



**Wydział
Elektryczny**

POLITECHNIKA WARSZAWSKA



Instytut Elektroenergetyki
Politechnika Warszawska

UKŁAD ZDALNEGO NADZORU ZABEZPIECZEŃ WYPOSAŻONY W FUNKCJE CYBERBEZPIECZEŃSTWA

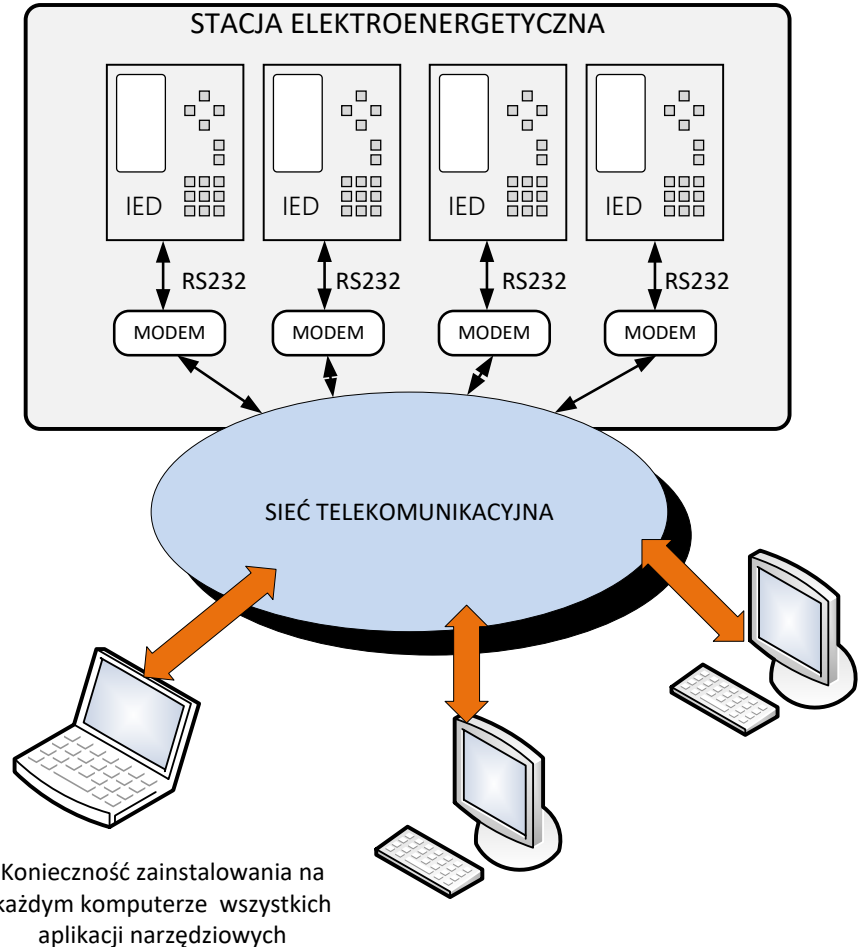
Ryszard KOWALIK, Marcin JANUSZEWSKI, Karol
KUREK,

PLAN PREZENTACJI

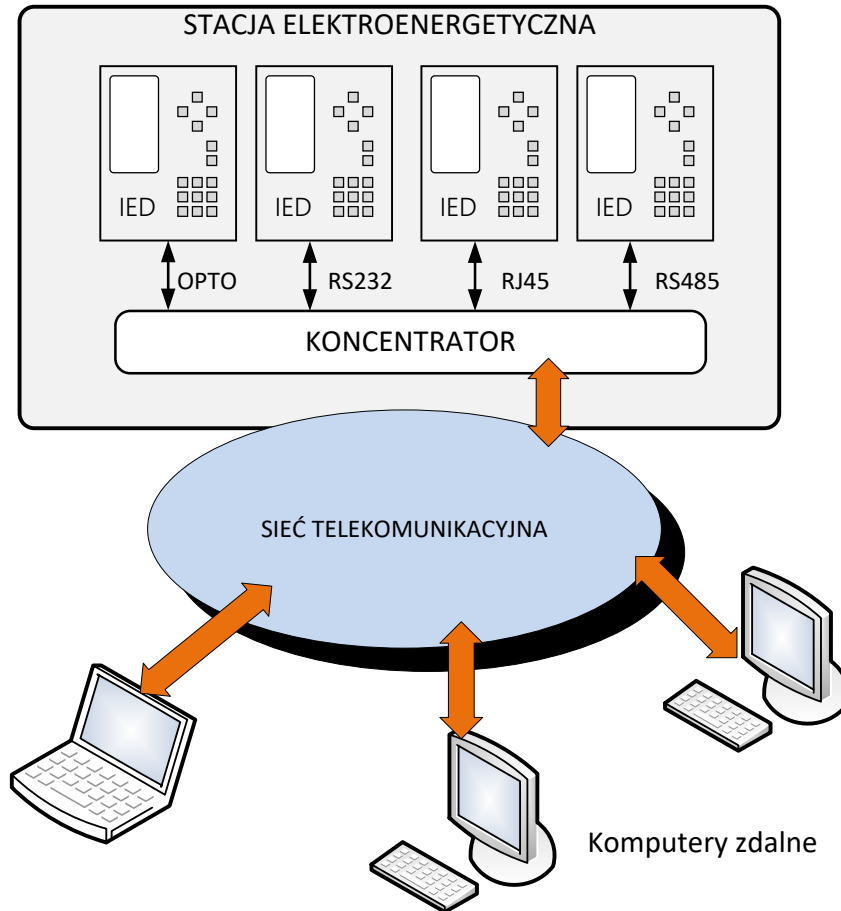
- Koncepcja koncentratora zabezpieczeń
- Najważniejsze cechy systemu zdalnego nadzoru najnowszej generacji
- Zagadnienia bezpieczeństwa informatycznego

GENEZA POWSTANIA PIERWSZYCH KONCENTRATORÓW — LATA 90 XX WIEKU

- Duże odległości
- Porty komunikacyjne w urządzeniach zabezpieczeniowych
- Połączenia rozległe oparte o modem

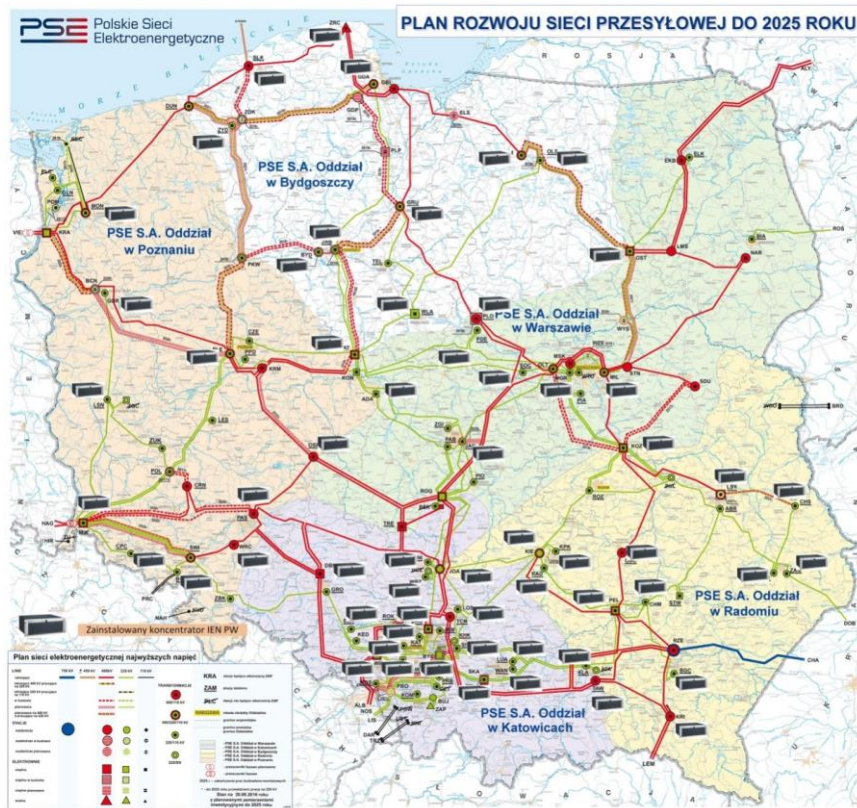


KONCEPCJA KONCENTRATORA ZABEZPIECZEŃ



- Lokalny komputer w stacji
- Komunikacja RS232 w sieci lokalnej
- W sieci rozległej kontrola komputera lokalnego

INSTALACJE

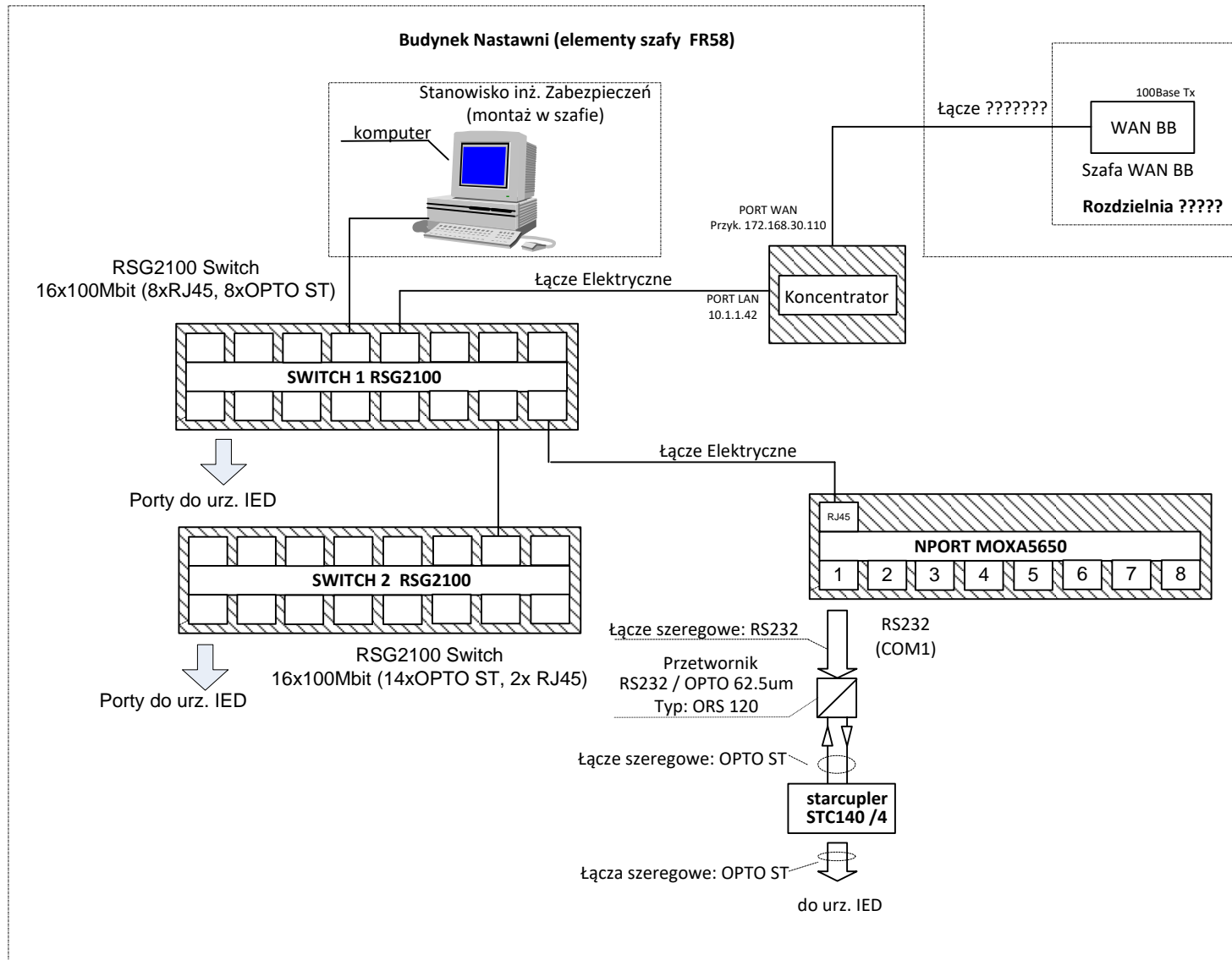


Graficzne przedstawienie lokalizacji wszystkich typów koncentratorów w stacjach elektroenergetycznych PSE S.A. (do 2015) (opracowane na bazie mapy dostępnej na stronie www.pse.pl) – aktualnie ponad 100 działających systemów



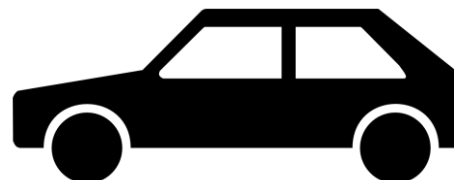
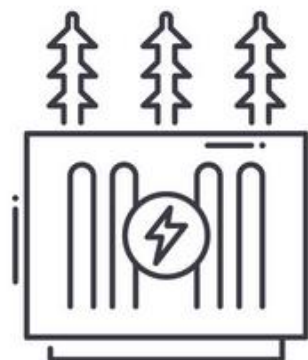
Platformy sprzętowe koncentratorów wykorzystywane od 2000 roku (najniżej na rysunku) do aktualnych (najwyżej)

ZALETY KONCENTRATORA ZABEZPIECZEŃ DZISIAJ



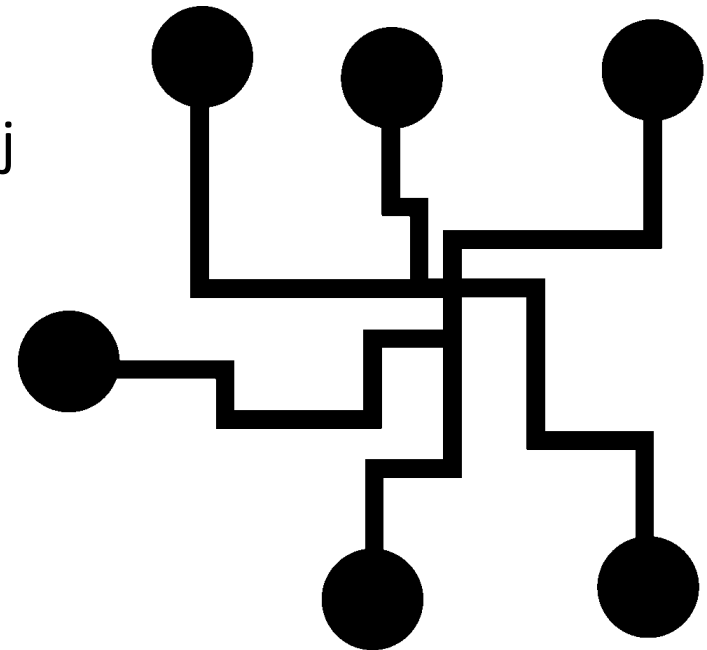
ZDALNY DOSTĘP DO NASTAW I REJESTRACJI ZAKŁÓCEŃ

Lepsze wykorzystanie zasobów i organizacja pracy



IZOLACJA KOMUNIKACJI WEWNĄTRZ SIECI LOKALNEJ

- Nieszyfrowane protokoły Modbus, DIGSI, 60870-5, COURIER, IEC 61850
- Unifikacja łącz różnych standardów
- Szyfrowanie transmisji w sieci rozległej



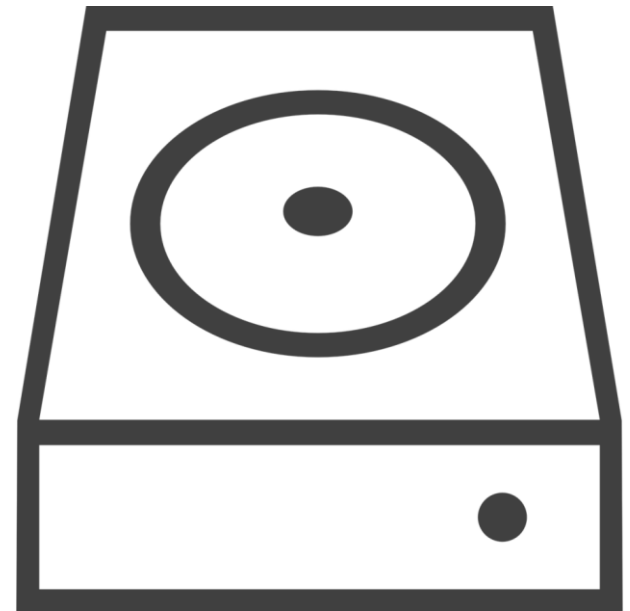
KONTROLA DOSTĘPU

- Koncentrator jako brama dostępową
- Indywidualne hasła
- Poziomy dostępu
- Integracja z usługami katalogowymi np. Active Directory



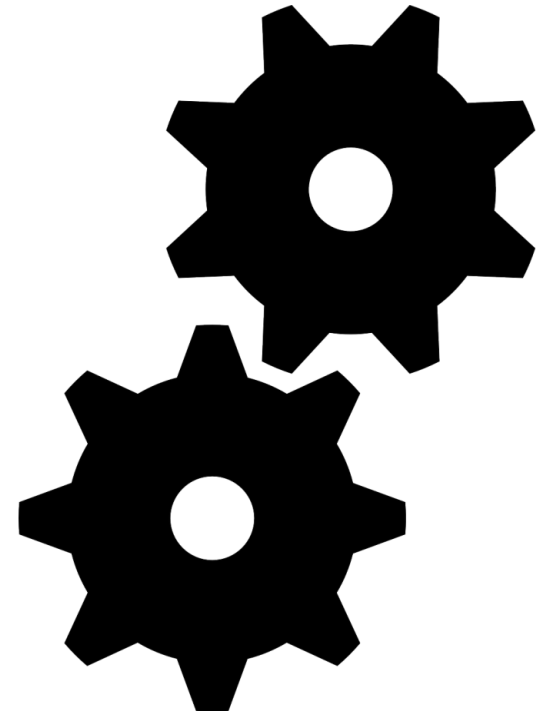
APLIKACJE I STEROWNIKI ZGROMADZONE W JEDNYM MIEJSCU

- Cały przekrój urządzeń współdziałających w stacji
- Szybki rozwój branży IT
 - Różne wersje aplikacji narzędziowych
 - Różne wersje systemów operacyjnych
- Gotowe narzędzie



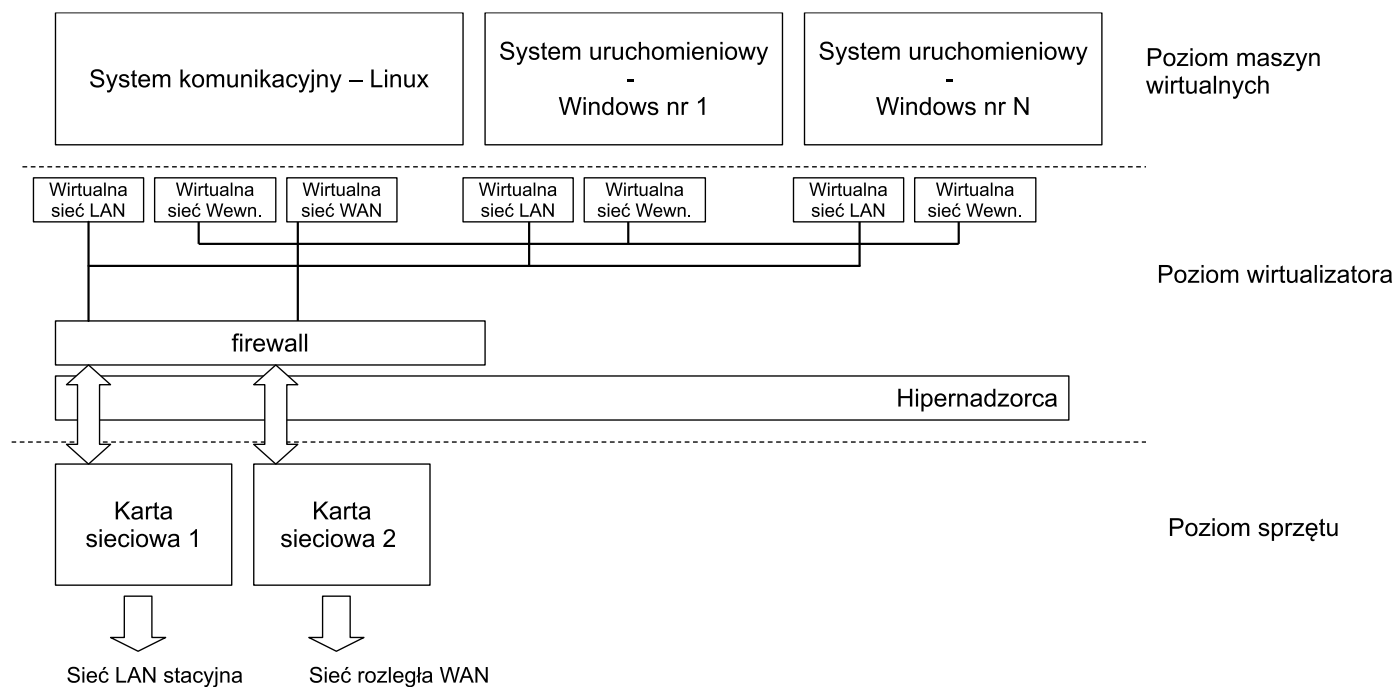
AUTOMATYZACJA RUTYNOWYCH CZYNNOŚCI

- Minimalizacja pomyłek
 - Dobór odpowiedniej wersji aplikacji
 - Gotowe projekty
 - Przypisane adresy IP
 - Automatyczne zestawianie ścieżek dla łączy szeregowych
- Proces uruchomienia łącza inżynierskiego

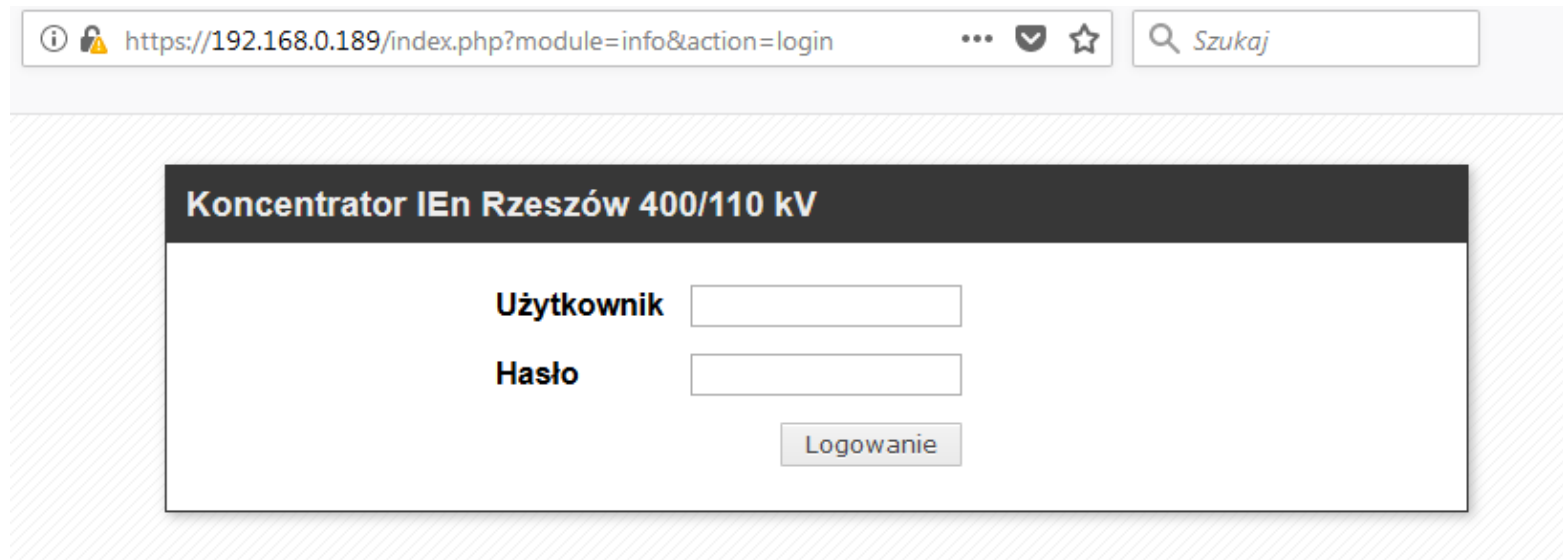


AKTUALNE ROZWIĄZANIE KS 2021

- Oparte o wirtualizację, główny system Linux i wiele systemów Windows służących za środowiska uruchomieniowe aplikacji
- Systemy Windows dowolnie dobierane w zależności od potrzeb danego obiektu



ZDALNY DOSTĘP PRZEZ PRZEGLĄDARKE PROTOKOŁEM HTTPS



https://192.168.0.189/index.php?module=info&action=login

Szukaj

Koncentrator IEn Rzeszów 400/110 kV

Użytkownik

Hasło

Logowanie

WIZUALIZACJA STACJI

Widok stacji

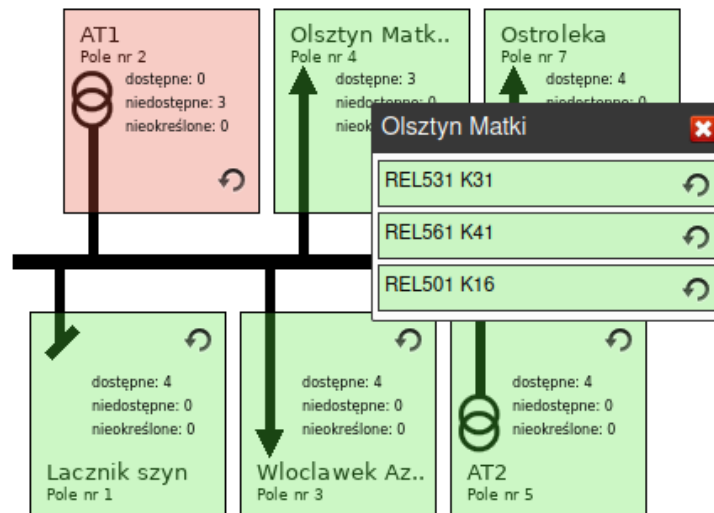
R.220kV R.110kV R.10.5kV

Odśwież urządzenia rozdzielni

Odśwież urządzenia stacji

Ogólnostacyjne	
ARST	nPort 5650
QRZ	
SZR-9 A23	

Ogólnorozdzielniane	
TL-6r	
TS-6	



Start

Stacja

Widok stacji

Konfiguracja stacji

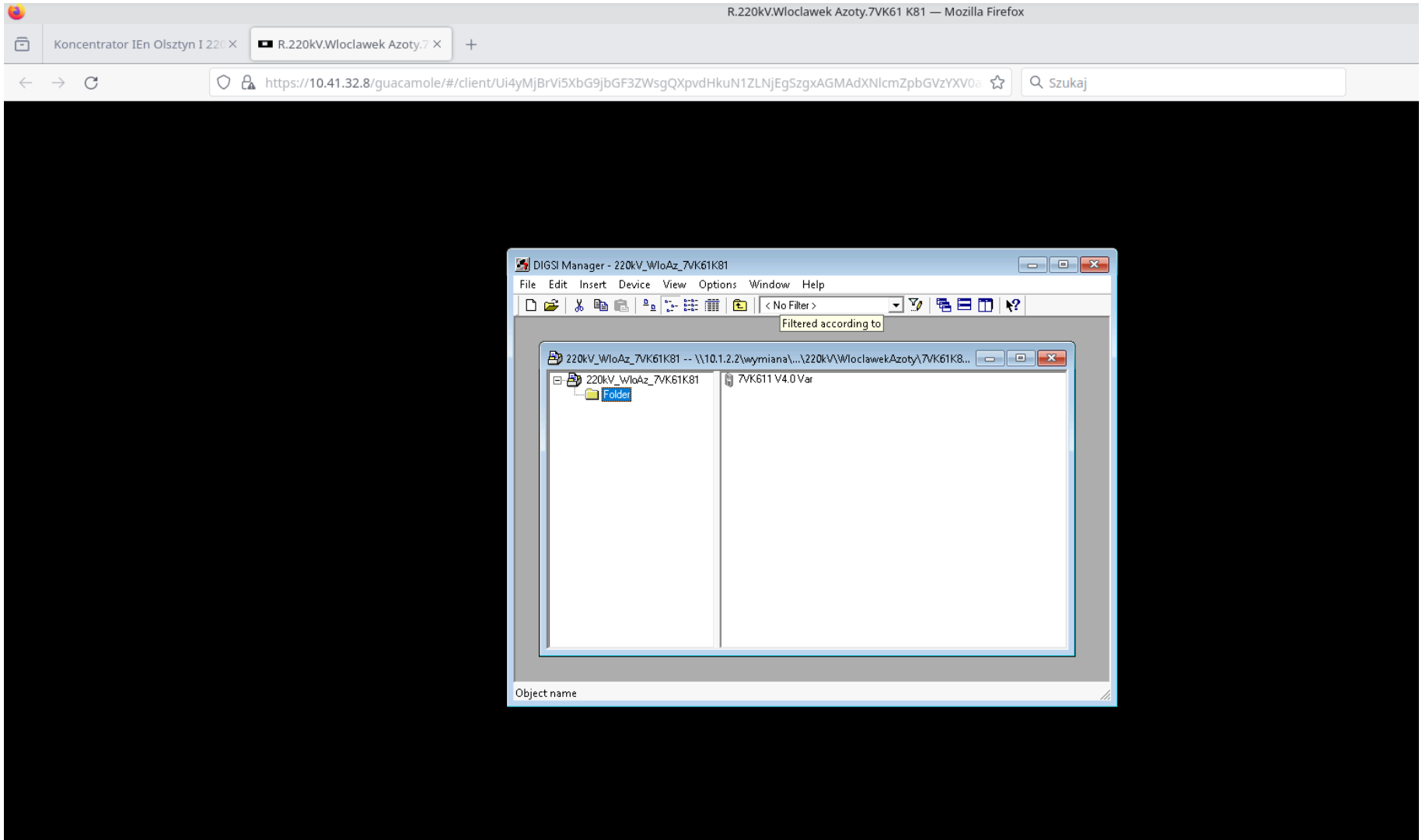
Administracja

Rejestr zdarzeń

Katalog wymiany

Wyloguj

WSPÓŁPRACA Z URZĄDZENIEM



AUTOMATYCZNE POBIERANIE REJESTRACJI ZAKŁÓCEŃ

- Istniejąca infrastruktura
- 2 razy na dobę lub ręcznie
- Powiadomienia
- Archiwizacja
- Unifikacja dostępu, bez użycia aplikacji producentów

Widok stacji

● R.110 kV ● R.15 kV s.A ● R.15 kV s.B ● R.15kV s.C ● R.15kV s.D Odśwież urządzenia rozdzielni

Ogólnostacyjne: e2Tango SZR

Ogólnorozdzielni: TSL-11

Rejestracje: 7UT86 A41

01.03.2024 09:06:08.781000	↓
05.01.2024 09:30:17.710000	↓
10.11.2023 09:06:24.131000	↓
02.10.2023 11:02:34.764000	↓
13.09.2023 09:57:23.567000	↓
18.08.2023 07:24:05.183000	↓
22.06.2023 09:04:52.615000	↓
19.06.2023 07:21:14.952000	↓
19.04.2023 15:08:46.730000	↓
03.03.2023 06:44:03.017000	↓
04.01.2023 09:09:06.963000	↓
07.12.2022 11:40:23.016000	↓
07.12.2022 11:30:59.139000	↓
07.12.2022 11:24:51.559000	↓
07.12.2022 11:06:52.545000	↓
07.12.2022 11:02:49.145000	↓
07.12.2022 11:01:44.795000	↓
07.12.2022 10:43:13.821000	↓

PRAKTYKI ZWIĄZANE Z BEZPIECZEŃSTWEM INFORMATYCZNYM

- Łącze inżynierskie będące bramą na styku dwóch rozwiązań – informatyki (IT) oraz automatyki przemysłowej
- Główne osiągnięcia w dziedzinie bezpieczeństwa informatycznego sieci i systemów zostały dokonane w dziedzinie IT.
- Odmienne praktyki stosowane przez służby IT oraz eksploatujące obiekty elektroenergetyczne

PRAKTYKI ZWIĄZANE Z BEZPIECZEŃSTWEM INFORMATYCZNYM

- Kontrola transmisji danych
 - Znane i przetestowane protokoły, szyfrowanie danych
 - Ograniczanie ruchu do wymaganego minimum
 - Izolacja systemów uruchomieniowych od sieci rozległej
- Dopasowanie oprogramowania
 - Minimalny zestaw oprogramowania do realizacji stawianych zadań
 - Minimalny zestaw uprawnień systemu operacyjnego
- Zbieranie i przesyłanie rejestrów do systemów nadrzędnych
- Eliminacja znanych podatności poprzez wgrywanie łatek bezpieczeństwa
- Okresowe testy penetracyjne realizowane przez niezależne laboratoria
- Kopie bezpieczeństwa

WDROŻENIE POPRAWEK BEZPIECZEŃSTWA

1. Okresowe monitorowanie podatności oraz określenie podatności.
2. Wgranie poprawek bezpieczeństwa w systemie testowym.
3. Testy bezpieczeństwa i stabilności systemu testowego w warunkach zbliżonych do produkcyjnych.
4. Implementacja poprawek bezpieczeństwa w systemach produkcyjnych.

PODSUMOWANIE

Do największych problemów, z którymi mierzą się koncentratory IEN PW nowej generacji należą:

- szybki rozwój branży IT,
- bardzo duża liczba urządzeń w stacji z różnych okresów produkcji,
- większe niż wcześniej zagrożenie atakami cybernetycznymi urządzeń i infrastruktury energetycznej.

PODSUMOWANIE

- Systemy najnowszej generacji instalowane od 2019 roku
 - PSE – 17 instalacji zakończone i 6 w trakcie,
 - STOEN Operator - 21 instalacji zakończonych i 6 w trakcie.
 - PGE o. Warszawa – 3 instalacje zakończone, 1 w trakcie.

Dziękuję za uwagę