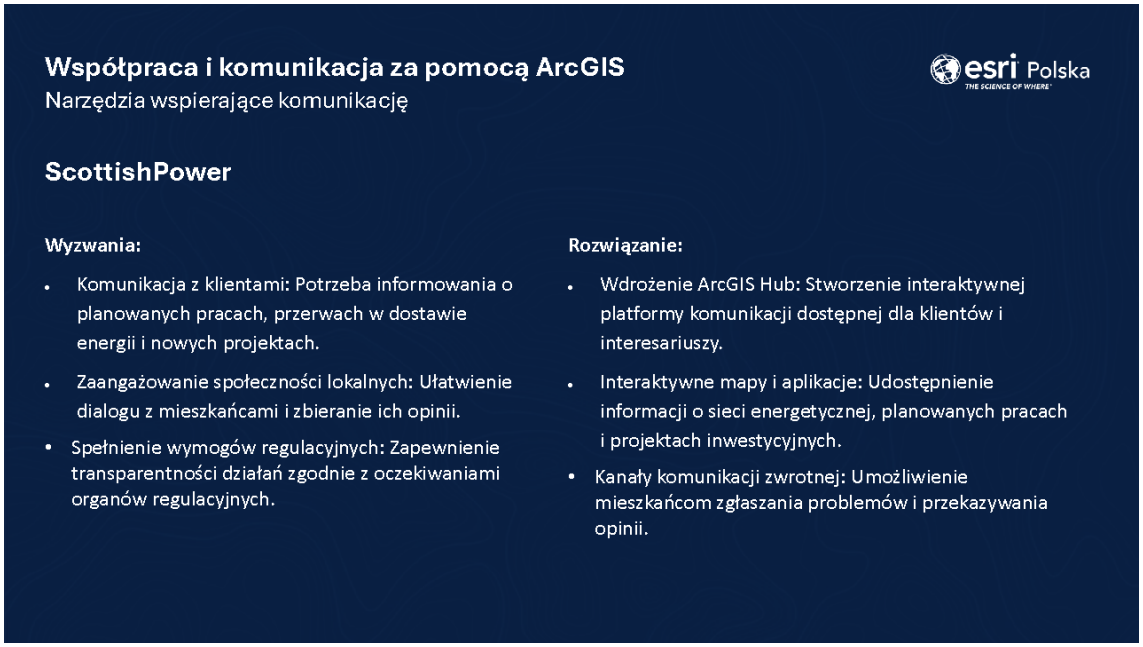
Korzyści:

- Zwiększona efektywność operacyjna: Lepsze zarządzanie siecią i szybsze reagowanie na awarie.
- Redukcja kosztów: Optymalizacja dystrybucji energii i zmniejszenie strat.
- Poprawa satysfakcji klientów: Szybsze rozwiązywanie problemów i lepsza komunikacja.

Przykładowe zastosowania:

- Monitorowanie sieci w czasie rzeczywistym: Wizualizacja stanu sieci na interaktywnych mapach.
- Wykrywanie anomalii: Identyfikacja nietypowych wzorców zużycia energii.
- Predykcyjne modelowanie popytu: Prognozowanie zapotrzebowania na energię.


esri Polska
THE SCIENCE OF WHERE
Współpraca i komunikacja


Współpraca i komunikacja za pomocą ArcGIS
Narzędzia wspierające komunikację
esri Polska
THE SCIENCE OF WHERE
ScottishPower
Wyzwania:
Komunikacja z klientami: Potrzeba informowania o planowanych pracach, przerwach w dostawie energii i nowych projektach.
Zaangażowanie społeczności lokalnych: Ułatwienie dialogu z mieszkańcami i zbieranie ich opinii.
Spełnienie wymogów regulacyjnych: Zapewnienie transparentności działań zgodnie z oczekiwaniami organów regulacyjnych.
Rozwiązanie:
Wdrożenie ArcGIS Hub: Stworzenie interaktywnej platformy komunikacji dostępnej dla klientów i interesariuszy.
Interaktywne mapy i aplikacje: Udostępnienie informacji o sieci energetycznej, planowanych pracach i projektach inwestycyjnych.
Kanały komunikacji zwrotnej: Umożliwienie mieszkańcom zgłaszania problemów i przekazywania opinii.

Współpraca i komunikacja za pomocą ArcGIS

Narzędzia wspierające komunikację

esri Polska
THE SCIENCE OF WHERE

ScottishPower

Korzyści:

- Zwiększona transparentność: Lepsze informowanie klientów o działaniach firmy.
- Poprawa relacji z klientami: Zwiększenie satysfakcji poprzez szybsze reagowanie na potrzeby i problemy.
- Efektywniejsze zarządzanie infrastrukturą: Lepsze planowanie prac dzięki informacjom zwrotnym od społeczności.

Przykładowe zastosowania:

- Mapy przerw w dostawie energii: Aktualne informacje o awariach i planowanych wyłączeniach.
- Informowanie o inwestycjach: Prezentacja nowych projektów i ich wpływu na lokalne społeczności.
- Zbieranie opinii: Ankiety i formularze zgłoszeniowe dla klientów.

Współpraca i komunikacja za pomocą ArcGIS

Raportowanie środowiskowe do organów regulacyjnych

esri Polska
THE SCIENCE OF WHERE

Ørsted

Wyzwania:

- Ochrona środowiska morskiego: Potrzeba minimalizacji wpływu inwestycji na ekosystemy morskie.
- Zgodność z regulacjami: Spełnienie surowych wymogów środowiskowych i raportowanie do organów nadzorczych.
- Zarządzanie danymi środowiskowymi: Integracja i analiza dużych ilości danych z różnych źródeł.

Rozwiązanie:

- Wdrożenie ArcGIS: Centralizacja danych środowiskowych, takich jak informacje o faunie i florze morskiej, prądach czy jakości wody.
- Analiza przestrzenna: Wykorzystanie narzędzi GIS do oceny potencjalnego wpływu na środowisko.
- Raportowanie i wizualizacja: Tworzenie map i raportów dla interesariuszy i organów regulacyjnych.

Współpraca i komunikacja za pomocą ArcGIS

Raportowanie środowiskowe do organów regulacyjnych

esri Polska
THE SCIENCE OF WHERE

Ørsted

Korzyści:

- Zwiększona odpowiedzialność środowiskowa: Lepsze zarządzanie wpływem na ekosystemy.
- Ułatwienie procesu regulacyjnego: Efektywne spełnianie wymogów raportowania.
- Poprawa wizerunku firmy: Budowanie zaufania wśród społeczności i inwestorów.

Przykładowe zastosowania:

- Monitoring populacji morskich: Śledzenie migracji i zachowań zwierząt.
- Analiza siedlisk: Identyfikacja obszarów wrażliwych ekologicznie.
- Planowanie lokalizacji turbin: Optymalizacja rozmieszczenia w celu minimalizacji wpływu.

Współpraca i komunikacja za pomocą ArcGIS

Informowanie społeczności o planowanych inwestycjach

esri Polska
THE SCIENCE OF WHERE

Vattenfall

Wyzwania:

- Kompleksowość projektów energetycznych: Trudności w przekazywaniu skomplikowanych informacji w przystępny sposób.
- Zaangażowanie społeczności lokalnych: Potrzeba zdobycia akceptacji dla nowych inwestycji.
- Transparentność działań: Spełnienie oczekiwań dotyczących otwartości i komunikacji.

Rozwiązanie:

- Wykorzystanie ArcGIS StoryMaps: Tworzenie interaktywnych opowieści łączących mapy, tekst, zdjęcia i multimedia.
- Prezentacja projektów: Przedstawienie planów budowy farm wiatrowych i słonecznych w angażujący sposób.
- Interaktywność: Umożliwienie użytkownikom eksploracji danych i zadawania pytań.

Współpraca i komunikacja za pomocą ArcGIS

Informowanie społeczności o planowanych inwestycjach

esri Polska
THE SCIENCE OF WHERE

Vattenfall

Korzyści:

- Zwiększone zaangażowanie: Lepsze zrozumienie projektów przez społeczności lokalne.
- Budowanie zaufania: Transparentność i otwartość komunikacji.
- Przyspieszenie procesów inwestycyjnych: Zwiększona akceptacja społeczna ułatwia uzyskanie pozwoleń.

Przykładowe zastosowania:

- Prezentacje online: Dostępne publicznie StoryMapy z informacjami o projektach.
- Konsultacje społeczne: Zbieranie opinii i odpowiedzi na pytania mieszkańców.
- Edukacja ekologiczna: Informowanie o korzyściach płynących z energii odnawialnej.

esri Polska
THE SCIENCE OF WHERE

Integracja z wybranymi technologiami

Integracja ArcGIS z nowoczesnymi technologiami

Wykorzystanie uczenia maszynowego i sztucznej inteligencji

esri Polska
THE SCIENCE OF WHERE

EDP Renewables

Wyzwania:

- Zapobieganie awariom: Potrzeba minimalizacji nieplanowanych przestojów i optymalizacji wydajności.
- Zarządzanie rozproszonymi aktywami: Kontrola nad tysiącami instalacji na całym świecie.
- Analiza dużych zbiorów danych: Przetwarzanie informacji z czujników i systemów monitoringu.

Rozwiązanie:

- Integracja AI z GIS: Wykorzystanie sztucznej inteligencji do analizy danych przestrzennych i operacyjnych.
- Predykcyjna konserwacja: Prognozowanie potencjalnych awarii na podstawie wzorców i anomalii.
- Centralizacja danych: Stworzenie platformy do zarządzania informacjami o wszystkich aktywach.

Integracja ArcGIS z nowoczesnymi technologiami

Wykorzystanie uczenia maszynowego i sztucznej inteligencji

esri Polska
THE SCIENCE OF WHERE

EDP Renewables

Korzyści:

- Redukcja kosztów operacyjnych: Mniejsze wydatki na naprawy i konserwacje awaryjne.
- Zwiększenie dostępności aktywów: Wyższa efektywność produkcji energii.
- Poprawa bezpieczeństwa: Zapobieganie potencjalnie niebezpiecznym awariom.

Przykładowe zastosowania:

- Monitorowanie turbin wiatrowych: Analiza danych z czujników wibracji i temperatury.
- Optymalizacja paneli słonecznych: Wykrywanie spadków wydajności i uszkodzeń.
- Zarządzanie flotą aktywów: Wizualizacja i kontrola stanu wszystkich instalacji.

Integracja ArcGIS z nowoczesnymi technologiami

Mobilne rozwiązania GIS

esri Polska

Enbridge

Wyzwania:

- Rozległa infrastruktura: Zarządzanie tysiącami kilometrów rurociągów i obiektów.
- Efektywność prac terenowych: Potrzeba lepszego narzędzia do zbierania danych i raportowania.
- Bezpieczeństwo i zgodność z regulacjami: Konieczność spełnienia surowych standardów bezpieczeństwa.

Rozwiązanie:

- Wdrożenie ArcGIS Field Maps: Wyposażenie pracowników terenowych w aplikacje mobilne do zbierania i aktualizacji danych.
- Synchronizacja w czasie rzeczywistym: Dane z terenu są natychmiast dostępne dla centralnych systemów.
- Integracja z istniejącymi systemami: Połączenie z bazami danych i narzędziami analitycznymi.

Integracja ArcGIS z nowoczesnymi technologiami

Mobilne rozwiązania GIS

esri Polska

Enbridge

Korzyści:

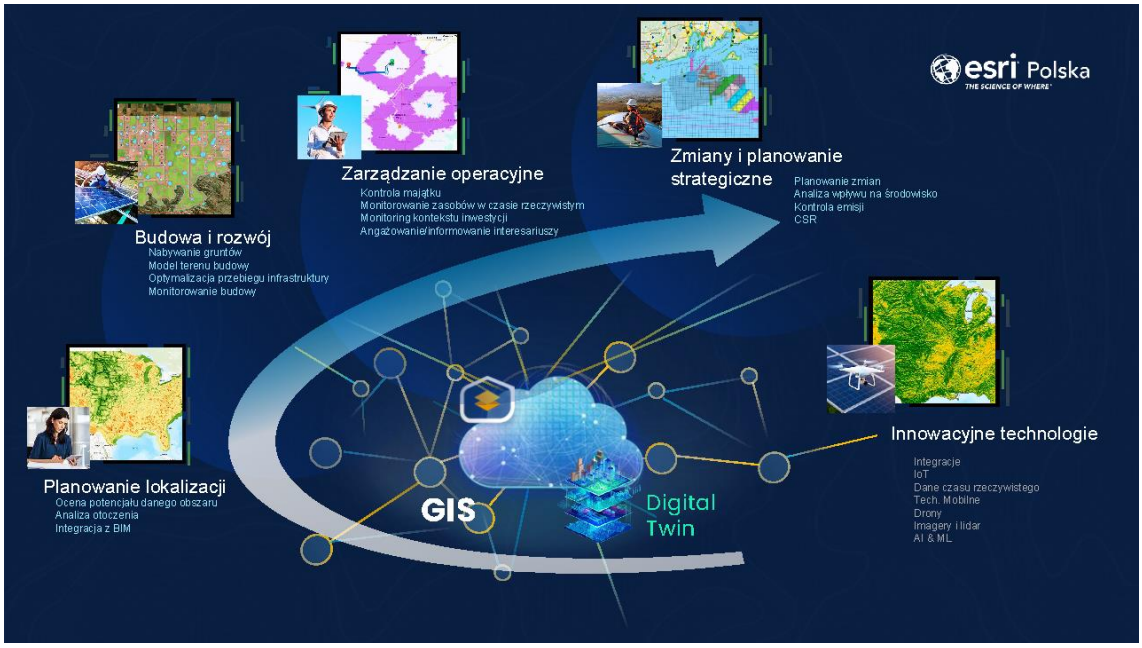
- Zwiększona efektywność operacyjna: Szybsze i dokładniejsze zbieranie danych.
- Poprawa bezpieczeństwa: Natychmiastowe raportowanie potencjalnych zagrożeń.
- Lepsze zarządzanie aktywami: Aktualne informacje o stanie infrastruktury.

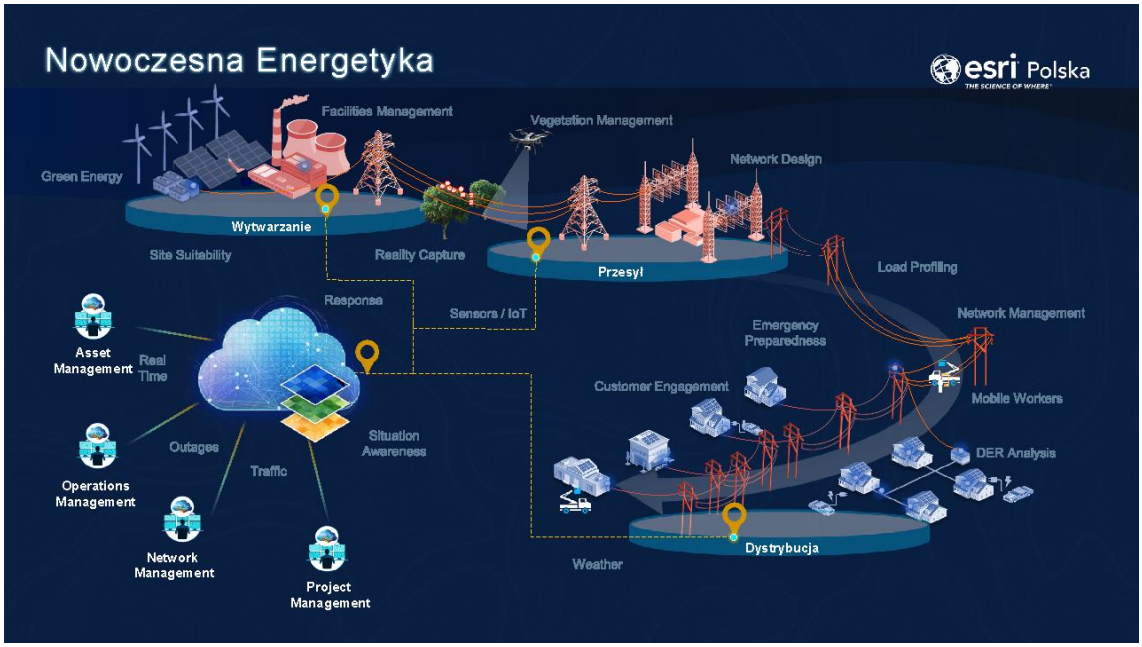
Przykładowe zastosowania:

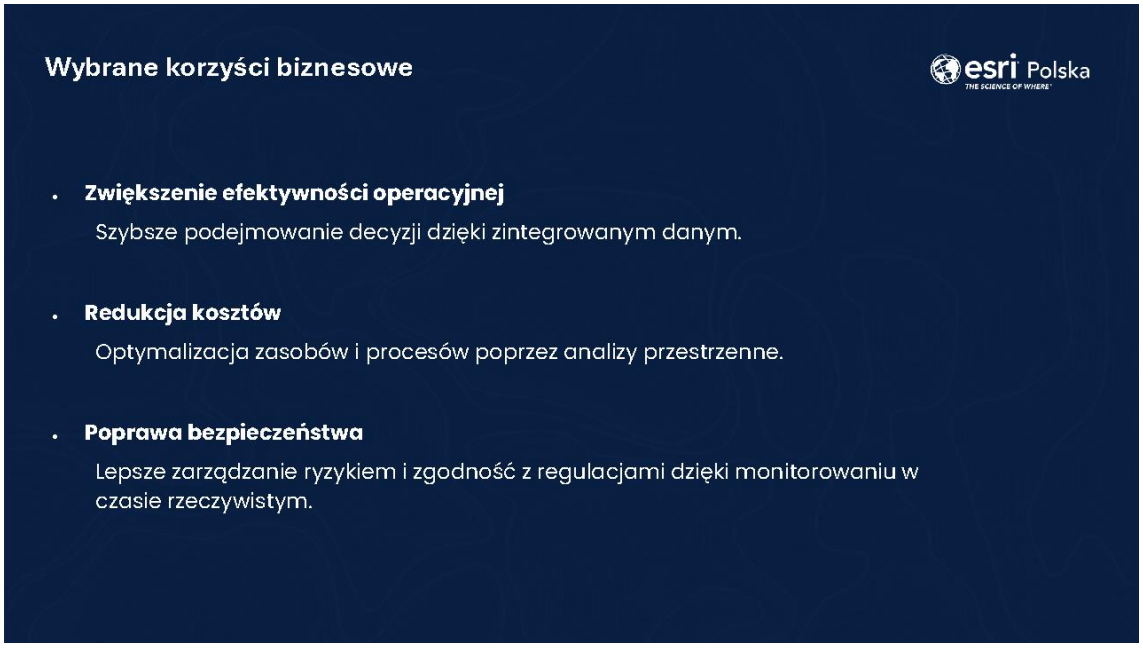
- Inspekcje rurociągów: Dokumentowanie stanu technicznego i wykrytych usterek.
- Prace konserwacyjne: Planowanie i śledzenie realizacji zadań.
- Zgłaszanie incydentów: Szybkie przekazywanie informacji o awariach i zagrożeniach.


esri Polska
Podsumowanie

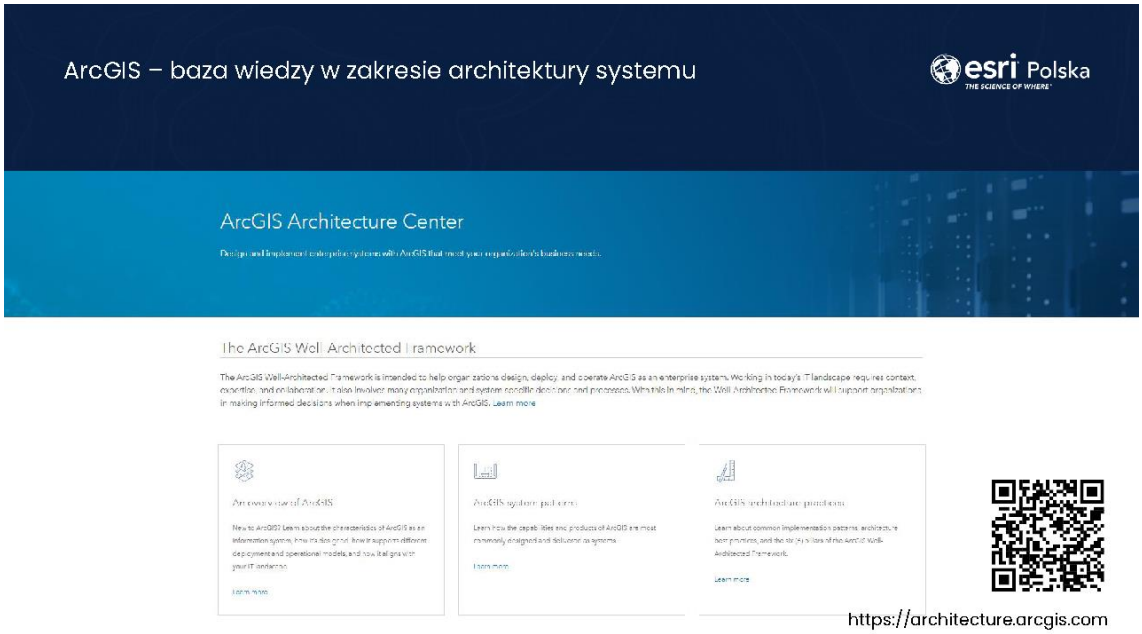

ArcGIS – kompleksowa Platforma zarządzania danymi i projektami
esri Polska
Integracja z danymi
i systemami zewnętrznymi
Dane geodezyjne
Dane środowiskowe
Sieci infrastrukturalne
Dane społeczno - ekonomiczne
Dane czasu rzeczywistego
Dane pomiarowe
Dane inżynieryjne (CAD),
Projekty / modele BIM,
Sieci infrastruktury technicznej
(energetyka, gaz, woda)
Dane pozyskiwane z satelit,
samolotów, dronów, dane
pozyskiwane w terenie.
GIS
Mapy i wizualizacja danych
Zarządzanie danymi
Analityka i modelowanie
Monitoring i raportowanie
Wsparcie procesów
decyzyjnych
Udostępnianie zasobów i współpraca między
interesariuszami
System zapisu
i zarządzania danymi
System wymiany
danych i współpracy
System analityczny
Dostępność dla wszystkich
grup odbiorców
AUTODESK
IBM
Microsoft
ORACLE
SAP
Trimble
aws


esri Polska
THE SCIENCE OF WHERE
Budowa i rozwój
Nabywanie gruntów
Model terenu budowy
Optymalizacja przebiegu infrastruktury
Monitorowanie budowy
Zarządzanie operacyjne
Kontrola majątku
Monitorowanie zasobów w czasie rzeczywistym
Monitoring kontekstu inwestycji
Angażowanie/informowanie interesariuszy
Zmiany i planowanie strategiczne
Planowanie zmian
Analiza wpływu na środowisko
Kontrola emisji
CSR
Planowanie lokalizacji
Ocena potencjału danego obszaru
Analiza otoczenia
Integracja z BIM
GIS
Digital Twin
Innowacyjne technologie
Integracje
IoT
Dane czasu rzeczywistego
Tech. Mobilne
Drony
Imagery i lidar
AI & ML

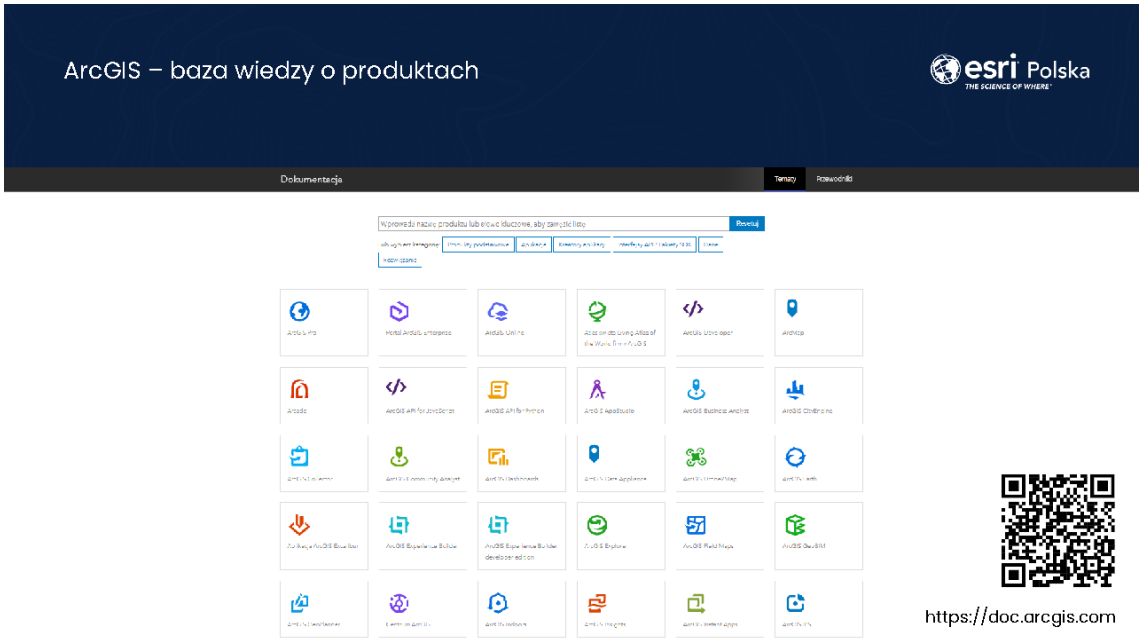

Nowoczesna Energetyka
esri Polska
THE SCIENCE OF WHERE
Green Energy
Facilities Management
Vegetation Management
Network Design
Wytwarzanie
Site Suitability
Reality Capture
Przesył
Load Profiling
Response
Sensors / IoT
Network Management
Emergency Preparedness
Asset Management
Real Time
Customer Engagement
Mobile Workers
Situation Awareness
Outages
Traffic
DER Analysis
Operations Management
Network Management
Project Management
Weather
Dystrybucja


Wybrane korzyści biznesowe
esri Polska
THE SCIENCE OF WHERE
Zwiększenie efektywności operacyjnej
Szybsze podejmowanie decyzji dzięki zintegrowanym danym.
Redukcja kosztów
Optymalizacja zasobów i procesów poprzez analizy przestrzenne.
Poprawa bezpieczeństwa
Lepsze zarządzanie ryzykiem i zgodność z regulacjami dzięki monitorowaniu w czasie rzeczywistym.

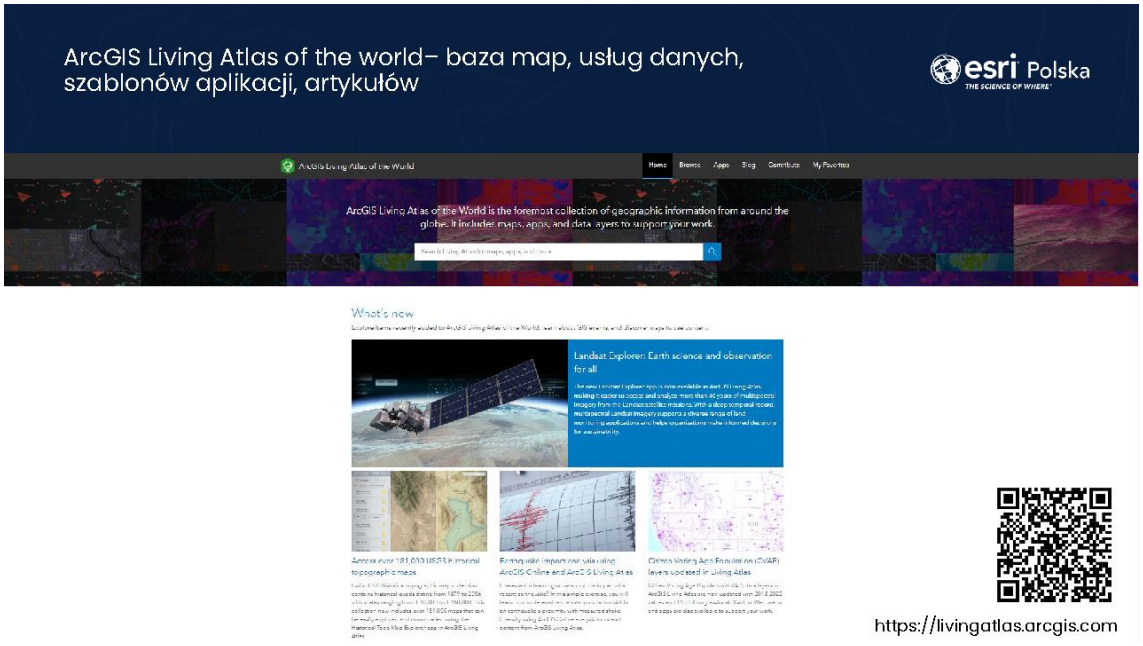

esri Polska
THE SCIENCE OF WHERE
Źródła wiedzy i zasoby Esri



https://architecture.arcgis.com



https://doc.arcgis.com


ArcGIS Living Atlas of the world– baza map, usług danych, szablonów aplikacji, artykułów
esri Polska
THE SCIENCE OF WHERE
ArcGIS Living Atlas of the World
Home
Browse
Apps
Blog
Contribute
My Favorites
ArcGIS Living Atlas of the World is the foremost collection of geographic information from around the globe. It includes maps, apps, and data layers to support your work.
What's new
Landsat Explorer: Earth science and observation for all
https://livingatlas.arcgis.com


esri Polska
THE SCIENCE OF WHERE
Grzegorz Bobola
gbobola@esri.pl
Tel. +48 602 538 565
Jerzy Kisiel
jkisiel@esri.pl
Tel. +48 508 972 137
Plac Konesera 9
03-736 Warszawa


esri Polska
THE SCIENCE OF WHERE
Widzimy, czego inni nie widzą.
Zamieniamy dane na decyzje.
Ty wiesz co i jak, my powiemy Ci gdzie i kiedy.
SIWE 2024

JAK CYFRYZACJA SIECI ELEKTROENERGETYCZNEJ MOŻE POMÓC OPERATOROWI?

Techinova AB

Plan wystąpienia:

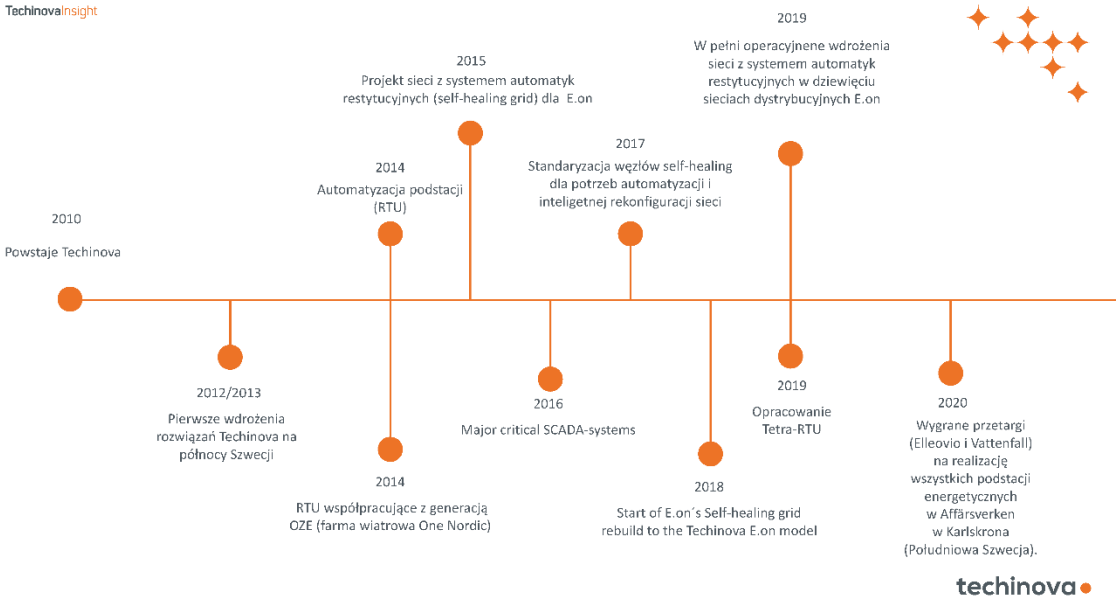
- Przybliżenie sylwetki firmy
- Przybliżenie portfolio produktów
- Konkurs dla uważnych słuchaczy

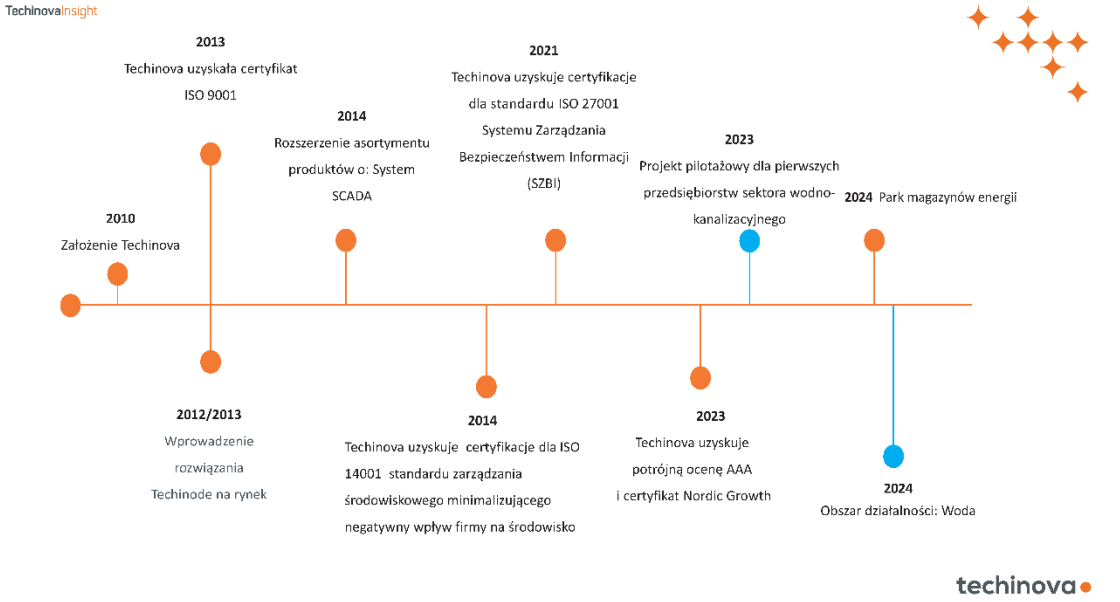
Rozwiązanie Techinova dla sieci dziś i jutro

W Techinova tworzymy i wdrażamy nowoczesne i inteligentne rozwiązania energetyczne.

Dysponując własną produkcją, obsługujemy zarówno nowe inwestycje, jak i zastaną infrastrukturę.

Aby sprostać wyzwaniom przyszłej transformacji energetycznej, integrujemy wdrożone rozwiązanie dodając inteligentną automatyzację sieci. Szczególny nacisk kładziemy na rozwiązania komunikacji bezprzewodowej, które są wykorzystywane przez naszych klientów.


TechinovaInsight
2010
Powstaje Techinova
2012/2013
Pierwsze wdrożenia rozwiązań Techinova na północy Szwecji
2014
Automatyzacja podstacji (RTU)
2014
RTU współpracujące z generacją OZE (farma wiatrowa One Nordic)
2015
Projekt sieci z systemem automatyk restytucyjnych (self-healing grid) dla E.on
2016
Major critical SCADA-systems
2017
Standaryzacja węzłów self-healing dla potrzeb automatyzacji i inteligetnej rekonfiguracji sieci
2018
Start of E.on´s Self-healing grid rebuild to the Techinova E.on model
2019
W pełni operacyjnene wdrożenia sieci z systemem automatyk restytucyjnych w dziewięciu sieciach dystrybucyjnych E.on
2019
Opracowanie Tetra-RTU
2020
Wygrane przetargi (Elleovio i Vattenfall) na realizację wszystkich podstacji energetycznych w Affärsverken w Karlskrona (Południowa Szwecja).
techinova


TechinovaInsight
2010
Założenie Techinova
2012/2013
Wprowadzenie rozwiązania Techinode na rynek
2013
Techinova uzyskała certyfikat ISO 9001
2014
Techinova uzyskuje certyfikacje dla ISO 14001 standardu zarządzania środowiskowego minimalizującego negatywny wpływ firmy na środowisko
2014
Rozszerzenie asortymentu produktów o: System SCADA
2021
Techinova uzyskuje certyfikacje dla standardu ISO 27001 Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)
2023
Techinova uzyskuje potrójną ocenę AAA i certyfikat Nordic Growth
2023
Projekt pilotażowy dla pierwszych przedsiębiorstw sektora wodno-kanalizacyjnego
2024
Park magazynów energii
2024
Obszar działalności: Woda
techinova

TechinovaInsight

Pracownicy Techinova z bogatym doświadczeniem i wiedzą domenową w branży energetycznej

Pracownicy Techinova posiadają wcześniejsze doświadczenia w pracy w branży energetycznej w firmach takich jak:

- ABB
- E.ON
- Radius
- Netcontrol
- Vattenfall
- Affärsverken

techinova

TechinovaInsight

Techinova – Nasi klienci

E.ON	Vattenfall Elnät	Ellevio	Hässleholms Vatten
One Nordic	Pite Energi	Holtab	Falu Energi och Vatten
GEAB	Jönköpings Energi	Ellevio	Orbit One
Skellefteå Kraft	Härnösand Energi	Gävle Energi	Österlen Kraft
Ljusdal Energi	och Miljö	Kungälv Energi	ELTEL Networks
Elkraftsbyggarna	Saab	Landskrona Energi	Affärsverken
Elektra Nät	Kraftringen	Malungs Elnät	
Hofors Elverk	Öresundskraft	Umeå Energi	

techinova

TechinovaInsight

Techinova – Nasi klienci

E.ON	Vattenfall Elnät	Ellevio	Hässleholms Vatten
One Nordic	Pite Energi	Holtab	Falu Energi och Vatten
GEAB	Jönköpings Energi	Ellevio	Orbit One
Skellefteå Kraft	Härnösand Energi	Gävle Energi	Österlen Kraft
Ljusdal Energi	och Miljö	Kungälv Energi	ELTEL Networks
Elkraftsbyggarna	Saab	Landskrona Energi	Affärsverken
Elektra Nät	Kraftringen	Malungs Elnät	
Hofors Elverk	Öresundskraft	Umeå Energi	

techinova

TechinovaInsight

Brodersen RTU32M

- Modularny
- Wspiera większość standardów komunikacyjnych
- IEC61850 Master/Client, IEC61870-101/104
- Straton PLC (moduły automatyzacji)
- Modernizacja lub nowe stacje elektroenergetyczne (obwody pierwotne i wtórne)
- Światłowód/Ethernet/Radio(np.TETRA)/4G

techinova

TechinovaInsight

Liczniki energii elektrycznej

- Pomiar energii elektrycznej
- Analiza jakości energi elektrycznej dla potrzeb wczesnego ostrzegania o zaburzeniach na sieci
- Analiza zakłóceń i zaburzeń na sieci
- Komunikacja z portam HAN
- Uproszczona instalacja

techinova

TechinovaInsight

Wyniesione wielofunkcyjne urządzenia pomiarowe

- Pomiar energii elektrycznej
- Pomiar jakości energii elektrycznej
- Wbudowane raportowanie
- Analiza zakłóceń i zaburzeń na sieci
- Proaktywne rozwiązanie – dla potrzeb wczesnego ostrzegania o zaburzeniach na sieci

techinova

TechinovaInsight

Zdalny czujnik/detector usterek na sieci

IPC4020/IPC4022

- Klient IEC60870-104
- FPI/EFI (wkaźnik zakłóceń/zwarcia/błąd izolacji)
- Ustawienia ochrony dla OC, EF, Dir EF
- IEC60870-104 Client
- Łatwa instalacja

techinova

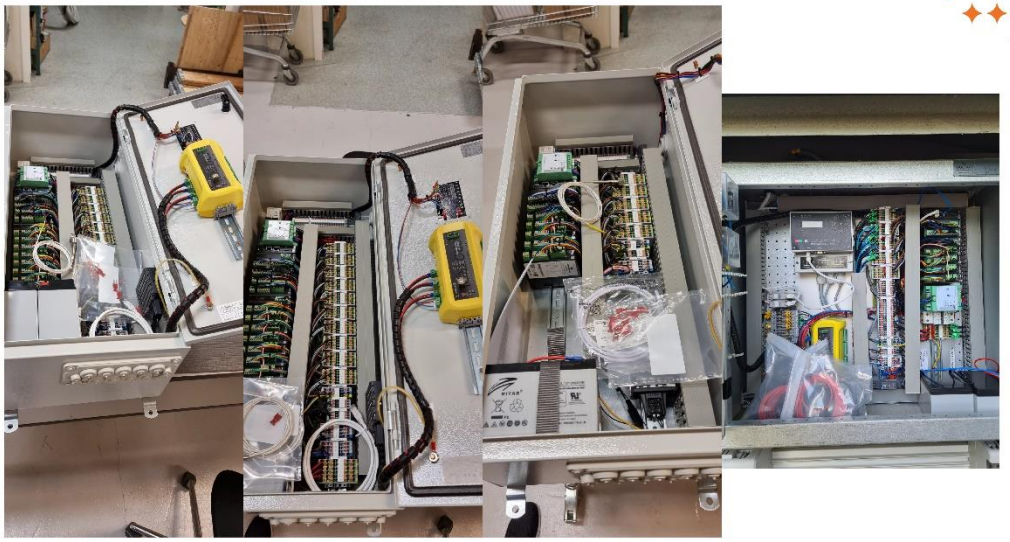
TechinovaInsight

TechinovaInsight

- Digitalization
- Smart grids
- Meassurements
- Proactive analysis
- Easy and clear visualisation

techinova

TechinovaInsight



techinova

TechinovaInsight

- The EU CISSAN Project
- Techinova goals with the project.

Techinova goal is to enhance their product portfolio with new ways of securing communication in the electricity grid application, making a field trial system to existing customer Affärsverken and identifying new markets.

Techinova	• 1 Field trial system in Affärsverkens electricity grid • 1 New way of secure communication for electricity grid application (preferably integration of early version of new standardized IoT-protocol) • 1 New identified market

techinova

TechinovaInsight

Implementation

Overview of the work packages

Work Package	Type of activity and task description	Lead participant	Partners
WP0: Project management	Coordinates project deliverables, activities and partners. It organizes project workshops and meetings, offers an online platform for information exchange, coordinates dissemination, and communications between various roles.	Blue Science Park	All
WP1: Continuous follow-up of the related research fields	To recognize essential research findings that may be applicable in the project. The followed research fields include among others radio technology, network technologies, threat intelligence, artificial intelligence, machine learning, set theories, pattern recognition, data filtering, intelligent control, cryptology, blockcham, distributed algorithms.	Blekinge Institute of Technology (BTH)	AddSecure, Arctos, BTH, Techinova
WP2: Definition of the system architecture	Designs an overall system architecture (CISSAN architecture) of the distributed cyber security platform through system elements. The system elements range from IoT devices to routers and cloud devices and services. The system architecture is composed of its constituent elements, and it defines how the elements relate to each other. It also describes the interfaces between the elements and how to encapsulate them in case of threats.	Techinova	AddSecure, Affärsv, Arctos, Techinova, Clavister, BTH
WP3: Business models	Recognizes possible models for IoT systems with distributed intelligent security and service provisioning mechanisms. The business model creation and validation work are strongly motivated by business-driven	AddSecure	AddSecure, Affärsv, Techinova, BTH, Blue

- Techinova
- Work package leader WP2
- Definition of system architecture
- (We see us as project managers for this work package. We will lead the work within this package, not do all the work).
- Since we have a pretty good knowledge of the distribution grids in Sweden, we believe that this work package will suit our competence.

techinova

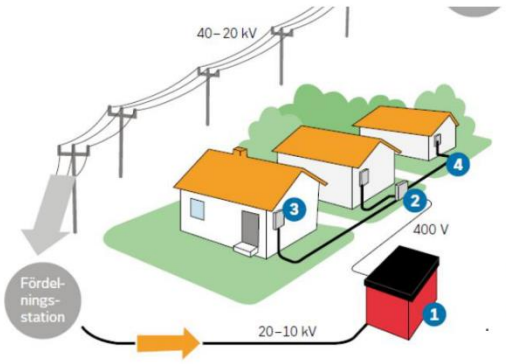
TechinovaInsight

	co-innovation towards innovative ecosystem.		
WP4: Data security, gathering and quality assessments	Gathers, integrates, verifies, stores and presents sensor data from IoT systems and simulation models developed.	AddSecure/ Techinova	BTH, Techinova, AddSecure, Affärsv, Blue
WP5: Distributed intelligent security mechanisms	Develops distributed intelligent security functionalities and develops distributed load balancing solutions. Moreover, the WP develops an overlay network solution for artificial intelligence traffic. Nodes interact with signaling and data traffic but also with artificial intelligence traffic, to transfer security information to each node. The WP also develops a novel, scalable and secure blockchain consensus protocol for IoT networks.	Arctos Labs	Affärsv, BTH, Arctos, Savantic, Techinova, Clavister, AddSecure
WP6: Proof of work	Demonstrates the CISSAN platform with the use case for electricity production	Affärsverken	Arctos, Techinova, Clavister, AddSecure, Affärsv, BTH, Blue
WP7: Standardizati on	Follows standardization forums, coordinates standardization related issues in other work packages and contributes to standardization.	BTH	AddSecure, Techinova, BTH

- Techinova
- Work package for WP4
- Data security, gathering and quality assessments.

techinova

TechinovaInsight



- When testing the AI we look at data from the primary substation. It have quite sophisticated fault-finding equipment. In the early stages of the traing this is the "true picture" of the anomalies detected in the secondary substations.
- Secondary substation has information about the local site. All secondary substation together has very much information about the grid as a whole.
- The initial AI training version one is done.
- The AI can already detect communication, data and grid behaviour anomalies that the Primary substation does not see.

- Primary substation has more information about a bigger part of the grid.

techinova

Perspektywa Szwedzka na sieć energetyczną

- Przerwy w dostawie energi elektrycznej mają swoje konsekwencje.
- Dla przykładu w Szwecji przerwy w dostawie prądu generują koszty na poziomie ok 1.6 miliarda SEK rocznie .
- Rośnie ilość przyłączanych źródeł OZE
- W rezultacie rośnie złożoność sieci energetycznej
- Admistracje rządowe chcą, aby automatyzacja sieci energetyczynych współgrała z ilością potrzebnych inwestycji.

techinova

TechinovaInsight

Odpowiedzią na to wyzwanie jest

TechinovaGrid

techinova

TechinovaInsight

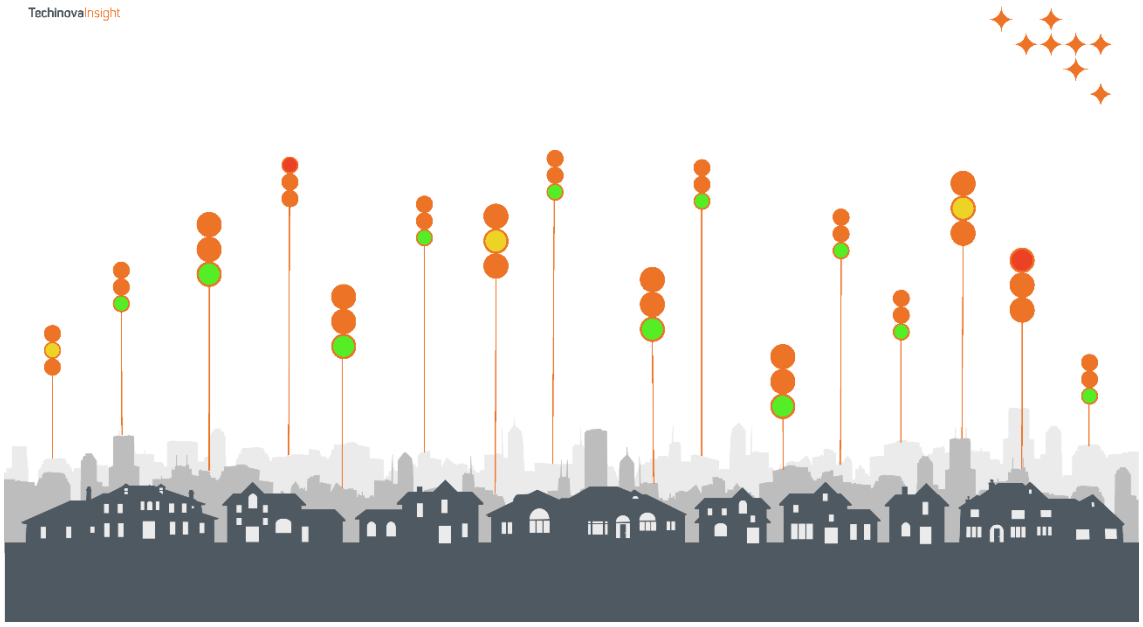
Odpowiedzią na to wyzwanie jest

TechinovaGrid

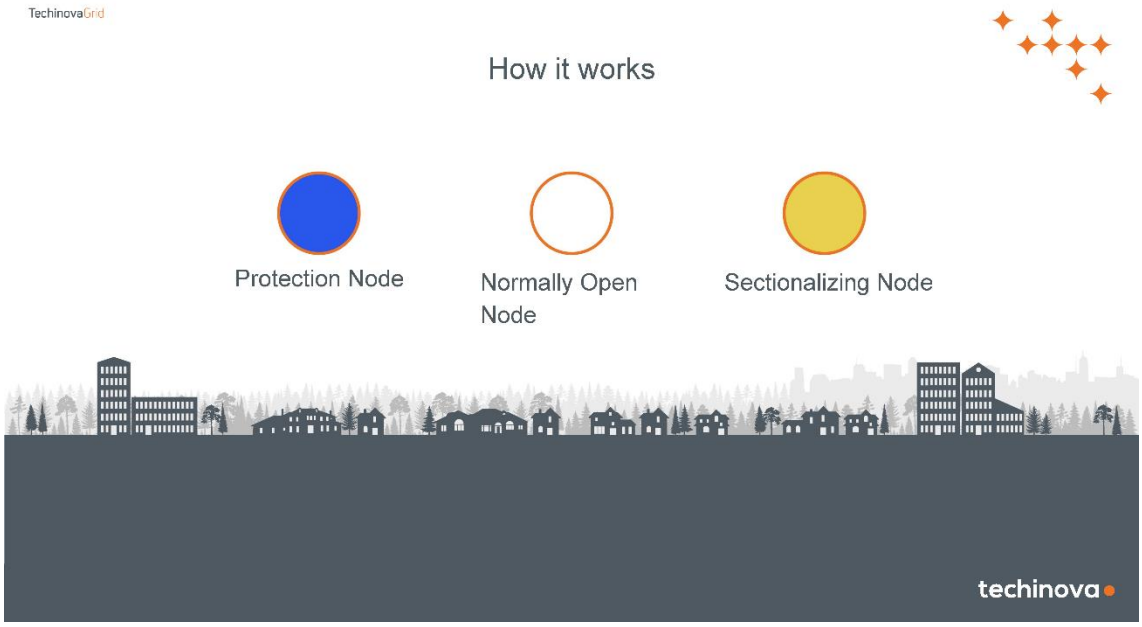
Prezentacje przejmuje Peter Fransson, który opowie więcej

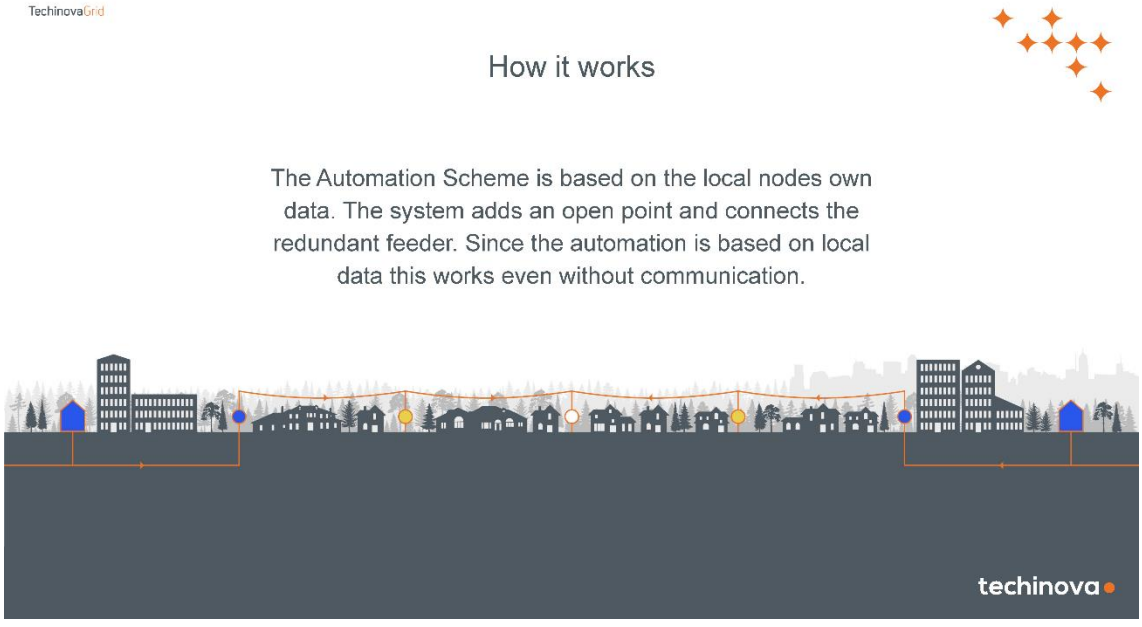
o TechniGrid i uzupełni informacje o Techninova

techinova


TechinovaInsight


TechinovaGrid
techinova


TechinovaGrid
How it works
Protection Node
Normally Open Node
Sectionalizing Node
techinova


TechinovaGrid
How it works
The Automation Scheme is based on the local nodes own data. The system adds an open point and connects the redundant feeder. Since the automation is based on local data this works even without communication.
techinova

TechinovaGrid

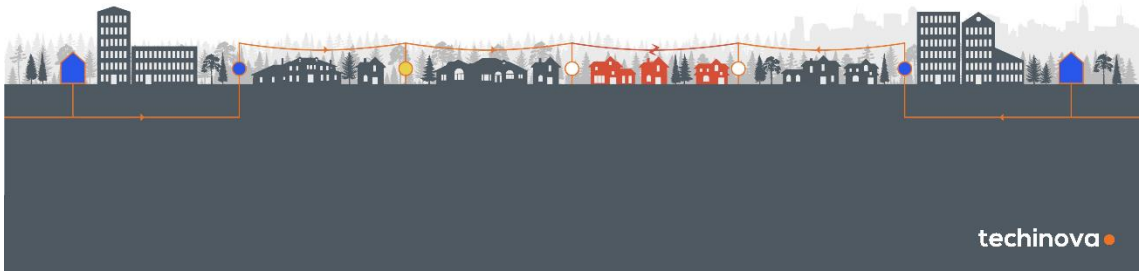
How it works

The Automation Scheme is based on the local nodes own data. The system adds an open point and connects the redundant feeder. Since the automation is based on local data this works even without communication.

TechinovaGrid

How it works

The Automation Scheme is based on the local nodes own data. The system adds an open point and connects the redundant feeder. Since the automation is based on local data this works even without communication.



TechinovaGrid

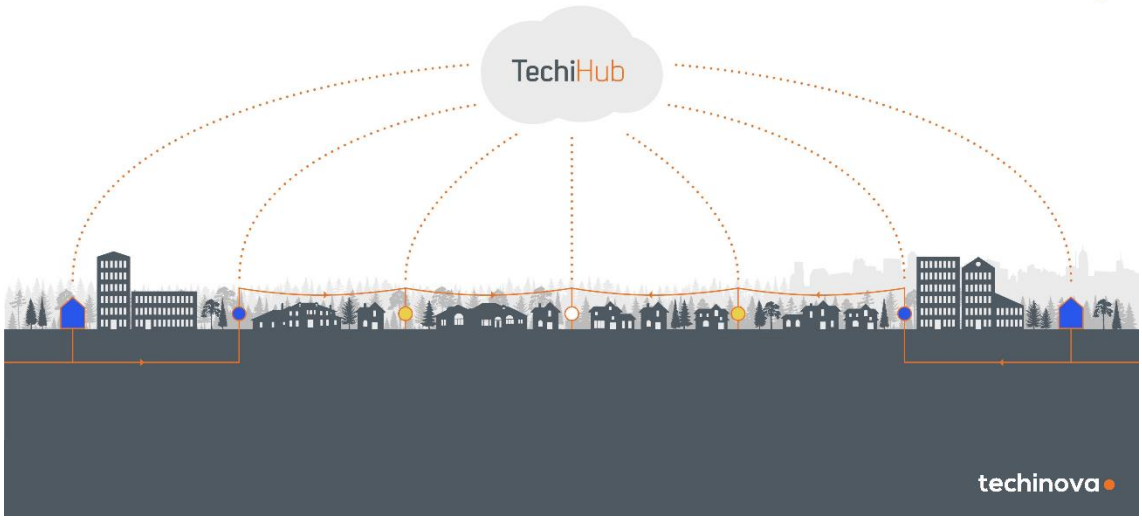
TechinovaGrid

How does it work?

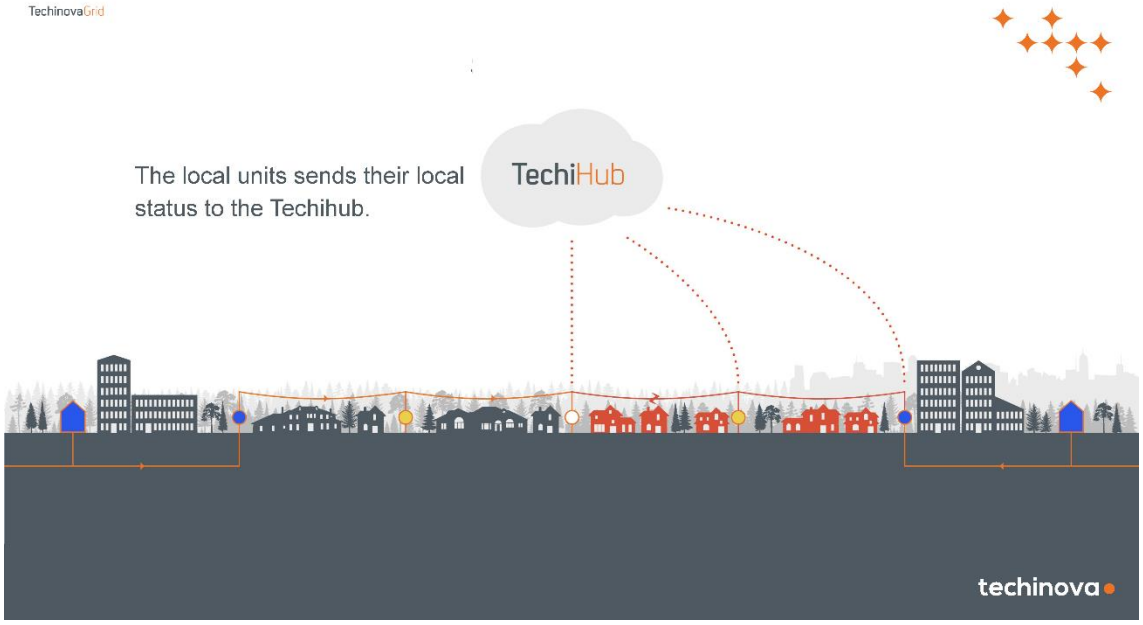
techinova

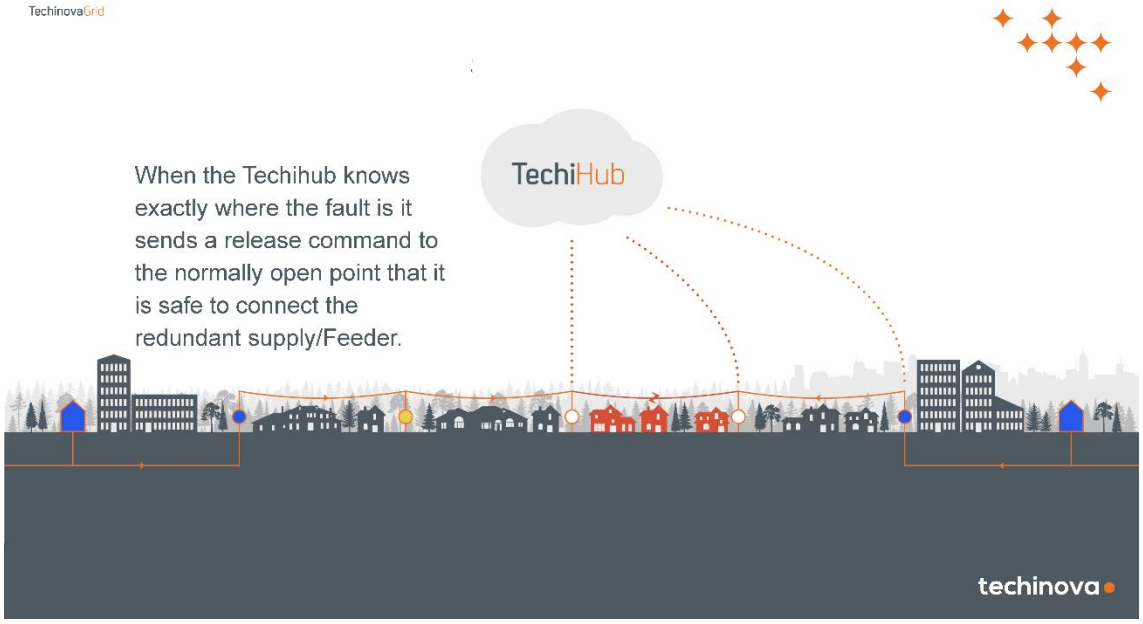
TechinovaGrid

How does it work?



techinova


TechinovaGrid
The local units sends their local status to the Techihub.
TechiHub
techinova

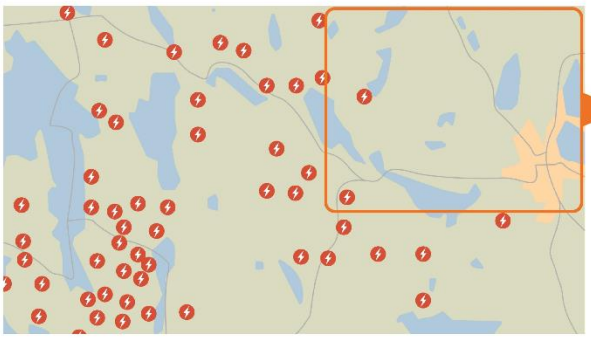

TechinovaGrid
When the Techihub knows exactly where the fault is it sends a release command to the normally open point that it is safe to connect the redundant supply/Feeder.
TechiHub
techinova

TechinovaGrid

Could be based on reclosers, substation breakers, disconnectors and swithes

techinova

TechinovaGrid



TechinovaGrid

- True example from the storm Alfrida / Aapeli (Januari 2019)
- The average amount of faults were reduced by approximately 80%.

techinova

TechinovaGrid

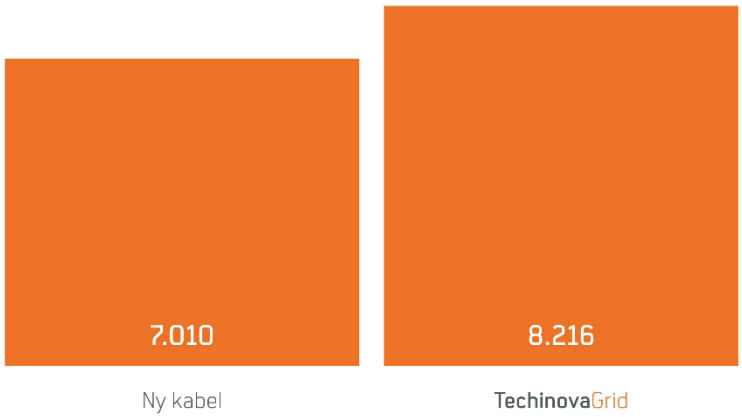
Reduced investment costs in Sweden due o automation
TechinovaGrid

techinova

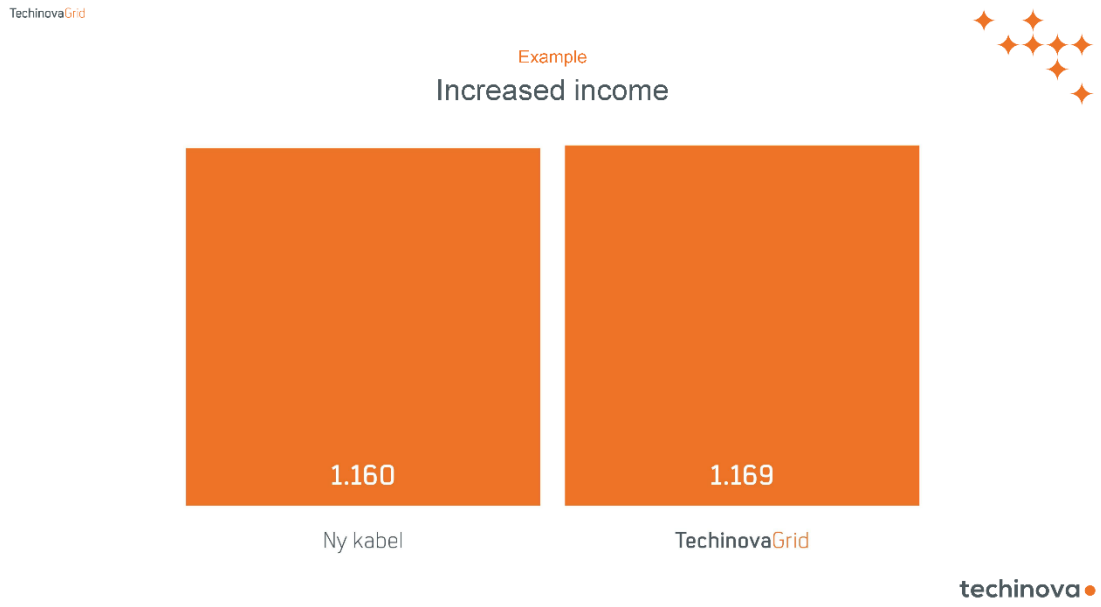
TechinovaGrid

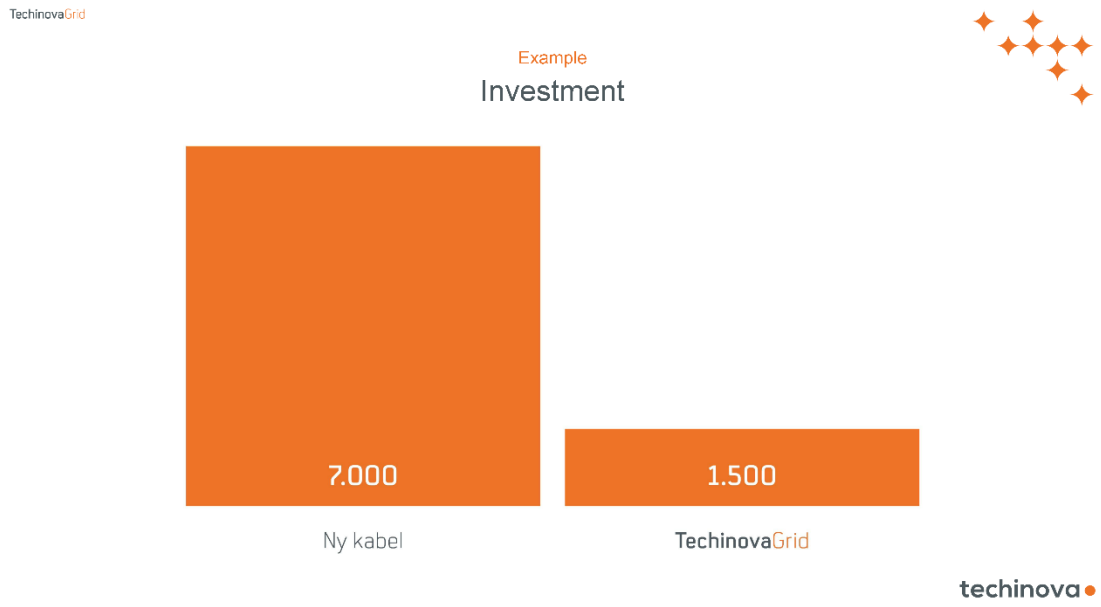
Example

Swedish earning model NUAK 2018



techinova

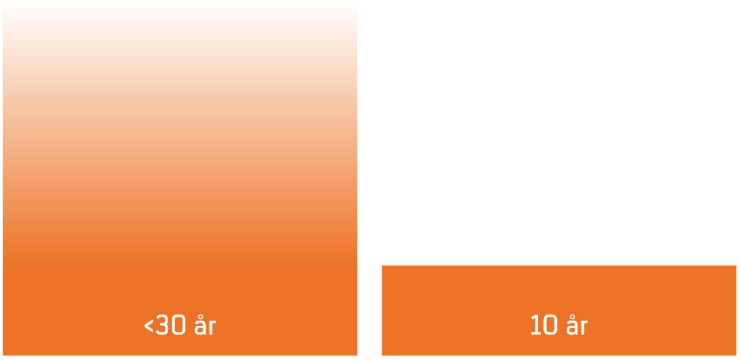

TechinovaGrid
Example
Increased income
1.160
1.169
Ny kabel
TechinovaGrid
techinova


TechinovaGrid
Example
Investment
7.000
1.500
Ny kabel
TechinovaGrid
techinova

TechinovaGrid

Example

Return of investment



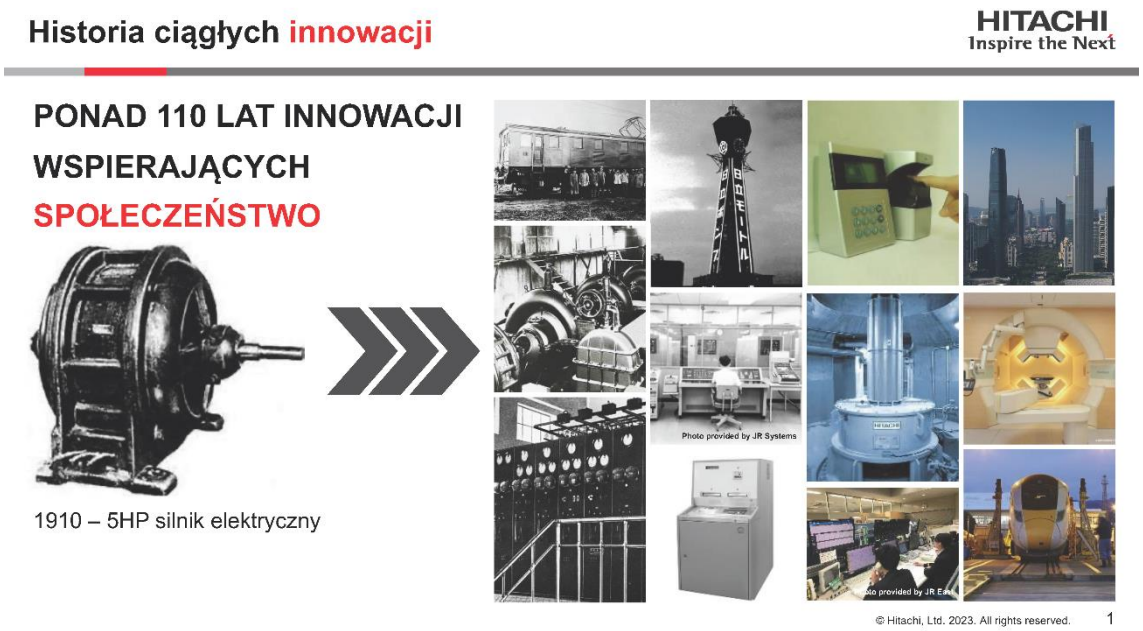
techinova

Dziękuję bardzo!

techinova

OPTYMALIZACJA NIEZAWODNOŚCI I WYDAJNOŚCI SIECI ENERGETYCZNYCH. KOMPLEKSOWE ROZWIĄZANIA IT DLA NOWOCZESNEJ ENERGETYKI

Łukasz Babiarz (Hitachi Energy)
Krzysztof Waszkiewicz (Hitachi Europe)



Hitachi aktywnie zmienia się, aby sprostać dzisiejszym potrzebom

HITACHI
Inspire the Next

Od 2009 roku HITACHI koncentruje się na …

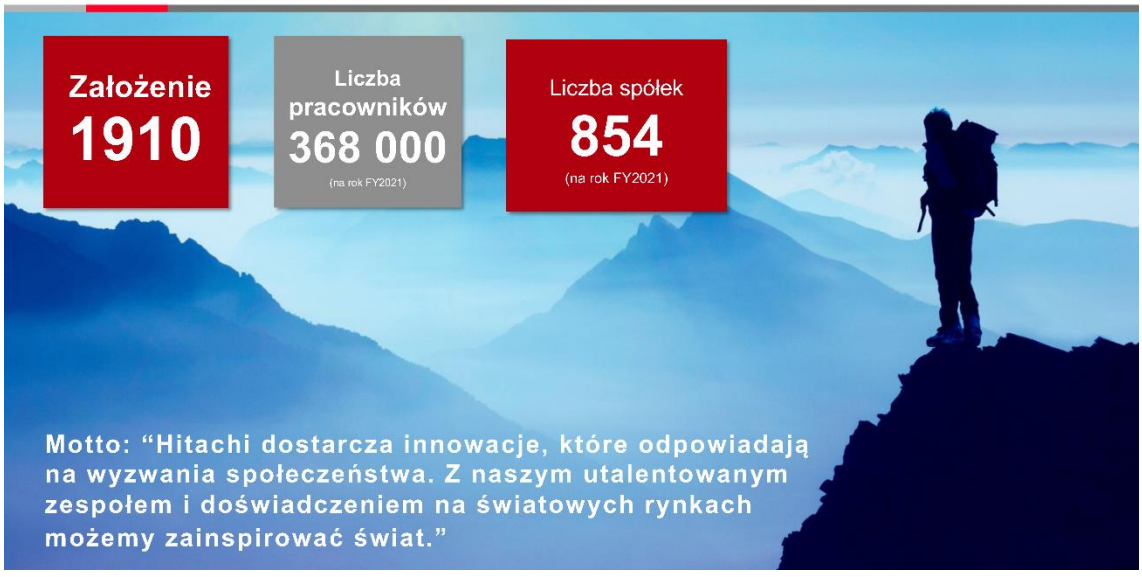
SOCIAL INNOVATION

Wprowadzanie innowacji i przekształcanie kluczowych elementów infrastruktury przyczynia się do zrównoważonego rozwoju społeczeństwa

 2

Grupa Hitachi

HITACHI
Inspire the Next



Optimize Asset Health and Replacement
Introducing Lumada APM Health

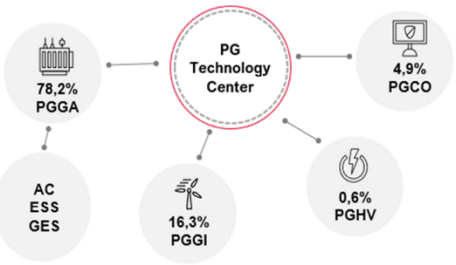
Hitachi Energy

Hitachi Energy - Technology Center in Krakow

HITACHI
Inspire the Next

Technology Center in Krakow is the largest single development unit of Hitachi Energy in the world that closely cooperates with all other business units in the field of:
- Development of new products and systems
- Digital solutions
- Software
- Cybersecurity

Lumada APM Suite applications developed in TC Krakow
- 100+ software engineers
- Local Customer Experience team
- Support from hardware SMEs
- Close cooperations with other product teams - PGTR, PGHV, PGGI



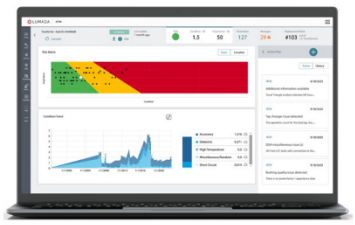
Different Nationalities on-board
18 different countries

Professionals
~554

Hitachi Energy

Lumada APM Suite

HITACHI
Inspire the Next



HEALTH RELIABILITY OPTIMIZATION

7

Hitachi Energy

APM Health users

HITACHI
Inspire the Next

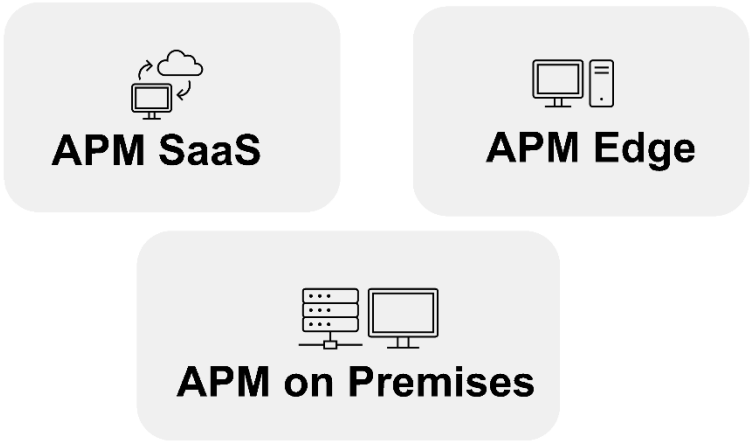
AMERICAN ELECTRIC POWER
Ameren
ENERGINET
TVA
CLP 中電

8

Hitachi Energy

APM Health installation options

HITACHI
Inspire the Next



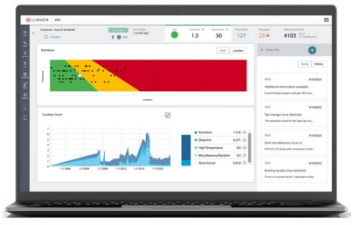
9

Hitachi Energy

Lumada APM: The health module

HITACHI
Inspire the Next

Visualize asset condition through data-driven modeling and prognostics.



Maximize availability
Monitor indicators, model asset degradation

Prevent catastrophic failure
Automated fault analysis via probability of failure (PoF)

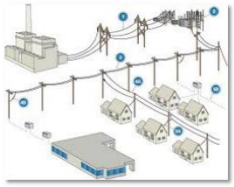
Predictive maintenance
Prescriptive recommendations

10

Hitachi Energy

Hitachi Energy's and Partner's APM Performance Models

HITACHI
Inspire the Next

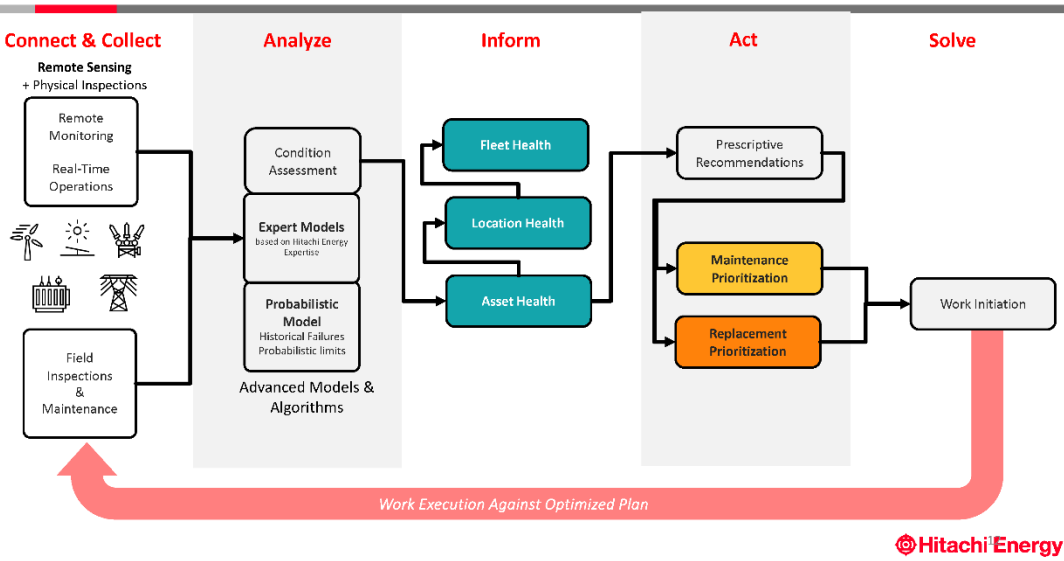
Substations	Transmission	Distribution	Generation
			
• Transformers • Breakers • Batteries • Surge Arresters • Capacitors • Instrument Transformers	Overhead Transmission Line models: • Towers/ Poles (wood, steel, composite, concrete) • Conductors • Static Wire (Shield Wire) models • Insulators UG cables • XLPE, PILC, HPFF, LPFF	• Reclosers • Switches • Network Transformers • Network Protectors Feeder Models • Hierarchical assets • Lines, Poles	• Pumps • Turbines • Motors / generators • Fans • Wind • Balance of Plant

Enables our customers to choose Hitachi models, partner models, or your own algorithms

Hitachi Energy

Lumada APM – an Optimized Strategic Asset Management

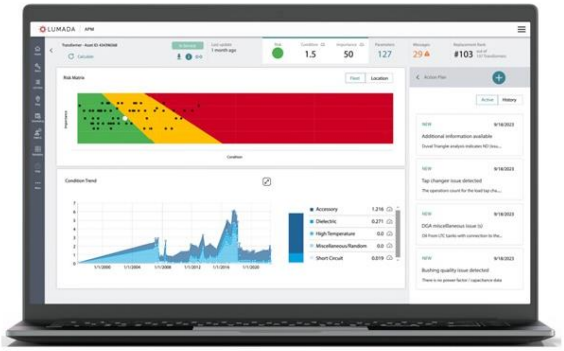
HITACHI
Inspire the Next



Hitachi Energy

DEMO

HITACHI
Inspire the Next



13

Hitachi Energy

Wprowadzenie

HITACHI
Inspire the Next

	Data Center stanowią podstawową infrastrukturę, na której opiera się era cyfrowa…		… i staje się infrastrukturą, która ma ogromny wpływ na zrównoważoną przyszłość
	2023	2030	
Użytkownicy sieci	5Bn	7Bn	Ograniczenie wykluczenia cyfrowego – powszechny dostęp do zasobów cyfrowych
Energia elektryczna	1%	8%	Wykładniczy wzrost zapotrzebowania na energię elektryczną – upowszechnienie technologii IoT oraz AI
Usługi Data Center	57GW	152GW	Globalny konsument energii elektrycznej
Emisja CO2	330 Mt CO2	Carbon Neutral (EU target)	Odpowiedzialność ESG dla zrównoważonej przyszłości dla nas wszystkich

 15

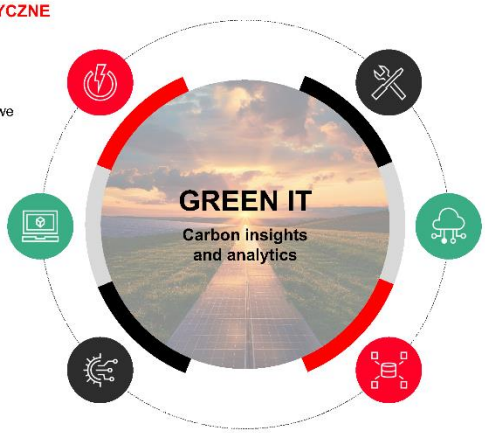
Kompleksowe rozwiązania IT dla nowoczesnej energetyki

HITACHI
Inspire the Next

ZASILANIE I URZĄDZENIA ENERGETYCZNE
- Optymalizacja strategii energetycznej
- Magazynowanie energii, źródła odnawialne
- Virtual Power Plants (VPPs)
- Transformatory, aparatura rozdzielcza, cyfrowe stacje elektroenergetyczne

INFRASTRUKTURA IT
- Energooszczędne zasoby IT
- Monitorowanie efektywności energetycznej i emisji dwutlenku węgla
- Alokacja obciążenia w czasie rzeczywistym
- Optymalizacja energetyczna obiektów

OPROGRAMOWANIE
- Optymalizacja emisji CO_2
- Green software development (DevOps)
- Cyberbezpieczeństwo



ARCHITEKTURA I INŻYNIERIA
- Projektowanie z myślą o niezawodności, odporności i zrównoważonym rozwoju
- Zarządzanie i racjonalizacja portfela aplikacji

STRATEGIE CHMUROWE
- Szczegółowe monitorowanie emisji gazów cieplarnianych
- Optymalizacja CO2 w chmurze (GreenOps)

ZARZĄDZANIE DANYMI
- Zarządzanie danymi w celu optymalizacji emisji CO2
- Zarządzanie cyklem życia danych
- Deduplikacja i kompresja danych
- Wirtualizacja i konsolidacja

 16

Kompleksowe rozwiązania IT dla nowoczesnej energetyki

HITACHI
Inspire the Next

Transformacja cyfrowa

ITOps
Niezrównana wydajność, niezawodność i bezpieczeństwo dostosowane do działalności, danych i usług klientów

AI/GenAI
Hitachi iQ: Zintegrowane portfolio rozwiązań AI, wbudowana inteligencja w chmurze hybrydowej, społeczność programistów GenAI Companions

Usługi konsultingowe
Nowoczesne rozwiązania IT dzięki ekosystemowi zintegrowanych niezależnych dostawców oprogramowania

Zarządzanie informacją

Zarządzanie danymi
Elastyczne rozwiązania zarządzania danymi

Data Protection, Governance
Zgodność danych, prywatność danych, bezpieczeństwo zarządzania cyklem życia danych i gwarancja nieusuwalności

AIOps
Automatyzacja i efektywność zasobów

Infrastruktura

Hybrydowa platforma udostępniania danych
Rozwiązania storage dla chmury hybrydowej

Zintegrowane rozwiązania
Nowoczesna architektura przechowywania danych

IaaS - EverFlex
Model IaaS zapewniający skalowalną infrastrukturę w chmurze hybrydowej, udostępniający zasoby na żądanie

 17

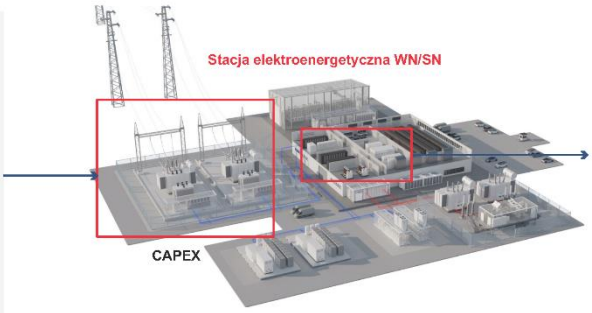
Kompleksowe rozwiązania IT dla nowoczesnej energetyki

HITACHI
Inspire the Next

Zintegrowane rozwiązania i usługi serwisowe

Projekt, dostawa, montaż i uruchomienie pełnego pakietu elektrycznego stacji elektroenergetycznej WN/SN

- Doradztwo w zakresie energetyki (badania)
- Projektowanie/inżynieria systemów
- Rozdzielnice WN
- Rozwiązania w zakresie jakości zasilania
- Transformatory
- Rozdzielnica SN
- System ochrony i kontroli
- Systemy pomiarowe
- Usługi pomocnicze
- Ochrona odgromowa
- Instalacja i uruchomienie



Kompletna i innowacyjna gama transformatorów dla niezawodnego i solidnego zasilania centrów danych

CAŁKOWITY KOSZT POSIADANIA W CAŁYM CYKLU ŻYCIA

- Usługi serwisowe

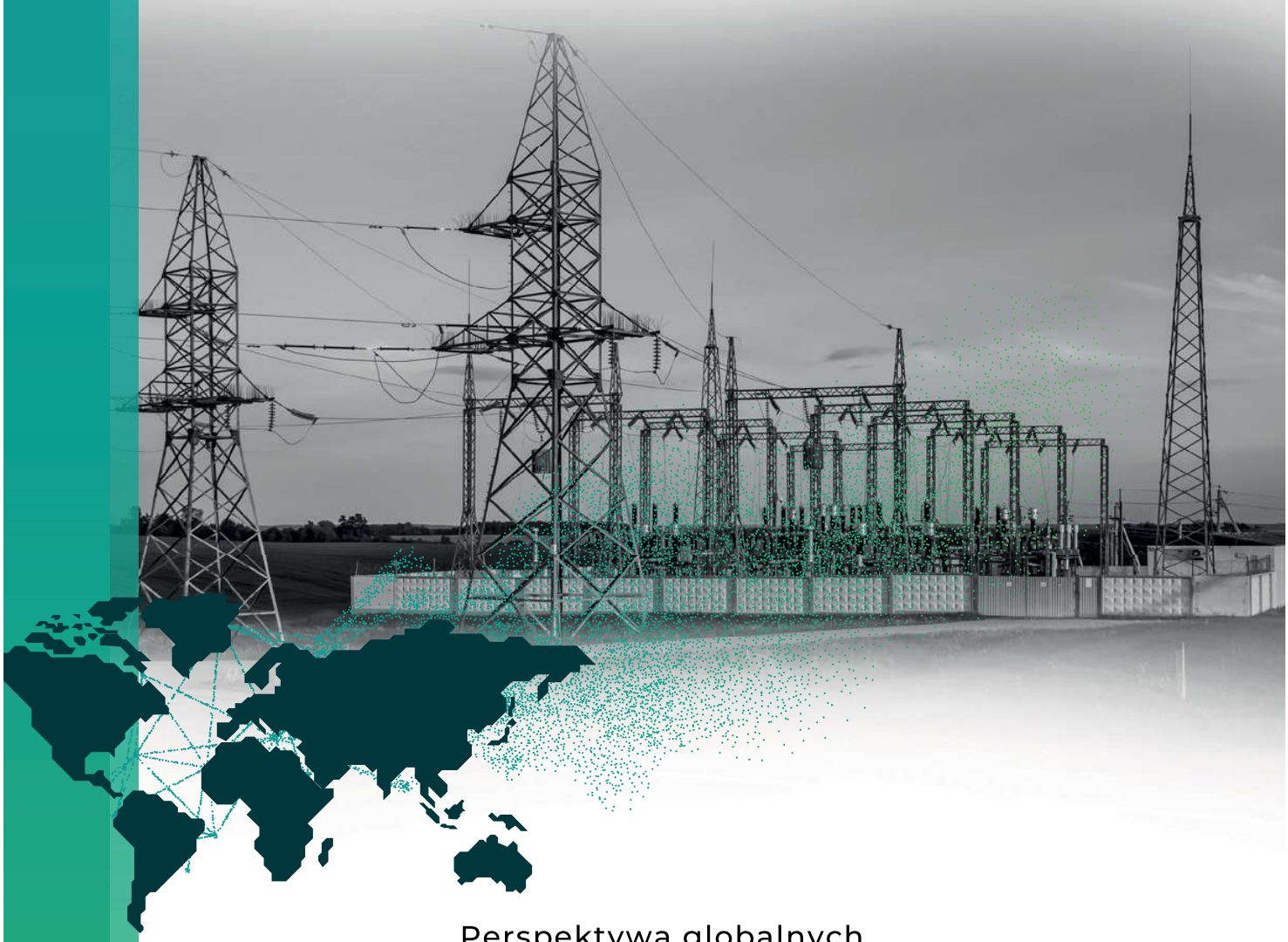
OPEX

 18


Hitachi Social Innovation is
POWERING GOOD

DRAGOS

apius TECHNOLOGIES



Perspektywa globalnych

zagrożeń elektroenergetycznych

info@dragos.com | www.dragos.com

spis treści

Podsumowanie wykonawcze

W 2000 roku Narodowa Akademia Inżynierii Stanów Zjednoczonych uznała elektryfikację rozległych sieci energetycznych za najważniejsze osiągnięcie inżynieryjne XX wieku. Jednak wraz ze wzrostem złożoności i znaczenia sieci energetycznych, stają się one coraz bardziej narażone na zaawansowane zagrożenia. Nowi aktorzy zagrażający—VOLTZITE, CHERNOVITE, KOSTOVITE, GANANITE, VANADINITE, RASPITE i PETROVITE—pojawili się, uzupełniając 11 grup, które Dragos monitoruje, a które mają na celu atakowanie lub są w stanie zaatakować organizacje sektora energetycznego. Dodatkowo, zmiany w krajobrazie geopolitycznym i technologicznym wprowadziły nowe zagrożenia i wektory ataków, na które obrońcy organizacji w sektorze energetycznym muszą zwrócić uwagę.

Od 2021 roku krytyczne i niespodziewane wydarzenia na świecie przekształciły krajobraz zagrożeń dla globalnego sektora energetycznego. Inwazja Rosji na Ukrainę w lutym 2022 roku była początkiem agresywnego połączenia ataków kinetycznych i cyberataków na infrastrukturę krytyczną, w tym zaawansowanych ataków złośliwego oprogramowania na operacje związane z energią elektryczną oraz wzrostu cyberataków ze strony hacktywistów kierowanych ideologią. Konflikt między Izraelem a Hamasem, który miał miejsce później w tym samym roku, odzwierciedlał podobne schematy, z rosnącą liczbą aktorów atakujących infrastrukturę energetyczną oraz operacjami cybernetycznymi wspierającymi ataki fizyczne. Te wydarzenia sugerują nową normę: infrastruktura krytyczna—włączając w to wszystkie aspekty związane z energią elektryczną—jest coraz bardziej zagrożona w kontekście konkurencji geopolitycznej.

Obok geopolitycznych zmian ewoluowała również natura cyberzagrożeń dla operacji związanych z energią elektryczną. Nastąpił znaczący wzrost liczby przeciwników, równolegle z eskalacją ich umiejętności i zasobów inwestowanych w ofensywne zdolności specyficzne dla systemów ICS. Analiza Dragos, opublikowana w marcu 2022 roku, wprowadziła PIPEDREAM oraz związaną z nim grupę zagrożenia CHERNOVITE jako siódmą rozpoznaną złośliwą aplikację zaprojektowaną specjalnie dla systemów ICS, wyróżniającą się modułowością i elastycznością. W 2023 roku uwaga skupiła się na VOLTZITE, nowo zidentyfikowanym, trwałym adwersarzu, który skoncentrował się na sektorze energetycznym. Techniki VOLTZITE podkreślają długotrwałe strategie angażowania, wykazując wysoką dbałość o bezpieczeństwo operacyjne oraz elastyczność w podejściu do komend i kontroli. Podobnie, ELECTRUM kontynuował znaczne inwestycje w swoje ofensywne zdolności ICS, czego dowodem są operacje w Ukrainie w 2022 roku.

Dodatkowo, zmiany technologiczne zmieniają pole walki dla obrońców w sektorze energetycznym. Segmenty dystrybucji i wytwarzania energii elektrycznej przechodzą istotne zmiany na całym świecie, co ma wpływ na operacje przesyłowe. Charakter wytwarzania energii zmienia się na DER w wielu krajach uprzemysłowionych, a przedsiębiorstwa dystrybucyjne coraz częściej integrują technologie "inteligentnej sieci", takie jak inteligentne liczniki czy inteligentne stacje podstacyjne. Chociaż te usprawnienia często wzmacniają odporność i wydajność sieci, wprowadzają również nowe, często słabo zrozumiane wektory ataków, które obrońcy muszą uwzględnić w swoich ocenach zagrożeń. Niniejsza Perspektywa Zagrożeń omawia niektóre z tych zmian technologicznych. Kluczowe jest, aby profesjonaliści zajmujący się bezpieczeństwem wyprzedzali te rozwijające się wyzwania, szczególnie gdy przeciwnicy atakujący sieć energetyczną nieustannie się doskonalą.

Pomimo wielu nieprzewidywalnych wydarzeń, wiele trendów utrzymało się zgodnie z prognozami z naszej poprzedniej Globalnej Perspektywy Zagrożeń dla Sektora Energetycznego. Na przykład, utrzymuje się stałe zagrożenie ze strony ransomware, napędzanego motywacjami finansowymi. Dragos odnotował niepokojący wzrost tempa, w jakim grupy ransomware są w stanie operacjonalizować nowe lub nawet zero-day exploity, stawiając je na poziomie porównywalnym z bardziej zaawansowanymi zagrożeniami. Ponadto, podatności w łańcuchu dostaw oraz zależność od zewnętrznych partnerów wciąż stanowią źródło ryzyka dla infrastruktury globalnego sektora energetycznego.

Jednakże cieszy fakt, że wysiłki mające na celu wzmocnienie bezpieczeństwa, szczególnie w sektorze energetycznym, nadal otrzymują uwagę i inwestycje. Historycznie, nacisk kładziono głównie na sieci IT przedsiębiorstw, nawet w sektorze energetycznym. Jednakże widoczna jest godna pochwały, ciągła zmiana w kierunku wzmacniania bezpieczeństwa OT. W Stanach Zjednoczonych odporność sieci energetycznych jest priorytetem, o czym świadczą aktualizacje przepisów NERC-CIP oraz ćwiczenia, takie jak GridEx, które zaplanowano na kolejną edycję w listopadzie 2023. Podobnie Unia Europejska również rozwija swoją agendę cyberbezpieczeństwa. W styczniu 2022 roku Europejska Sieć Operatorów Systemów Przesyłowych Energii Elektrycznej (ENTSO-E) wprowadziła swój Kodeks Sieci dotyczący Cyberbezpieczeństwa (NCCS). Kodeks ten, mający zostać wdrożony do stycznia 2024 roku, jest zgodny z nowymi przepisami UE dotyczącymi wewnętrznego rynku energii elektrycznej i dąży do harmonizacji protokołów cyberbezpieczeństwa dla transgranicznych przepływów energii elektrycznej. Na całym świecie podmioty w sektorze energetycznym inwestują coraz więcej w zwiększanie odporności na cyberzagrożenia i osiąganie pełnej widoczności operacyjnej.

Jednak zwiększona widoczność to miecz obosieczny. W miarę jak branża uzyskuje bezprecedensowy wgląd w swoje operacje, musi być świadoma i gotowa na wyzwania, które z tego wynikają. Niniejszy raport ma być przewodnikiem, oferującym przegląd zagrożeń dla globalnego sektora energetycznego na listopad 2023 roku. Dragos dąży do wyposażenia obrońców sektora energetycznego w wiedzę i kontekst potrzebne do skutecznej obrony poprzez analizę krajobrazu faza po fazie oraz dogłębną analizę istotnych studiów przypadku.

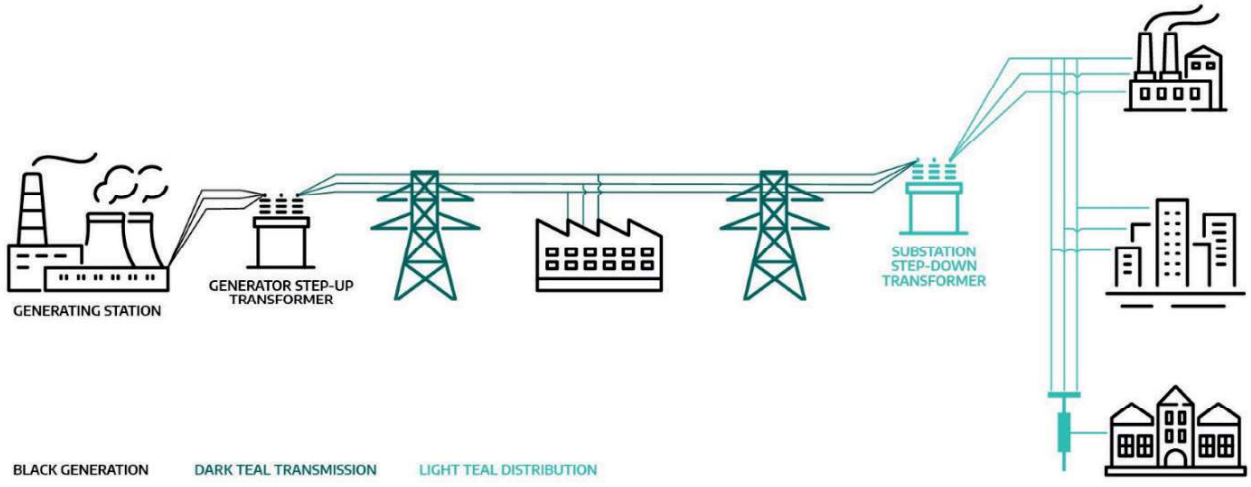
Kluczowe wnioski:

- Dragos monitoruje obecnie 18 aktywnych grup zagrożeń, które albo celują w sektor energetyczny, miały wpływ na organizacje w tym sektorze w przeszłości, albo mają zdolność wpływania na operacje energetyczne, co stanowi znaczny wzrost w porównaniu z 11 grupami w 2021 roku.
- Grupy zagrożeń monitorowane przez Dragos wykazują również rosnący poziom zaawansowania oraz inwestycji w możliwości specyficzne dla systemów ICS, czego dowodem są operacje ELECTRUM w Ukrainie w 2022 roku oraz publiczne ujawnienie i analiza PIPEDREAM w marcu 2022 roku, siódmego znanego złośliwego oprogramowania zaprojektowanego specjalnie dla ICS.
- Napięcia geopolityczne i zawirowania przyczyniły się do szybkich zmian w krajobrazie zagrożeń dla sektora energetycznego, ponieważ ma on bezpośrednie znaczenie dla bezpieczeństwa narodowego. Takie zmiany nadal stanowią źródło dynamizmu w krajobrazie zagrożeń cybernetycznych dla organizacji sektora energetycznego.
- Dragos ocenia z umiarkowaną pewnością, że segment przesyłowy nowoczesnej sieci energetycznej nadal pozostaje najbardziej prawdopodobnym celem przeciwników dążących do osiągnięcia szeroko zakrojonych efektów zakłócających.
- Chociaż generalnie solidny, atak cybernetyczny na DER (rozproszone wytwarzanie energii) stanowi coraz bardziej realny, choć słabo rozumiany, wektor ataku dla przeciwników. Dragos ocenia z wysoką pewnością, że w miarę wzrostu adopcji DER, prawdopodobieństwo skoordynowanych ataków cybernetycznych na te aktywa wzrośnie proporcjonalnie.
- Stosunkowo zdecentralizowany i rozproszony charakter nowoczesnego segmentu dystrybucji energii elektrycznej stwarza unikalne wyzwania związane z bezpieczeństwem. Ponadto operacje dystrybucyjne przechodzą zmiany technologiczne w związku z wprowadzaniem technologii "inteligentnej sieci", takich jak inteligentne liczniki czy inteligentne stacje podstacyjne, co wprowadza nowe i mniej zrozumiane wektory ataków.
- Ransomware pozostaje stałym zagrożeniem dla sektora energetycznego. Dragos zaobserwował znaczący wzrost w przypadku czołowych grup ransomware, które uzyskują lub wykorzystują podatności w publicznie dostępnych urządzeniach lub oprogramowaniu – taktyka zwykle kojarzona z bardziej tradycyjnymi, zaawansowanymi zagrożeniami.

Przegląd zagrożeń dla infrastruktury energetycznej

Często postrzegana jako jednolita całość, "sieć energetyczna" jest w rzeczywistości bardziej skomplikowanym i dynamicznym systemem. To seria sieci, które nieustannie ewoluują i dostosowują się do zmieniającego się krajobrazu energetycznego. System energetyczny składa się z wielu etapów, które zapewniają, że odpowiednia ilość energii wygenerowanej z różnych źródeł dociera do domów, firm i usług o kluczowym znaczeniu w użytecznej formie.

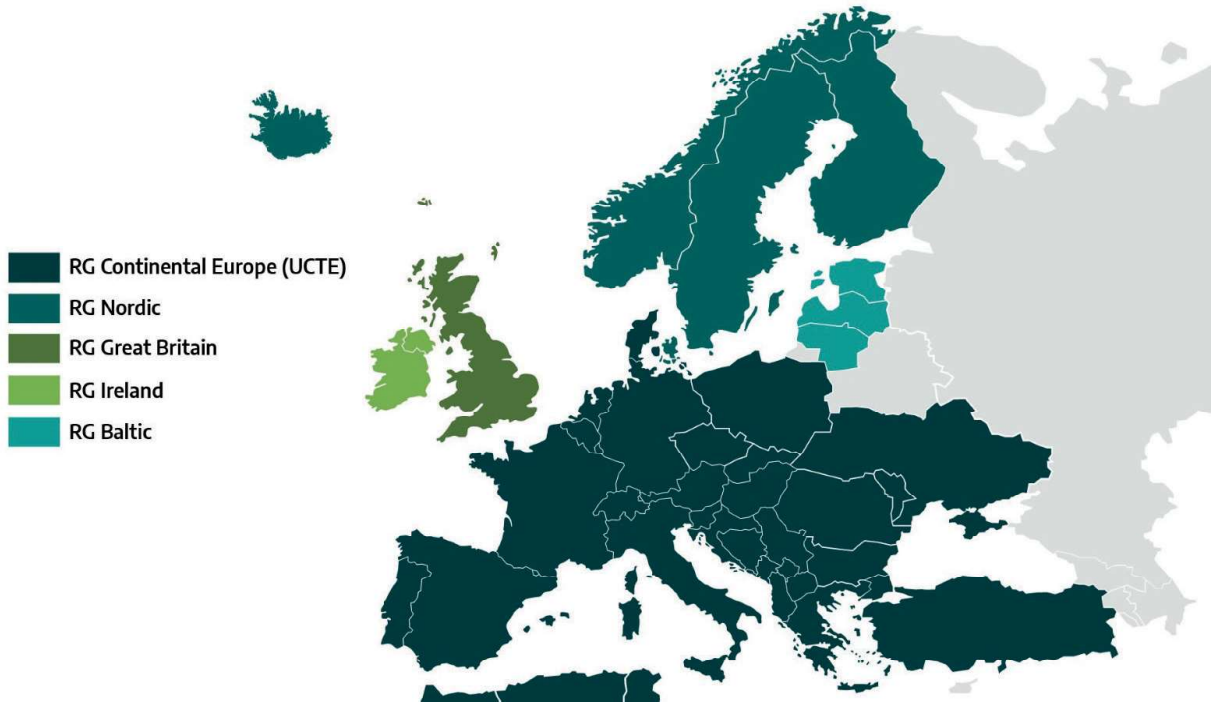
Głównymi elementami systemu energetycznego są wytwarzanie, przesył i dystrybucja. Wytwarzanie to proces produkcji energii z różnych źródeł, takich jak elektrownie jądrowe, węglowe, gazowe, słoneczne, wiatrowe oraz wodne. Gdy energia jest już wyprodukowana, musi zostać przetransportowana tam, gdzie jest potrzebna. Na początku robi to sieć przesyłowa, a następnie sieć dystrybucyjna. Linie przesyłowe wysokiego napięcia pełnią rolę autostrad energetycznych, transportując energię elektryczną na duże odległości. Stacje transformatorowe po drodze obniżają napięcie w miarę zbliżania się energii do miejsca docelowego. W momencie, gdy energia elektryczna zbliża się do obszarów mieszkalnych lub komercyjnych, wkracza w fazę dystrybucji. Na tym etapie transformatory obniżają napięcie do poziomu odpowiedniego dla domów i przedsiębiorstw. Ostatecznie rozprowadzona energia zasila nasze miasta, napędza przemysł i stymuluje innowacje. To przedstawia Rysunek 1 poniżej.



RYSUNEK 1 PRZEDSTAWIENIE FAZ PRZEPŁYWU ENERGII ELEKTRYCZNEJ W NOWOCZESNEJ SIECI ENERGETYCZNEJ

Geograficznie Ameryka Północna działa w oparciu o dwa główne, szerokie synchroniczne systemy sieci: Interkoneksję Wschodnią i Interkoneksję Zachodnią. Oprócz nich istnieją trzy mniejsze sieci: Interkoneksja Alaski, Interkoneksja Teksasu oraz Interkoneksja Quebecu. Te systemy zapewniają płynny przepływ energii elektrycznej na rozległych obszarach Ameryki Północnej. Interkoneksje Wschodnia, Zachodnia oraz Teksasu są połączone w różnych punktach za pomocą łączy prądu stałego (DC), co umożliwia przesył energii elektrycznej w obrębie kontynentalnych Stanów Zjednoczonych, Kanady oraz części Meksyku.

W Europie nadzór nad siecią energetyczną sprawuje Europejska Sieć Operatorów Systemów Przesyłowych Energii Elektrycznej (ENTSO-E). Obszar geograficzny objęty działalnością członkowskich Operatorów Systemów Przesyłowych (TSO) ENTSO-E jest podzielony na pięć obszarów synchronicznych oraz dwa systemy izolowane, mianowicie Cypr i Islandię. Obszary synchroniczne reprezentują grupy państw połączone swoją specyficzną infrastrukturą energetyczną. Do obszarów synchronicznych należą: Europa Kontynentalna, region nordycki, region bałtycki, Wielka Brytania oraz Irlandia-Północna Irlandia. Oprócz tych stałych grup, Komitet Operacji Systemowych zarządza dwoma dobrowolnymi grupami regionalnymi (RG): Europa Północna oraz Systemy Izolowane. Warto odnotować, że w 2022 roku Ukraina i Mołdawia połączyły swoje sieci energetyczne z obszarem synchronicznym Europy Kontynentalnej. Pięć synchronicznych grup regionalnych w Europie przedstawiono na Rysunku 2.



RYSUNEK 2 MAPA PIĘCIU OBSZARÓW SYNCHRONICZNYCH SIECI ENERGETYCZNYCH W EUROPIE

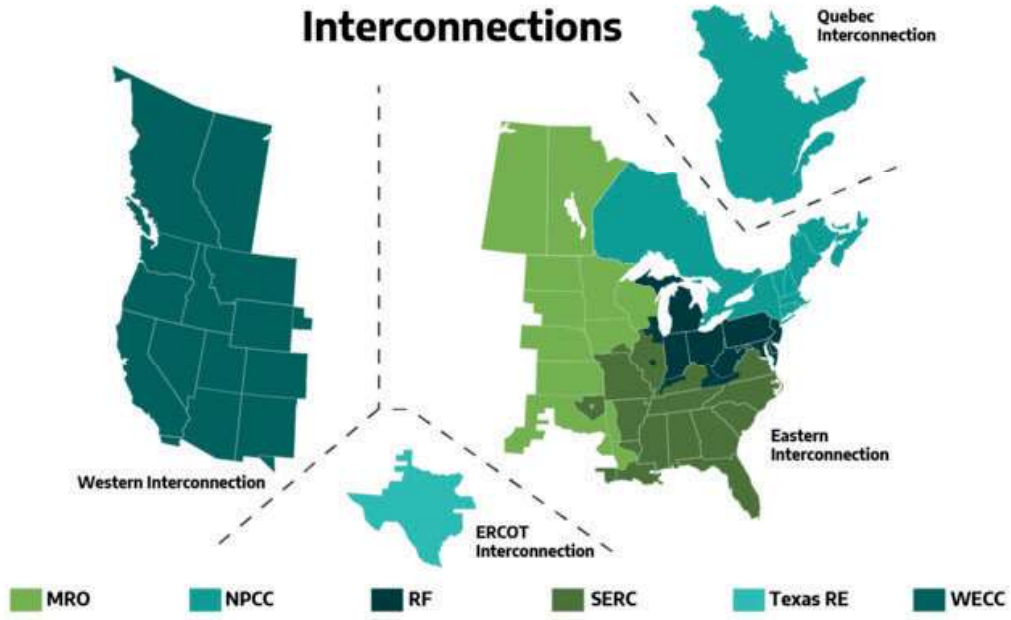
Australia natomiast operuje trzema odrębnymi systemami sieci energetycznych. Największy z nich to sieć wschodniego wybrzeża, która obsługuje Queensland, Nową Południową Walię, Australijskie Terytorium Stołeczne, Wiktorię, Australię Południową oraz Tasmanię, a jest połączona podmorskim kablem Basslink. Ta rozległa sieć jest znana jako National Electricity Market (NEM) i jest jednym z największych na świecie zintegrowanych systemów energetycznych. Poza NEM, Australia Zachodnia posiada własną sieć energetyczną, obejmującą Północno-Zachodni Zintegrowany System (NWIS) oraz Południowo-Zachodni Zintegrowany System (SWIS). Trzeci system sieciowy działa na Terytorium Północnym (NT) i składa się z trzech regulowanych sieci oraz ośmiu elektrowni, którymi zarządza Territory Generation.

Ogólnie rzecz biorąc, stan sieci energetycznej na kontynencie afrykańskim jest zróżnicowany. Historycznie, krajowe sieci energetyczne na tym kontynencie były silnie zmonopolizowane na wszystkich etapach produkcji i przesyłu energii, a znaczna część populacji wciąż nie ma dostępu do elektryczności. Jednak trwają nieustanne wysiłki na rzecz modernizacji. Generalnie, sieci energetyczne w Afryce można podzielić na pięć głównych sieci. W Afryce Północnej sieci energetyczne są zintegrowane w ramach Unii Maghrebu Arabskiego (AMU) za pośrednictwem Comité Maghrébin de l'Électricité (CME). Komitet ten został założony w celu koordynacji polityki energetycznej i działań liberalizacyjnych, zwłaszcza w odniesieniu do sieci przesyłowych państw członkowskich. Egipt odgrywa kluczową rolę, łącząc północnoafrykańską sieć z Bliskim Wschodem i Europą, poprzez połączenia z Jordanią oraz sieć między Marokiem a Hiszpanią.

Dalej na południe, Południowoafrykańska Wspólnota Energetyczna (SAPP) integruje infrastrukturę energetyczną państw członkowskich Wspólnoty Rozwoju Afryki Południowej (SADC), ułatwiając współdzielenie rynku energii w tym regionie. W Afryce Zachodniej Wspólnota Energetyczna Afryki Zachodniej (WAPP) działa pod auspicjami Wspólnoty Gospodarczej Państw Afryki Zachodniej (ECOWAS), starając się stworzyć niezawodną sieć energetyczną od momentu powstania w 2010 roku. Afryka Wschodnia jest połączona poprzez Wschodnioafrykańską Wspólnotę Energetyczną (EAPP), która wykorzystuje nadwyżki mocy w krajach członkowskich, aby zapewnić efektywny handel energią. Tymczasem Centralnoafrykańska Wspólnota Energetyczna (PEAC), lub Pool Energetique de L'Afrique Centrale, dąży do połączenia sieci energetycznych dziesięciu krajów Afryki Środkowej, co ma na celu usprawnienie wymiany energii między swoimi członkami.

Taka interkoneksja, będąca charakterystycznym elementem współczesnych systemów energetycznych, zwiększa niezawodność, umożliwiając przepływ energii przez różnorodne szlaki. Ponadto pełni funkcję ochronną, izolując potencjalne zakłócenia. Jednak wbudowana złożoność tych zintegrowanych systemów może stanowić wyzwanie dla odporności wobec zaawansowanych zagrożeń cybernetycznych.

Aby stawić czoła rzeczywistym wyzwaniom, przedsiębiorstwa energetyczne wdrażają różnorodne strategie łagodzenia skutków zakłóceń. Procesy wzajemnej pomocy są powszechne, umożliwiając dotkniętym zakłóconym podmiotom uzyskanie wsparcia od sąsiednich jednostek w przypadku przerw spowodowanych burzami, pożarami lub nawet cyberatakami. Partnerstwa regionalne wzmacniają tę solidarność, zapewniając stabilizację i szybkie odbudowy.



RYSUNEK 3 MAPA POŁĄCZEŃ SIECI ENERGETYCZNEJ W AMERYCE PÓŁNOCNEJ

Jeśli chodzi o regulacje, właściciele i operatorzy aktywów przesyłowych i generacyjnych w Ameryce Północnej przestrzegają standardów NERC-CIP. Meksyk współpracuje z NERC, jednocześnie mając własne ramy regulacyjne, zarządzane przez Komisję Regulacyjną Energii (Comisión Reguladora de Energía, CRE). Rysunek 1 powyżej przedstawia mapę połączeń sieci energetycznych w Ameryce Północnej. Na całym świecie regulacje różnią się, jednak wiele z nich jest zgodnych ze standardami Międzynarodowej Komisji Elektrotechnicznej (IEC) i Międzynarodowej Organizacji Normalizacyjnej (ISO). Unia Europejska opracowała swój program cyberbezpieczeństwa dla przedsiębiorstw energetycznych poprzez Kodeks Sieci dotyczący Cyberbezpieczeństwa. Australia wzmocniła swoje krajowe środki cyberbezpieczeństwa dla przedsiębiorstw energetycznych, szczególnie poprzez rozszerzony Akt o Bezpieczeństwie Infrastruktury Krytycznej z 2018 roku (SOCI Act), który nakłada obowiązek zgłaszania istotnych incydentów cybernetycznych, oraz Australijski Ramowy Program Cyberbezpieczeństwa Sektora Energetycznego (AESCSF), który integruje zarówno międzynarodowe standardy, jak i specyficzne dla Australii środki kontroli.

W istocie sieć energetyczna to nie tylko linie przesyłowe i stacje, ale świadectwo ludzkiej pomysłowości, połączenie technologii i strategii, które zapewnia, że społeczeństwa są zasilane i rozwijają się bez przeszkód.

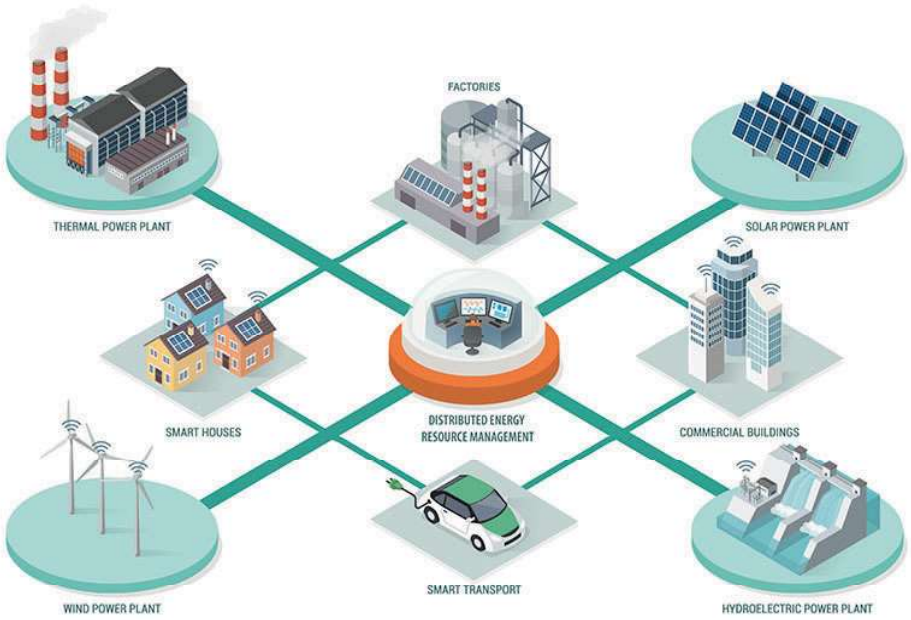
Segmenty operacyjne energii elektrycznej

GENERACJA

Krajobraz zagrożeń

Dragos monitoruje siedem grup zagrożeń, które stanowią specyficzne ryzyko dla aktywów generacyjnych: KOSTOVITE, CHERNOVITE, XENOTIME, GANANITE, STIBNITE, PETROVITE i WASSONITE. CHERNOVITE, twórca PIPEDREAM, posiada zaawansowane kompetencje w zakresie sieci OT, co może potencjalnie zakłócić funkcjonowanie elektrowni, jeśli otrzyma wystarczająco dużo czasu na rozwój. Naruszenie bezpieczeństwa przez XENOTIME w zakładzie petrochemicznym świadczy o jego zamiarach i możliwościach w sektorze ropy naftowej i gazu ziemnego. WASSONITE, aktywny od 2017 roku, zaatakował Elektrownię Jądrową Kudankulam w 2018 roku i regularnie wykorzystuje złośliwe oprogramowanie AppleSeed, koncentrując się na sektorach w Azji oraz sięgając do Ameryki Północnej. Warto zauważyć, że KOSTOVITE, PETROVITE, STIBNITE i GANANITE wszystkie atakowały lub naruszały bezpieczeństwo podmiotów operujących odnawialnymi źródłami energii.

Chociaż wiele z tych grup wykazało swoje zdolności w stosunku do bardziej tradycyjnej infrastruktury energetycznej, ostatnie trendy w sektorze energetycznym sugerują, że pole bitwy się zmienia. Znacząca transformacja może głęboko wpłynąć na charakter i skalę cyberataków na architekturę i dynamikę generacji energii. Historycznie rzecz biorąc, Dragos obserwował cyberataki na zasoby generacyjne, które były bardzo ukierunkowane i specyficzne dla danej lokalizacji. Ataki te nie miały na celu szeroko zakrojonego zakłócenia, częściowo ze względu na wyzwania związane z ich skalowalnością. Jednak globalny trend w kierunku rozproszonych źródeł energii (DER) – zdecentralizowanych, modułowych źródeł energii, takich jak energia wiatrowa lub słoneczna, które mogą działać niezależnie lub w połączeniu z główną siecią energetyczną – zmienia tę dynamikę. Szacuje się, że zdolność generacyjna DER wzrośnie o 322 procent w okresie od 2020 do 2025 roku, a ten trend prawdopodobnie utrzyma się do lat 30. XXI wieku, co oznacza znaczącą transformację architektury i dynamiki generacji energii w globalnej sieci energetycznej.



RYSUNEK 4 PRZEDSTAWIENIE SIECI ENERGETYCZNEJ ZINTEGROWANEJ Z ROZPROSZONYMI ŹRÓDŁAMI ENERGII

Część wytwórcza tradycyjnej sieci, ukształtowana przez ponad stulecie inwestycji rządowych, komunalnych i naukowych, działa na podstawie dobrze zrozumianych zasad zachowania opartych na fizyce i ogólnych modelach. System ten ma wbudowane właściwości samokorygujące, na przykład pozwalając na korektę generatorów wykazujących nieoptymalne działanie poprzez mechanizmy wewnętrzne sieci. W przeciwieństwie do tego, sieć oparta na rozproszonych źródłach energii (DER) działa inaczej. Zamiast scentralizowanej operacji energetycznej, rozproszony charakter instalacji DER wymaga silnego polegania na telekomunikacji, często z wykorzystaniem internetu, w celu zdalnego sterowania i monitorowania.

Ta transformacja ma swoje plusy i minusy. Z jednej strony DER zwiększa odporność sieci dzięki połączonym, mniejszym urządzeniom do generacji i magazynowania energii. Z drugiej strony naraża sieć na nowe cyberzagrożenia. Na przykład w przypadku tradycyjnego generatora łatanie oprogramowania jest starannie skoordynowanym procesem realizowanym na miejscu, natomiast w systemach DER sytuacja wygląda zupełnie inaczej. Poprawki mogą wymagać zastosowania w tysiącach zróżnicowanych systemów rozproszonych w różnych lokalizacjach, a proces łatania może być kontrolowany przez dostawców DER, a niekoniecznie przez operatorów sieci. Taki szeroko zakrojony i potencjalnie zdecentralizowany proces łatania niesie za sobą większe ryzyko błędów i nieporozumień, zwiększając szanse na to, że luki w systemach DER pozostaną niezałatane. Wymaga to również, aby aktywa DER były w pewnym stopniu połączone z siecią w celu otrzymania poprawek, co powiększa potencjalną powierzchnię ataku.

Dodatkowo, wzrost globalnej adopcji zielonej energii, w tym odnawialnych źródeł takich jak energia słoneczna, wiatrowa i wodna, sprawia, że powiązane systemy sieci energetycznych, magazynów energii i inteligentnych technologii stają się coraz bardziej atrakcyjnym celem dla cyberataków. Ostatnim przykładem, choć nie do końca adekwatnym, jest CVE-2023-23333, prosta luka polegająca na wstrzyknięciu komend w zestaw rozwiązań monitorujących dla małych i średnich

instalacji fotowoltaicznych. Z setkami takich rozwiązań dostępnych online w momencie ujawnienia podatności, stanowią one potencjalne słabe ogniwo. Chociaż obecnie udane przejęcie kontroli nad kilkoma systemami monitorującymi jednostki DER może wydawać się nieistotne z punktu widzenia operacji sieci, skoordynowany cyberatak na wiele systemów DER lub na systemy kontrolujące je mógłby być katastrofalny. Co więcej, potencjalne szkody wynikające z udanego ataku zależą od charakteru podatnego urządzenia, sieci, do której urządzenie jest zintegrowane, oraz kreatywności i śmiałości przeciwnika.

Jak wskazuje ostatni raport Departamentu Energii, wraz z rozwojem wdrażania DER, nawet 30-procentowe przejęcie w stosunku do szczytowego obciążenia zaczyna wykazywać konsekwencje na poziomie całej sieci. Ataki te byłyby szczególnie niszczące, jeśli byłyby skoordynowane z momentami, w których przejęte DER zmusiłyby sprzęt sieciowy do pracy poza zakresem jego zamierzonego działania. Wraz z ciągłym rozwojem umiejętności cyberatakujących i ich koncentracją na nowych systemach, zagrożenie dla DER prawdopodobnie będzie rosło w czasie. W obliczu tych zmieniających się wyzwań kluczowe jest priorytetowe traktowanie opracowywania metodologii badań ryzyka cybernetycznego związanych z DER. Poprawa higieny cybernetycznej, regularne aktualizacje systemów i intensywne monitorowanie są niezbędne, aby zapewnić bezpieczeństwo i funkcjonalność przyszłej infrastruktury zielonej energii.

Ocena

Pojawienie się DER oznacza zmianę paradygmatu w globalnym krajobrazie generacji energii, oferując zarówno większą odporność, jak i nowe podatności. W miarę jak zasoby generacyjne ewoluują od scentralizowanych, dobrze rozumianych systemów do zdecentralizowanej, połączonej sieci DER, krajobraz zagrożeń cybernetycznych jednocześnie się rozszerza. Grupy zagrożeń, takie jak ELECTRUM, CHERNOVITE i XENOTIME, które wcześniej koncentrowały się głównie na tradycyjnej infrastrukturze energetycznej, mogą zacząć wykorzystywać nowe podatności, korzystając z ogromnej skali i rozproszenia systemów DER. Dodatkowo, złożoność i wyzwania związane z monitorowaniem i łatanie tysięcy zróżnicowanych instalacji DER czynią je atrakcyjnymi celami. Dragos ocenia z wysoką pewnością, że w miarę wzrostu wdrażania DER, prawdopodobieństwo skoordynowanych cyberataków na te zasoby wzrośnie proporcjonalnie.

Dziś stoimy na rozdrożu, gdzie szybki rozwój DER przekształca oblicze generacji energii. Z jednej strony, zdecentralizowana natura DER obiecuje większą odporność; z drugiej strony, otwiera „puszkę Pandory" nowych podatności. Te znormalizowane technologie mogą być mieczem obosiecznym. Jeśli przeciwnicy, nieustannie rozwijający swoje umiejętności, zidentyfikują powszechną lukę, mogliby teoretycznie zdestabilizować całe krajowe sieci energetyczne. Ważne jest, aby zrozumieć, że te wyzwania nie są tylko problemem przyszłości; są to bezpośrednie zagrożenia. Przeciwnicy nie czekają na idealne okazje, lecz je tworzą. W miarę jak stają się coraz bardziej śmiali, bycie jedynie reaktywnym jest strategią skazaną na porażkę.

Równolegle z prognozowanym wzrostem mocy DER do lat 30. XXI wieku, zagrożenie dla tradycyjnych zasobów generacyjnych nie zmniejsza się. Dragos przewiduje, że aktorzy zagrożeń, tacy jak CHERNOVITE, będą nadal inwestować zasoby w zrozumienie i wykorzystywanie sieci OT oraz procesów. Wraz z zacieraniem się granic między operacjami fizycznymi a cyfrowymi, zasoby generacyjne pozostają istotnym celem. Rozszerzająca się adopcja narzędzi cyfrowych i interfejsów w operacjach stwarza wiele punktów wejścia dla potencjalnych cyberataków. Dlatego utrzymanie rygorystycznej i adaptacyjnej postawy bezpieczeństwa, połączone z współpracą międzysektorową i wymianą informacji, jest kluczowe dla zapobiegania i łagodzenia wieloaspektowych zagrożeń, które nas czekają.

PRZESYŁ

Krajobraz zagrożeń

Spośród 18 grup zagrożeń monitorowanych przez Dragos, które stanowią ryzyko dla sektora energetycznego, dwie grupy stanowią bezpośrednie i specyficzne zagrożenie dla operacji przesyłowych: ELECTRUM i KAMACITE. KAMACITE regularnie celuje w infrastrukturę krytyczną i sektory przemysłowe, odgrywając kluczową rolę w operacjach, takich jak zakłócenia zasilania w Ukrainie w latach 2015 i 2016. Choć KAMACITE, zgodnie z ocenami Dragos, nie przeprowadził bezpośrednich zakłóceń systemów ICS, jego główną rolą było umożliwienie innym podmiotom, zwłaszcza ELECTRUM, przygotowanie się do zaawansowanych destrukcyjnych ataków. Taka strategia współpracy, gdzie KAMACITE specjalizuje się w dostępie początkowym, a ELECTRUM w realizacji ataków, podkreśla synergistyczne zagrożenie, jakie wspólnie stwarzają dla operacji przesyłowych w sektorze energetycznym.

Segment przesyłowy współczesnej sieci energetycznej w wielu aspektach stanowi „klejnot w koronie", jeśli chodzi o potencjalny efekt zakłócenia, który mógłby wynikać z udanego ataku. Jest on kluczowym elementem sieci, łączącym generację energii z jej konsumpcją. Segment przesyłowy utrzymuje delikatną równowagę między podażą a popytem na energię elektryczną, co jest kluczowe z powodu ograniczeń technologicznych związanych z obecną zdolnością do przechowywania energii na dużą skalę. Działa jak centralny układ nerwowy sieci, szybko dostosowując przepływy na podstawie bieżących potrzeb, zapewniając nieprzerwane dostawy energii i zapobiegając potencjalnym awariom na szeroką skalę. Dlatego segment przesyłowy przyciąga znaczną uwagę cyberprzestępców, którzy dążą do osiągnięcia zakłóceń o dużym zasięgu, i jest najbardziej prawdopodobnym celem takich ataków w przyszłości.

Złożoność współczesnej sieci energetycznej wymaga, aby atakujący starannie dobierali i dostosowywali swoje strategie do specyficznych celów. Sieć dystrybucyjna nie jest idealnym celem ataku zakłócającego, ponieważ wymagałaby kompromitacji wielu stacji rozdzielczych, które mogą być pod kontrolą różnych przedsiębiorstw energetycznych. Przykładem tego jest pierwszy udany cyberatak na sieć energetyczną, który wywołał fizyczne skutki w 2015 roku w Ukrainie, koncentrując się na części systemu dystrybucyjnego. Atak ten spowodował przerwy w dostawie prądu dla około 225 000 klientów na kilku obszarach, trwające przez kilka godzin. Chociaż atak prawdopodobnie osiągnął swój cel, wymagał, aby ELECTRUM naruszyło trzy różne ukraińskie przedsiębiorstwa energetyczne, w połączeniu z ręcznymi regulacjami sprzętu elektrycznego – metodologia ta była trudna do zautomatyzowania i miała ograniczoną skalowalność. Ponadto kompromitacja wielu podmiotów zwiększa ryzyko wykrycia i zneutralizowania działań przeciwników.

W porównaniu do tego, chociaż etap generacji energii może wydawać się bardziej atrakcyjnym celem, wiąże się z wieloma wyzwaniami. Elektrownie opierają się na bardzo skomplikowanych i specyficznych dla danego miejsca procesach, są obsługiwane przez całą dobę i wyposażone w liczne środki ochrony, w tym systemy bezpieczeństwa fizycznego, co sprawia, że ataki na nie są znacznie trudniejsze. Dodatkowo, nawet jeśli zasób generacyjny zostanie naruszony, jego zdolność może być szybko przywrócona. Przykładem tego była eksplozja na Cyprze w 2011 roku, kiedy elektrownia Vassilikos o mocy 767 megawatów (MW), która dostarczała 60 procent mocy na wyspie, została zniszczona. Pomimo izolacji sieci energetycznej Cypru, kraj szybko zaspokoił zapotrzebowanie na energię dzięki rozproszonej generacji dostarczanej przez Izrael i Grecję.

Dla atakującego, który równoważy wyzwania i złożoność ataku z jego potencjalnym wpływem, sieć przesyłowa jest najbardziej logicznym celem. Oferuje możliwość szeroko zakrojonej, kaskadowej destabilizacji, stwarzając jednocześnie najmniej przeszkód dla atakującego. Co więcej, stacje przesyłowe często są bezobsługowe i zlokalizowane w odizolowanych, niezamieszkałych regionach. Historia potwierdza tę obserwację – 11 z 14 najbardziej dotkliwych przerw w dostawach energii elektrycznej od 1965 roku, pod względem liczby dotkniętych osób, wynikało bezpośrednio z awarii w segmencie przesyłowym sieci, zazwyczaj spowodowanych niespodziewanym wyłączeniem jednej lub więcej linii przesyłowych wysokiego napięcia podczas okresów dużego obciążenia sieci.

Przeciwnicy są doskonale świadomi krytycznego znaczenia sieci przesyłowej, co potwierdza ewolucja ataków skierowanych na sieci energetyczne. Rok po ataku na zakłady dystrybucyjne w Ukrainie w 2015 roku, ELECTRUM zorganizował atak na stację przesyłową w Pivnichnej, Ukraina. Chociaż skutki były mniej wyraźne niż w przypadku incydentu z 2015 roku, analiza Dragos przypisuje to nie ograniczeniu zakresu ataku, lecz błędom technicznym ELECTRUM. Udany atak mógł spowodować znaczne zniszczenia, potencjalnie prowadząc do przerw w dostawach energii dla nawet dwóch milionów klientów, według niektórych szacunków.

W kwietniu 2022 roku, w trakcie trwającej wojny rosyjsko-ukraińskiej i miesiąc po strategicznym odłączeniu Ukrainy od rosyjskiej sieci energetycznej i połączeniu z siecią synchroniczną Europy Kontynentalnej, ELECTRUM przeprowadził trzeci ukierunkowany atak na sieć energetyczną Ukrainy. Zamiast ponownie atakować zakłady dystrybucyjne, ELECTRUM postanowił spróbować naprawić błędy swojego ataku z 2016 roku na system przesyłowy. Chociaż według publicznych raportów ten atak się nie powiódł, analiza Dragos wskazała na nieustanne zaangażowanie ELECTRUM w doskonalenie swoich umiejętności w manipulowaniu i zakłócaniu procesów przesyłowych.

Co więcej, począwszy od października 2022 roku i trwając aż do początku 2023 roku, rosyjskie wojsko przeprowadziło brutalną i długotrwałą kampanię wymierzoną w zasoby energetyczne Ukrainy, która zbiegła się z początkiem zimy w Europie Wschodniej. Większość ataków była skierowana na stacje przesyłowe wysokiego napięcia zlokalizowane w centralnej i zachodniej Ukrainie, podczas gdy wiele kluczowych aktywów generacyjnych pozostało nietkniętych, mimo że ich lokalizacje były znane i statyczne. Kampania ta prawdopodobnie stanowiła skoordynowaną próbę rosyjskiego wojska, aby wywołać katastrofalny upadek całej ukraińskiej sieci, wymagający technicznie trudnego „black-startu" (ponownego uruchomienia sieci). Bohaterskie wysiłki ukraińskich techników zapobiegły jednak tej katastrofie. Co więcej, strategia atakowania stacji przesyłowych była wspierana przez głęboką wiedzę rosyjskich inżynierów elektrycznych na temat ukraińskiej sieci i jej podatności. To dodatkowo podkreśla kluczowe znaczenie segmentu przesyłowego dla stabilności sieci i dostarcza kontekstu do ciągłych inwestycji ELECTRUM w rozwijanie swoich narzędzi i umiejętności.

Ocena

Historyczne dowody wspierają umiarkowaną ocenę Dragos, że segment przesyłowy będzie głównym celem cyberprzestępców dążących do spowodowania szeroko zakrojonych katastrofalnych szkód w przyszłości. Chociaż historyczne zapisy świadczą o odporności współczesnej sieci energetycznej oraz o wyzwaniach związanych z przeprowadzeniem skutecznego ataku zakłócającego, pokazują również zdolność przeciwników do adaptacji taktyk oraz ich gotowość do cynicznego ignorowania wpływu na ludzkie życie.

Dla obrońców sieci operatorów systemów przesyłowych ta analiza jest zarówno ostrzeżeniem, jak i wezwaniem do działania. Z racji swojej natury i znaczenia segment przesyłowy pozostaje w centrum uwagi zdecydowanych i zaawansowanych technicznie aktorów cyberzagrożeń. Historia ukazuje siłę i odporność współczesnych systemów energetycznych, ale również podkreśla zdolność przeciwników do adaptacji i ich śmiałość. Oznacza to, że nasze strategie obronne nie mogą pozostawać statyczne. Musimy nieustannie innowować, uczyć się na podstawie przeszłych incydentów i przygotowywać na nieznane taktyki. Potencjalne koszty ludzkie udanego ataku, na co wskazuje dotychczasowa ignorancja przeciwników wobec życia, sprawiają, że ta misja jest nie tylko wyzwaniem technicznym, ale także głęboko moralnym obowiązkiem.

DYSTRYBUCJA

Krajobraz zagrożeń

Sieć dystrybucyjna, odmienna od segmentu przesyłowego, stoi w obliczu unikalnych wyzwań wynikających ze swojej zdecentralizowanej struktury. Badania rynkowe wskazują, że na całym świecie przypada około siedem przedsiębiorstw dystrybucyjnych na każdego operatora systemu przesyłowego. Niestety, zdecentralizowana natura tych sieci często oznacza, że wiele przedsiębiorstw dystrybucyjnych nie dysponuje odpowiednimi zasobami na zapewnienie pełnej ochrony cybernetycznej, co utrudnia im korelację informacji wywiadowczych i identyfikację zbiorowych zagrożeń. Ta podatność jest dodatkowo pogłębiona przez mniej rygorystyczny nadzór w wielu krajach, gdzie przedsiębiorstwa dystrybucyjne często unikają rygorystycznych wymogów cyberbezpieczeństwa, które są nakładane na ich odpowiedniki w sektorze przesyłowym. Badania sugerują, że przedsiębiorstwa objęte bardziej rygorystycznym nadzorem regulacyjnym doświadczają mniej przerw w dostawach energii, co może wskazywać na podobny związek w zakresie przestrzegania wymogów cyberbezpieczeństwa. Ponadto pojawienie się technologii takich jak inteligentne liczniki wprowadza nowe i mniej zrozumiane podatności, co poszerza powierzchnię ataku i stwarza wyzwania, które wymagają pilnej uwagi w celu ochrony infrastruktury energetycznej.

Obecnie Dragos monitoruje większą liczbę grup zagrożeń, które wcześniej atakowały lub obecnie atakują przedsiębiorstwa dystrybucyjne w porównaniu do tych skupiających się na operacjach przesyłowych. W szczególności Dragos śledzi 11 grup zagrożeń, które stanowią zagrożenie dla przedsiębiorstw dystrybucyjnych: VOLTZITE, KOSTOVITE, TALONITE, VANADINITE, MAGNALLIUM, PARISITE, DYMALLOY, ELECTRUM, KAMACITE, STIBNITE oraz XENOTIME.

Dodatkowo, spośród grup ransomware, które Dragos monitoruje i które wpłynęły na podmioty sektora energetycznego, większość dotknęła małe i średnie przedsiębiorstwa dystrybucyjne o charakterze miejskim lub regionalnym. Obserwowany trend prawdopodobnie wynika z większej liczby przedsiębiorstw dystrybucyjnych w porównaniu do operatorów przesyłu lub właścicieli zasobów generacyjnych. Ponadto nierównomierne wdrażanie środków bezpieczeństwa cybernetycznego w tych licznych przedsiębiorstwach dystrybucyjnych stwarza wiele możliwości dla złośliwych aktorów.

Na całym świecie przedsiębiorstwa dystrybucyjne wykazują znaczne zróżnicowanie pod względem inwestycji i nadzoru nad cyberbezpieczeństwem. Chociaż ogólne dyrektywy UE próbują zapewnić jednolitość w Europie, krajowe adaptacje prowadzą do różnic w środkach cyberbezpieczeństwa między państwami członkowskimi. Podobnie w Australii, pomimo wytycznych Australian Cyber Security Centre, różnice na poziomie stanowym wprowadzają niespójności w praktykach cyberbezpieczeństwa wśród przedsiębiorstw. Sytuacja w Stanach Zjednoczonych

jest bardziej rozproszona, ponieważ przedsiębiorstwa dystrybucji energii elektrycznej regulowane na poziomie stanowym są zazwyczaj zwolnione z przestrzegania przepisów NERC-CIP i często przyjmują federalne wytyczne, takie jak te od DOE (Departament Energii) i CISA (Agencja Cyberbezpieczeństwa i Infrastruktury), na zasadzie dobrowolnej, co prowadzi do różnorodnych zestawów standardów. Tymczasem połączona sieć energetyczna Rady Współpracy Zatoki Perskiej (GCC) nie przekłada się na jednolite regulacje dotyczące cyberbezpieczeństwa; kraje członkowskie, mimo wspólnych obaw związanych z przeszłymi zagrożeniami cybernetycznymi, wykazują różny poziom dojrzałości swoich ram bezpieczeństwa cybernetycznego, a niektóre z nich opierają się na międzynarodowych współpracach w celu wzmocnienia ochrony.

Heterogeniczność regulacji, inwestycji i praktyk w zakresie cyberbezpieczeństwa wśród przedsiębiorstw dystrybucyjnych na całym świecie stwarza dogodne warunki dla mniej zaawansowanych, oportunistycznych cyberprzestępców. Ta niespójność umożliwia operatorom ransomware, znanym z szerokiego poszukiwania podatnych systemów, liczne okazje do odnalezienia słabych punktów. Podobnie, brokerzy dostępu, dążący do zarabiania na dostępach do systemów, mogą wykorzystywać regiony, gdzie standardy bezpieczeństwa cybernetycznego są mniej rygorystyczne lub słabo wdrożone. Chociaż tacy aktorzy mogą nie mieć zaawansowanych umiejętności porównywalnych z przeciwnikami sponsorowanymi przez państwa, nadal mogą powodować poważne zakłócenia z powodu fragmentarycznego charakteru standardów bezpieczeństwa. Brak jednolitości nie tylko stwarza luki w zabezpieczeniach, ale także utrudnia skoordynowaną odpowiedź, co dodatkowo zwiększa ryzyko stwarzane przez tych aktorów.

Dodatkowo, komplikacje wynikające z tego zróżnicowanego krajobrazu regulacyjnego pogłębia integracja nowych technologii z siecią energetyczną. Innowacje, mimo że mają na celu modernizację i poprawę efektywności infrastruktury energetycznej, wprowadzają również nowe podatności. Przykładem jest rosnąca adopcja inteligentnych liczników. Badania Oregon State University College of Engineering ujawniły, że urządzenia te, centralne dla zaawansowanej infrastruktury pomiarowej (AMI), mają teoretyczne podatności, które mogłyby zostać wykorzystane do destabilizacji przesyłu energii w skali całej sieci. Chociaż obecnie te podatności mają głównie charakter akademicki, historia pokazuje, że przeciwnicy potrafią dostosować się i często wykorzystują nowe technologie w nieprzewidywalny i innowacyjny sposób. Dla obrońców kluczowe jest przewidywanie takich zmian. Równowaga między innowacją a bezpieczeństwem staje się coraz bardziej krucha, co wymaga czujności i proaktywnych badań w celu identyfikacji, zrozumienia i łagodzenia nowych zagrożeń w ewoluującej infrastrukturze energetycznej.

Ocena

Globalny krajobraz środków cyberbezpieczeństwa dla przedsiębiorstw dystrybucyjnych charakteryzuje się różnicami w nadzorze regulacyjnym oraz integracją nowych technologii. Te z natury zdecentralizowane przedsiębiorstwa borykają się z następującymi wyzwaniami:

- brak zasobów na kompleksowe środki cyberbezpieczeństwa,
- niedoskonałości uniwersalnych wytycznych regulacyjnych, oraz
- ciągle ewoluujący krajobraz zagrożeń wynikający z wprowadzania nowych technologii i pojawiania się nowych aktorów zagrożeń.

Te niespójności w podejściach do cyberbezpieczeństwa sprawiają, że przedsiębiorstwa te są szczególnie narażone, oferując atrakcyjne możliwości dla oportunistycznych cyberprzestępców, zarówno zaawansowanych, jak i mniej wyrafinowanych.

Patrząc w przyszłość, w miarę jak przedsiębiorstwa dystrybucyjne na całym świecie dążą do modernizacji i innowacji, muszą jednocześnie poruszać się w skomplikowanym tańcu, jakim jest zabezpieczanie swoich systemów. Choć technologie takie jak inteligentne liczniki przynoszą pozorne korzyści, ich szybka adopcja niesie ze sobą ukryte podatności. Przeciwnicy wielokrotnie udowodnili swoją zdolność do ewolucji, wykorzystując nieprzewidziane luki technologiczne w celach złośliwych. Dla przedsiębiorstw energetycznych nadchodzące lata będą wymagały proaktywnego i przewidującego podejścia do cyberbezpieczeństwa — takiego, które nie tylko chroni przed dzisiejszymi zagrożeniami, ale także przewiduje i przeciwdziała zagrożeniom przyszłości.

Grupy zagrożeń

Dragos monitoruje aktywne grupy zagrożeń, które atakowały lub mają ocenianą zdolność do znaczącego wpływu na organizacje działające w co najmniej jednej fazie sektora energetycznego. Więcej informacji technicznych na temat klasyfikacji i monitorowania aktywnych grup zagrożeń przez zespół Dragos Threat Discovery można znaleźć w webinarze „The Diamond Model: An Analyst's Best Friend".

VOLTZITE

W 2023 roku Dragos opublikował raport na temat działalności grupy zagrożeń VOLTZITE, która głównie atakuje sektor energetyczny w Stanach Zjednoczonych oraz inne elementy infrastruktury krytycznej. VOLTZITE jest zgodna z grupą opisywaną przez Microsoft jako "Volt Typhoon" oraz innym przeciwnikiem profilowanym przez amerykańską Agencję Cyberbezpieczeństwa i Infrastruktury (CISA). Grupa ta systematycznie prowadziła rozpoznanie wśród kilku amerykańskich podmiotów energetycznych, stosując dyskretne i długotrwałe podejście do angażowania się w interakcje z zasobami wystawionymi na działanie Internetu. W 2023 roku VOLTZITE kontynuowała rozszerzanie swojej działalności, celując w podmioty energetyczne w krajach afrykańskich. Operacje VOLTZITE charakteryzują się dbałością o bezpieczeństwo operacyjne i częstymi zmianami w infrastrukturze dowodzenia i kontroli. Dragos ocenia z wysoką pewnością, że VOLTZITE jest jednym z najbardziej aktywnych i istotnych zagrożeń dla obrońców organizacji z sektora energetycznego na dzień publikacji tego raportu.

Powiązania: Volt Typhoon, BRONZE SILHOUETTE

ELECTRUM

ELECTRUM, wcześniej znana z przeprowadzania cyber-fizycznych zakłóceń sieci energetycznej Ukrainy w latach 2015/2016, kontynuowała poszerzanie i udoskonalanie swoich operacji w latach 2022 i 2023. W 2022 roku ELECTRUM była powiązana z wdrożeniem INDUSTROYER2, zaawansowanego złośliwego oprogramowania, zaprojektowanego do manipulowania operacjami energetycznymi. Kolejna analiza Dragos podkreśliła rozwijające się umiejętności operacyjne ELECTRUM, co jest widoczne w porównaniu INDUSTROYER2 z jego poprzednikiem, CRASHOVERRIDE. W październiku 2022 roku ELECTRUM prawdopodobnie przeprowadziła drugi cyber-fizyczny atak na ukraińską stację przesyłową, stosując techniki OT na poziomie "Living off the Land" (LOTL) w celu wywołania przerw w dostawie prądu, wraz z użyciem nowej wersji CADDYWIPER do zakłóceń IT. Oprócz tych działań, Dragos powiązał ELECTRUM z długotrwałą kampanią, w której regularnie stosowano destrukcyjne oprogramowanie typu wiper przeciwko różnym celom na Ukrainie w trakcie wojny rosyjsko-ukraińskiej. Te operacje podkreślają ciągłe inwestycje w zdolności ELECTRUM i jego elastyczność w tworzeniu i wdrażaniu zakłócających możliwości cybernetycznych, zarówno dla środowisk IT, jak i OT. Z potwierdzonym doświadczeniem w działaniach związanych z ICS i szybką zdolnością adaptacyjną, ELECTRUM stanowi istotne zagrożenie dla operacji energetycznych. Chociaż działalność ELECTRUM była głównie skierowana na Ukrainę, jej kierunek może się zmieniać w zależności od celów jej sponsorów.

Powiązania: SANDWORM, Telebots, Voodobear, Seashell Blizzard, FROZENBARENTS

KAMACITE

KAMACITE, oceniana przez Dragos jako grupa ułatwiająca początkowy dostęp dla ELECTRUM, charakteryzuje się uporczywymi działaniami, skupionymi na atakowaniu infrastruktury krytycznej i sektorów przemysłowych, których ślady można prześledzić przynajmniej od 2014 roku. Grupa ta miała znaczący udział w ułatwieniu operacji związanych z ICS, w tym wydarzeń związanych z przerwami w dostawie energii na Ukrainie w latach 2015 i 2016. Pomimo swojej historycznej roli, metody operacyjne KAMACITE niewiele się zmieniły w ciągu ostatnich sześciu lat. Ich najnowsze działania, szczególnie od początku 2022 roku, pokazują duże zainteresowanie lukami w różnorodnych urządzeniach, od routerów po kamery IP, ze szczególnym naciskiem na infrastrukturę ukraińską. Używając narzędzi takich jak złośliwe oprogramowanie CYCLOPS BLINK oraz powszechnie dostępne złośliwe oprogramowanie, takie jak DarkCrystal RAT, grupa przeprowadza szeroko zakrojone rozpoznanie, wykorzystując oportunistyczne podejście do zdobywania początkowych przyczółków w potencjalnie zaawansowanych operacjach. Chociaż analiza Dragos pokazuje, że KAMACITE nie była bezpośrednim wykonawcą zdarzeń zakłócających ICS, podkreśla kluczową rolę grupy w potencjalnym ułatwieniu takich działań.

Powiązania: SANDWORM

CHERNOVITE

Na początku 2022 roku Dragos poinformował o PIPEDREAM, zaawansowanym złośliwym oprogramowaniu zaprojektowanym dla systemów sterowania przemysłowego (ICS) przez grupę CHERNOVITE, stanowiącym siódmy przykład wysoce specyficznego złośliwego oprogramowania dla ICS, podobnego do STUXNET i CRASHOVERRIDE. Ewoluując z technik obserwowanych we wcześniejszych atakach, PIPEDREAM od CHERNOVITE wykazuje zaawansowane możliwości, umożliwiając operatorom skanowanie, kompromitowanie, a nawet wyłączanie docelowych urządzeń przemysłowych. Podczas gdy ELECTRUM wykorzystała protokół Open Platform Communications Data Access (OPC-DA), CHERNOVITE korzysta z nowszego protokołu Open Platform Communications Unified Architecture (OPC-UA). Komponenty PIPEDREAM dostarczają przeciwnikom narzędzi nie tylko do manipulacji sterownikami PLC, ale także do penetracji urządzeń z systemem Windows. Co istotne, Dragos uważa, że PIPEDREAM nie zostało jeszcze aktywnie użyte, co stwarza rzadką okazję do prewencyjnych działań obronnych. Biorąc pod uwagę, że PIPEDREAM jest zaprojektowane z myślą o infrastrukturze skroplonego gazu ziemnego (LNG) i energetyce, a także jego potencjalną adaptacyjność, istnieją mocne przesłanki, że CHERNOVITE może wykorzystać lub dostosować możliwości PIPEDREAM do szerszej gamy celów w przyszłości.

Powiązania: PIPEDREAM jest znane również jako INCONTROLLER w innych publikacjach. CHERNOVITE nie jest powiązana z żadną grupą monitorowaną przez inne organizacje w momencie publikacji tego raportu.

XENOTIME

XENOTIME ma bogatą historię działań wymierzonych w sektor energetyczny. Grupa zyskała rozgłos po ataku z 2017 roku na zakład naftowo-gazowy w Arabii Saudyjskiej, gdzie użyto złośliwego oprogramowania TRISIS, co zapoczątkowało nową fazę ataków na systemy sterowania przemysłowego (ICS), poprzez celowanie w systemy zabezpieczeń przemysłowych (SIS). Ten atak został zaprojektowany, aby współpracować z kontrolerami bezpieczeństwa Triconex, co pokazało, że XENOTIME rozumie i zamierza manipulować specyficznym sprzętem przemysłowym. W 2018 roku grupa poszerzyła swoje działania, celując w systemy SIS poza kontrolerami Triconex. W 2019 roku XENOTIME ponownie rozszerzył zakres swoich działań, atakując przedsiębiorstwa energetyczne w Ameryce Północnej oraz firmy z branży naftowej i gazowej na różnych kontynentach. Grupa włamała się także do kilku dostawców i producentów ICS, co wskazuje na zagrożenie związane z łańcuchem dostaw. Chociaż rok 2019 oznaczał większy zakres działań, do 2022 roku Dragos zaobserwował, że XENOTIME zintensyfikował swoje działania rozpoznawcze w stosunku do amerykańskich podmiotów zajmujących się ropą naftową i gazem ziemnym (ONG) oraz skroplonym gazem ziemnym (LNG), szczególnie w odniesieniu do komponentów i procesów kluczowych dla operacji LNG. Pomimo braku dowodów bezpośrednich ataków, zwiększone zainteresowanie XENOTIME stanowi zagrożenie dla sektora energetycznego, szczególnie dla interesariuszy zintegrowanych z procesami LNG.

Powiązania: Temp.Veles

KOSTOVITE

W marcu 2021 roku KOSTOVITE z powodzeniem przeniknęła do operatora odnawialnych źródeł energii, osiągając 2. etap ICS Cyber Kill Chain, uzyskując potwierdzony dostęp do sieci i urządzeń OT. Grupa wykorzystała lukę typu zero-day w Ivanti Connect Secure, wcześniej znanym jako Pulse Secure, aby naruszyć obwód sieci ICS/OT. Wykazując się solidną dyscypliną operacyjną i dogłębną wiedzą na temat urządzeń sieciowych, KOSTOVITE skutecznie stosowała strategię "living-off-the-land", używając przejętych uprawnień administratora. To pozwoliło KOSTOVITE na lateralne przenikanie do środowisk OT w wielu obiektach na dwóch kontynentach. Mimo pewnych podobieństw w taktyce operacyjnej do VOLTZITE, Dragos śledzi te dwie grupy jako oddzielne jednostki z powodu braku technicznego nakładania się operacji.

Powiązania: UNC2630

GANANITE

Pierwszy raz zidentyfikowana w 2023 roku, GANANITE to grupa zagrożeń skupiająca się głównie na infrastrukturze krytycznej oraz sektorach rządowych w obrębie Wspólnoty Niepodległych Państw (WNP) i terytoriach Azji Centralnej. Grupa stosuje podejście skoncentrowane na szpiegostwie, połączone ze zdolnościami kradzieży danych, wykazując możliwość przekazywania początkowych uprawnień dostępu innym grupom zagrożeń. Ich uporczywe działania obejmują różne narzędzia infiltracji, w tym StinkRAT oraz komercyjne i open-source'owe zdalne trojany dostępu (RAT). Grupa wykorzystywała również publiczne exploity proof-of-concept, skierowane na punkty wystawione na działanie internetu. Co ciekawe, w ich zestawie narzędzi znajduje się złośliwe oprogramowanie przypisywane państwom.

Powiązania: YOROTROOPER, TOMIRIS, STURGEON PHISHER

PARISITE

PARISITE działa co najmniej od 2017 roku, koncentrując się na różnych systemach sterowania przemysłowego w wielu sektorach, w tym w sektorach użyteczności publicznej, takich jak woda, energia elektryczna, gaz, przemysł lotniczy oraz ropa i gaz. Grupa ma szeroki zasięg geograficzny, celując w podmioty w Ameryce Północnej, Europie, na Bliskim Wschodzie i w Australii. Poza sektorami przemysłowymi, aktywność PARISITE obejmuje także organizacje rządowe i pozarządowe. Grupa głównie wykorzystuje narzędzia open-source do kompromitacji infrastruktury i jest znana z wykorzystywania luk w sieciach VPN do uzyskania początkowego dostępu. Dragos ocenia z umiarkowaną pewnością, że PARISITE działa jako grupa uzyskująca wstępny dostęp, przygotowując teren dla dalszych operacji prowadzonych przez MAGNALLIUM.

Powiązania: Pioneer Kitten, Lemon Sandstorm

MAGNALLIUM

MAGNALLIUM od wielu lat wykazuje trwałe i ewoluujące zainteresowanie kluczowymi sektorami infrastruktury krytycznej. Grupa, która ma istotne powiązania z irańskimi interesami strategicznymi, zwróciła uwagę amerykańskiego Dowództwa Cybernetycznego (USCC) w 2019 roku z powodu możliwych powiązań z destrukcyjnymi wydarzeniami SHAMOON. Mimo tego historycznego związku, MAGNALLIUM wykazał zdolność i zamiar, szczególnie po zmianie swojego celu na podmioty w USA. W 2020 roku Dragos odkrył, że wdrażane przez MAGNALLIUM złośliwe oprogramowanie jest podobne do trojana POWERTON opartego na PowerShell. To złośliwe oprogramowanie oparte na platformie .NET, które komunikuje się z platformami powiązanymi z MAGNALLIUM, w połączeniu z ich wcześniejszym zainteresowaniem sektorami takimi jak ropa i gaz, energetyka oraz produkcja, szczególnie w Zatoce Perskiej i Ameryce Północnej, ukazuje rozszerzające się zdolności grupy i jej agresywną postawę, prawdopodobnie pogłębioną przez napięcia geopolityczne związane z Iranem. Chociaż w 2022 roku nastąpiło spowolnienie jawnych operacji MAGNALLIUM, ustalenia Dragos sugerowały, że grupa utrzymywała aktywną infrastrukturę, co wskazuje na dalsze, choć mniej widoczne zagrożenie dla organizacji przemysłowych. W 2023 roku MAGNALLIUM wyraźnie powróciło, przeprowadzając kampanię polegającą na rozsyłaniu haseł, skierowaną na sektory obrony i górnictwa.

Powiązania: APT 33, Elfin, PARISITE

DYMALLOY

Od momentu zidentyfikowania w 2015 roku, DYMALLOY wykazywała stałe zainteresowanie globalnym sektorem energetycznym, koncentrując się szczególnie na podmiotach w Ukrainie, Ameryce Północnej, Europie i Turcji. Obszerne analizy Dragos na przestrzeni lat ujawniają, że DYMALLOY wykorzystuje zarówno publicznie dostępne, jak i specjalnie opracowane narzędzia, takie jak złośliwe oprogramowanie HERIPLOR, w celu infiltracji sieci systemów sterowania przemysłowego (ICS). Grupa ta głównie stosuje taktyki takie jak ataki typu "watering hole" oraz spear-phishing. Chociaż nie zaobserwowano u DYMALLOY zamiarów destrukcyjnych lub zakłócających, z powodzeniem przenikała do sieci ICS, zbierając dane, które mogą zostać wykorzystane w przyszłych działaniach zakłócających. Mimo że operacje grupy znacząco osłabły po 2020 roku, a ostatnia godna uwagi aktywność była prawdopodobnie związana z nimi w październiku 2020 roku, Dragos pozostaje czujny, uznając możliwość ich ponownego pojawienia się, biorąc pod uwagę ich dotychczasowy wzorzec ataków i ekspertyzę w dziedzinie energetyki.

Powiązania: Dragonfly 2.0, Berserk Bear

ALLANITE

Po raz pierwszy zauważona w 2017 roku, ALLANITE głównie atakowała sektor energetyczny, zwłaszcza w USA, Wielkiej Brytanii i Niemczech. Wykorzystując taktyki, takie jak kompromitowanie stron internetowych ("watering hole" ataki) oraz phishing e-mailowy, ALLANITE systematycznie starała się uzyskać dostęp do sieci IT i OT, wykazując szczególne zainteresowanie systemami sterowania przemysłowego (ICS). Grupa ta często bazowała na przechwytywaniu i ponownym używaniu poświadczeń użytkowników, wykorzystując szeroko stosowane techniki, takie jak protokół SMB (Server Message Block) oraz RDP (Remote Desktop Protocol), oraz stosowała strategie "living off the land" i publiczne skrypty do lateralnych ruchów w sieci. Chociaż ich działania były wyraźnie powiązane z rosyjskimi interesami strategicznymi, jak dotąd nie ma konkretnych dowodów na to, że ALLANITE posiada intencje lub zdolności do działań destrukcyjnych lub zakłócających. Niemniej jednak Dragos uważa ALLANITE za znaczące potencjalne zagrożenie, biorąc pod uwagę ich ciągłe naruszanie środowisk ICS. Mimo zauważalnego spadku aktywności ALLANITE po 2020 roku, Dragos pozostaje ostrożny wobec możliwości ich ponownego pojawienia się na globalnym krajobrazie zagrożeń dla sektora energetycznego.

Powiązania: PALMETTO FUSION, Dragonfly 2.0, Berserk Bear

CHRYSENE

CHRYSENE celuje głównie w organizacje z sektorów ropy i gazu, petrochemicznego oraz generacji energii elektrycznej. Początkowo zidentyfikowana w 2017 roku ze względu na swoje działania na Bliskim Wschodzie, CHRYSENE rozszerzyła swój zasięg geograficzny na Europę i Amerykę Północną, stosując mieszankę innowacyjnych i adaptacyjnych taktyk, takich jak spear-phishing, ataki typu "watering hole", rozwijające się złośliwe oprogramowanie oraz mechanizmy dowodzenia i kontroli oparte na systemie DNS. Grupa ta była historycznie powiązana z destrukcyjnymi kampaniami złośliwego oprogramowania, takimi jak SHAMOON, i wykorzystywała luki, takie jak CVE-2017-0199. Działania CHRYSENE sugerują stałe zainteresowanie podmiotami związanymi z systemami ICS, z naciskiem na unikanie wykrycia, utrzymywanie trwałej obecności oraz potencjalne umożliwienie bardziej strategicznych ataków. Choć taktyki CHRYSENE zmieniały się, a aktywność grupy była czasami ograniczona, analizy Dragos podkreślają potrzebę stałej czujności wobec ewoluujących technik, taktyk i procedur (TTPs) grupy dla obrońców organizacji z sektora energetycznego.

Powiązania: APT 34, GREENBUG, OilRig

WASSONITE

WASSONITE, monitorowana przez Dragos od 2017 roku, zyskała rozgłos po włamaniu do Elektrowni Jądrowej Kudankulam (KKNPP) w Indiach w 2018 roku. Grupa ta wykazuje stałe zainteresowanie sektorami przemysłowymi, szczególnie w dziedzinie energii jądrowej. Spektrum jej operacji obejmuje celowanie w podmioty z branż energii jądrowej, elektrycznej, ropy i gazu, lotnictwa, centrów danych oraz zaawansowanej produkcji, z koncentracją geograficzną na Azji Południowej i Wschodniej, a także na Ameryce Północnej. Monitoring Dragos wykazał, że WASSONITE konsekwentnie wykorzystuje złośliwe oprogramowanie AppleSeed, które umożliwia działania takie jak rejestrowanie naciśnięć klawiszy, przechwytywanie zrzutów ekranu i zdalne wykonywanie poleceń. Przykładem tego była kampania spear-phishingowa z 2022 roku, której tematem była energia jądrowa, oraz wcześniejsze przypadki kompromitacji podmiotów z różnych sektorów w 2021 roku. Działania WASSONITE głównie koncentrują się na początkowej fazie (Stage 1) operacji w ramach Industrial Control Systems (ICS) Cyber Kill Chain.

Powiązania: Lazarus Group, COVELLITE

RASPITE

RASPITE, po raz pierwszy zidentyfikowana przez Dragos jako aktywna w 2017 roku lub wcześniej, wykazuje wzorzec ataków na różnorodne sektory, w tym energetykę, przemysł spożywczy, sektor rządowy, finansowy oraz edukacyjny. Grupa ta działa na obszarach takich jak Arabia Saudyjska, Japonia, Europa Zachodnia oraz Stany Zjednoczone. RASPITE wykorzystuje strategiczne kompromitacje stron internetowych, aby skłonić ofiary do łączenia się z infrastrukturą kontrolowaną przez grupę przy użyciu techniki server message block (SMB). Umożliwia to grupie RASPITE pozyskiwanie poświadczeń logowania do systemu Windows, co ułatwia dalszą infiltrację sieci ofiar poprzez dodawanie kont typu backdoor i umożliwianie zdalnych połączeń. W 2023 roku RASPITE przeprowadziła operacje skanowania SMB, szczególnie koncentrując się na usługach SMB wystawionych na działanie internetu. Chociaż nie ma bezpośrednich dowodów na wpływ tych działań na systemy ICS, takie operacje mogą wskazywać na potencjalne złośliwe zamiary lub taktyki mające na celu uzyskanie dostępu do sieci IT i OT. RASPITE pozostaje głównie zaangażowana w operacje związane z uzyskiwaniem początkowego dostępu, ale jej koncentracja na organizacjach przemysłowych sugeruje szersze ambicje.

Powiązania: Leafminer

VANADINITE

VANADINITE działa co najmniej od połowy 2019 roku, skupiając się głównie na organizacjach przemysłowych oraz niektórych podmiotach rządowych i edukacyjnych. Modus operandi VANADINITE obejmuje wykorzystywanie luk w urządzeniach i usługach dostępnych zewnętrznie, co umożliwia instalację backdoorów i mechanizmów utrzymywania obecności w systemie, otwierając drogę do kolejnych etapów ataków. VANADINITE nakłada się na inne znane grupy, takie jak Winnti, APT41 i LEAD. Większość ich działań ma charakter szpiegowski lub kryminalny. Departament Sprawiedliwości Stanów Zjednoczonych oraz Federalne Biuro Śledcze (FBI) ujawniły akty oskarżenia, które bezpośrednio wiążą kilka operacji powiązanych z VANADINITE z obywatelami Chińskiej Republiki Ludowej (PRC). Chociaż VANADINITE znajduje się obecnie w okresie niskiej aktywności, grupa nadal stanowi poważne zagrożenie, zwłaszcza dla sektorów infrastruktury krytycznej.

Powiązania: Wicked Panda, Winnti, APT41

TALONITE

Od momentu swojej pierwszej identyfikacji w lipcu 2019 roku, TALONITE nieustannie stanowi zagrożenie dla sektora energetycznego w USA, skupiając się głównie na kompromitacjach związanych z początkowym dostępem. Grupa ta jest znana ze stosowania spear-phishingu oraz wdrażania niestandardowych rodzin złośliwego oprogramowania, takich jak LookBack i FlowCloud. Operacje TALONITE często celują w mniejszych amerykańskich dostawców energii, szczególnie w inżynierów i operatorów, prawdopodobnie w celu zbierania danych i prowadzenia rozpoznania do późniejszych działań zakłócających. W sierpniu 2023 roku Dragos opublikował raport AA-2023-26, który dostarcza informacji o najnowszych ustaleniach po okresie względnej nieaktywności TALONITE. Kluczowe wnioski z tego raportu sugerują możliwe celowanie w regiony azjatyckie, szczególnie w populacje chińskojęzyczne, a także wskazują na potencjalną ewolucję złośliwego oprogramowania FlowCloud, które może być dostarczane za pomocą USB. Taka ewolucja mogłaby zwiększyć ryzyko dla organizacji przemysłowych, gdyż umożliwiłaby przełamanie zabezpieczeń sieci odizolowanych od internetu.

Powiązania: TA410, APT10

STIBNITE

STIBNITE regularnie atakuje sektor energetyczny w Azerbejdżanie, z szczególnym naciskiem na odnawialne źródła energii, zwłaszcza farmy wiatrowe. Dowody z ich kampanii, takie jak specyficzne ataki na Yashma Wind Park, podkreślają to skoncentrowane zainteresowanie. Kampanie spear-phishingowe w 2020 roku i na początku 2021 roku, w tym jedna wykorzystująca przynętę związaną z Państwową Spółką Naftową Republiki Azerbejdżanu (SOCAR), były skierowane głównie na azerbejdżańskie podmioty rządowe i profesjonalistów z branży odnawialnych źródeł energii. STIBNITE używało złośliwego oprogramowania PoetRAT, a ich działania koncentrowały się głównie na wczesnych etapach ICS Cyber Kill Chain, tj. uzyskaniu dostępu i gromadzeniu informacji. Chociaż nie wykazali zdolności do bezpośrednich zakłóceń systemów ICS, ich stałe zainteresowanie sektorem odnawialnych źródeł energii oraz zgromadzone dane sugerują potencjalne zaawansowane działania w tym sektorze w przyszłości.

Powiązania: PoetRat

PETROVITE

PETROVITE wykazuje stałe zainteresowanie sektorami górniczym, energetycznym i generacji energii, szczególnie w Kazachstanie. Operacje PETROVITE, w tym ataki na operacje elektryczne związane z kazachstańskimi producentami zasobów naturalnych, charakteryzują się wdrażaniem ukierunkowanych kampanii spear-phishingowych, dostarczających wariant złośliwego oprogramowania ZEBROCY. Do 2023 roku PETROVITE rozszerzyła zakres swoich ataków, co pokazuje kampania przeciwko Ukraińskim Kolejom Państwowym (JSC "Ukrzaliznytsia"), w której wdrożono wariant Zebrocy o nazwie DolphinCape. Działania PETROVITE w przeważającej mierze pokrywają się z pierwszym etapem ICS Kill Chain, skupiając się na początkowym dostępie i gromadzeniu informacji.

Powiązania: KAMACITE, APT28, Zebrocy

Inne wpływy na sieć energetyczną

WOJNA ROSYJSKO-UKRAIŃSKA

Przełomowym momentem w krajobrazie zagrożeń dla globalnego sektora energetycznego był luty 2022 roku, kiedy Rosja rozpoczęła inwazję militarną na Ukrainę. Ten wieloaspektowy konflikt doprowadził do wielokrotnych ataków na ukraińską infrastrukturę krytyczną, zarówno za pomocą środków kinetycznych, jak i cybernetycznych. Wojna rosyjsko-ukraińska spowodowała istotne zmiany w krajobrazie zagrożeń dla globalnego sektora energetycznego, w tym:

- uporczywe ataki ELECTRUM na ukraińskie zasoby energetyczne, w tym nieudany atak z użyciem INDUSTROYER2 na stację wysokiego napięcia w kwietniu 2022 roku oraz późniejsze skuteczne zakłócenie sieci energetycznej w październiku 2022 roku,
- szybkie odłączenie Ukrainy od rosyjskiej sieci energetycznej, a następnie integracja z siecią Unii Europejskiej,
- pierwsze przypadki cyberfizycznych szkód ubocznych dla infrastruktury energetycznej sąsiednich krajów oraz
- znaczące przekształcenie podziemnej gospodarki cyberprzestępczej, któremu towarzyszył wzrost liczby politycznie motywowanych ataków hakerskich na infrastrukturę krytyczną po obu stronach konfliktu.

Szkody uboczne

W przeddzień inwazji Rosji na Ukrainę w lutym 2022 roku firma komunikacji satelitarnej ViaSat padła ofiarą cyberataku, w wyniku którego uszkodzone zostały modemy KA-SAT. W następstwie tego ataku 5,800 turbin wiatrowych firmy Enercon w Niemczech straciło łączność, co utrudniło ich zdalne monitorowanie i kontrolę. Złośliwe oprogramowanie, które prawdopodobnie ułatwiło ten atak, później zidentyfikowane przez badaczy z SentinelOne jako 'AcidRain', zostało niejednoznacznie powiązane z wcześniejszymi kampaniami cybernetycznymi przypisywanymi rządowi rosyjskiemu. AcidRain, które brutalnie wymazuje system plików, wykazywało podobieństwa do złośliwego oprogramowania VPNFilter, wcześniej przypisywanego rosyjskim podmiotom.

Przerwa w działaniu ViaSat wpłynęła na tysiące urządzeń na Ukrainie, ale także zakłóciła zdalne możliwości turbin wiatrowych w Niemczech, łącząc czas tej awarii z działaniami Rosji na Ukrainie. Choć ViaSat wskazał na dwutorowy atak obejmujący blokadę usług z modemów na Ukrainie i masowe usunięcie modemów, późniejsze badania SentinelOne sugerowały atak na łańcuch dostaw poprzez mechanizm zarządzania KA-SAT. W takim scenariuszu atakujący wdrożyli wiper zaprojektowany specjalnie dla modemów i routerów, co podkreśla złożony charakter takich cyberataków.

Incydent ViaSat i późniejsze zakłócenia w pracy niemieckich turbin wiatrowych stanowią pierwszy przypadek szkód ubocznych w infrastrukturze krytycznej państwa, które nie uczestniczyło bezpośrednio w konflikcie zbrojnym. Zdarzenie to podkreśla głęboki stopień współzależności we współczesnej infrastrukturze narodowej oraz stale rosnące zagrożenia, jakie niesie ta współzależność. Współczesne sieci energetyczne, które przechodzą znaczącą transformację cyfrową, rozszerzają swoje interfejsy cyber-fizyczne. Choć taka integracja jest kluczowa dla zrównoważonego rozwoju, zwiększa również powierzchnię ataku cybernetycznego. Wraz ze wzrostem połączeń między sieciami energetycznymi staje się coraz trudniej przewidzieć, jak i gdzie mogą pojawić się szkody uboczne w wyniku nagłych zmian geopolitycznych, takich jak wojna na Ukrainie.

Zamieszanie w cyberprzestępczym podziemiu

Rozpoczęcie inwazji Rosji na Ukrainę w lutym 2022 roku wywołało istotne zmiany w środowisku cyberprzestępczym, szczególnie wśród rosyjskojęzycznych społeczności hakerów i w krajach Wspólnoty Niepodległych Państw (WNP). W miarę postępu wojny podziemny ekosystem uległ podziałowi—niektóre frakcje wyraziły silną lojalność wobec rosyjskiej administracji, inne podzieliły się z powodu ideologicznych różnic, podczas gdy jeszcze inne dostrzegły w chaosie okazję do zarobku i starały się zmonetyzować geopolityczne zamieszanie. Ta nowa dynamika stanowi potencjalne zagrożenie dla globalnego sektora energetycznego, ponieważ rozszerza powierzchnię ataku i wprowadza nowych potencjalnych przeciwników o zróżnicowanych celach, od zysków finansowych po cyberwojnę sponsorowaną przez państwa.

Wymowną konsekwencją inwazji był bezpośredni i pośredni udział grup cyberprzestępczych w konflikcie geopolitycznym. Organizacje takie jak Conti otwarcie deklarowały swoją lojalność wobec Moskwy. Co więcej, różne narzędzia złośliwego oprogramowania dostępne na rosyjskojęzycznych forach cyberprzestępczych, takie jak DarkCrystal RAT, Colibri Loader i WarZoneRAT, stały się instrumentami dla zaawansowanych grup, takich jak KAMACITE, które atakowały ukraińskie podmioty. To przejście od narzędzi cyberprzestępczych do cyberwojennych stanowi poważne zagrożenie dla globalnej infrastruktury energetycznej. W miarę jak te grupy dywersyfikują swoje cele, międzynarodowe sieci energetyczne i zasoby energetyczne, zwłaszcza należące do krajów wspierających wysiłki wojenne Ukrainy, mogą znaleźć się na ich celowniku.

Dodatkowo krajobraz komplikuje złożona relacja między rosyjskim państwem a tymi aktorami cybernetycznymi. Długotrwałe, ciche porozumienie między rosyjskimi agencjami rządowymi a podziemiem cyberprzestępczym objawia się w skoordynowanych operacjach cybernetycznych i informacyjnych. Taka współpraca daje rosyjskiemu państwu możliwość zaprzeczenia bezpośredniego zaangażowania, z grupami cyberprzestępczymi działającymi jako pośrednicy. Dla globalnego sektora energetycznego oznacza to, że zagrożenie jest dwojakie: z jednej strony ryzykują atakami niezależnych grup przestępczych, które dążą do zysków lub innych korzyści, z drugiej zaś—państwowo skoordynowanych operacji cybernetycznych o celach politycznych lub strategicznych. Biorąc pod uwagę kluczową rolę energii elektrycznej w bezpieczeństwie narodowym i codziennym życiu, ochrona infrastruktury energetycznej przed tym ewoluującym i wieloaspektowym krajobrazem zagrożeń staje się priorytetem.

Wnioski

Choć ważne jest, aby nie przeceniać zagrożenia, należy uznać, że zbliżając się do drugiego roku wojny, świat nie był świadkiem długo obawianego cybernetycznego "Pearl Harbor" ani masowych ataków na infrastrukturę państw zachodnich. Niemniej jednak obrońcy organizacji w sektorze energetycznym powinni utrzymać realistyczną, świadomą perspektywę i nie popadać w samozadowolenie. Wojna rosyjsko-ukraińska uwypukliła złożoną i rosnącą sieć zagrożeń cybernetycznych, przed którymi stoi globalny sektor energetyczny. W miarę jak sieci energetyczne na całym świecie przechodzą transformację cyfrową, rośnie również ich potencjalna powierzchnia ataku. Wojna podkreśliła kruchość systemów połączonych i dodatkowo uwydatniła rosnące połączenie między państwowymi aktorami a podziemiem cyberprzestępczym.

Dla globalnego sektora energetycznego oznacza to konieczność zmierzenia się z dwojakim wyzwaniem: po pierwsze, technicznym wyzwaniem zabezpieczenia coraz bardziej złożonych i powiązanych systemów, a po drugie, nawigowaniem w politycznym i strategicznym labiryncie zagrożeń cybernetycznych sponsorowanych przez państwo i tych niezależnych, szczególnie gdy granice między nimi są niewyraźne. Jest oczywiste, że w dzisiejszym zglobalizowanym świecie konsekwencje wydarzeń geopolitycznych wykraczają poza ich bezpośrednie teatry konfliktu. Ochrona infrastruktury krytycznej, takiej jak sieć energetyczna, nie polega już tylko na zapewnieniu nieprzerwanej dostawy energii; chodzi o ochronę fundamentów nowoczesnej cywilizacji.

RANSOMWARE

Krajobraz ataków ransomware szybko się zmienia, ewoluując z typowych wiadomości phishingowych w bardziej wyrafinowane podejście. Od 2021 roku Dragos zaobserwował wyraźną zmianę w kierunku bezpośredniego wykorzystywania luk w aktywach peryferyjnych sieci. Prominentne grupy ransomware skupiają się obecnie na zdobywaniu luk typu zero-day, zarówno poprzez własne badania, jak i poprzez zakup z szarego rynku, aby zwiększyć skuteczność swoich ataków. Co więcej, aktorzy ransomware wykazują zdolność i zainteresowanie szybkim wykorzystaniem niedawno ujawnionych luk.

Przykładem jest grupa ransomware Cl0p (znana również jako CloP). Wykorzystali lukę typu zero-day związaną z SQL injection w oprogramowaniu GoAnywhere firmy Fortra (CVE-2023-0669), aby przeprowadzić ataki na kilka znaczących firm. Kilka miesięcy później wykorzystali kolejną odkrytą przez siebie lukę typu zero-day w aplikacji do transferu plików MOVEit firmy Progress Software (CVE-2023-34362), atakując wiele dużych globalnych organizacji. Po tym, jak zaczęli wykorzystywać luki zero-day, liczba ich ofiar wzrosła dziewięciokrotnie w ciągu pierwszego kwartału 2022 roku w porównaniu z pierwszym kwartałem bieżącego roku. Inne bardzo aktywne grupy ransomware, takie jak LockBit i ALPHV (często określane jako BlackCat), również sieją zniszczenie, wykorzystując świeżo ujawnione luki. Te luki często są wykorzystywane, zanim organizacje zdążą wdrożyć poprawki dostarczone przez dostawców. Wśród godnych uwagi przypadków jest wykorzystanie luk w systemie PaperCut w kwietniu 2023 roku (CVE-2023-27350 i CVE-2023--27351) oraz luk znalezionych w serwerach VMware ESXi.

Studium przypadku 1

Krytyczna luka typu SQL injection (CVE-2023-34362) została zidentyfikowana w oprogramowaniu MoveIt Transfer firmy Progress Software, produkcie do zarządzania transferami plików (MFT), pod koniec maja. Mimo że firma szybko wprowadziła poprawkę tego samego dnia jego ujawnienia, zgłoszono, że już zostało wykorzystane w środowisku produkcyjnym. W czerwcu badania Microsoftu przypisały to wykorzystanie podmiotowi o nazwie „Lace Tempest", powiązanemu z grupą ransomware Cl0p.

W kolejnych miesiącach nastąpił gwałtowny wzrost ataków polegających na wymuszaniu danych w wyniku wykorzystania luki CVE-2023-34362. Wiele organizacji zgłosiło naruszenia, począwszy od prywatnych podmiotów w Wielkiej Brytanii po amerykańskie agencje federalne. Wiele z nich, w tym globalny koncern naftowy Shell, znalazło swoje nazwy na stronie wycieków grupy Cl0p, która groziła ujawnieniem skradzionych danych. Shell zmierzył się z podobnym naruszeniem dwa lata wcześniej, związanym z wykorzystaniem przez Cl0p innego produktu MFT, Accellion File Transfer Appliance.

Publiczne badania dotyczące tej kampanii wykazały, że skutki ataków były ogromne, co pokrywało się z ocenami Dragos. Badacze bezpieczeństwa doliczyli się 250 odrębnych ofiar exploitów MoveIt, co miało wpływ na ponad 18 milionów osób. Dane te w dużej mierze pochodzą z witryny wycieków Cl0p, chociaż niektóre z wymienionych podmiotów zakwestionowały twierdzenia o kompromitacji. Co ciekawe, w czerwcu Cl0p twierdził, że usunął dane związane z podmiotami rządowymi i organami ścigania, doradzając im, aby nie nawiązywali kontaktu.

Motywy Cl0p pozostają przedmiotem spekulacji. Nie wiadomo, czy ich decyzja o usunięciu danych rządowych była strategicznym posunięciem mającym na celu uniknięcie wzmożonej uwagi organów ścigania. Niemniej jednak 16 czerwca 2023 roku Departament Stanu USA ogłosił na Twitterze nagrodę do 10 milionów dolarów za informacje, które mogłyby połączyć grupę Cl0p lub jakiekolwiek inne złośliwe podmioty cybernetyczne atakujące infrastrukturę krytyczną USA z rządem obcego państwa.

Chociaż sektor energetyczny nie był bezpośrednim celem tych ataków ransomware, konsekwencje są ważne. Przejście operatorów ransomware na wykorzystywanie luk typu zero-day w zewnętrznie dostępnej infrastrukturze podkreśla zaawansowany krajobraz zagrożeń, przed którym stoją organizacje z sektora energetycznego. Jeśli Cl0p lub inny podmiot ransomware odkryje lukę w publicznie dostępnych aplikacjach powszechnie wykorzystywanych w sektorze energetycznym, te organizacje staną się natychmiastowymi celami. Jest to wyraźne przypomnienie, że nawet najbardziej bezpieczne lub pozornie nieistotne systemy mogą zostać skompromitowane, co podkreśla potrzebę ciągłej czujności, proaktywnych działań oraz nowoczesnych strategii obronnych w sektorze energetycznym.

Zalecenia dotyczące obrony

Aby skutecznie bronić naszą sieć energetyczną przed stale ewoluującym krajobrazem zagrożeń, Dragos zaleca, aby obrońcy korzystali z pięciu kluczowych kontroli bezpieczeństwa cybernetycznego dla systemów sterowania przemysłowego (ICS) jako przewodnika:

Kontrola nr 1: Specyficzny dla ICS plan reagowania na incydenty

- Podstawą cyberbezpieczeństwa jest przygotowanie się na incydent, a nie tylko reagowanie na niego.
- Priorytetyzuj działania na podstawie potencjalnego wpływu operacyjnego, koncentrując się na tym, jak funkcjonować podczas ataku.
- Uzyskaj możliwość analizy przyczyn źródłowych, co jest niezbędne do przywrócenia bezpiecznej operacji.

Plan reagowania na incydenty specyficzny dla ICS

Plan reagowania na incydenty dostosowany do systemów sterowania przemysłowego (ICS) specyficznych dla sieci energetycznej jest niezbędny. Taki plan powinien z wyprzedzeniem uwzględniać złożoność oraz operacyjne potrzeby segmentów generacji, przesyłu i dystrybucji, a także zapewnić ciągłość działania i bezpieczeństwo. Zrozumienie unikalnych cech sieci energetycznej pozwala interesariuszom przewidywać podatności, poprawiać strategie wykrywania zagrożeń i zapewnić, że metody zbierania danych są zgodne z wymaganiami reagowania na incydenty. Ponadto, w związku z przejściem na technologie rozproszonych zasobów energetycznych (DER) i inteligentnych sieci oraz związanymi z nimi potencjalnymi zagrożeniami, potrzeba analizy przyczyn źródłowych jest teraz bardziej istotna niż kiedykolwiek. Niezależnie od tego, czy zdarzenie awaryjne ma charakter cybernetyczny, czy nie, szybka identyfikacja i ograniczenie szkód mogą zapobiec poważnym zniszczeniom i wzmocnić odporność operacyjną.

Kontrola nr 2: Obronna architektura

- Wdrażaj projekty systemów, które uwzględniają ryzyka oraz interwencję człowieka.
- Choć takie ramy, jak model Purdue lub architektury ISA/IEC 62443, oferują wskazówki, należy je dostosować do potrzeb organizacji.

Systemy sieci energetycznej są rozległe, rozprzestrzenione na duże obszary geograficzne i stale się rozwijają. W związku z tym uniwersalne architektury bezpieczeństwa nie są wskazane. Obronna architektura dostosowana do sieci energetycznej staje się kluczowa. Obejmuje to integrację projektów systemów, które w naturalny sposób minimalizują ryzyko, jednocześnie umożliwiając ludziom radzenie sobie z nieprzewidzianymi wyzwaniami. Wdrożenie ram takich jak model Purdue czy ISA/IEC 62443 to dobry punkt wyjścia, ale dla sieci energetycznej konieczne jest dostosowanie tych ram do zróżnicowanych potrzeb operacyjnych, wyzwań geograficznych i specyficznych zagrożeń, przed którymi stoi każdy segment sieci. Chociaż struktury technologiczne zapewniają podstawy, to ludzka zdolność do adaptacji przekształca obronną architekturę w skutecznie bronioną.

Kontrola nr 3: Widoczność i monitorowanie sieci ICS

- Zapewnij solidne monitorowanie sieci specyficznej dla ICS, w tym głęboką inspekcję pakietów dla natywnych protokołów ICS.
- Ta kontrola pomoże w wykrywaniu scenariuszy ryzyka i weryfikacji wyborów architektonicznych, zapewniając odporność nawet w przypadkach niezwiązanych z cyberatakami.

Biorąc pod uwagę skomplikowaną sieć przepływu danych w obrębie sieci energetycznej, monitorowanie nie powinno być ograniczone do powierzchownej kontroli. Głęboka inspekcja pakietów natywnych protokołów ICS jest niezbędna. Tak szczegółowa analiza pozwala na wczesne wykrywanie nieprawidłowości, co umożliwia szybkie podjęcie działań naprawczych. Poza bezpieczeństwem, monitorowanie sieci specyficznej dla ICS może dostarczyć informacji o nieefektywnościach operacyjnych, oferując podwójne korzyści. Zwłaszcza w miarę rozwoju sieci energetycznej, w tym integracji DER i technologii inteligentnych sieci, takie monitorowanie staje się kluczowe dla równoważenia efektywności z bezpieczeństwem.

Kontrola nr 4: Bezpieczny dostęp zdalny

- W dzisiejszym zdigitalizowanym świecie zdalny dostęp jest nieunikniony, ale może stanowić istotną podatność.
- Wdrażaj bezpieczne protokoły, biorąc pod uwagę, że przeciwnicy często celują w punkty dostępu zdalnego, pomijając sieci IT.

W dzisiejszych czasach rozległy charakter sieci energetycznej i rosnąca potrzeba dostępu do danych w czasie rzeczywistym sprawiają, że zdalny dostęp jest operacyjną koniecznością. Choć korzyści są oczywiste, zwłaszcza w przypadku nieprzewidzianych sytuacji, takich jak globalne pandemie, wprowadza to również istotne podatności cybernetyczne. Pytanie nie brzmi już, czy zdalny dostęp jest konieczny, ale jak można go zabezpieczyć. Ze względu na liczne punkty dostępu sieć energetyczna staje się atrakcyjnym celem dla przeciwników szukających luk w urządzeniach zdalnego dostępu. Wdrożenie solidnych, specyficznych dla sieci energetycznej mechanizmów kontroli dostępu zdalnego może przeciwdziałać tym zagrożeniom. Dzięki naciskowi na szyfrowane komunikacje, wieloskładnikowe uwierzytelnianie oraz rygorystyczne kontrole dostępu, sieć energetyczna może pozostać dostępna, nie stając się przy tym podatna na ataki.

Kontrola nr 5: Program zarządzania podatnościami oparty na ocenie ryzyka

- Skup się na podatnościach, które niosą największe ryzyko dla organizacji.
- Zastosuj podejście oparte na ocenie ryzyka, priorytetyzując podatności, które dodają nową funkcjonalność do środowiska lub są aktywnie wykorzystywane przez przeciwników.

W strukturze tak złożonej jak sieć energetyczna podatności są nieuniknione. Jednak nie wszystkie podatności niosą ze sobą takie samo ryzyko. Program zarządzania podatnościami oparty na ocenie ryzyka koncentruje się na eliminowaniu najbardziej krytycznych słabych punktów, tych, które mogą potencjalnie zakłócić przepływ energii elektrycznej na dużą skalę lub naruszyć integralność sieci. W kontekście sieci energetycznej nacisk nie jest jedynie na załatanie każdej zidentyfikowanej podatności, ale na strategiczne podejście do tych, które stanowią największe zagrożenie. Integracja wniosków z kontroli nr 3 i nr 2 pozwala na precyzyjne adresowanie podatności, zapewniając, że sieć energetyczna pozostanie odporna na rozwijające się zagrożenia.

Wnioski

Globalny sektor energetyczny, uznawany za jedno z największych osiągnięć inżynierskich XX wieku, w XXI wieku staje przed coraz bardziej złożonym i wyrafinowanym krajobrazem zagrożeń. Od skromnych początków sektor ten rozwinął się w istotną i skomplikowaną infrastrukturę, stając się celem dla rosnącej liczby cyberprzeciwników. Pojawienie się siedmiu nowych aktorów zagrażających sektorowi energetycznemu, obok działań już wcześniej zidentyfikowanych grup, podkreśla narastające wyzwania, przed którymi stoi ta krytyczna infrastruktura. Wydarzenia geopolityczne, takie jak inwazja Rosji na Ukrainę, dodatkowo komplikują sytuację, ukazując wrażliwość sektora energetycznego w obliczu międzynarodowych konfliktów oraz jego kluczową rolę w bezpieczeństwie narodowym. Te napięcia geopolityczne i wprowadzenie zaawansowanych narzędzi cybernetycznych, takich jak PIPEDREAM, zapowiadają nową erę, w której infrastruktura krytyczna nie jest już tylko biernym uczestnikiem, ale bezpośrednim celem w globalnych rozgrywkach o władzę.

Postępy technologiczne, choć napędzają sektor ku nowym wyżynom, wprowadzają również nowe podatności. Rosnące wykorzystanie rozproszonych zasobów energetycznych (DER) i technologii "inteligentnych sieci" obiecuje większą efektywność i odporność. Jednak te innowacje wprowadzają także nowe wyzwania dla obrońców, z którymi muszą się zmierzyć. Podczas gdy innowacje przekraczają granice możliwości w dystrybucji i zarządzaniu energią, wymagają one również głębszego zrozumienia i minimalizacji potencjalnych wektorów ataku. Ciągła ewolucja ransomware, w połączeniu z rosnącą jego złożonością, dodatkowo podkreśla potrzebę solidnych, proaktywnych strategii obronnych, dostosowanych do specyficznych wymagań sektora energetycznego.

Zalecenia Dragos dostarczają kompleksowej mapy drogowej do wzmocnienia obrony w odpowiedzi na te wieloaspektowe wyzwania. Od podkreślania znaczenia dostosowanego do ICS planu reagowania na incydenty, po wdrożenie programu zarządzania podatnościami opartego na ocenie ryzyka, te kontrole priorytetyzują zarówno proaktywne przygotowanie, jak i reaktywną zwinność. Globalny sektor energetyczny stoi na rozdrożu — po jednej stronie czekają innowacje, po drugiej zagrożenia związane z zakłóceniami. W miarę jak wkraczamy w erę definiowaną przez integrację technologiczną i złożoność geopolityczną, niezwykle ważne jest, aby interesariusze sektora energetycznego pozostali czujni, dobrze poinformowani i elastyczni, korzystając z wniosków i strategii ekspertów w celu ochrony naszej najważniejszej infrastruktury.

ABOUT DRAGOS, INC.

Dragos, Inc. ma globalną misję ochrony cywilizacji przed tymi, którzy próbują zakłócić infrastrukturę przemysłową, od której zależy nasza codzienność. Dragos jest prywatną firmą z siedzibą w rejonie Waszyngtonu, DC, z obecnością regionalną na całym świecie, w tym w Kanadzie, Australii, Nowej Zelandii, Europie oraz na Bliskim Wschodzie. Aby dowiedzieć się więcej na temat subskrypcji Dragos Threat Intelligence, skontaktuj się z nami w celu demonstracji.

Niniejszy raport został przygotowany i udostępniony klientom Dragos Threat Intelligence w październiku 2023 roku. Zawarte w nim informacje wywiadowcze dotyczące zagrożeń są nadal aktualne i mają zastosowanie.

info@dragos.com @DragosInc @Dragos, Inc.

CyberSecurity is in our **DNA** . apius | DRAGOS

Zapraszamy do współpracy.

Wiedza	Doświadczenie	Zaufanie	Skuteczność
80+ EKSPERTÓW I INŻYNIERÓW	430+ TECHNOLOGII I CERTYFIKATÓW	700+ ZADOWOLONYCH KLIENTÓW	1800+ ZREALIZOWANYCH PROJEKTÓW

Jesteśmy w TOP 3 rankingu dostawców rozwiązań cyberbezpieczeństwa w 2023!

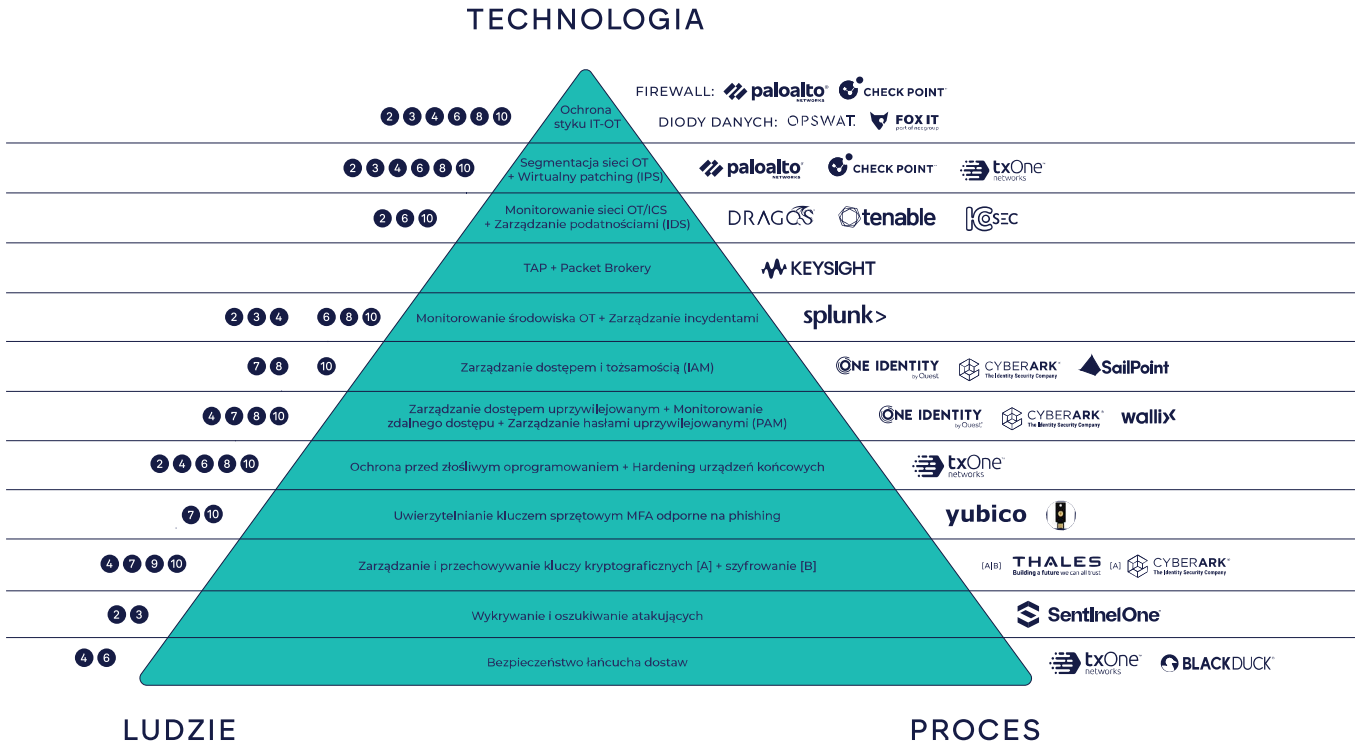
COMPUTERWORLD TOP200

Skontaktuj się z nami w celu przeprowadzenia demonstracji systemów cyberbezpieczeństwa w naszej lub Twojej infrastrukturze!

www.apius.pl

sales@apius.pl

Dyrektywa unijna NIS2. | **OT Security z Apius.**



1. Polityki dotyczące analizy ryzyka i cybersecurity
2. Obsługa incydentów
3. Ciągłość biznesowa
4. Bezpieczeństwo łańcucha dostaw
5. Ocena efektywności działań cybersecurity
6. Bezpieczeństwo w pozyskiwaniu, rozwoju i utrzymywaniu produktów, w tym zarządzanie lukami
7. Silne uwierzytelnianie i bezpieczne systemy komunikacji
8. Cyberhigiena
9. Kryptografia i szyfrowanie
10. Bezpieczeństwo zasobów ludzkich, kontrola dostępu i zarządzanie aktywami

Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej
ul. Wołyńska 22, 60-637 Poznań
tel. +48 61 846-02-00, fax: +48 61 846-02-09, www.ptpiree.pl, ptpiree@ptpiree.pl
NIP: 777-00-04-090, REGON: 004845964
SANTANDER Bank Polska 30 1090 1362 0000 0000 3601 8167