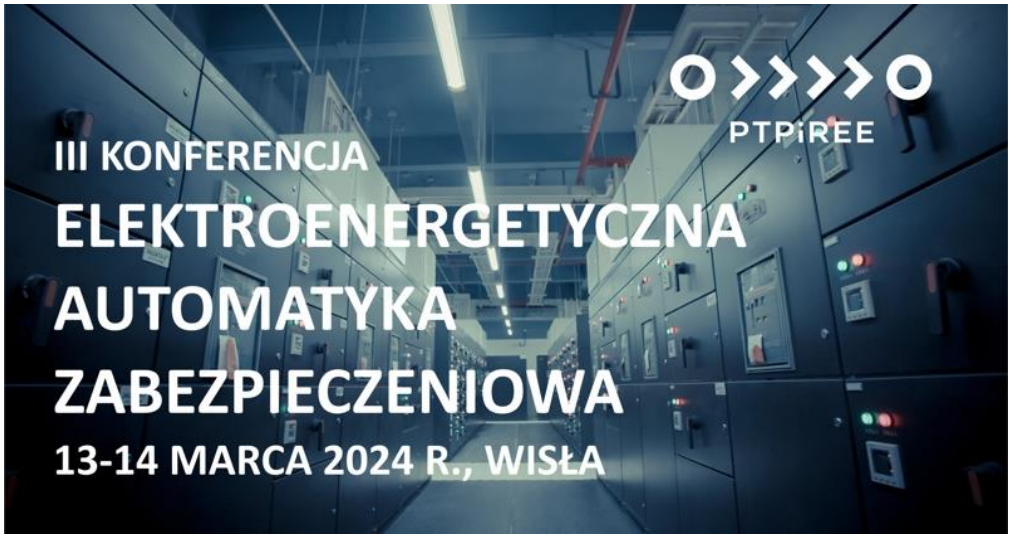
PTPiREE

III KONFERENCJA

ELEKTROENERGETYCZNA AUTOMATYKA ZABEZPIECZENIOWA

13-14 marca 2024 r., Wisła

PTPiREE



III Konferencja

ELEKTROENERGETYCZNA AUTOMATYKA ZABEZPIECZENIOWA

13-14 marca 2024 r., Wisła (Hotel Gołębiewski)

Organizator

PTPiREE

Patronat medialny

ENERGIA Elektryczna

Materiały konferencyjne
zostały przygotowane na podstawie
składów komputerowych
dostarczonych przez Autorów

Wydawca: 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 e-mail: ptpiree@ptpiree.pl

SPIS TREŚCI

Referaty zostały umieszczone w materiałach zgodnie z kolejnością nadsyłania

UKŁAD ZDALNEGO NADZORU ZABEZPIECZEŃ WYPOSAŻONY W FUNKCJE CYBERBEZPIECZEŃSTWA

Ryszard Kowalik, Karol Kurek, Marcin Januszewski (Politechnika Warszawska)

Streszczenie

W artykule przedstawiono opis rozwiązania układu zdalnego nadzoru zabezpieczeń, spełniającego wymagania cyberbezpieczeństwa stacji elektroenergetycznych. Opisano zalety stosowania tego rodzaju systemu nazywanego czasami łączem inżynierskim wyposażonym w koncentrator zabezpieczeń. Pokazano zmiany zachodzące w ostatnich latach w wykonaniu i pełnionych funkcjach takich systemów oraz przedstawiono kilka innowacyjnych cech nowego rozwiązania opracowanego przez autorów. W artykule dodatkowo opisano najważniejsze praktyki pozwalające na zwiększenie bezpieczeństwa eksploatowanych systemów zdalnego dostępu do urządzeń automatyki zainstalowanych w stacjach elektroenergetycznych oraz doświadczenia zdobyte w trakcie instalacji i eksploatacji kilkudziesięciu układów tego typu zainstalowanych w stacjach przesyłowych oraz dystrybucyjnych.

1. Wstęp

Układy Automatyki Elektroenergetycznej stosowane w Krajowym Systemie Elektroenergetycznym od początku lat 90 zeszłego stulecia, wyposażano w urządzenia mikroprocesorowe, które miały porty telekomunikacyjne pozwalające na łatwą zamianę nastawień za pomocą programów narzędziowych uruchamianych na komputerach PC.

Zabezpieczenia początkowo były wyposażane w porty asynchroniczne zazwyczaj RS232, pozwalające na transmisję na niewielkie odległości (do kilkudziesięciu m) z niedużymi prędkościami (do kilkunastu kb/s). Porty te były dedykowane do lokalnej zmiany nastawień i w założeniu miały ułatwić proces nastawiania cyfrowych zabezpieczeń. Potencjalna możliwość zdalnego nastawiania zabezpieczeń w odległych stacjach elektroenergetycznych (bez konieczności odbywania długich dojazdów), spowodowała chęć opracowania bezpiecznej metody zdalnego dostępu.

Wychodząc naprzeciw tym oczekiwaniom, w 1996r w Instytucie Elektroenergetyki PW został opracowany pierwszy polski system zdalnego nadzoru nad urządzeniami automatyki stacji elektroenergetycznej nazywany często łączem inżynierskim, ponieważ był używany przez inżynierów wydziałów zabezpieczeń.

Pierwsza wersja łącz inżynierskich jako platformy sprzętowej wykorzystywała komputer przemysłowy z zainstalowanym systemem Windows i aplikacjami inżynierskimi właściwymi do wymiany danych z mikroprocesorowymi urządzeniami zabezpieczeniowymi zainstalowanymi w danej stacji. W stacji musiała zostać wykonana infrastruktura telekomunikacyjna (łącza telekomunikacyjne) pomiędzy jednostką centralną łącza inżynierskiego, a urządzeniami zabezpieczeniowymi podlegającymi nadzorowi. Zdalne połączenie do systemu możliwe było przy wykorzystaniu dodatkowego oprogramowania takiego jak pcAnywhere lub klient RDP.

W czasie ponad dwudziestu lat zmianom uległy zarówno urządzenia zabezpieczeniowe instalowane w stacji, jak i ich porty komunikacyjne, oprogramowanie inżynierskie oraz wymagania stawiane bezpieczeństwu informatycznemu systemów instalowanych w systemie

elektroenergetycznym. Dzisiaj nowa infrastruktura telekomunikacyjna stacji budowana jest w przeważającej większości w oparciu o sieci standardu Ethernet, co pociąga za sobą nowe wyzwania dla bezpieczeństwa urządzeń i stacyjnej sieci telekomunikacyjnej.

Biorąc pod uwagę czas życia stacji elektroenergetycznych można w nich spotkać cały przekrój urządzeń, korzystających z łącz RS232, RS485 i Ethernet jak również często wymagających specjalistycznego oprogramowania opracowanego w czasach systemów operacyjnych Windows 2000 czy XP. W 2018 roku biorąc pod uwagę rosnącą świadomość bezpieczeństwa informatycznego i w celu sprostania specyfice stacji elektroenergetycznych stworzona została nowa wersja łącza inżynierskiego. Pozwala ona nie tylko zapewnić bezpieczeństwo informatyczne połączeń zdalnych, ale również zapewnić dużą elastyczność eksploatacyjną integrując wszystkie urządzenia automatyki stacji elektroenergetycznej (co warto podkreślić bez względu na generację), w jeden spójny system.

2. Korzyści z zastosowania koncentratora zabezpieczeń

Podstawowym zadaniem koncentratora zabezpieczeń jest udostępnienie możliwości pewnego i niezawodnego zdalnego nadzoru nad urządzeniami zabezpieczeniowymi stacji elektroenergetycznej. Jak wspomniano we wstępie był to główny cel przyświecający powstaniu pierwszego koncentratora zabezpieczeń. Aktualnie wraz z rozwojem techniki i skomplikowaniem urządzeń wchodzących w skład układów zabezpieczeń, lista wyzwań z jakimi musi mierzyć się eksploatujący je inżynier znacznie wzrosła. Poniżej zebrano i zaprezentowano główne korzyści ze stosowania koncentratora zabezpieczeń.

2.1. Zdalny dostęp do nastaw i rejestracji zakłóceń

System elektroenergetyczny z uwagi na swoją rozległą strukturę sprawia, że każda konieczność przeglądu stanu czy ingerencji w ustawienia urządzeń zabezpieczeniowych wiąże się z podróżą do często odległego miejsca. Ograniczone zasoby ludzkie i czas potrzebny na przejazdy mogą powodować, że praca zespołów eksploatujących urządzenia zabezpieczeniowe staje się nieefektywna. Stan ten potęguje się w momencie wystąpienia zdarzenia wpływającego na pracę systemu elektroenergetycznego, wymagającego jak najszybszego dotarcia do wielu miejsc w jak najkrótszym czasie. Zdalny dostęp do stacji pozwala na lepsze wykorzystanie zasobów i organizację pracy.

2.2. Izolacja komunikacji wewnątrz sieci lokalnej

Dostęp zdalny do urządzeń bez wykorzystania koncentratora zabezpieczeń może być zrealizowany przez bezpośrednie wykorzystanie sieci technologicznej spółki. W takim przypadku zwykle urządzenia zabezpieczeniowe włączane są z wykorzystaniem dedykowanych portów Ethernet lub przez serwery portów szeregowych do sieci rozległej. W związku z powyższym wymiana danych między urządzeniem automatyki zainstalowanym w stacji elektroenergetycznej oraz komputerem inżyniera zlokalizowanym zwykle w siedzibie spółki, jest realizowana przez sieć rozległą. Takie podejście wiąże się z dwoma zagrożeniami: zagrożeniem bezpieczeństwa wymiany danych oraz zagrożeniem stabilności połączenia. Dla tego rodzaju rozwiązania zagrożenie bezpieczeństwa wymiany danych wiąże się z tym, że urządzenia zabezpieczeniowe w przeważającej większości wykorzystują nieszyfrowane protokoły telekomunikacyjne takie jak modbus lub protokoły z rodziny 60870-5. Ponadto urządzenia

umożliwiają często bezpośrednie sterowanie swoimi wyjściami lub zmianę nastaw przy pomocy zmiany rejestrów nieszyfrowanym protokołem bez dodatkowej autoryzacji. W związku z powyższym przy zdalnym dostępie bez koncentratora zabezpieczeń każda osoba uzyskująca dostęp do sieci spółki jest więc w stanie wpłynąć na dowolne parametry pracy zabezpieczeń oraz sterować np. łącznikami w polach stacji.

Stacje elektroenergetyczne budowane zwykle na peryferiach miast często wykorzystują do wymiany danych łącza radiowe, które mogą być niestabilne. Zakłócenie wymiany danych podczas transferu np. nastaw z aplikacji narzędziowej do zabezpieczenia może spowodować w skrajnym przypadku uszkodzenie integralności jego nastaw i w konsekwencji niewłaściwe działanie.

Zastosowanie koncentratora zabezpieczeń pozwala na zamknięcie nieszyfrowanej transmisji danych na drodze między aplikacją narzędziową i urządzeniem zabezpieczeniowym, czyli w sieci lokalnej stacji, cechującej się dużo większą stabilnością i niezawodnością – opartej często na połączeniach światłowodowych. Na zewnątrz stacji pomiędzy terminalem użytkownika w siedzibie spółki, a koncentratorem zabezpieczeń pojawia się jedynie szyfrowany ruch protokołu https, w którym przesyłane są jedynie ruchy myszki, dane pochodzące z klawiatury lub inne sterowania pracą koncentratora. Zakłócenie komunikacji pomiędzy użytkownikiem, a koncentratorem zabezpieczeń nie ma żadnego wpływu na komunikację z urządzeniem zabezpieczeniowym. Transfer nastawień do zabezpieczenia zostanie ukończony nawet w przypadku pełnego zerwania komunikacji zewnętrznej do stacji elektroenergetycznej.

2.3. Kontrola dostępu

Koncentrator zabezpieczeń stanowi bramę dostępu do urządzeń zabezpieczeniowych. Zwykle jest instalowany na styku dwóch sieci – lokalnej sieci stacyjnym oraz sieci rozległej. W celu komunikacji z urządzeniami stacyjnymi konieczne jest zalogowanie do systemu osobistym hasłem. Pozwala to na wprowadzenie dodatkowej bariery uniemożliwiającej niepowołanym użytkownikom na dostęp do urządzeń zabezpieczeniowych. W związku z tym nawet uzyskanie fizycznego dostępu do sieci technologicznej spółki nie będzie skutkowało automatyczną możliwością ingerencji w stan urządzeń stacji i sterowanie ich pracą. Koncentrator zabezpieczeń pozwala ponadto na zróżnicowane poziomy dostępu – jednym użytkownikom udostępniając tylko podstawowe możliwości komunikacyjne, natomiast innym pozwalając na czynności administracyjne i wpływanie na konfigurację wewnętrzną koncentratora. Dodatkową możliwością zwiększenia bezpieczeństwa jest autoryzacja w oparciu o zewnętrzny serwer uwierzytelniający np. ActiveDirectory, dający możliwość bieżącej kontroli nad tym kto i z jakim poziomem uprawnień powinien mieć dostęp do systemu. Warto dodać, że działania każdego użytkownika są również rejestrowane i możliwe do prześledzenia za pośrednictwem rejestru zdarzeń (logowania, połączenie z zabezpieczeniem, zmiana konfiguracji, pobranie i wysłanie plików).

2.4. Aplikacje narzędziowe i sterowniki zgromadzone w jednym miejscu

Wraz z rozwojem urządzeń, pojawianiem się ich nowych wersji i kolejnych generacji rośnie poziom skomplikowania zestawu narzędzi potrzebnych do poprawnej wymiany danych. Dodatkowym problemem jest szybkość pojawiania się nowych wersji systemów operacyjnych, których czas życia jest zdecydowanie krótszy od czasu życia stacji elektroenergetycznych.

Inżynier zabezpieczeń chcący prowadzić eksploatację urządzeń zabezpieczeniowych musi zbudować swoją własną bazę aplikacji i sterowników do urządzeń na własnym komputerze. Biorąc pod uwagę konieczność wymiany danych z urządzeniami zainstalowanymi nawet ponad 20 lat temu oraz różnorodności wersji oprogramowania wewnętrznego tych samych przekaźników, wymaga to posiadania starszych wersji aktualnie niewspieranych systemów operacyjnych, co jest zwykle bardzo trudnym zadaniem, pochłaniającym więcej czasu niż zadanie np. zmiany parametrów funkcji zabezpieczeniowej, które należy przy ich pomocy wykonać. Biorąc pod uwagę rotację pracowników może to być czynnik znacznie obniżający efektywność wykonywanej pracy.

Koncentrator zabezpieczeń jest urządzeniem, w którym zainstalowany jest właściwa liczba właściwych systemów operacyjnych, aplikacji narzędziowych w odpowiednich wersjach oraz potrzebnych sterowników do komunikacji ze wszystkimi urządzeniami stacji elektroenergetycznej. Inżynier zabezpieczeń niezależnie od swojego stażu pracy, dostaje dostęp do systemu wyposażonego we wszystkie potrzebne narzędzia i pozwala na skupienie się na wykonywanym zadaniu. Jedyną aplikacją wymaganą do komunikacji z koncentratorem jest przeglądarka internetowa.

2.5. Automatyzacja rutynowych czynności

Praca z urządzeniami infrastruktury krytycznej jakimi są zabezpieczenia elektroenergetyczne nie powinna być związana z dużym ryzykiem pomyłek. Inżynier zabezpieczeń chcąc zmienić zdalnie nastawy zabezpieczeń musi znać nie tylko wersję aplikacji i sterowników które potrzebuje do danego urządzenia, ale również musi wprowadzić właściwy adres IP lub przełączyć ręcznie kanały urządzeń telekomunikacyjnych takich jak multipleksery optyczne. Wykonanie pomyłki w którejś z czynności może powodować zmianę nastaw w niewłaściwym urządzeniu i w konsekwencji błędne działanie zabezpieczeń.

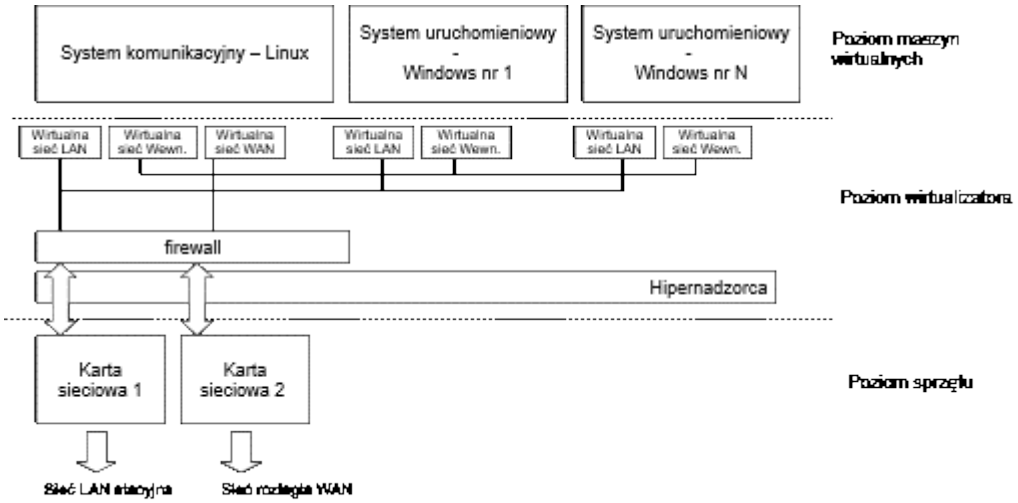
Koncentrator zabezpieczeń zdejmuje z użytkownika konieczność pamiętania adresów IP czy numerów kanałów komunikacyjnych. W procesie uruchomienia łącza inżynierskiego powiązania systemu są każdorazowo sprawdzane, dostarczając użytkownikowi system, w którym musi jedynie kliknąć w nazwę urządzenia, z którym chce się skomunikować. Wszystkie czynności takie jak aplikacji i projektu ze skonfigurowanymi parametrami komunikacyjnymi i zestawienie kanałów telekomunikacyjnych są wykonywane automatycznie.

3. Obecny układ bramy zdalnego dostępu do urządzeń automatyki stacji elektroenergetycznej

Bazując na zdobytych przez ponad 20 lat doświadczeniach oraz analizując potrzeby aktualnych użytkowników, w 2018r. powstała kolejna generacja łącza inżynierskiego nazywanego obecnie bramą zdalnego dostępu do urządzeń automatyki stacji elektroenergetycznej (GRA), zgodna z wymaganiami zawartymi w [2], [3]. Wykorzystuje przede wszystkim rozwiązania typowo sieciowe, jednak zachowana została pełna wsteczna kompatybilność z oprogramowaniem narzędziowym oraz infrastrukturą połączeń istniejącą nawet w starszych stacjach elektroenergetycznych. Zachowana została możliwość wykorzystania istniejącej w stacjach infrastruktury połączeń telekomunikacyjnych między starymi rozwiązaniami koncentratorów a urządzeniami IED.

Nowa wersja łącza inżynierskiego została oparta o technologię wirtualizacji systemów operacyjnych (Rys. 1). Zaletami wirtualizacji jest możliwość obsługi urządzeń dowolnej generacji, w tym zarówno urządzeń z końca XX wieku jak i najnowszych, dopiero wprowadzanych na rynek. Co więcej tego rodzaju technologia umożliwia również rozwiązanie potencjalnych problemów związanych z niekompatybilnością wersji oprogramowania. Problem ten daje się zauważyć podczas prac eksploatacyjnych. Może wystąpić np. podczas prowadzonych zmian na stacji, w przypadku, gdy instalowane są przekaźniki w wersjach oprogramowania nowszych niż przekaźniki już istniejące. Powoduje to problem różnych wersji aplikacji narzędziowych, ponieważ nowy, instalowany właśnie przekaźnik wymaga wersji nowszej niż już zainstalowana na koncentratorze, natomiast starsze przekaźniki wymagają wersji używanej podczas ich uruchomienia. Rozwiązaniem jest zainstalowanie kilku wersji tej samej aplikacji na różnych systemach wirtualnych, dzięki czemu nie ingeruje się w już systemy współpracujące z działającymi dotychczas na stacji przekaźnikami i gwarantuje się ich bezproblemowe dalsze działanie.

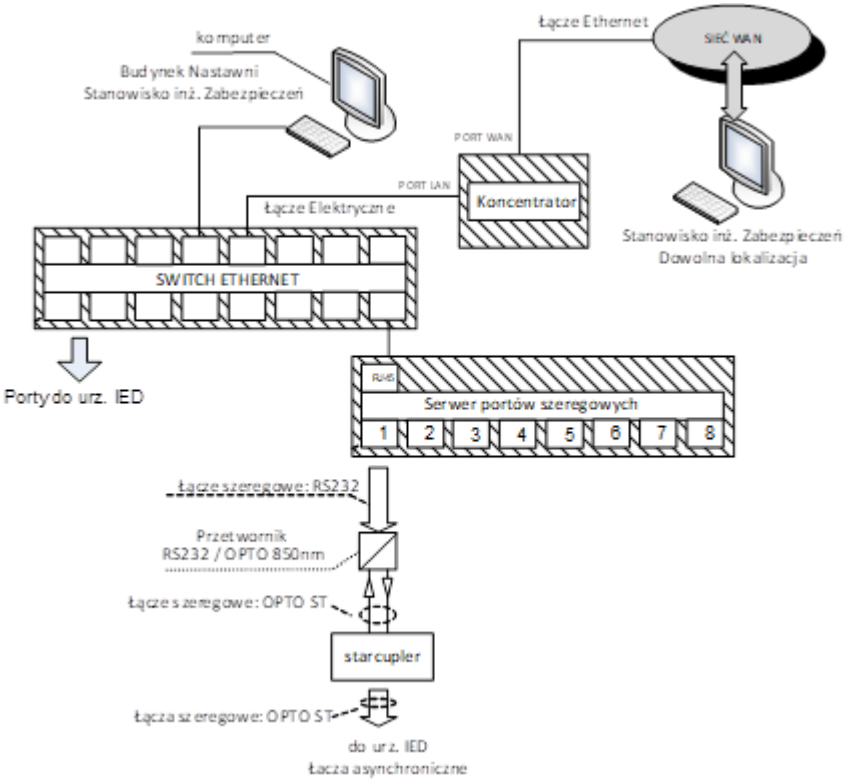
Ważną cechą nowej wersji bramy zdalnego dostępu do urządzeń automatyki stacji elektroenergetycznej jest system Linux pełniący funkcje komunikacyjne tj. udostępniający wszystkie usługi sieciowe widoczne na zewnątrz koncentratora takie jak serwer WWW (dostęp do interfejsu koncentratora protokołem https) i serwer IEC 61850 (raportowanie stanu koncentratora do SSiN) oraz inne usługi pomocnicze np. tester drożności kanałów komunikacyjnych. Systemy Windows pełnią rolę środowisk uruchomieniowych dla aplikacji narzędziowych, a ich liczba i rodzaj jest uzależniony tylko możliwościami technicznymi sprzętu na jakim zrealizowano koncentrator. Pozwala to na uruchomienie kilku równoległych systemów Windows, pozostawiając rezerwę dla nowych systemów w przyszłości.



Rys. 1. *Struktura koncentratora zabezpieczeń oparta o wirtualizację*

W nowym rozwiązaniu główny nacisk położono na wykorzystanie do wymiany danych z zabezpieczeniami połączeń Ethernet, a w mniejszym zakresie połączeń asynchronicznych. Odpowiada to zmianom zachodzącym w urządzeniach i układach automatyki stacji elektroenergetycznych. Praktycznie wszyscy producenci urządzeń przechodzą aktualnie na łącza Ethernet, a porty asynchroniczne np. RS232 stopniowo zanikają. W związku z tym, zmianie ulegają również połączenia telekomunikacyjne wykorzystywane w układzie bramy zdalnego dostępu do urządzeń automatyki stacji elektroenergetycznej, co przedstawiono na rys. 2. Głównymi elementami w infrastrukturze wspomnianych połączeń telekomunikacyjnych są

przełączniki Ethernet, natomiast połączenia asynchroniczne realizowane są poprzez serwery portów szeregowych i zachowane ze starszych wdrożeń przełączniki optyczne łącz asynchronicznych. Dzięki zachowaniu takiej struktury łącz telekomunikacyjnych możliwe jest łatwe dopasowanie starych układów połączeń do nowej wersji bramy zdalnego dostępu.



Rys. 2. *Przykładowy, uproszczony, schemat infrastruktury telekomunikacyjnej dla bramy zdalnego dostępu do urządzeń automatyki elektroenergetycznej, dla aktualnego rozwiązania bazującego na rozwiązaniach sieciowych*

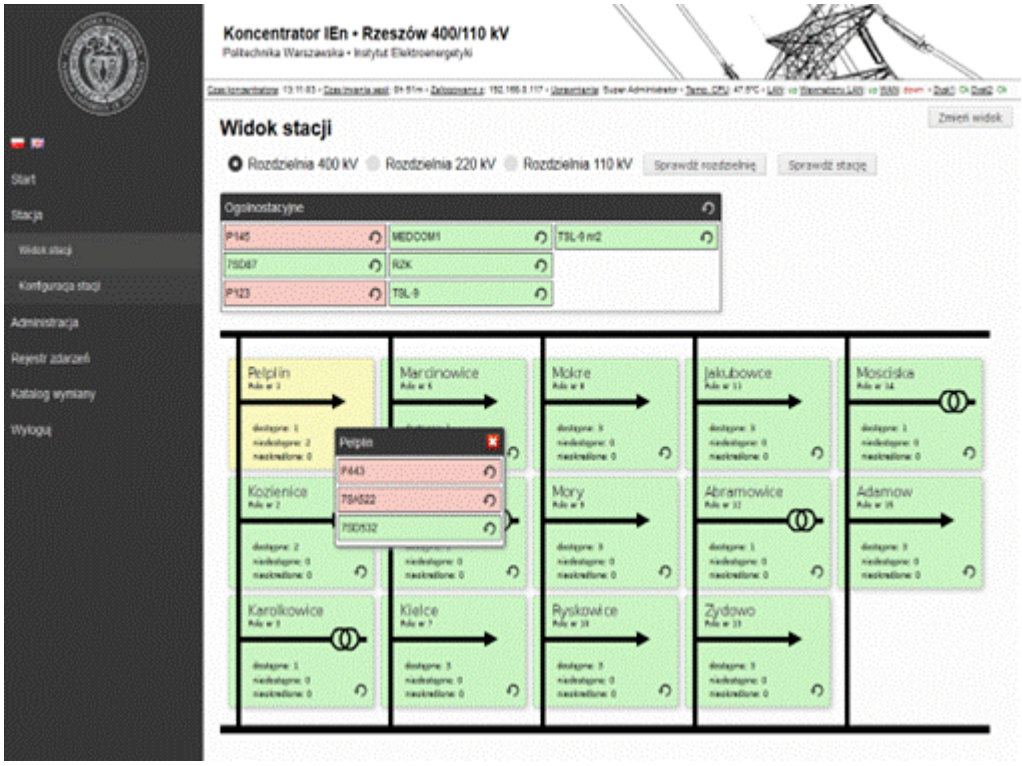
Nowa wersja łącza inżynierskiego wykorzystuje do obsługi zdalnych połączeń szyfrowany protokół https. Oznacza to, że do połączenia z koncentratorem i zdalnego nastawiania oraz nadzoru zabezpieczeń, wystarczy jedynie przeglądarka internetowa zainstalowana na własnym komputerze i znajomość numeru IP koncentratora. Widok aplikacji z pokazanymi przekaźnikami podłączanymi do przykładowej stacji pokazano na rys. 3. Za jej pomocą na koncentratorze można wykonać operacje takie jak:

- wizualizacja struktury i stanu stacji (rozdzielnie, pola, urządzenia),
- praca z programem narzędziowym i wymiana danych z urządzeniami IED,
- automatyczne zestawianie połączeń punkt-punkt z wybranym urządzeniem,
- automatyczne uruchamianie projektu aplikacji narzędziowej, z dostępem tylko do wybranego urządzenia,
- dostęp do plików zapisanych na koncentratorze przez tzw. katalog wymiany, pozwalający na pobranie i wysłanie np. rejestracji zakłóceń,
- dostęp do funkcji administracyjnych takich jak:
  - rejestr zdarzeń,
  - administracja użytkownikami,
  - administracja uruchomieniowymi systemami operacyjnymi (zmiana oprogramowania inżynierskiego),
  - ustawienia wewnętrzne koncentratora,

Dostępność poszczególnych funkcji koncentratora, zależy od poziomu dostępu konta, na które użytkownik wykonał logowanie. Każdy z użytkowników systemu powinien posiadać osobiste konto, według którego rozliczana jest jego aktywność w rejestrach zdarzeń. System pozwala na pracę jednego użytkownika w danej chwili. Logowanie posiada podstawowe zabezpieczenia w postaci czasowej blokady po kilkukrotnym wpisaniu nieprawidłowego hasła.

Typowym schematem pracy z koncentratorem jest wybór jednej z rozdzielni (rys. 3), następnie pól i urządzenia, z którym ma zostać nawiązana komunikacja. Po jego wybraniu zostaną automatycznie wykonane następujące czynności:

- zestawienie kanału komunikacyjnego tylko do wybranego urządzenia (poprzez multiplekser optyczny bądź wybór portu przełącznika sieciowego),
- uruchomienie aplikacji narzędziowej dedykowanej do obsługi urządzenia wybranego typu,
- załadowanie projektu z dostępnym tylko pojedynczym wybranym urządzeniem,
- otwarcie nowej karty przeglądarki, umożliwiającej zdalny dostęp do systemu uruchomieniowego z przygotowaną do pracy aplikacją narzędziową.



Rys. 3. *Ekran wizualizacji stacji, brama zdalnego dostępu najnowszej generacji*

Jedną z dodatkowych funkcjonalności koncentratora jest automatyczne sprawdzenie drożności kanałów do poszczególnych zabezpieczeń. Jest to wykonywane z zadanym interwałem jak również może być wykonane na żądanie użytkownika. Stan kanału jest odnotowywany poprzez zmianę koloru podświetlenia przycisku wybranego zabezpieczenia oraz stosowny wpis do rejestru zdarzeń. Nową funkcjonalnością rozwojową którą łącze inżynierskie może dokonywać podczas sprawdzeń drożności kanałów jest sprawdzenie dostępności nowych rejestracji zakłóceń w nadzorowanych urządzeniach zabezpieczeniowych. Rejestracje te są automatyczne ściągane i archiwizowane w jednostce centralnej, a użytkownik jest powiadamiany o nowych zdarzeniach z możliwością ich przejrzenia bez wykorzystania aplikacji producenckich.

Funkcjonalność automatycznego odczytywania rejestracji uruchomiona na koncentratorze w stacji, może stanowić wstęp stworzenia do centralnego systemu archiwizacji rejestracji zakłóceń umożliwiającego odbieranie i archiwizację rejestracji pochodzących ze wszystkich stacji objętych systemami łącza inżynierskiego. Centralne dane mogłyby pozwolić do tworzenia cyklicznych np. dobowych raportów z działania automatyki zabezpieczeniowej.

W stanie niezalogowania koncentrator wykonuje stały nadzór nad kanałami telekomunikacyjnymi z określonym interwałem, odnotowując ich zmiany w rejestrze zdarzeń. Ponadto są one raportowane do systemu sterowania i nadzoru protokołem IEC 61850. Dodatkową informacją przesyłaną do systemu sterowania jest stan zalogowania do koncentratora.

4. Praktyki związane z bezpieczeństwem informatycznym

Główne osiągnięcia w dziedzinie bezpieczeństwa informatycznego sieci i systemów zostały dokonane w dziedzinie informatyki (IT).

Łącze inżynierskie jest elementem będącym na styku dwóch rozwiązań– świata rozwiązań IT oraz automatyki przemysłowej. Obydwa działy cechują się zasadniczo odmiennym podejściem do stawianych im zadań. Dla osób zajmujących się automatyką najważniejszym zadaniem jest zapewnienie ciągłości nadzorowanego procesu. Jego przerwanie może prowadzić do bezpośrednich strat finansowych i utraty stabilności systemu elektroenergetycznego. Zorientowanie na nieprzerwalność procesu nie pojawia się zwykle w systemach, z którymi pracują osoby zajmujące się zagadnieniami IT. Podobnie zapewnienie bezpieczeństwa informacji jest kluczowym czynnikiem w typowych systemach IT, natomiast w systemach produkcyjnych automatyki jest zdecydowanie mniej ważne od bezpieczeństwa obsługi i ciągłości procesu.

Bezpieczeństwo informatyczne powinno stanowić jeden z fundamentów przy projektowaniu łącza inżynierskiego, jednak zastosowane praktyki powinny brać pod uwagę wymagania zarówno automatyki jak i IT. W tabeli 1 zebrano wybrane różnice pomiędzy podejściem dla typowego systemu IT oraz systemu automatyki EAZ [5].

Tabela 1. *Analiza zdarzeń i skutków dla systemów IT i systemów EAZ [5]*

Problem	System IT	System EAZ
Stosowanie łatek bezpieczeństwa	Łatki oprogramowania nakładane rutynowo w systemach produkcyjnych.	Łatki oprogramowania nakładane okazjonalnie, jedynie w przypadku wykrycia krytycznych podatności, w porozumieniu z producentami urządzeń. Łatane systemy powinny zostać przetestowane poza środowiskiem produkcyjnym.
Oprogramowanie bezpieczeństwa/antywirusowe	Powszechnie stosowane	Może zostać zastosowane, jednak nie powinno wpływać na dostępność mocy obliczeniowej.
Wymiana urządzeń	Dokonywana w sposób ciągły	Systemy pracujące bez większych zmian w okresach kilkunastu lat.

Utrata danych	Odtworzenie danych zwykle odbywa się bez poważnych konsekwencji	Utrata danych może powodować zaburzenie procesu i stworzenie niebezpiecznych warunków.
Utrata dostępności	Dopóki dostępność nie jest tracona w długim okresie czasu, jej efekty nie są katastroficzne. Dostępność jest jednak jednym z krytycznych parametrów.	Systemy powinny być odporne na utratę dostępności. Utrata dostępności może prowadzić do poważnych konsekwencji.
Utrata poufności danych	Biorąc pod uwagę rodzaj danych, konsekwencje mogą być nieznaczące lub poważne (informacje kluczowe dla przedsiębiorstwa, dane osobiste)	Brak poważnych konsekwencji
Poprawność danych	Biorąc pod uwagę rodzaj danych, konsekwencje mogą być nieznaczące lub poważne.	Poważne konsekwencje, gdyż błędy danych mogą prowadzić do podjęcia niewłaściwych decyzji przez obsługę.
Wydajność systemu	Akceptowane są czasowe problemy	Wydajność jest krytyczna

Od strony komunikacyjnej w koncentratorze zabezpieczeń do obsługi połączeń zdalnych zastosowane powinny zostać znane i przetestowane protokoły zapewniające szyfrowaną transmisję danych przez sieć rozległą. Przychodzący ruch sieciowy powinien zostać za pomocą reguł firewalla ograniczony do minimum pozwalającego na poprawną pracę – np. otwarcie jedynie portu obsługującego szyfrowaną transmisję https. Szyfrowanie transmisji https powinno być dodatkowo zabezpieczone automatyczną generacją nowych certyfikatów https, co określony czas. Systemy Windows jako środowiska uruchomieniowe dla oprogramowania inżynierskiego powinny zostać wyizolowane sieciowo poprzez brak powiązania z interfejsami sieciowymi do sieci rozległej.

Systemy operacyjne powinny posiadać minimalny zestaw usług i oprogramowania pozwalający na realizowanie stawianych zadań. Nadmiar aplikacji mógłby potencjalnie zwiększyć ilość potencjalnych wektorów ataku. Systemy operacyjne, szczególnie główny system dostarczający usługi komunikacyjne powinien pozwalać na zbieranie i przesyłanie rejestrów do systemów nadrzędnych, które mogłyby dokonywać automatycznej analizy lub pozwolić na ich analizę ręczną. Do zakresu zbieranych rejestrów powinny wejść rejestry dostępu kluczowych procesów uruchomionych w systemie – a więc informacja o tym co robią poszczególne procesy takie jak np. serwer www. Może to pozwolić na wykrycie podejrzanego zachowania i być podstawą wyłączenia czasowego systemu z eksploatacji.

Zapewnienie bezpieczeństwa dla systemów informatycznych – w tym również i dla łącza inżynierskiego jest procesem ciągłym. Zagadnieniem wymagającym ciągłej uwagi jest eliminacja znanych podatności oprogramowania realizowana poprzez wgrywanie łatek bezpieczeństwa. W przypadku systemów produkcyjnych proces ten składa się z kolejnych etapów, pozwalających zapewnić wysoką niezawodność i dostępność. Proces ten powinien odbywać się z rozwagą tylko dla krytycznych podatności. Są to odpowiednio:

- Okresowe monitorowanie podatności oraz określenie krytyczności wykrytych luk z punktu widzenia dostarczanej przez łącze inżynierskie funkcjonalności.
- Wgranie poprawek bezpieczeństwa w systemie testowym.

- Testy bezpieczeństwa i stabilności systemu testowego w warunkach zbliżonych do produkcyjnych.
- Implementacja poprawek bezpieczeństwa w systemach produkcyjnych.

Inną formą zapewnienia bezpieczeństwa są okresowe testy penetracyjne, przeprowadzane zwykle przez niezależne laboratoria. Testy te mogą być prowadzone w kilku wariantach. Wariant black box – kiedy tester nie ma informacji dotyczących atakowanego systemu, grey box – kiedy tester zna system i posiada do niego dane autoryzacyjne oraz white box – tester zna strukturę oraz ma dostęp do kodu źródłowego. Zespół testujący poznaje działanie systemu oraz próbuje wykorzystać typowe schematy nadużyć mając na celu nieautoryzowane wykorzystanie systemu atakowanego. W wyniku testów penetracyjnych testowany system powinien zostać zaktualizowany w celu zlikwidowania wykrytych potencjalnych wektorów ataku i zwiększenia jego bezpieczeństwa.

System łącza inżynierskiego powinien również podlegać kopiom bezpieczeństwa na wypadek jego awarii. Kopie te pozwalają na szybkie przywrócenie sprawności systemu po awarii sprzętu lub uszkodzenia oprogramowania w wyniku działania osób trzecich.

5. Podsumowanie

Systemy łącza inżynierskiego rozwinęły się znacząco na przestrzeni ostatnich 25 lat. Ich pierwotnym przeznaczeniem było uzyskanie bezbłędnie działających łącz telekomunikacyjnych między komputerem użytkownika, zainstalowanym w biurze operatora systemowego, a koncentratorem, w którym uruchomiono program do obsługi przekaźnika zainstalowanego na stacji elektroenergetycznej, położonej nawet setki km od wspomnianego biura.

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

- szybki rozwój branży IT powodujący, że zarówno systemy operacyjne jak i aplikacje inżynierskie ulegają ciągłym zmianom, co wymusza wykorzystywanie wielu wersji programów narzędziowych, sterowników do urządzeń itp., dostosowanych do określonych wersji urządzeń zabezpieczeniowych,
- bardzo duża liczba urządzeń w stacji, ich łącz telekomunikacyjnych, zastosowanych konwerterów, zasilaczy itp., co przekłada się na większą liczbę niesprawnych urządzeń, łączy telekomunikacyjnych itp.,
- większe niż wcześniej zagrożenie atakami cybernetycznymi urządzeń i infrastruktury energetycznej.

Z powyższych względów głównym wyzwaniem stawianym przed współczesnymi bramami dostępu do urządzeń automatyki stacji elektroenergetycznej, dawniej nazywanymi koncentratorami zabezpieczeń, jest ułatwienie pracy służb eksploatacyjnych, automatyzacja pracy, zapewnienie szerokiej kompatybilności z aplikacjami narzędziowymi oraz zwiększenie poziomu cyberbezpieczeństwa. Opisane w artykule łącze inżynierskie IEN PW wprowadza innowacyjne rozwiązanie wykorzystujące wirtualizację, rozwiązującą szereg wspomnianych powyżej problemów, z którymi zmagają się służby eksploatacji zajmujące się w wielu spółkach dystrybucyjnych i przesyłowych urządzeniami automatyki stacji elektroenergetycznych. Nowe rozwiązanie oferuje zwiększony zakres kompatybilności koncentratora z aplikacjami narzędziowymi, pozwalając na instalację aplikacji zaprojektowanych w ubiegłym stuleciu, obecnych i tych które zostaną opracowane w przyszłości, jak również umożliwia współdziałanie różnych wersji tej samej aplikacji. Przeniesienie systemów operacyjnych, do warstwy

wirtualnego sprzętu, pozwala na precyzyjną izolację zasobów udostępnianych na zewnątrz, poprawiając bezpieczeństwo układu zdalnego dostępu do zabezpieczeń. Niewykorzystywany dotąd kanał dostępu do zasobów łącza inżynierskiego poprzez szyfrowany protokół https, poza podwyższonym bezpieczeństwem, w połączeniu z wysoką automatyzacją czynności wykonywanych w tle, ułatwia korzystanie z systemu i pozwala na eliminację potencjalnych błędów ludzkich, co w dobie coraz bardziej rozbudowanych aplikacji producenckich jest bardzo istotną kwestią.

Zapewnienie bezpieczeństwa informatycznego dla systemów Łącza inżynierskiego jest niewątpliwie koniecznością jednak powinno być planowane i wykonywane z rozwagą, biorąc pod uwagę zarówno dobre praktyki IT jak i wymagania stawiane układom automatyki takie jak stabilność i wysoka dostępność.

Literatura

[1] Ryszard Kowalik, Marcin Januszewski, Kamil Gontarz, Emil Bartosiewicz, „Wymagania dla teraźniejszych oraz przyszłych układów zdalnego nadzoru urządzeń automatyki elektroenergetycznej” Przegląd Elektrotechniczny 08/2013 Str. 5

[2] Polskie Sieci Elektroenergetyczne Operator S.A., STANDARDOWE SPECYFIKACJE TECHNICZNE – PSE-ST.Łącze inżynierskie/2012v1 – Łącze inżynierskie, Warszawa, 2012

[3] Polskie Sieci Elektroenergetyczne, Departament Eksploatacji, STANDARDOWE SPECYFIKACJE TECHNICZNE – PSE-ST.EAZ.NN.WN/2016 – Urządzenia elektroenergetycznej automatyki zabezpieczeniowej i układy z nią współpracujące, stosowane na stacjach elektroenergetycznych WN i NN, Konstancin Jeziorna, grudzień 2016, https://www.pse.pl/documents/20182/8c217ef3-c1e9-4ae0-aac1-1759d4044ad4?safeargs=646f776e6c6f61643d74727565

[4] Emil Bartosiewicz, Łukasz Nogal, Marcin Januszewski „Brama zdalnego dostępu do urządzeń automatyki elektroenergetycznej i stawiane jej wymagania” electo.info 5/2019

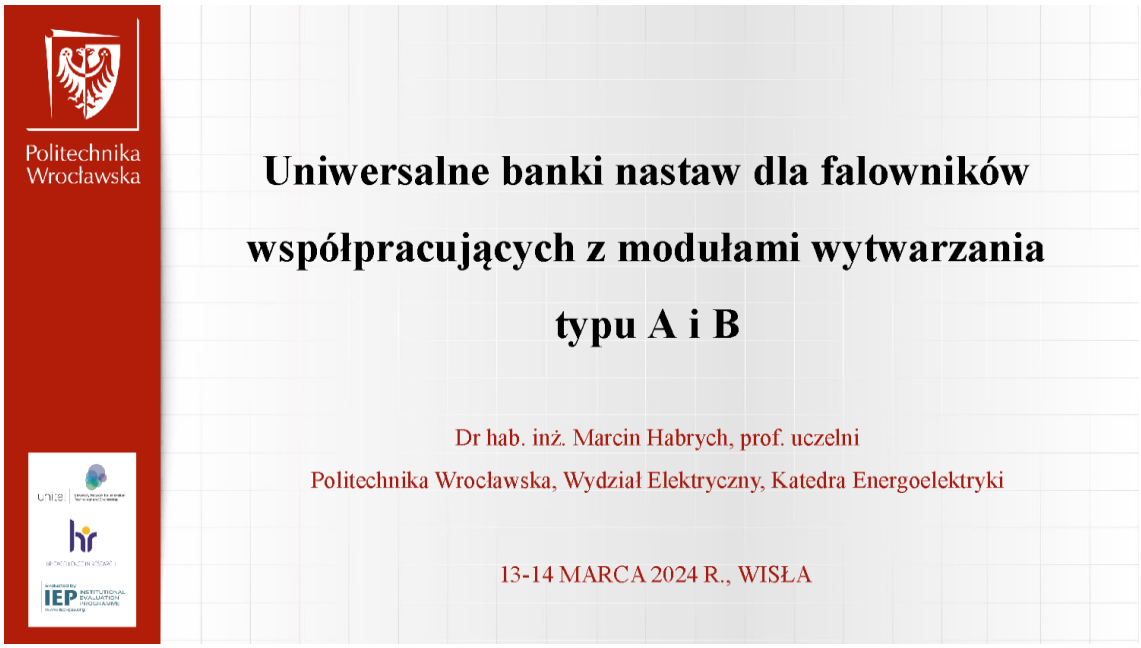
[5] Ronald L. Krutz, “Industrial Automation and Control System Security Principles: Protecting the Critical Infrastructure” Second Edition, 2017 International Society of Automation

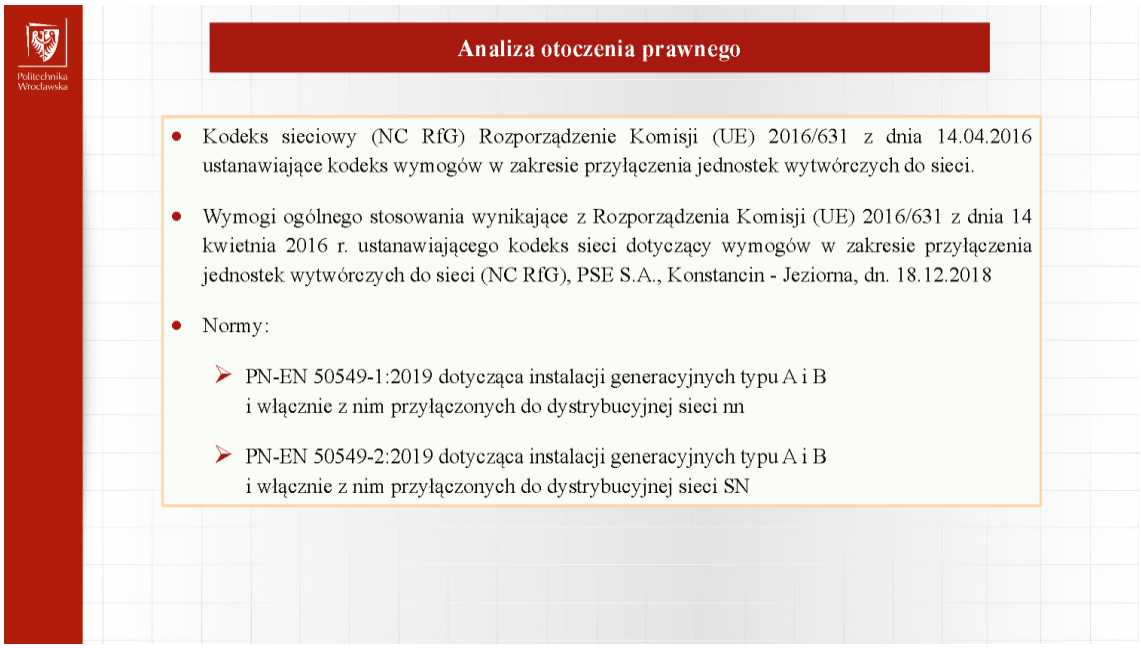
[6] Marcin Januszewski, Ryszard Kowalik, Karol Kurek, Desire Rasolomampionona, Mariusz Kłos, "Remote Access Gateway to Power Plant Automation Equipment With Cybersecurity Functions (Functionalities, Work Systems)", IEEE Power and Energy Society General Meeting, 2022, pp. 1-5, lipiec, IEEE

[7] „Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design”, ISA-62443-3-2-2020

UNIWERSALNE BANKI NASTAW DLA FALOWNIKÓW WSPÓŁPRACUJĄCYCH Z MODUŁAMI WYTWARZANIA TYPU A I B

Marcin Habrych (Politechnika Wrocławska)
Marek Wancerz (Politechnika Lubelska)



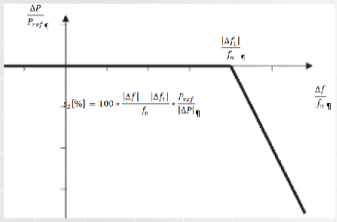


Analiza otoczenia prawnego

- Instrukcje Ruchu i Eksploatacji Sieci Dystrybucyjnej (IRiESD):
  - *IRiESD - ENEA Operator Sp. z o.o.*
  - *IRiESD - TAURON Dystrybucja S.A,*
  - *IRiESD - PGE Dystrybucja S.A*
  - *IRiESD - ENERGA Operator S.A.*
  - *IRiESD - STOEN Operator Sp. z o.o.*
- *Zaktualizowane wymogi ogólnego stosowania wynikające z Rozporządzenia Komisji (UE) 2016/631 z dnia 14 kwietnia 2016 r. ustanawiającego kodeks sieci dotyczący wymogów w zakresie przyłączenia jednostek wytwórczych do sieci (NC RfG),*
- Zbiór wymagań dla modułów wytwarzania energii typu A, w tym mikroinstalacji – wydany przez każdego OSD.

Analiza otoczenia prawnego

Dla trybu **LFSM-O** (moduły typ A) moduł wytwarzania energii musi mieć zdolność do aktywowania rezerwy mocy czynnej w odpowiedzi na wzrost częstotliwości, przy odpowiednich parametrach progu częstotliwości i ustawieniach statyzmu



Wymaganie	Normy 50549	NC RfG
LFSM-O	Zdolność do ustawienia progu częstotliwości trybu LFSM-O w zakresie **50,2 Hz–52 Hz** - **Pref dla PPM jako moc czynną generowaną przed zadziałaniem LFSM-O** *Artykuł 4.6.1*	Zdolność do ustawienia progu częstotliwości trybu LFSM-O w zakresie **50,2 Hz – 50,5 Hz** (50,2 Hz wartość domyślna) - **Pref dla PPM jako moc czynną maksymalną PPM** albo **rzeczywista mocy czynnej PPM**, gdy osiągnięty jest próg LFSM-O *Artykuł 13 ust. 2 lit. a)*
Odłączenie zamiast LFSM-O	Dla modułów **typu A i B** dopuszczone jest wyłączanie poszczególnych jednostek wchodzących w skład PGM przy różnych częstotliwościach równomiernie rozłożonych w zakresie progu zadziałania do 52 Hz. *Artykuł 4.6.1*	Dopuszczone jest przystosowania tylko PGM **typu A** do trybu LFSM-O poprzez stopniowe wyłączanie poszczególnych źródeł wytwórczych wchodzących w skład PGM. *Artykuł 13 ust. 2 lit. b)*

Bank nastaw

Dla modułu wytwarzania typu A:

Wybór opcji w inwerterze „Bank nastaw - Polska”, który automatycznie uruchomi i nastawi następujące zabezpieczenia i charakterystyki regulacyjne (wartości podane względem U_{LN}):

- **Zabezpieczenie podnapięciowe U<**

  Wartość rozruchowa: 0,85 U_n = 195,5 V; Czas opóźnienia: 1,2 s;

- **Zabezpieczenie nadnapięciowe pierwszego stopnia U>**

  Wartość rozruchowa: 1,1 U_n = 253 V (mierzona jako średnia 10-minutowa mierzona w oknie przesuwnym - zgodnie z normą EN 50160. Szczegółowe wymagania w zakresie pomiaru wartości średniej zawarte są w normie PN-EN 50549). Czas opóźnienia: 3 s;

- **Zabezpieczenie nadnapięciowe drugiego stopnia U>>**

  Wartość rozruchowa: 1,15 U_n = 264,5 V; Czas opóźnienia: 0,1 s;

- **Zabezpieczenie podczęstotliwościowe f<**

  Wartość rozruchowa: 47,5 Hz; Czas opóźnienia: 0,3 s;

Bank nastaw

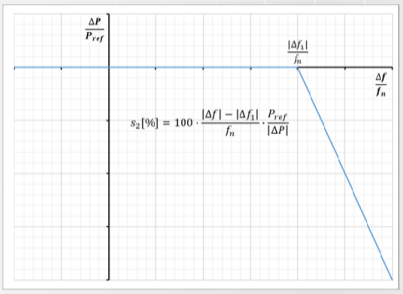
- **Zabezpieczenie nadczęstotliwościowe f>**

  Wartość rozruchowa: 52 Hz; Czas opóźnienia: 0,3 s;

- **Zabezpieczenie od pracy wyspowej LoM - kryterium RoCoF df/dt**

  Wartość rozruchowa: 2,5 Hz/s; Max. czas działania: 0,5 s;

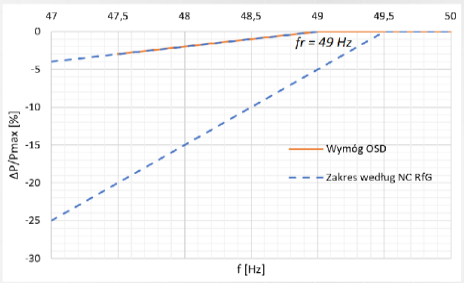
- **Charakterystyka LFSM-O:**



Wartość rozruchowa: 50,2 Hz; Wartość statyzmu: 5%; Pref – rzeczywista wyjściowa moc czynna w momencie osiągnięcia progu LFSM-O

Bank nastaw

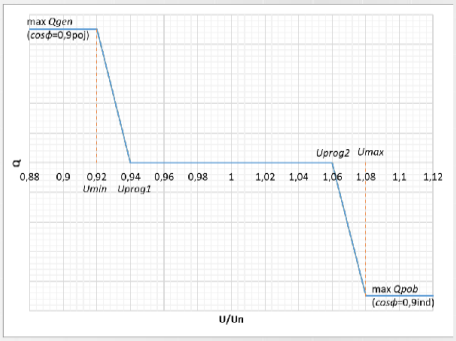
- **Charakterystyka dopuszczalnej redukcji mocy:**



Wartość rozruchowa: 49 Hz; Wartość redukcji mocy: 2% mocy maksymalnej na każdy 1 Hz spadku częstotliwości poniżej 49 Hz

Bank nastaw

- **Charakterystyka sterowania mocą bierną w funkcji napięcia na zaciskach generatora (tryb Q(U)):**

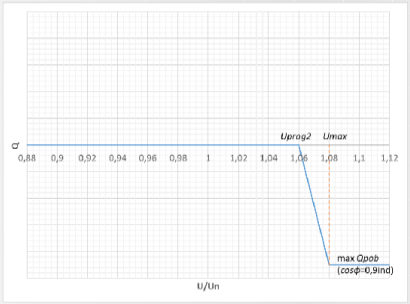


Punkty na charakterystyce: maxQpob = -0,4843P (odpowiada cosφ =0,9ind); maxQgen = 0,4843P (odpowiada cosφ =0,9poj); Uprog1 = 0,94U p.u.; Uprog2 = 1,06 U p.u. Umin = 0,92 U p.u.; Umax = 1,08U p.u.; statyzm = 2,222

Bank nastaw

- **Charakterystyka sterowania mocą bierną w funkcji napięcia na zaciskach generatora (tryb Q(U)):**

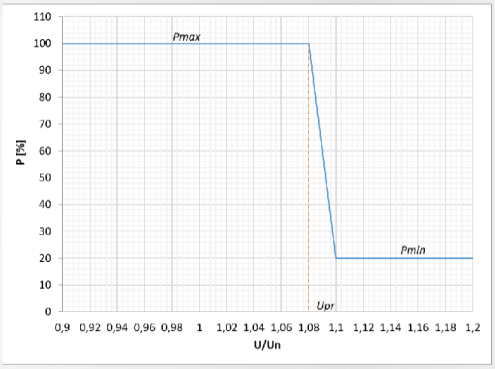
Dla falowników przyłączonych do sieci 1-fazowo możliwy kształt charakterystyki:



Punkty na charakterystyce: maxQpob = -0,4843P (odpowiada cosφ =0,9ind); Uprog2 = 1,06 U p.u. Umax = 1,08U p.u.; statyzm = 2,222

Bank nastaw

- **Charakterystyka sterowania mocą czynną w funkcji napięcia (tryb P(U)):**



Punkty na charakterystyce: U_{pr} = 1,08 p.u.; statyzm = 2,5

Bank nastaw

- **Warunki automatycznego przyłączania modułu wytwarzania energii do sieci (resynchronizacja z siecią):**

Spełnione muszą zostać łącznie wszystkie poniższe warunki:

– częstotliwość napięcia w przedziale 49 Hz – 50, 05 Hz,

– zwłoka czasowa wynosząca 60 s, liczona od czasu powrotu częstotliwości do przedziału 49 Hz – 50, 05 Hz,

– maksymalny przyrost generowanej mocy czynnej wynoszący 10% mocy maksymalnej na minutę.

Bank nastaw

Dla modułu wytwarzania typu B:

Wybór opcji w falowniku „Bank nastaw - Polska”, który automatycznie uruchomi i nastawi następujące zabezpieczenia i charakterystyki regulacyjne. **Ustawienia poziomów napięć działania zabezpieczeń powinny być w każdym przypadku zweryfikowane jako specyficzne dla obiektu - wartości progowe napięć w punkcie przyłączenia, przy których może nastąpić automatyczne odłączenie obiektu powinny być skorelowane z wartościami granicznymi napięć dopuszczalnymi przez właściwego Operatora Systemu w sieci SN**, którą zarządza; dodatkowo:

❖ nastawa zabezpieczeń podnapięciowych powinna być niższa niż minimalna wartość napięcia, przy której PGM (moduł wytwarzania energii) powinien zachować zdolność do pracy w sieci,

❖ nastawa zabezpieczeń nadnapięciowych powinna być wyższa niż maksymalna wartość napięcia, przy której PGM powinien zachować zdolność do pracy w sieci.

Politechnika Wrocławska

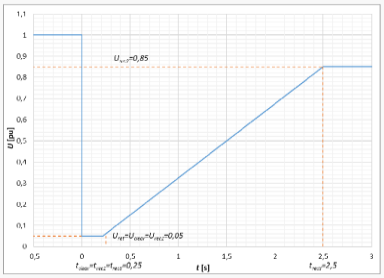
Bank nastaw

Dla modułu wytwarzania typu B:

Falowniki typu B powinny mieć aktywne funkcjonalności (wg ustalonej charakterystyki):

- FRT (ang. Fault Ride Through) - profil pozostawania w pracy podczas zwarcia dla modułu wytwarzania energii,
- zdolności do generacji dodatkowego, szybkiego prądu zwarciowego zabezpieczenie podnapięciowe nie powinno uniemożliwiać realizacji powyższych funkcjonalności.

Politechnika Wrocławska

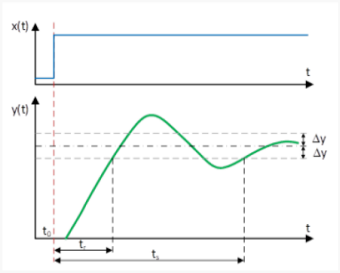
Kryterium	Wymagana nastawa	Reakcja falownika
Charakterystyka FRT (ang. Fault Ride Through) - profil pozostawania w pracy podczas zwarcia dla modułu wytwarzania energii		Pozostawanie w pracy zgodnie z charakterystyką napięciowo-czasową

Parametry napięcia [pu]		Parametry czasu [s]	
U_{rst}	0,05	t_{clear}	0,25
U_{clear}	0,05	t_{rec1}	0,25
U_{rec1}	0,05	t_{rec2}	0,25
U_{rec2}	0,85	t_{rec3}	2,50

14

Kryterium	Wymagana nastawa	Reakcja falownika
PPM powinien być zdolny do generacji dodatkowego, szybkiego prądu zwarciowego	W przypadku wystąpienia zwarć poza instalacją wewnętrzną PPM, moduł wytwarzania energii powinien posiadać zdolność do generacji dodatkowego prądu biernego. **1. Dla zwarć symetrycznych wsparcie prądem biernym powinno być:** – proporcjonalne do zmiany składowej zgodnej napięcia w punkcie przyłączenia ΔU_1 spowodowanej zakłóceniem (wartością odniesienia jest wartość średnia składowej zgodnej napięcia za okres 1 minuty sprzed zakłócenia $\overline{U_1}$), – proporcjonalne do wartości współczynnika wzmocnienia K_1, – blokowane, gdy wartość składowej zgodnej napięcie jest większa niż wartość wyzwalania U_{trig} $\Delta I_{Q1} = K_1 \cdot \Delta U_1, gdzie: \Delta U_1 = \begin{cases} 0 \; dla \; U_1 \geq U_{trig} \\ \dfrac{U_1 - \overline{U_1}}{U_n} \; dla \; U_1 < U_{trig} \end{cases}$ gdzie: - K_1 = 2 (możliwość zmian K_1 w zakresie od 2 do 6 z krokiem 0,5), - U_{trig} = 0,85 U_n (możliwość zmiany wartości U_{trig} w zakresie od 0,8 do 1,0 U_n).	Generacja dodatkowego prądu biernego zgodnie z wymaganiami

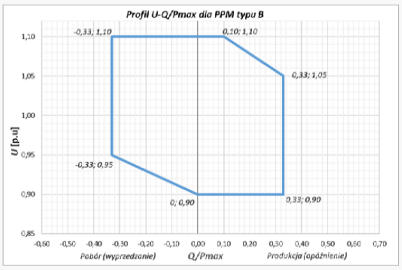
15

Kryterium	Wymagana nastawa	Reakcja falownika
PPM powinien być zdolny do generacji dodatkowego, szybkiego prądu zwarciowego	**Właściwości dynamiczne układu regulacji dodatkowym prądem biernym:** - czas odpowiedzi prądowej t_r na spadek napięcia – max. 30 ms, - czas ustalania odpowiedzi prądowej t_s – max. 60 ms, - dopuszczalna tolerancja odpowiedzi prądowej: od -10 % do +20%.  Δy – dokładność układu regulacji, Nie definiuje się wymogów odnośnie wsparcia prądem biernym w przypadku wystąpienia napięć niższych niż 0,15 Un	Generacja dodatkowego prądu biernego zgodnie z wymaganiami

16

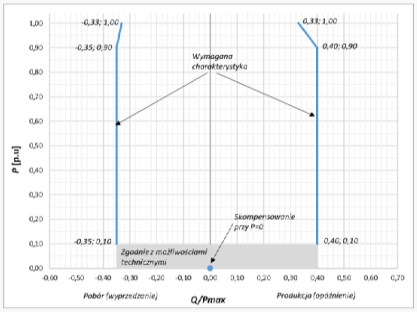
Kryterium	Wymagana nastawa	Reakcja falownika
PPM powinien być zdolny do generacji dodatkowego, szybkiego prądu zwarciowego	**2. Dla zwarć niesymetrycznych wsparcie prądem biernym powinno być zgodnie z zasadą superpozycji:** – składowej zgodnej dodatkowego prądu biernego, zgodnie z zasadami zdefiniowanymi dla zwarć symetrycznych, – składowej przeciwnej dodatkowego prądu biernego, którego wartość jest proporcjonalna do zmiany składowej przeciwnej napięcia ΔU_2 (wartością odniesienia jest wartość średnia składowej przeciwnej napięcia za okres 1 minuty sprzed zakłócenia $\overline{U_2}$) i współczynnika wzmocnienia K_2. $$\Delta I_{Q2} = K_2 \cdot \Delta U_2, gdzie\ \Delta U_2 = \frac{(U_2 - \overline{U_2})}{U_n}$$ Dodatkowo: – K_2 = 2 (możliwość zmian K_2 w zakresie od 2 do 6 z krokiem 0,5), – prąd bierny ΔI_Q, będący sumą wektorów odpowiedzi składowej zgodnej i przeciwnej ($\Delta I_{Q1} + \Delta I_{Q2}$), nie powinien powodować przekroczenia dopuszczalnej wartości prądu fazowego w żadnej z faz, – właściwości dynamiczne odpowiedzi prądowej – jak dla zwarć symetrycznych.	Generacja dodatkowego prądu biernego zgodnie z wymaganiami

17

Kryterium	Wymagana nastawa	Reakcja falownika
Charakterystyka sterowania mocą bierną w funkcji napięcia w punkcie przyłączenia **Charakterystyka U-Q/Pmax**	Wymagania minimalne regulaci mocy biernej przedstawione na profilu U-Q/Pmax, gdzie U-Q/Pmax – wartość względna napięcia w zakresie zmian mocy biernej (Q) w stosunku do mocy maksymalnej (Pmax). 	Możliwość zmiany mocy biernej w określonych granicach

18

Politechnika Wrocławska

Kryterium	Wymagana nastawa	Reakcja falownika
Charakterystyka sterowania mocą bierną w funkcji napięcia w punkcie przyłączenia **Charakterystyka U-Q/Pmax**	W przypadku generacji przez Moduł Parku Energii mocy czynnej poniżej mocy maksymalnej, wymaganą zdolność do zapewnienia mocy biernej w punkcie przyłączenia przedstawiono na rysunku:  gdzie: P-Q/Pmax - stosunek rzeczywistej mocy czynnej PPM do mocy maksymalnej, względem stosunku mocy biernej (Q) do mocy maksymalnej (Pmax).	Możliwość zmiany mocy biernej w określonych granicach

19

Politechnika Wrocławska

Kryterium	Wymagana nastawa	Reakcja falownika
Charakterystyka sterowania mocą bierną w funkcji napięcia w punkcie przyłączenia **Charakterystyka U-Q/Pmax**	Uwagi: ❖ Przy obciążeniu PPM mocą czynną poniżej 0,1 mocy maksymalnej należy udostępnić całą dostępną moc bierną, zgodnie z możliwościami technicznymi, ❖ PPM musi posiadać zdolności techniczne do skompensowania mocy biernej w punkcie przyłączenia przy braku generacji mocy czynnej. ❖ Jeżeli wymagana jest praca przy napięciu poniżej 0,9 pu w punkcie przyłączenia, wówczas PPM powinien udostępnić całą dostępną moc bierną, zgodnie ze swymi możliwościami technicznymi.	Możliwość zmiany mocy biernej w określonych granicach

20

Wnioski ogólne

- Na podstawie rozmów przeprowadzonych z producentami/dystrybutorami inwerterów, z instalatorami instalacji PV a także przeszukując branżowe fora internetowe stwierdzamy, że obecnie obowiązujące przepisy i wymagania odnośnie kryteriów zabezpieczeniowych oraz charakterystyk regulacyjnych zaimplementowanych w falownikach (w wielu przypadkach) nie są respektowane. Pierwszym problemem są zabezpieczenia i charakterystyki, które muszą być ustawione przez instalatorów w momencie uruchamiania instalacji.

Wnioski ogólne

- Zdarza się, iż instalatorzy instalacji PV błędnie konfigurują inwertery. Ten problem można prosto wyeliminować – załączając w inwerterze „Bank nastaw - Polska”. Wtedy wszystkie wartości rozruchowe kryteriów zabezpieczeniowych oraz charakterystyki będą uruchamiały się automatycznie z wymaganymi parametrami.
- Drugim problemem jest poszukiwanie przez użytkowników instalacji PV kodów dostępowych do inwerterów, celem nieuprawnionych zmian nastaw parametrów sieci, zabezpieczeń czy charakterystyk regulacyjnych. W sieci można znaleźć gotowe instrukcje jak można poradzić sobie z wyłączającymi się inwerterami. **Poszczególni OSD mają ograniczone możliwości skutecznego reagowania na wykryte nieprawidłowości.**


Politechnika
Wrocławska
DZIĘKUJĘ ZA UWAGĘ

WYKRYWANIE PODZIAŁU SYSTEMU Z ZASTOSOWANIEM SYNCHROFAZORÓW ORAZ SYMULACJA DZIAŁANIA ALGORYTMU Z WYKORZYSTANIEM RTDS

Łukasz Kajda, Adam Babś (Instytut Energetyki – Państwowy Instytut Badawczy, Oddział Gdańsk)

Wykrywanie podziału systemu z zastosowaniem synchrofazorów oraz symulacja działania algorytmu z wykorzystaniem RTDS

14 marca 2024 r.

Adam Babś
Łukasz Kajda

Czym jest (synchro)fazor ?

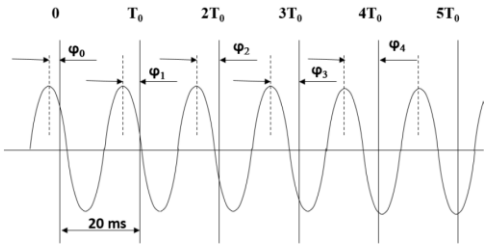
Synchrofazor (lub fazor synchroniczny) jest wartością napięcia lub prądu sinusoidalnego wyrażoną w postaci liczby zespolonej wyznaczaną jest na podstawie ciągu próbek wielkości mierzonej zbieranych przez stały, niezmienny czas (np. 20 ms)

$$\bar{U} = Ue^{j\varphi}$$

U – moduł (wartość skuteczna) napięcia
φ – odległość kątowa do początku pomiaru synchronicznego
dla wszystkich układów pomiarowych synchrofazorów (*PMU*)na świecie

Czym jest (synchro)fazor ?

Synchrofazor (lub fazor synchroniczny) jest wartością pomiaru napięcia lub prądu sinusoidalnego wyrażoną w postaci liczby zespolonej tj. modułu i kąta. Wartość ta wyznaczana jest na podstawie ciągu próbek wielkości mierzonej zbieranych przez stały, niezmienny czas (np. 20 ms), którego początek jest synchroniczny dla wszystkich układów pomiarowych synchrofazorów (*PMU*) na świecie - synchronizacja impulsem GPS z dokładnością 1 µs



$$\bar{X} = Xe^{j\varphi}$$

X – moduł (wartość skuteczna)

φ – odległość kątowa wyznaczona w odniesieniu do początku pomiaru

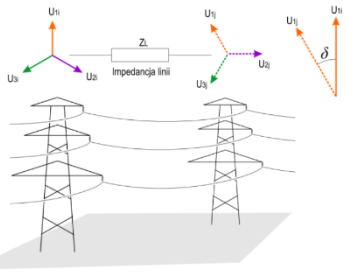
0 – początek sekundy synchronizowany przez GPS

T_0 – czas okna pomiarowego 20 ms dla częstości obliczania synchrofazorów 50 Hz

Wielkoobszarowy system pomiaru synchrofazorów
WAMS – Wide Area Measurement System

Funkcje systemu WAMS wynikają z możliwości wykorzystania obliczanych synchrofazorów dostępnych np. co 20 ms do bieżącej analizy zjawisk dynamicznych w systemie elektroenergetycznym.

Co 20 ms wylicza się szybkość zmiany częstotliwości *(RoCoF)*

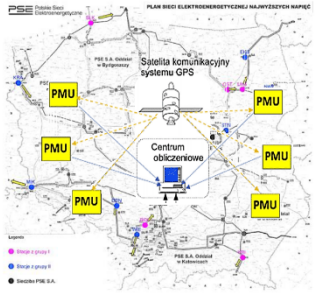


$$P = \frac{U_i U_j}{Z} \sin(\delta)$$

P – moc czynna wypływająca z gałęzi

U_i, U_j – moduły napięć na początku/końcu gałęzi

δ – kąt obciążenia, $\delta = \delta_i - \delta_j$ różnica kątów napięć na początku i końcu gałęzi

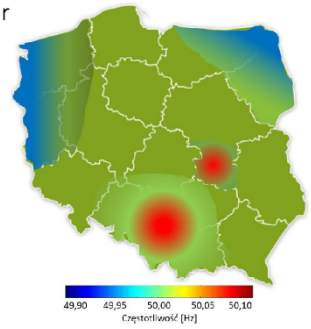


Świadomość sytuacyjna
monitorowanie zjawisk dynamicznych

- kąty fazowe napięć silnie korelują z ogólnym obciążeniem systemu oraz podatnością systemu na oscylacje międzyobszarowe.
- Wyznaczanie trendu kątów fazowych w stosunku do wartości granicznych kątów fazowych, może być wykorzystywane do identyfikacji rosnących obciążeń systemu;
- Szybkość zmian różnicy kątów fazowych jest ważnym wskaźnikiem rosnącego obciążenia systemowego (*growing system stress*) i może być podstawą alarmów operatora (przykład: blackout północno – wschodnie USA w 2003 r. i w 2008 r

Przekroczenie kątów fazowych, ponad wcześniej wyliczone off-line wartości graniczne, może być podstawą do podjęcia środków zaradczych

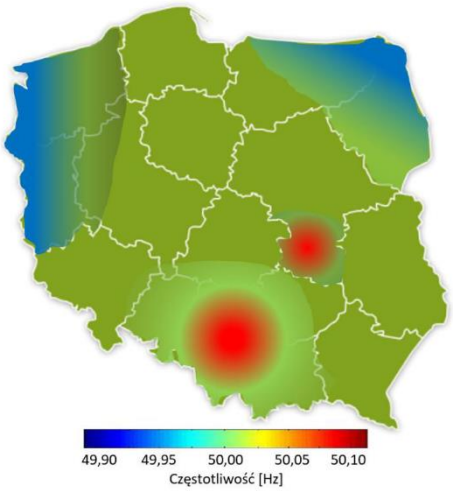
(zwiększenie generacji, modyfikacji przepływów gałęziowych, inne)



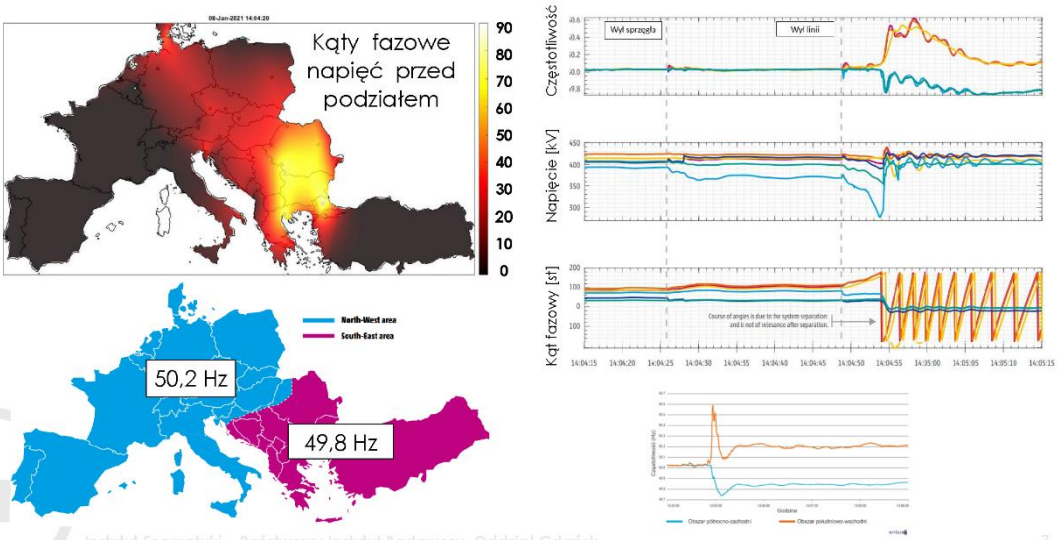
Świadomość sytuacyjna
monitorowanie zjawisk dynamicznych

Przyczyny zagrożenia stabilności pracy (podziału systemu):

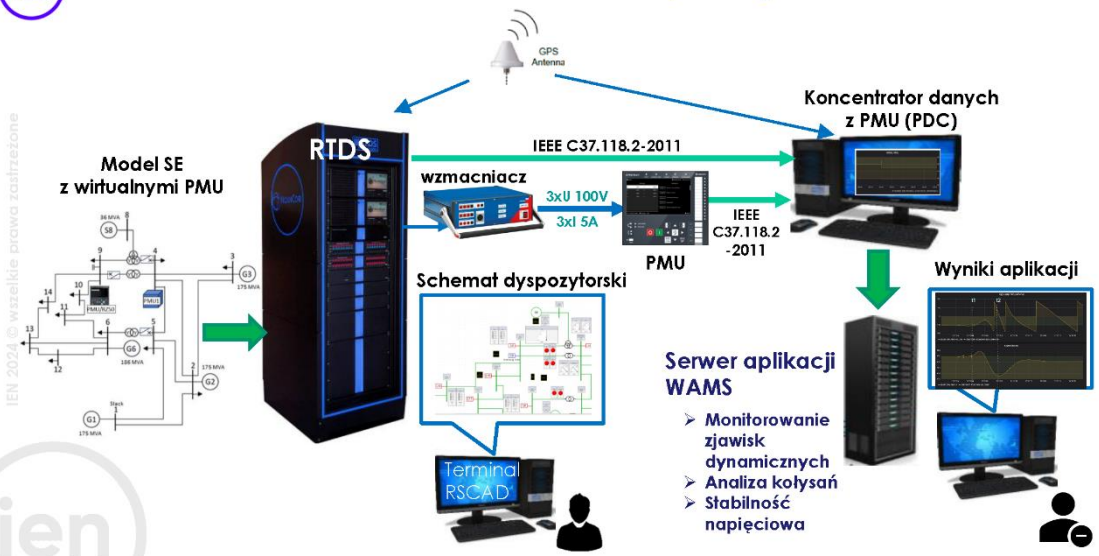
- Przejściowe zakłócenia, np.: wyłączenie dużego obciążenia lub generacji skutkujące:
  - Pogłębiającą się różnicą częstotliwości pomiędzy skrajnymi obszarami
  - Zwiększaniem różnicy kątowej aż do ponad 180 st.
  - Powstanie narastających oscylacji
- Przeciążenie w stanie ustalonym n-1 po wypadnięciu (wyłączeniu jednego elementu), zwłaszcza w połączeniu z lokalnym zadziałaniem automatyki SCO lub sterowaniem częstotliwością regulatora centralnego



Podział systemu europejskiego 8 stycznia 2021



Stanowisko testowe dla aplikacji WAMS



Symulator RTDS

Symulacja czasu rzeczywistego
Czas trwania zjawiska symulowanego komputerowo jest taki sam, jak czas trwania zjawiska rzeczywistego

RTDS – Real Time Digital Simulator umożliwia symulowanie m.in:

- Działania urządzeń i infrastruktury energetycznej w ujęciu trójfazowym, dla wszystkich poziomów napięć
- Mechaniki urządzeń energetycznych
- Systemów wymiany komunikacji danych
- Zjawisk fizycznych i zakłóceniowych

Symulator RTDS – możliwości badań

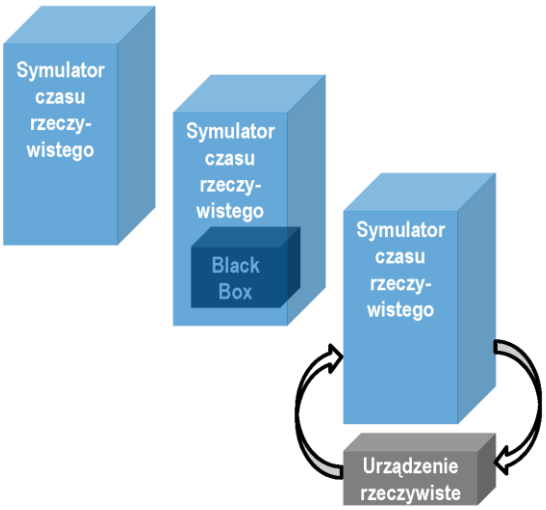
1. **Układy zabezpieczeń i sterowania**
   Regulatory napięcia maszyn synchronicznych (AVR)
   Przekształtniki HVDC
2. **Przekaźniki zabezpieczeniowe**
   Testowanie poszczególnych przekaźników i systemów przekaźników
   Wide Area Monitoring , Protection and Control Systems (WAMS / WAMPAC)
3. **Energoelektronika**
   Układy HVDC, FACTS oraz SFC (Static Frequency Converter)
4. **Systemy elektroenergetyczne**
   Stabilność przejściowa, WAMS, układy reg. pierwotnej, wtórnej i trójnej
5. **Układy Smart Grid i OZE**
   Turbiny wiatrowe, źródła PV, magazyny energii (w tym wodorowe)

RTDS - przeznaczenie

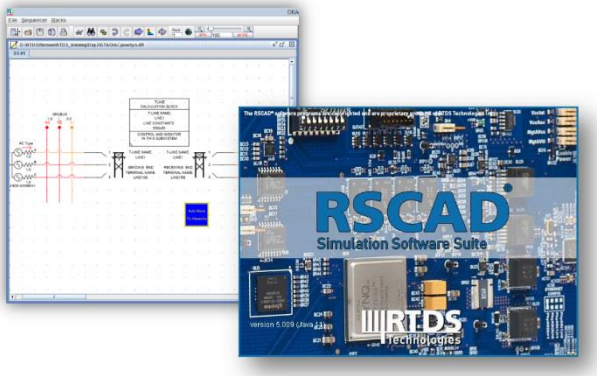
Symulacje czasu rzeczywistego
- Szkolenia
- Budowanie świadomości dynamiki zjawisk rzeczywistych
- Odtworzenie zdarzeń historycznych

Badania Black Box
- Badania działania algorytmów bez wykorzystania sprzętu

Badania HIL czyli Hardware-In-the-Loop
- Badania urządzeń rzeczywistych w symulowanym środowisku testowym



Symulator RTDS - sprzęt i oprogramowanie



RTDS Technologies – producent systemów **RTDS**
- **NovaCor** – sprzęt, najnowsza wersja
- **RSCAD** – oprogramowane symulacyjne

Symulator RTDS - interfejsy

- karta komunikacyjna – dostępne protokoły:
  - MODBUS TCP/IP
  - IEC 61850+GOOSE+SV
  - DNP3
  - IEC 60870-5-104
  - C37.118 (standard dla PMU)

- 12 optycznie izolowanych wyjść analogowych

- 12 optycznie izolowanych wejść analogowych

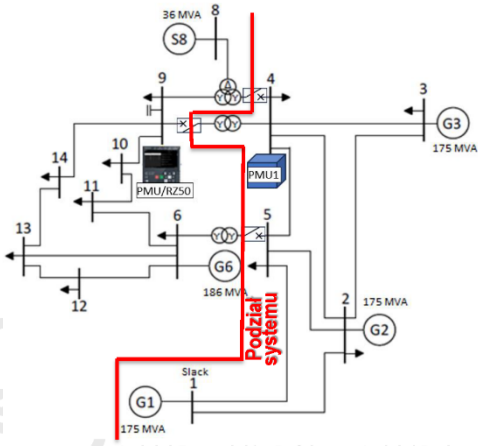
- 64 optycznie izolowane wejścia binarne

- 64 optycznie izolowane wyjścia binarne

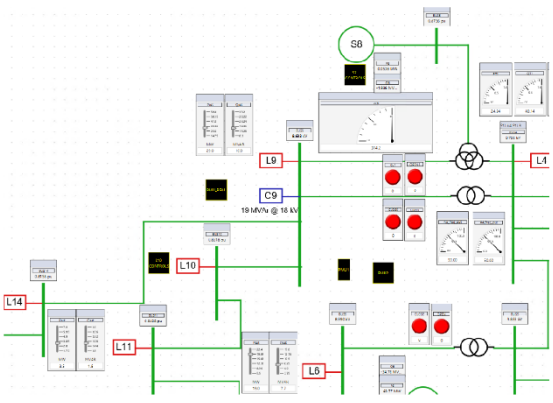
Wykrywanie podziału systemu
przykład realizacyjny z wykorzystaniem RTDS

Model symulacyjny systemu elektroenergetycznego

Model referencyjny sieci IEEE 14 szynowy



Widok modelu referencyjnego w programie RTDS - RSCAD



Model symulacyjny systemu elektroenergetycznego
model IEEE 14-szynowy - parametry modelu

- Konfiguracja modelu IEEE 14
  - Dane elementów pasywnych zgodne z modelem referencyjnym sieci
  - System wzbudzenia: model regulatora napięcia *IEEET1* - matematyczna reprezentacja układu wzbudzania używana w dynamicznych symulacjach w systemach elektroenergetycznych
  - Regulator turbiny - model *TGOV1*
    - Modelowanie z blokadą prędkości obrotowej wirnika (utrzymanie wartości zadanej, synchronicznej)
    - Dopuszczenie zmiany kąta wirnika
- Konfiguracja PMU z wykorzystaniem oprogramowania RTDS
- Konfiguracja wyjść analogowych dla PMU/RZ50
- Konfiguracja rzeczywistego PMU typu: PMU/RZ50
- Parametryzacja OpenPDC

Algorytm wykrywania podziału systemu
wykorzystujący pomiary fazorów napięcia, częstotliwości i ROCOF

Metoda różnicy częstotliwości

Polega na zlokalizowaniu miejsc, w których różnica częstotliwości pomiędzy PMU w danej lokalizacji a częstotliwością mierzoną przez PMU referencyjne (f_{ref}) przekracza próg przez pewien czas (T_{th1}).

$$\begin{cases} |f_i(t) - f_{\mathrm{ref}}| \geq f_{\mathrm{th}}, \ \forall t \in [T_m, T_n] \\ T_n - T_m > T_{\mathrm{th1}} \end{cases}$$

$f_i(t)$ - częstotliwość mierzona w czasie t, przez każdy z układów pomiarowych,
f_{ref} - częstotliwość odniesienia,
f_{th} - wartość progowa różnicy częstotliwości
T_{th1} - wartość progowa czasu trwania różnicy częstotliwości ponad próg $[T_m, T_n]$.

Metoda zmiany kąta fazowego

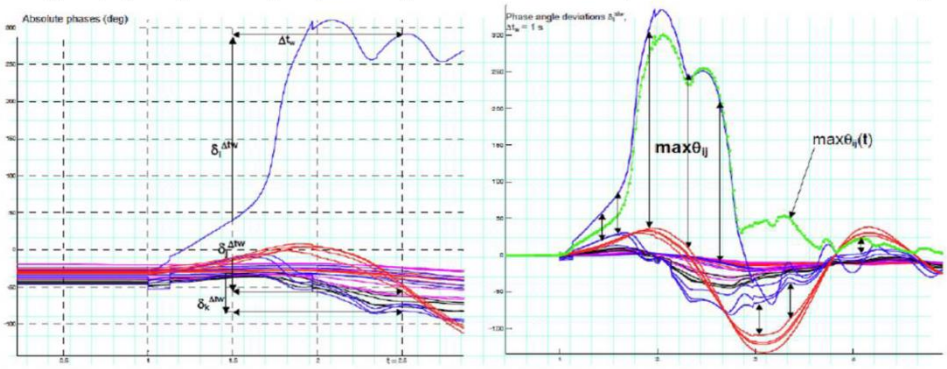
Na podstawie danych z systemu pomiaru fazorów porównywane jest narastanie różnicy kątowej pomiędzy pomiarami napięcia składowej zgodnej w wielu miejscach.

$$\begin{cases} |\theta_{iR}(t+T) - \theta_{iR}(t)| \geq \theta_{\mathrm{th}}, \ \forall t \in [T_m, T_n] \\ T_n - T_m > T_{\mathrm{th2}} \end{cases}$$

θ_{iR} - kąt fazowy między szynami i a R w czasie t,
T - przedział czasu dla porównania kąta fazowego,
θ_{th} - wartość progowa różnicy kątów,
T_{th2} - wartość progowa czasu trwania różnicy kątów ponad wartość progową

Monitorowanie zjawisk dynamicznych (przykład)

Kąty napięć w poszczególnych stacjach | **Różnice kątowe w stosunku do średniej**



Możliwość wyliczania średniej wartości kąta (wartość referencyjna) i wyboru lokalizacji gdzie różnica w stosunku do wartości referencyjnej jest największa

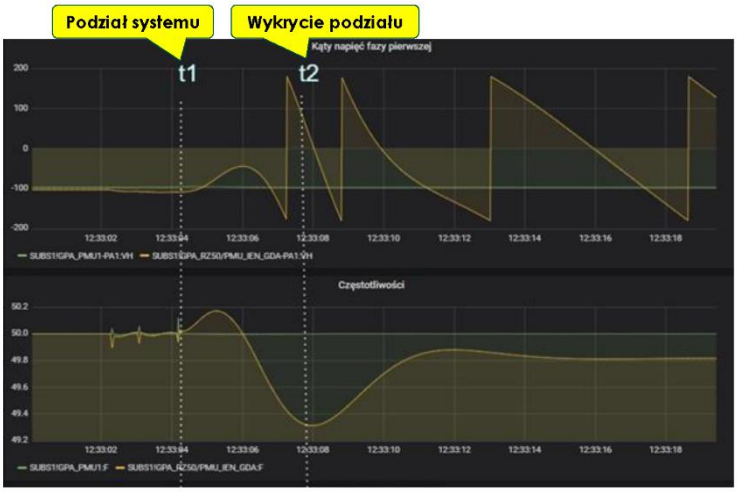
Sposób wykrywania podziału systemu

1. Ciągła rejestracja synchrofazorów z PMU1 i PMU/RZ50 tj. zmian częstotliwości i kata fazowego w obu częściach podzielonego systemu, różnica kątów fazowych napięć $\Delta\theta$ liczona narastająco
2. Jako wartości graniczne świadczące o podziale systemu przyjęto:
   - narastająca różnica kątowa $\Delta\theta_{th2} > \Delta\theta_{th1} = 30$ stopni
   - czas utrzymywania się różnicy kątowej ponad wartość graniczną ($t_{\Delta\theta} > 3$ s)

$$\Delta\theta = \left|\theta U1_{\,PMU1} - \theta U1_{\,PMU/RZ50}\right|$$

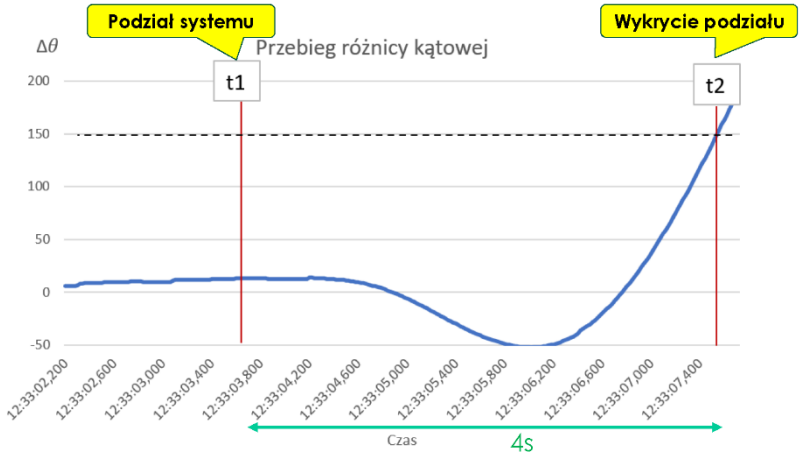
Wyniki wykrywania podziału systemu

Rejestracja katów napięć oraz częstotliwości przed i po wydzieleniu fragmentu sieci



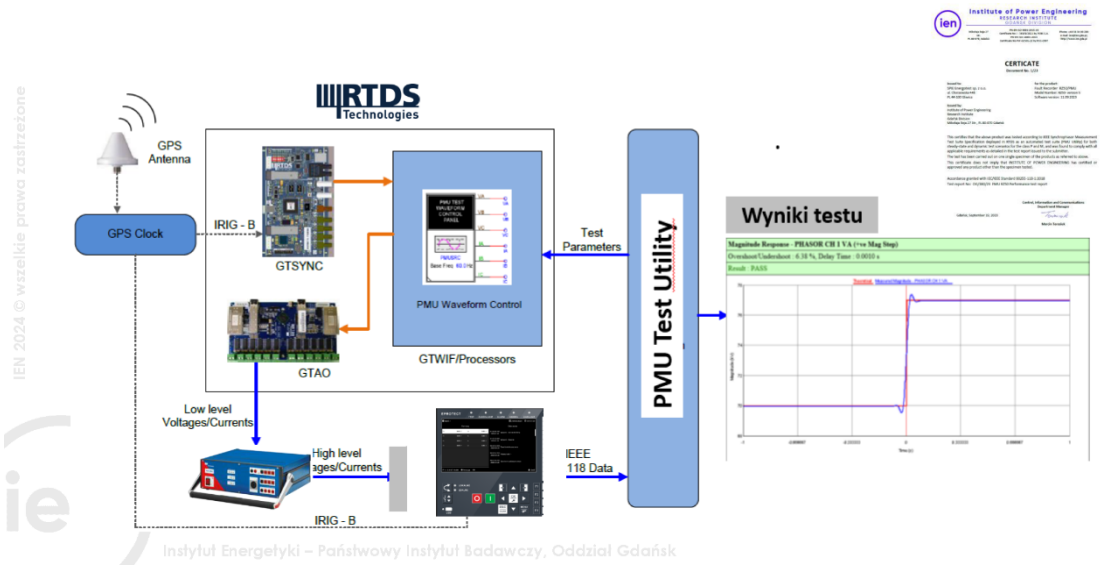
Wyniki wykrywania podziału systemu

Przebieg różnicy kątowej

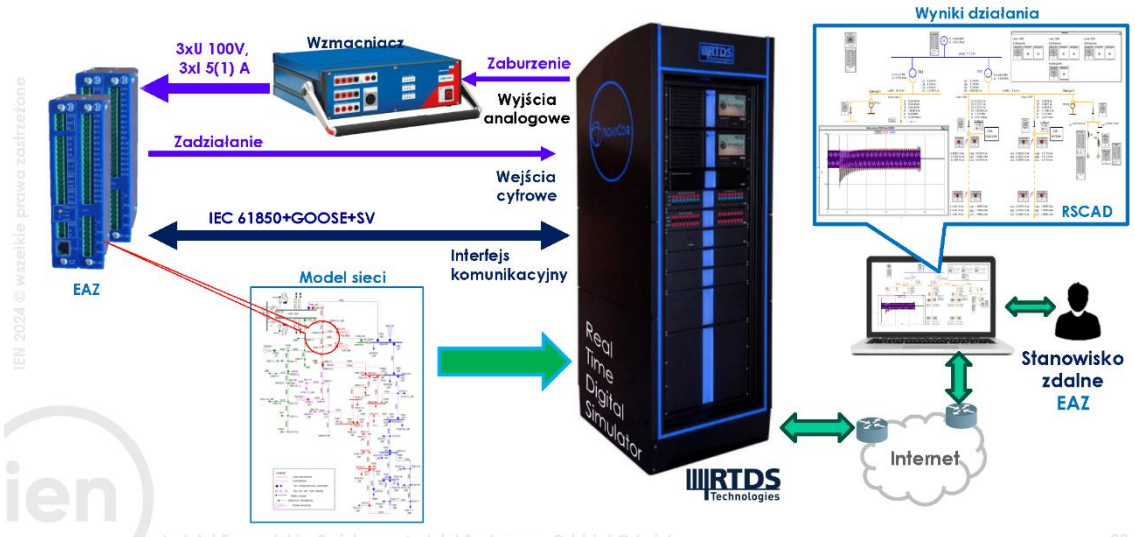


Test urządzenia na zgodność z IEC/IEEE 60255-118-1 i C37.118.2

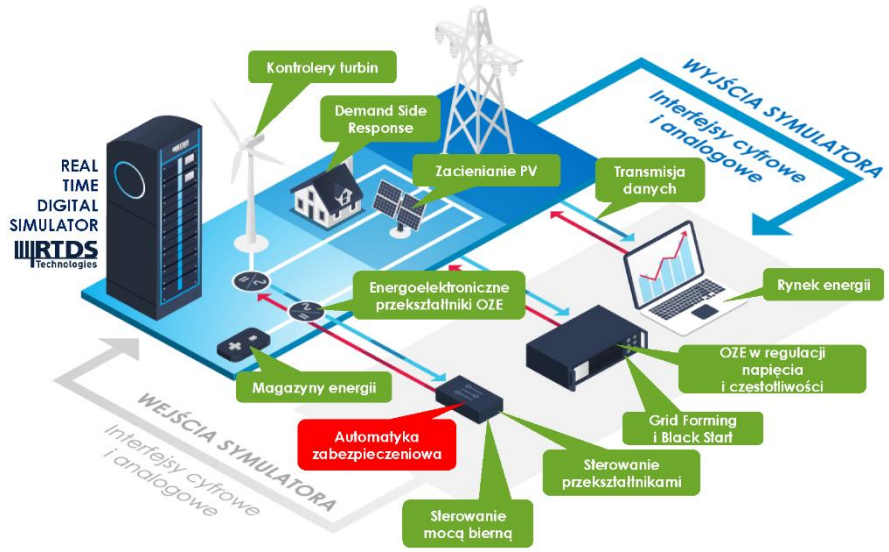
conformance test



Testy funkcjonalne układów EAZ - Hardware in the loop

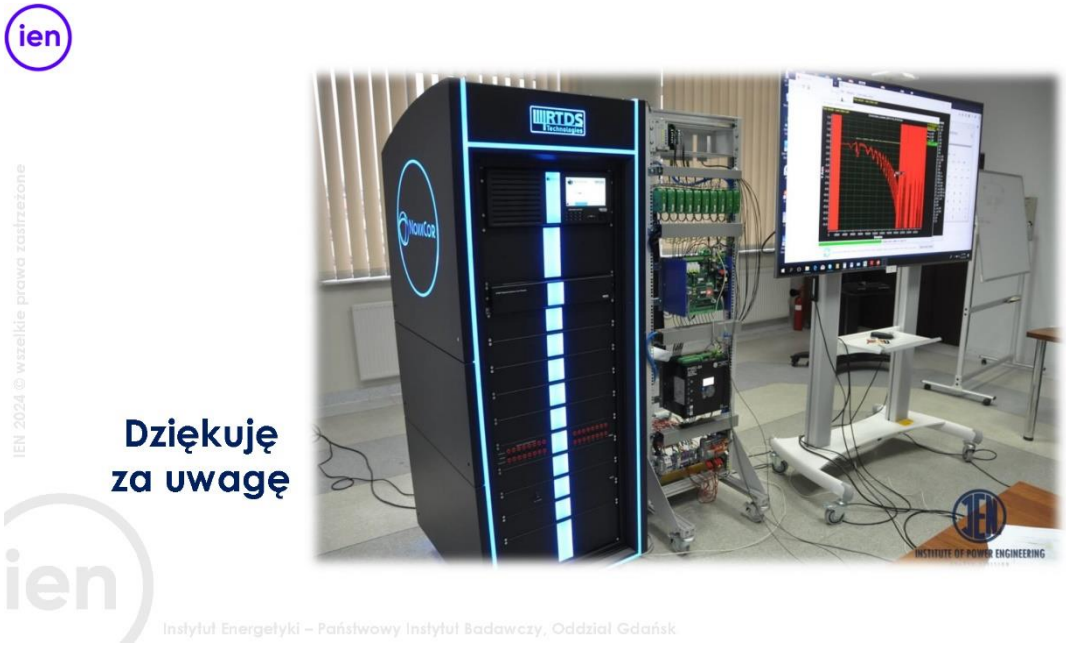


Symulator RTDS – obszary wykorzystania



Podsumowanie i wnioski

1. Opracowano stanowisko przeznaczone do testowania aplikacji wykorzystujących pomiary synchrofazorów w sieci elektroenergetycznej z zastosowaniem symulatora RTDS w technice „hardware in the loop". Zastosowane narzędzia sprzętowe oraz oprogramowanie PDC są w pełni przydatne do symulacji procesów w systemach nadzoru i sterowania takich jak: wizualizacja stanu sieci, monitorowanie zjawisk dynamicznych, wykrywanie zagrożeń i stanów nienormalnych.
2. Badanie aplikacji do wykrywania na podstawie pomiarów synchrofazorów podziału systemu potwierdziły przydatność opracowanego algorytmu. Do badań symulacyjnych wykorzystano model referencyjny IEEE 14-szynowy, skonfigurowany dla celów wykrywania podziału systemu. Jako źródło informacji pomiarów synchrofazorów wykorzystano rzeczywisty układ pomiarowy PMU/RZ50 zasilany danymi analogowymi z RTDS (pomiarami napięć i prądów) oraz układ pomiarowy wirtualny, wbudowany w RTDS .
3. Stanowisko umożliwia przeprowadzanie testów działania (performance test) urządzeń EAZ w symulowanym środowisku sieci elektroenergetycznej – dostępny tryb zdalny.
4. Z wykorzystaniem RTDS i programu testującego wykonano test urządzenia (PMU) na zgodność z normą.


ien
Dziękuję
za uwagę
RTDS
INSTITUTE OF POWER ENGINEERING
IEN 2024 © wszelkie prawa zastrzeżone
Instytut Energetyki – Państwowy Instytut Badawczy, Oddział Gdańsk
25

ADVANCED AUTOMATED DIGITAL FAULT RECORDING DATA COLLECTION AND OPERATIONAL TECHNOLOGY SDN CYBERSECURITY FOR CRITICAL INFRASTRUCTURE, EXAMPLES OF SEL SOLUTIONS - SCHWEITZER ENGINEERING LABORATORIES, USA

Andrey Veselinski (SEL - Schweitzer Engineering Laboratories, Inc.)

1

2


Tworzymy
JAKOŚĆ oraz
NIEZAWODNOŚĆ
projektując nasze produkty
w myśl idei prostoty

3


OBSŁUGA KLIENTA
10-Lat Gwarancji bez zadawania pytań
Serwis reaguje szybko na każdy zwrócony produkt
SEL nigdy nie pobiera opłat za naprawę czegokolwiek
Jeśli nie możemy czegoś naprawić, SEL wymienia urządzenie za darmo

4


Seria zabezpieczeń SEL
WYTWARZANIE
PRZESYŁ
DYSTRYBUCJA
PRZEMYSŁ
ZABEZPIECZENIA i STEROWANIE dla każdego systemu

5


Platforma sterownika automatyki w czasie rzeczywistym
SEL (Real-Time Automation Controller - RTAC)
Main Substation Overview
Kompleksowe rozwiązania z zakresu AUTOMATYKI

6


DOSTARCZAMY KOMPLEKSOWE ROZWIĄZANIA
• Zabezpieczenia i sterowanie
• Automatyka
• Informatyka
• Oprogramowanie
• Synchronizacja czasu
• Bezpieczeństwo infrastruktury krytycznej
• Pomiary
• Łączność
• Usługi inżynierskie
• Szkolenie
Generacja
Przesył
Centrum sterowania
Dystrybucja
Odbiór

7


SHIP FROM STOCK
WORLD'S FASTEST RELAY— WITH FASTEST SHIPPING!
TYPICALLY SHIPS IN TWO DAYS
Wysyłka z magazynu
5-dniowy czas realizacji

8

Kontroler automatyki czasu rzeczywistego (RTAC) nowość w systemach SCADA oraz zdalnego dostępu

SEL

9

Przegląd rodziny kontrolerów RTAC

Zaawansowane zarządzanie ciepłem

>10 razy większa niezawodność od typowych komputerów przemysłowych

Najwyższej jakości komponenty przemysłowe (dyski SLC, pamięci ECC)

Możliwość wymiany SSD podczas pracy, obsługa aplikacji RAID 0 i 1*

Brak otworów wentylacyjnych i ruchomych części

10-letnia, bezproblemowa gwarancja

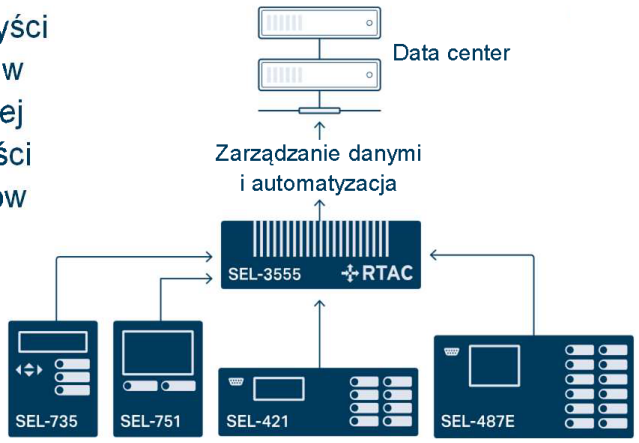
Zaprojektowane, wyprodukowane i przetestowane w USA

*Dla wybranych modeli

10

Kompleksowe monitorowanie stacji

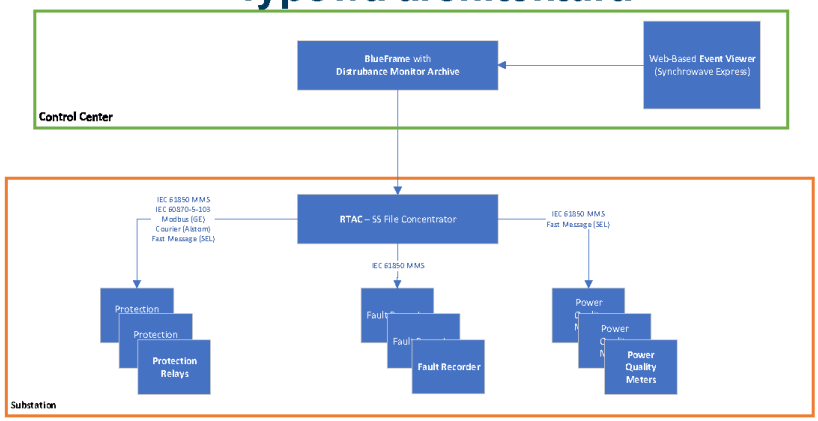
Uzyskanie większej korzyści z danych gromadzonych w stacji elektroenergetycznej w celu poprawy wydajności oraz zmniejszenia kosztów eksploatacji i zarządzania



RTAC (Real-Time Automation Controller) może pełnić funkcję kompletnego systemu monitorowania zakłóceń w czasie rzeczywistym. Zbiera zdarzenia za pośrednictwem wielu protokołów SEL CEV i COMTRADE, GE Modbus, IEC 6IEC 61850 MMS File Transfer. Ogólnie MMS File Transfer umożliwia kompleksowe gromadzenie informacji z urządzeń zgodnych z IEC 61850.

11

Typowa architektura

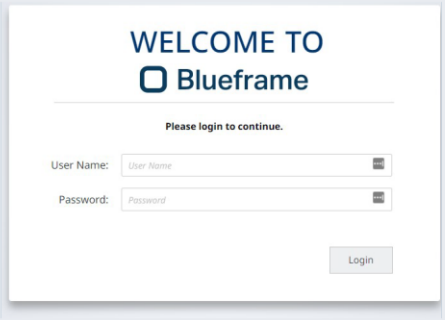


RTAC zainstalowany w stacji elektroenergetycznej może zbierać i tworzyć pliki COMTRADE z wielu źródeł (przekaźniki EAZ, rejestratory zwarć, mierniki jakości energii) przy użyciu dowolnego z obsługiwanych protokołów (61850 MMS, 60870-5-103, Modbus (przekaźniki GE), Courier (Alstom), Fast Messages (Przekaźniki SEL). Pliki są dostępne w stacji elektroenergetycznej przez interfejs HMI RTAC WebBased, ale mogą być także udostępnione na Paltformie Blueframe w centrum sterowania poza stacją.
Platforma Blueframe zawiera przeglądarkę COMTRADE i zbiera dane z RTAC przy użyciu uwierzytelnionego i szyfrowanego połączenia z bazą danych. RTAC zainstalowany w stacji może tworzyć COMTRADE ze strumieni 37.118 PMU lub również z modułów SEL CT/PT Axion.

12

Platforma aplikacyjna Blueframe

Modułowa, bezpieczna platforma OT do instalowania aplikacji SEL oraz do zarządzania i wymiany danych między wyspecjalizowanymi aplikacjami



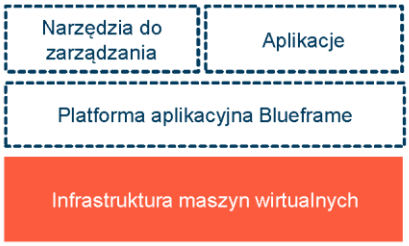
Specjalnie zaprojektowana platforma w celu wspierania automatyzacji wymiany danych i potrzeb aplikacji w bezpiecznym środowisku. Dzięki wbudowanej i modułowej konstrukcji opartej na architekturze tzw. kontenerowej, platforma Blueframe obsługuje dostosowany wybór aplikacji, które pomagają rozwiązywać i wspierać problemy systemowe. Technologia kontenerowa pozwala na korzystanie z zabezpieczonego systemu operacyjnego opartego na Linux, kładąc nacisk na bezpieczeństwo i prostotę. To sprawia, że platforma Blueframe jest lepszą technologią systemu operacyjnego w stacji elektroenergetycznej w porównaniu z Windows.

13

Bezpieczne, modułowe i wszechstronne skalowalnie do potrzeb

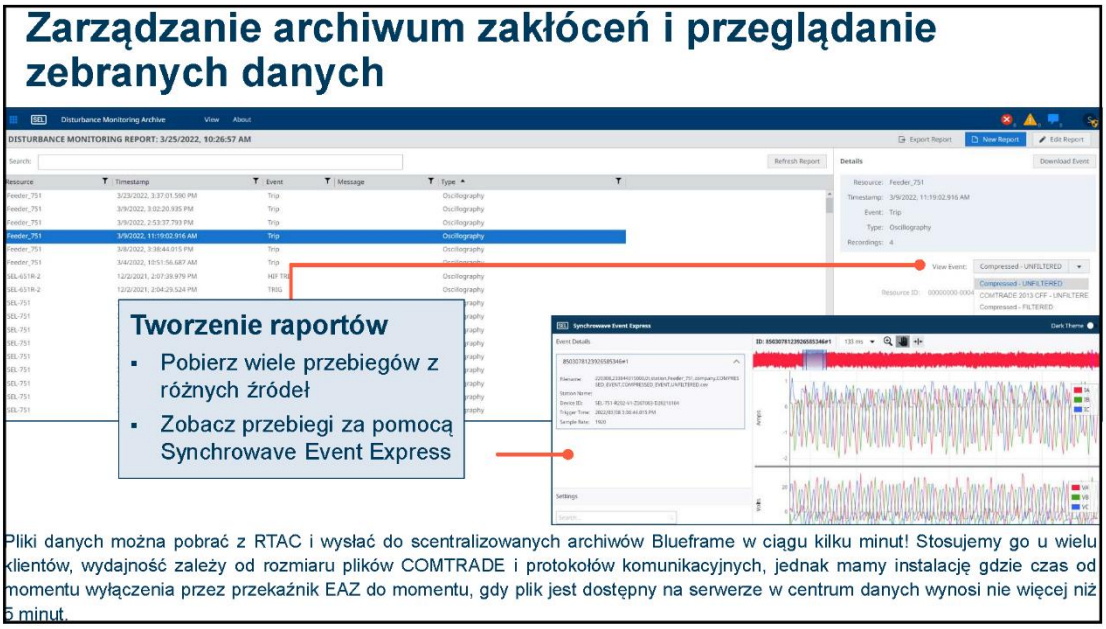
Platforma zbudowana na kontrolerach SEL do zastosowań w stacjach elektroenergetycznych i w przemyśle

Zwirtualizowane i wdrażane we wspólnej infrastrukturze maszyn wirtualnych w celu skalowania zgodnie z potrzebami przedsiębiorstwa

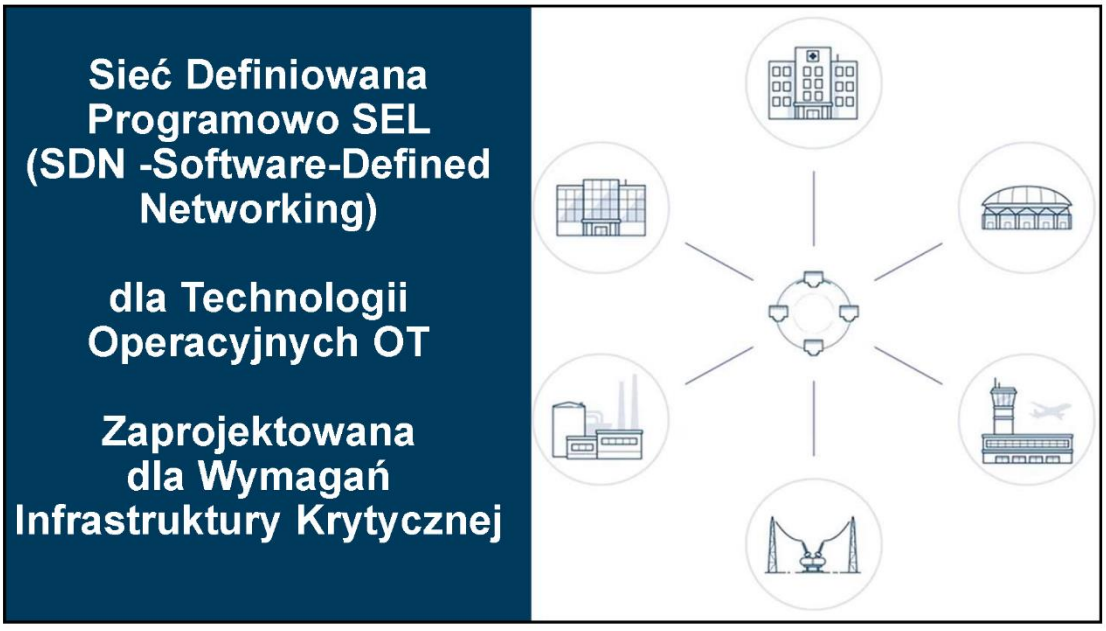


Platforma aplikacji Blueframe została zaprojektowana tak, aby była elastyczna i skalowalna, aby obsługiwać wiele różnych potrzeb klientów teraz i w nadchodzących latach.

14


Zarządzanie archiwum zakłóceń i przeglądanie zebranych danych
Tworzenie raportów
Pobierz wiele przebiegów z różnych źródeł
Zobacz przebiegi za pomocą Synchrowave Event Express
Pliki danych można pobrać z RTAC i wysłać do scentralizowanych archiwów Blueframe w ciągu kilku minut! Stosujemy go u wielu klientów, wydajność zależy od rozmiaru plików COMTRADE i protokołów komunikacyjnych, jednak mamy instalację gdzie czas od momentu wyłączenia przez przekaźnik EAZ do momentu, gdy plik jest dostępny na serwerze w centrum danych wynosi nie więcej niż 5 minut.

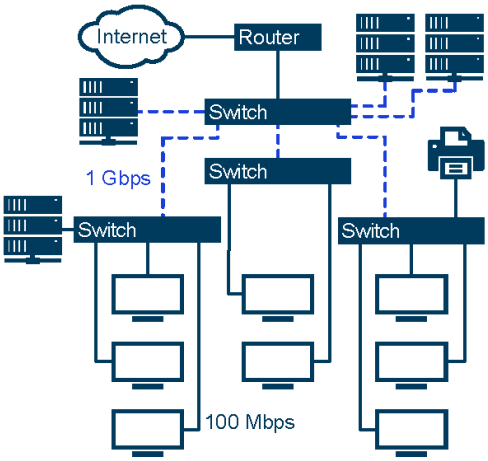
15


Sieć Definiowana Programowo SEL (SDN -Software-Defined Networking)
dla Technologii Operacyjnych OT
Zaprojektowana dla Wymagań Infrastruktury Krytycznej

16

Charakterystyka sieci LAN dla IT

- Funkcjonalność plug-and-play
- Niezawodna łączność
- Złożona topologia
- Dynamiczne środowisko
- Ścieżka redundantna tylko po awarii łącza

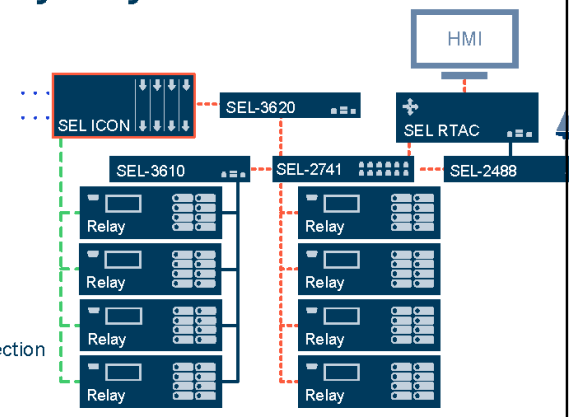


Tradycyjne przełącznice Ethernet przeznaczone są do sieci IT. Funkcja plug-and-play jest kluczowym wymaganiem systemowym sieci IT, ponieważ użytkownicy często podłączają różne urządzenia do sieci. Środowisko IT jest dynamiczne, z wykorzystaniem wielu protokołów danych i z często zmieniającą się topologią sieci. Protokół Rapid Spanning Tree Protocol (RSTP) musi stale uczyć się konfiguracji sieci i definiować ścieżki redundantne na wypadek zakłóceń łącza.

17

Charakterystyka sieci LAN dla OT w stacjach elektroenergetycznych

- Zaprojektowana struktura sieci
- Niewiele zmian
- Komunikacja typu Pub/Sub
- Większe wymagania związane z cyberbezpieczeństwem
- Konieczność szybkiego przełączania awaryjnego



Technologia operacyjna (OT) sieci LAN jest pod wieloma względami przeciwieństwem sieci IT LAN. sieć LAN dla OT nie jest dynamiczna i wykorzystuje tylko kilka protokołów. Technologia „plug-and-play” nie jest pożądana, ponieważ z punktu widzenia cyberbezpieczeństwa ważniejsza jest domyślna odmowa dostępu. Ponadto czasy przełączania awaryjnego sieci OT są bardziej krytyczne.

18

Czym są sieci SDN ?

(SDN - Software-Defined Networking - Sieci programowalne)

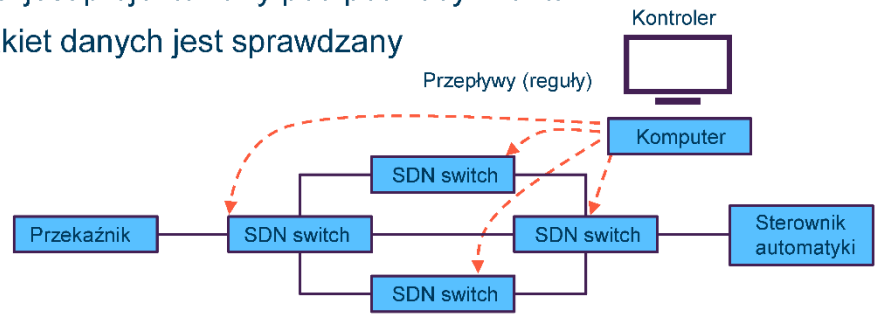
Wyodrębnienie funkcji kontroli sieci z urządzeń sieciowych i przeniesienie ich do centralnego kontrolera poprzez oddzielenie warstwy sterowania od warstwy danych.

SDN umożliwia projektowanie sieci komunikacyjnych na stacji przy zastosowaniu tych samych profesjonalnych praktyk, które są stosowane w prowadzeniu ruchu systemów elektroenergetycznych, ponieważ funkcje sterowania siecią i przesyłania danych są przeniesione do lokalizacji centralnej. Sieć SDN można wstępnie zaprojektować i skonfigurować nie tylko dla wszystkich głównych dróg komunikacji, ale także dla każdego przypadku awarii. SDN poprawia także wydajność sieci, ponieważ urządzenia dokładnie wiedzą, co należy zrobić w przypadku awarii, zamiast definiować wymagane działania urządzeń za każdym razem. Tradycyjnie przełącznik zarządzalny ma warstwę sterowania i warstwę danych w przełączniku. Sterownik ruchu pakietów danych lub kontroler to centralne oprogramowanie zarządzające płaszczyzną sterowania dla wszystkich przełączników.

19

Scentralizowana kontrola

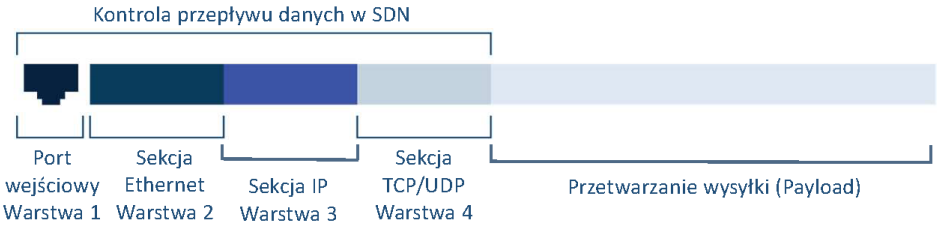
- Ruch pakietów danych (reguły) jest konfigurowany w kontrolerze
- Ruch pakietów danych jest "wypychany" do przełączników (SDN switch)
- Ruch sieci jest projektowany pod potrzeby klienta
- Każdy pakiet danych jest sprawdzany



Kontroler ruchu pakietów danych może konfigurować, monitorować i kontrolować całą sieć. Kontroler ruchu pakietów danych można zainstalować lokalnie w każdej stacji lub jako kontroler scentralizowany, który może zarządzać wieloma lokalizacjami.

20

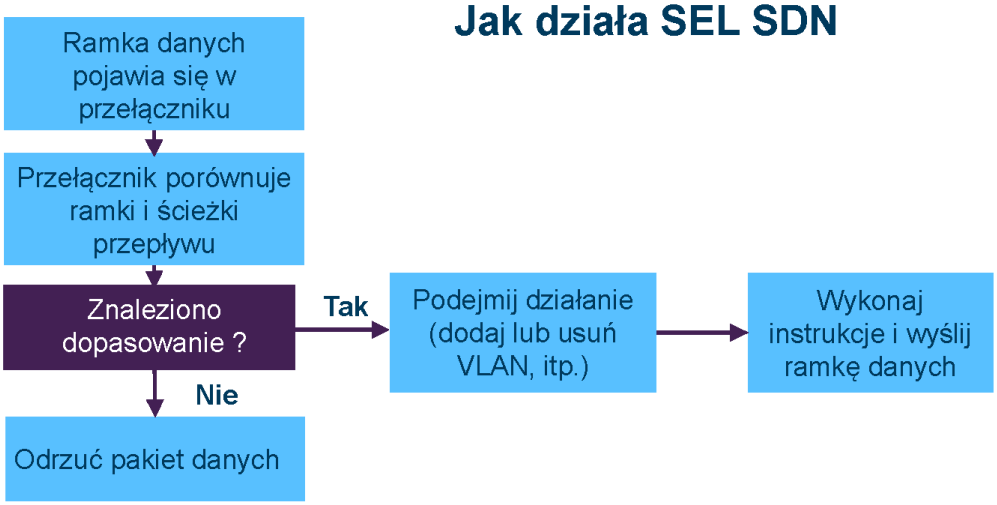
OT w SDN daje bezpośrednią kontrolę



Jest to zasadnicza kwestia, która odróżnia SEL SDN od starszych rozwiązań sieciowych. Starsze rozwiązania sieciowe to stosowana od kilkudziesięciu lat technologia, która kieruje ruchem pakietów danych w oparciu o niewielki podzbiór informacji faktycznie dostępnych w ramce Ethernet. Po co się do tego ograniczać, skoro nie musimy? SDN nie zmienia niczego w warstwie Ethernetu, nie jest też prawnie zastrzeżony, jest to po prostu inna struktura interpretacji danych, które otrzymujemy, aby lepiej odpowiadały potrzebom aplikacji. Więcej informacji na temat aplikacji znajduje się na następnym slajdzie. To właśnie to co robi SEL. Podważanie status quo w inny i lepszy sposób leży u podstaw SEL. Wszystko zaczęło się od SEL-21, a obecnie robimy to samo i w tym przypadku, ale w zakresie sieci Ethernet o znaczeniu krytycznym.

21

Jak działa SEL SDN



22

SEL SDN jest zoptymalizowany pod kątem OT

	SEL SDN	Przełączniki starszych wersji (RSTP)
Bezpieczeństwo	Domyślna odmowa dostępu	Domyślne udzielenie dostępu
Przełączenie awaryjne	Wstępnie zdefiniowane (<0.1 ms)	Dynamiczne (10–30+ ms)
Sposób wymiany danych	Zaprojektowana pod kątem celu i zastosowania	Plug-and-play
Kontrola	Pełna kontrola, brak decyzji opartych na przełącznikach	Mała kontrola, przełączniki mogą podejmować decyzje
Świadomość sytuacyjna	Każde urządzenie zna topologię, wymiana danych dotyczących topologii	Tabele MAC oraz liczniki RX/TX

23

Korzyści

- Mikrosekundowy czas restytucji ruchu w sieci
- Scentralizowana świadomość sytuacyjną
  - Monitorowanie sieci (łącze, węzeł, itp.)
  - Monitorowanie urządzeń
  - Baza IDS - systemu wykrywania włamań
  - Mierniki i liczniki (na port i na aplikację)
  - Obwody tymczasowe/czasowe
- Współpracuje z tradycyjną siecią Ethernet
- Umożliwia użytkownikom zmianę kontroli/zarządzania

24

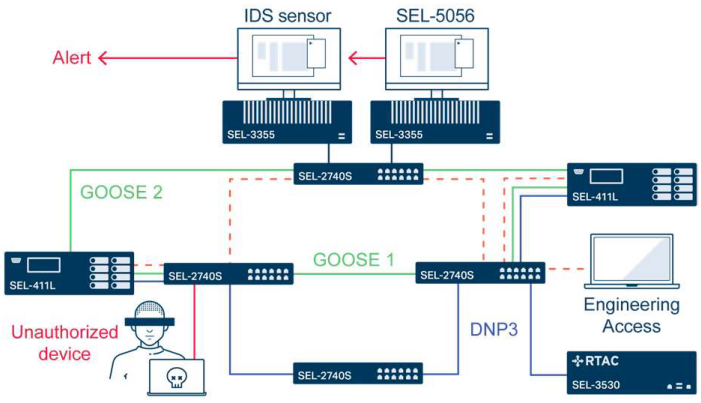
Cechy bezpieczeństwa

- Domyślna odmowa dostępu LAN
- Ukierunkowane transmisje
- Zmniejszona możliwość skanowania portów
- Wielowarstwowa inspekcja pakietów danych przy każdym przeskoku

- Tradycyjny atak
  - MAC spoofing (podszywanie się pod zaufanego hosta)
  - ARP infekowanie pamięci podręcznej
  - Skanowanie zasobów i ustawień sieci
  - Ataki DDoS (zmasowane zajmowanie zasobów w celu zablokowania usług)
  - Płaszczyzna sterowania podatna na ataki

25

Próba nieautoryzowanego dostępu



SEL SDN przejmuje ruch danych, który nie został zdefiniowany do przekazania

SEL SDN filtruje nieodebrane, skażone pakiety danych i wysyła je do czujnika włamania

26

Dziennik zdarzeń

Znaleziono nieznane urządzenie

Połączenie portu C2 jest włączone

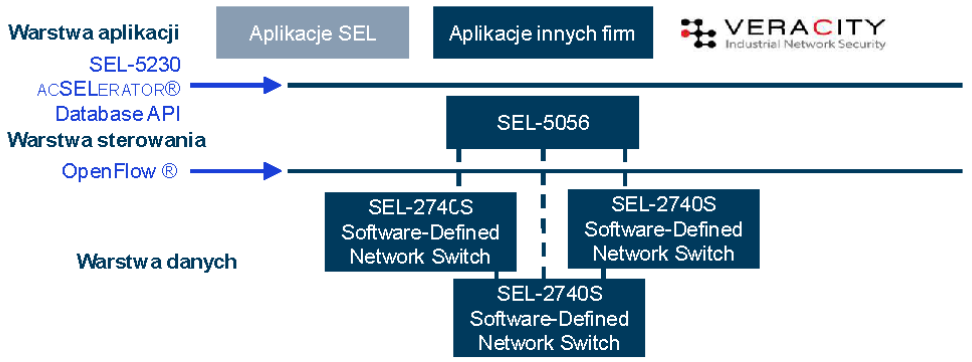
Znany host jest rozłączony i połączenie portu C2 nie działa

Time	IP	Host	Facility	Priority	Tag	Message
May 14 15:30:04	172.20.20.20		user	aler	1	TopologyManager:Device OperationalNetworkNode IP:172.20.20.71 disconnected
May 14 15:30:04	172.20.20.20		user	warning		OpenFlowPlugin:OpenFlow port OpenFlow:00000030A71A7972:C2(6) on switch 00000030A71A7972 is down
May 14 15:30:04	172.20.20.20		user	aler		TopologyManager:Device OperationalNetworkLink a7f5a390c6d1f4ea19aefea45265ed9f disconnected
May 14 15:30:04	172.20.20.20		user	aler		TopologyManager:Device OperationalNetworkPort IP:172.20.20.71 disconnected
May 14 15:30:06	172.20.20.20		user	info	2	OpenFlowPlugin:OpenFlow port OpenFlow:00000030A71A7972:C2(6) on switch 00000030A71A7972 is up
May 14 15:30:06	172.20.20.20		user	info		TopologyManager:Adopted reconnected OperationalNetworkLink a7f5a390c6d1f4ea19aefea45265ed9f
May 14 15:30:07	172.20.20.20		user	info	3	TopologyManager:Found unadopted OperationalNetworkPort IP:172.20.20.123
May 14 15:30:07	172.20.20.20		user	info		TopologyManager:Found unadopted OperationalNetworkNode IP:172.20.20.123
May 14 15:30:07	172.20.20.20		user	info		TopologyManager:Found unadopted OperationalNetworkLink aca38f246b2dc43f5803cc6cfdf926bf

Oprócz tego, że SEL-5056 wyświetla nowe urządzenie i jego lokalizację, SEL-5056 może również generować dzienniki Syslog z przydatnymi informacjami dotyczącymi zdarzeń systemowych.

27

SEL API umożliwia tworzenie aplikacji skoncentrowanych na konkretnym rozwiązaniach



OpenFlow® to protokół komunikacyjny, który można uznać za element konstrukcyjny ogólnej architektury SDN. Firma SEL zaadoptowała standard OpenFlow, aby umożliwić współpracę przełącznika sieciowego SEL-2740S ze sterownikami ruchu pakietów danych innych producentów. Dzięki temu firma SEL może skoncentrować się na rozwoju sterownika przepływu danych przeznaczonego dla OT zastosowanych w stacjach, który nadal może być używany w zastosowaniach informatycznych (IT) wykorzystujących sterowniki ruchu danych zorientowane na technologię IT. Warstwa aplikacji zapewnia interfejs umożliwiający tworzenie określonych funkcji na wyższym poziomie w celu wspierania zadań operacyjnych, administracyjnych i konserwacyjnych (OAM). Aplikacje otwierają możliwości wykorzystania SDN do rozwiązywania różnych problemów. Na przykład można zarządzać profilami zabezpieczeń sieci (bankami nastaw) za pośrednictwem aplikacji, bez konieczności wchodzenia przez użytkownika w szczegóły reguł konfiguracji warstwy sterowania niskiego poziomu.

28

SEL-2742S: Programowalny przełącznik sieciowy

- 12 portów, w tym 2 porty PoE
- Możliwość montażu na szynie DIN lub natynkowo
- Zgodność z IEEE 1613
- Zakres temperatury roboczej: –40° do +85°C
- Obsługa standardu PTP
- Dwa redundantne źródła zasilania

29

SEL-2741 Programowalny przełącznik sieciowy

SZYBSZY, WIĘCEJ PORTÓW, WIĘKSZA ELASTYCZNOŚĆ

- 24 porty
- 100 Mbps/1 Gbps – porty elektryczne lub optyczne SFP
- Dwa wejścia dwustanowe
- 10 lat gwarancji
- Konfigurowalność
- Precyzyjny zegar PTP
- Niewielka głębokość montażu
- IEC 61850-3 i IEEE 1613

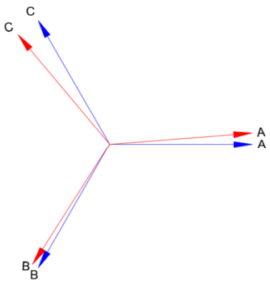
30

AUTOMATYKA SYNCHRO CHECK W SIECIACH 110 KV

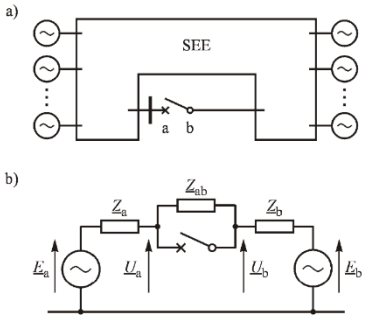
Krzysztof Łowczowski (Politechnika Poznańska)
Piotr Miller (Politechnika Lubelska)

Automatyka Synchro-Check w sieciach 110 kV

Krzysztof Łowczowski - Politechnika Poznańska
Piotr Miller - Politechnika Lubelska



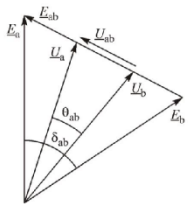
Wyznaczanie początkowego prądu załączenia



(a) układ wyjściowy, (b) schemat zastępczy

Prąd załączenia można opisać wzorem:

$$\underline{I}_{ab} = \frac{\underline{U}_{ab}}{\underline{Z}_{Th}} = \frac{\underline{U}_{ab}}{\underline{Z}_a + \underline{Z}_b}\left(1 + \frac{\underline{Z}_a + \underline{Z}_b}{\underline{Z}_{ab}}\right)$$

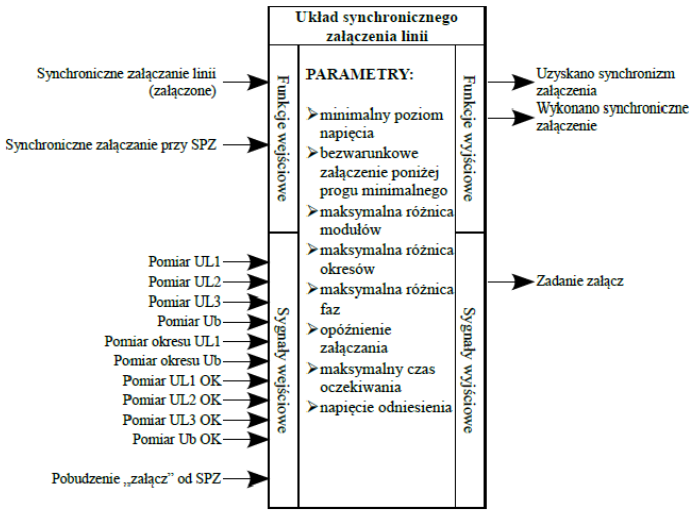


Wartości początkowych prądów załączenia w funkcji wartości impedancji zastępczej

dla kąta łączenia 30°							
U_a	U_b	ΔU		U_{ab}	Z_{Th} [Ω]		
					10	20	30
[kV]	[kV]	[pu]	[kV]	[kV]	I_{ab} [A]		
121	121	0	0	62,6	6263,4	3131,7	2087,8
121	99	0,2	22	60,8	6077,6	3038,8	2025,9
99	99	0	0	51,2	5124,6	2562,3	1708,2
dla kąta łączenia 60°							
U_a	U_b	ΔU		U_{ab}	Z_{Th} [Ω]		
					10	20	30
[kV]	[kV]	[pu]	[kV]	[kV]	I_{ab} [A]		
121	121	0	0	121,0	12100,0	6050,0	4033,3
121	99	0,2	22	111,6	11163,8	5581,9	3721,3
99	99	0	0	99,0	9900,0	4950,0	3300,0

Analiza wykazała, że korelacja pomiędzy wartościami napięć U_{ab} i ΔU występuje przy kątach łączenia Θ_{ab} w granicach do 25°. Dla większych kątów łączenia decydujące o wartości napięć U_{ab} są poziomy napięć w węzłach reprezentujących otwarte bieguny wyłącznika. Wydaje się więc, że zarówno zachowawcze nastawianie urządzeń Synchro-Check w zakresie różnicy modułów napięć, w granicach 0.1÷0.2 U_n, jak i nastawy w zakresie kątów łączenia w granicach 10°÷20°, nie znajduje uzasadnienia.

Zabezpieczenia odległościowe z funkcją Synchro-Check



Moduł synchronicznego załączania linii jest elementem funkcjonalnym, którego działanie warunkują:

1) funkcje wejściowe: synchroniczne załączenie linii aktywne, synchroniczne załączenie przy SPZ,

2) sygnały pomiarowe: UL1, UL2, UL3, Ub oraz te, określające poprawność ich pomiarów, okresów, przesunięć fazowych,

3) parametry robocze nastawiane przez użytkownika,

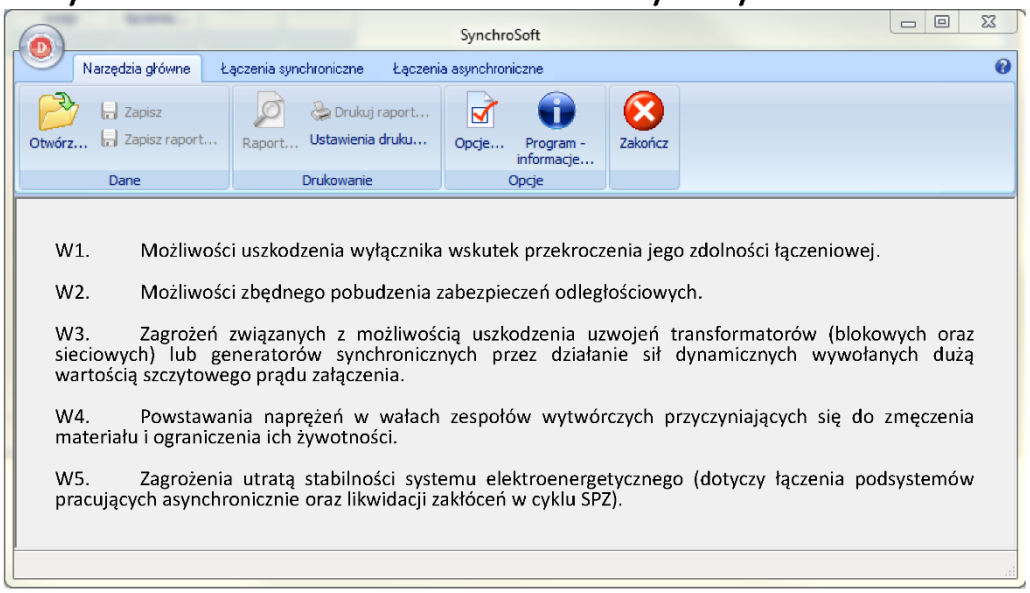
4) sygnały wejściowe: pobudzenia od automatyki SPZ-u.

W wyniku działania zabezpieczenia generowane są:

1) funkcje wyjściowe: o uzyskaniu synchronizmu i wykonaniu synchronicznego załączenia,

2) sygnały żądające załączenia linii (dla modułu sterowania wyłącznikiem).

Kryteria doboru nastaw automatyki Synchro-Check



Spodziewane różnice parametrów wyznaczone w programie SynchroSoft

Model: zima szczyt		Model: lato szczyt	
Kąt łączenia θ_{ab} [°]	ΔU [kV]	Kąt łączenia θ_{ab} [°]	ΔU [kV]
4,6	8,2	6,6	0,6
4,7	1,8	4,3	4,3
5,5	2,1	5,0	3,2
20,9	1,5	9,1	7,5
0,1	0,0	0,0	0,0
19,8	0,5	8,7	6,6
6,2	1,4	1,9	6,0
17,4	4,3	2,3	5,9
5,3	0,7	5,2	4,7
4,1	2,3	5,6	3,9
2,9	7,8	13,5	2,7
3,9	0,7	5,8	5,5
16,9	6,1	14,5	5,2
0,2	0,2	0,2	0,2
3,9	6,8	16,3	3,5
5,0	6,8	9,0	6,2
1,9	11,5	11,0	2,0
1,5	1,7	2,2	3,6
5,0	0,8	4,7	0,9
0,1	0,1	0,1	0,1

Małe wartości rozchyłów kątowych (poniżej 5°) na otwartych biegunach wyłącznika w warunkach normalnych to na ogół niemal pewność, że trudno będzie znaleźć takie warunki pracy sieci, w których te rozchyły osiągnęłyby znaczne wartości.

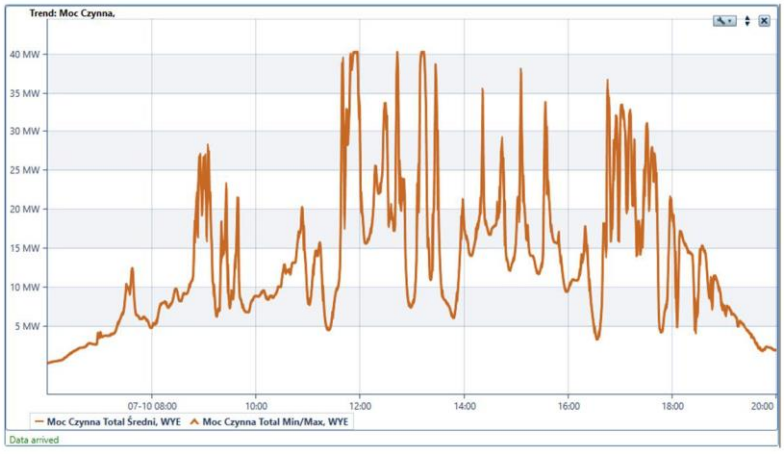
W tabeli wyróżniono te punkty łączenia, w których wartości rozchyłów kątowych przekraczają wartość 10° już w warunkach normalnych, co może świadczyć o tym, że punkty te są podatne na zmianę warunków pracy sieci. Są to potencjalnie punkty łączenia, w których należy w pierwszej kolejności rozważyć zastosowanie automatyki SynchroCheck i skupić się na poprawnym wyznaczeniu nastaw tej automatyki.

Ponadto jeżeli wyłączenie linii prowadzi do wydzielenia układu wyspowego zainstalowanie automatyki SynchroCheck jest niezbędne.

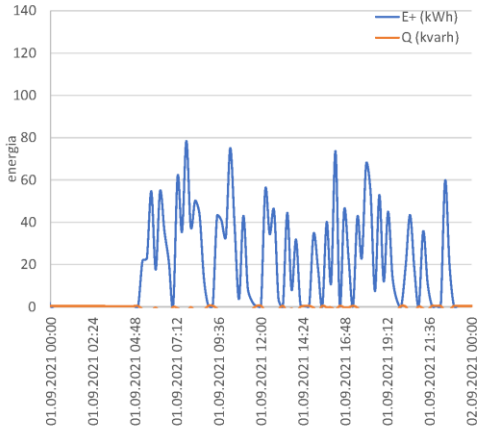
Zmienność pracy źródeł

Na potrzeby zbadania wpływu automatyki SPZ na różnice napięć i prądów wykonano badania symulacyjne oraz pomiary pracy źródeł – źródła wiatrowego o mocy około 50 MW oraz elektrowni fotowoltaicznej (EF) 50 MW w celu oceny dynamiki zmian i określono, że spodziewana zmiana parametrów w trakcie cyklu SPZ jest mała ~300kW/40ms. Zmiany mocy dla obserwowanej elektrowni wiatrowej (EW) nie przekraczają około 200 kW/1 s. Jednocześnie sam fakt otwarcia wyłącznika powoduje, że różnica potencjałów może być znaczna.
Automatyka SC występuje również w sieciach SN w celu ochrony przed nieprawidłowymi operacjami i nieplanowaną pracą wyspową

Zmienność mocy w przypadku nieudanego SPZ (ponowne połączenie po osiągnięciu znacznej różnicy parametrów)



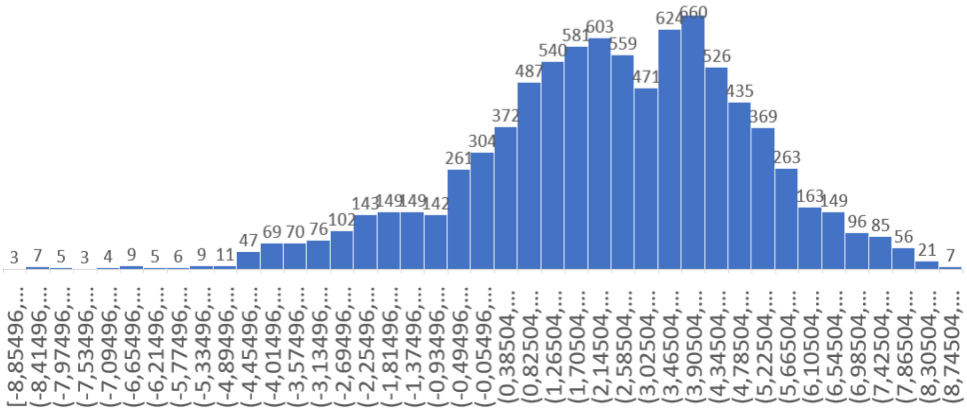
Czynniki zwiększające rozchył kątowy i różnice napięć



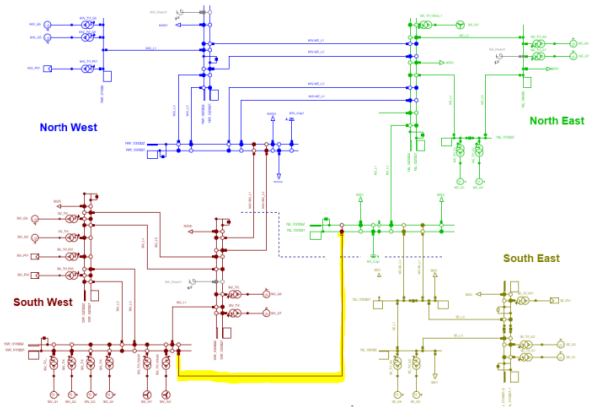
Wśród czynników zwiększających różnice kątów i amplitud napięć można wymienić:

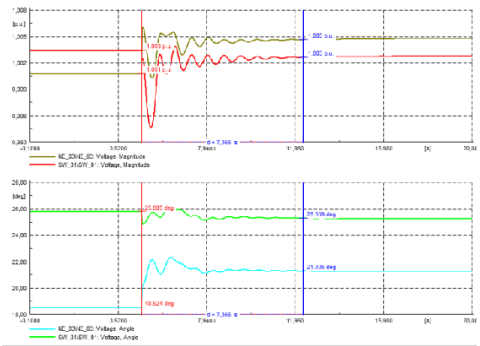
- duże pobory lub generacje mocy czynnej wynikające z pracy źródeł, magazynów energii i dużych odbiorników pobierających moc czynną np. stacji ładowania pojazdów
- dynamiczne zmiany poborów np. sieć trakcyjna
- różnice parametrów elektrycznych linii po obu stronach ciągu np. linie kablowo – napowietrzne,
- niekorzystne warunki sieciowe prowadzące do rozchyłu kątowego np. duże miasta cechujące się poborem mocy czynnej oraz niewielkiej ilości mocy biernej oraz sąsiadujące GPZ z dużym udziałem źródeł lokalnych lub źródła lokalne.

Spodziewana różnica napięć dla przykładowej stacji w przypadku hipotetycznej pracy z otwartym wyłącznikiem

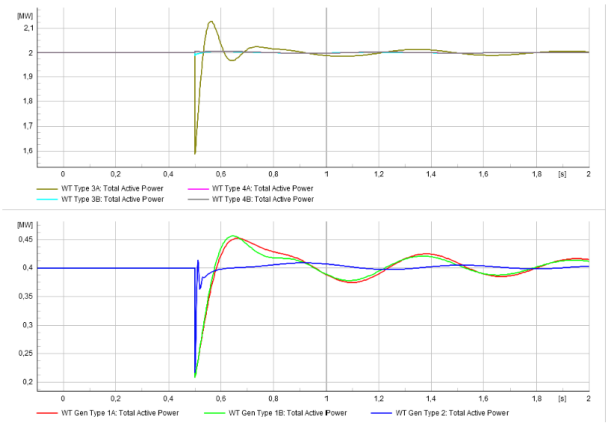


Analizy stanów przejściowych





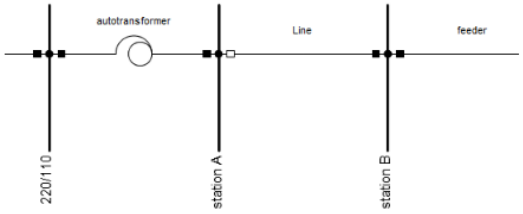
Udary mocy w zależności od rodzaju elektrowni



Na podstawie dostarczonych danych stwierdzono, że źródła wiatrowe pracujące w sieci 110 kV to źródła 3 i 4 typu, które dzięki częściowej lub całkowitej separacji od sieci są zdecydowanie mniej podatne na udary mocy niż źródła wiatrowe 1 i 2 typu, co przedstawiono na Rysunku. Źródła 1 i 2 typu są jednak wciąż obecne w sieciach SN.

Źródła fotowoltaiczne oraz wiatrowe 4 typu są całkowicie odseparowane od sieci poprzez przekształtnik dzięki czemu są niewrażliwe na udary mechaniczne. Nie należy jednak zapominać o udarach elektrycznych np. udarach prądowych oddziałujących negatywnie na znajdujące się wewnątrz układy elektroniczne.

Ograniczanie różnic napięć i kątów



Parametr	Wartość	Akcja
Różnica kątów Różnica napięć	Powyżej progu Znacznie poniżej progu	Zmiana mocy czynnej
Różnica kątów Różnica napięć	Znacznie poniżej progu Powyżej progu	Zmiana mocy biernej
Różnica kątów Różnica napięć	Powyżej progu Powyżej progu	Zmiana mocy czynnej oraz biernej jeżeli jest to wymagane

Ograniczanie różnic napięć i kątów

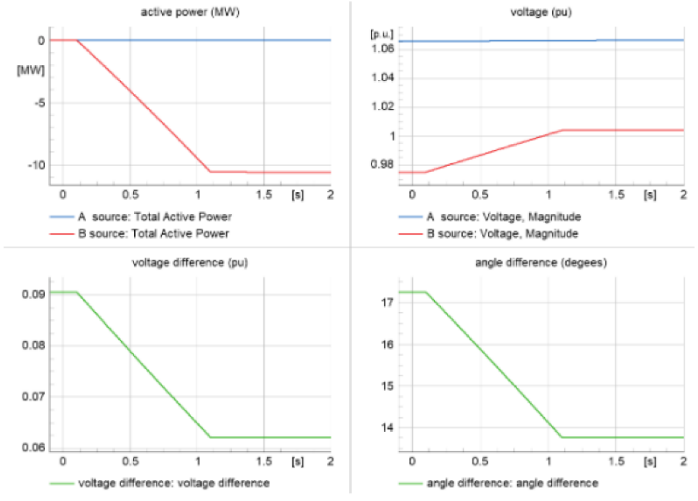


Figure 11. Impact of active power change at the feeder side on voltage and angle differences.

Ograniczanie różnic napięć i kątów

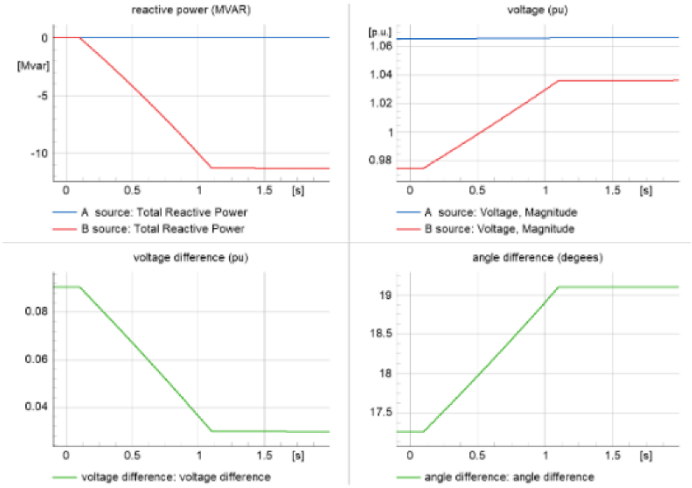


Figure 9. Impact of reactive power change at the feeder side on voltage and angle differences.

Wnioski

Dalsza rozbudowa OZE oraz dużych odbiorów takich jak elektromobilność, trakcja, odbiory przemysłowe itp. sprzyjają powstawaniu dużych różnic napięć i kątów pomiędzy biegunami wyłącznika, co powoduje że znaczenie automatyki Synchro-Check rośnie.

Istnieje możliwość ograniczania różnic napięć i kątów przed wykonaniem operacji łączeniowej poprzez odpowiednie sekwencje sterowania pracą źródeł i magazynów.

Ze względu na znaczne różnice warunków sieciowych, konieczne jest wykonywanie niezależnych analiz pod kątem automatyki Synchro-Check dla poszczególnych obszarów sieci elektroenergetycznej.

Konieczne są dalsze badania – realizacja charakterystyk P(f) zgodnie z kodeksem NCRFG jest nadrzędna i nadpisuje działania mające na celu minimalizacje różnic napięć i kątów. Wskazane są dalsze badania i wypracowanie optymalnych rozwiązań.

CYBERBEZPIECZEŃSTWO W OBSZARZE AUTOMATYKI ZABEZPIECZENIOWEJ

Cezary Bryczek (GE Grid GmbH)

GE VERNOVA
Our portfolio of energy businesses

Cyberbezpieczeństwo w obszarze automatyki zabezpieczeniowej

Cezary Bryczek

Marzec 2024

GE VERNOVA
Our portfolio of energy businesses

Cyberbezpieczeństwo

Powstrzymywanie „złych aktorów” od robienia „złych rzeczy” ludziom i/lub organizacjom za pomocą metod cyfrowych.

 2

GE VERNOVA
Our portfolio of energy businesses

IT versus OT Cybersecurity

 3

Cyberbezpieczeństwo IT versus OT

GE VERNOVA
Our portfolio of energy businesses

IT

Dane i przepływ informacji cyfrowych

- Systemy informatyczne służą przede wszystkim do przechowywania i przetwarzania danych.
- Cyberbezpieczeństwo IT koncentruje się głównie na ochronie wrażliwych informacji, takich jak numery ubezpieczenia społecznego, wrażliwe informacje dotyczące zdrowia etc.
- Wpływ cyberataku na wrażliwe dane może na przykład skutkować utratą reputacji, kradzieżą, stratami finansowymi lub karami finansowymi.

OT

Procesy technologicze oraz urządzenia/maszyny służące do ich przeprowadzania

- Systemy OT kontrolują procesy technologiczne i zapewniają nadzór and urządzeniami IED.
- Cyberbezpieczeństwo OT koncentruje się na zapewnieniu bezpieczeństwa i niezawodności infrastruktury krytycznej w branżach takich jak ropa i gaz, chemiczna, elektryczna, transport i produkcja.
- Wpływ cyberataku na OT w organizacjach zajmujących się infrastrukturą krytyczną może skutkować tragicznymi konsekwencjami, w tym przestojami w zasilaniu/produkcji, awarią sprzętu, a nawet może spowodować eksplozje oraz zagrożenie dla życia i zdrowia ludzi.

-GE NON-PUBLIC- 4

GE VERNOVA
Our portfolio of energy businesses

10 złotych zasad cyberbezpieczeństwa

 5

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 1

WSZYSTKO sprowadza się do RYZYKA. Ile ryzyka jest akceptowalne w porównaniu do tego, ile zainwestować w ochronę przed czymś co może się wydarzyć.

„To gra liczbowa – wszystko sprowadza się do matematyki. ”

 6

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 2

Golden RULES

Zapobieganie cyberincydentowi jest o 1 000 000% lepsze i mniej kosztowne niż próba naprawienia sytuacji i powrotu do „znanego dobrego stanu”.

„Profilaktyka jest zawsze lepsza od leczenia. ”

 7

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 3

Golden RULES

Nie zakładaj, że wszyscy „źli aktorzy” są „nieznani” lub spoza organizacji.

„Zagrożenia wewnętrzne mogą być równie złe a nawet gorsze niż zagrożenia zewnętrzne. ”

 8

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 4

Różnica między dobrą a świetną strategią cyberbezpieczeństwa polega na uznaniu, że jedno rozwiązanie nie jest „tym” rozwiązaniem.

„Wielopoziomowa strategia cyberbezpieczeństwa jest zawsze lepsza. ”

 9

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 5

Ustanowienie dobrej „cyber-higieny” w swoim życiu osobistym i w swojej organizacji – poprzez szkolenia cybernetyczne.

„Nigdy nie przestawaj uczyć się o najlepszych praktykach w zakresie cyberbezpieczeństwa. ”

 10

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 6

Golden RULES

Źle zaprojektowane, zainstalowane i skonfigurowane rozwiązania cyberbezpieczeństwa doprowadzą do fałszywego poczucia bezpieczeństwa i doprowadzą do katastrofalnych zdarzeń.

“Przeanalizuj trzy razy zanim wprowadzisz rozwiązanie.”

 11

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 7

Golden RULES

Ufaj, ale sprawdzaj . . .
wszystkich i wszystko.

„Zastosuj podejście Zero Zaufania do cyberbezpieczeństwa. ”

 12

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 8

Przeanalizuj dokładnie, co należy chronić i dlaczego, a nawet przed kim, zanim podejmiesz decyzję w jaki sposób.

„Zacznij od dokładnego zrozumienia, co wymaga ochrony. ”

 13

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 9

Pamiętaj, że skuteczne powstrzymanie jednego cyberataku nie oznacza, że powstrzymałeś wszystkie przyszłe cyberataki.

„Zli aktorzy są nieustępliwi i nigdy nie przestają. ”

 14

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Golden RULES

Zasada 10

Nie zakładaj i nigdy nie myśl, że jesteś „gotowy”.

„Zagrożenia cybernetyczne stale ewoluują; tak samo powinno być w przypadku cyberbezpieczeństwa. ”

 15

GE VERNOVA
Our portfolio of energy businesses

Przykładowe incydenty cybernetyczne w sektorze energetycznym

 16

Colonial Pipeline - 2021

GE VERNOVA
Our portfolio of energy businesses

- Udany atak ransomware przez: DarkSide
- Colonial Pipeline zapłacił okup 4,4 miliona dolarów w Bitcoinach.
- **Przyczyna**: Brak ram cyberbezpieczeństwa zarówno w zakresie przygotowania, jak i reagowania na incydenty
- Luki w zabezpieczeniach, wykorzystanie starego nieużywanego konta
- **Skutek**: Zakłócenia w dostawach ropy naftowej na wschodnim wybrzeżu USA

Inne ostatnie cyberataki w sektorze energetycznym

GE VERNOVA
Our portfolio of energy businesses

Saudi Aramco – nieudana próba wymuszenia

Sellafield (UK) –atak przez hakerów (**Chiny i Rosja**)

Litewska państwowa grupa energetyczna Ignitis

Ukraińska energetyka jądrowa Energoatom

Największy dostawca gazu ziemnego w Grecji DESFA

Israel Company →

Unitronics PLCs

Inne cyberataki w sektorze energetycznym

GE VERNOVA
Our portfolio of energy businesses

Cybersecurity incidents against global commodity industries

March 2017 through June 2023

Affected industry

- Petchems
- Oil
- Nuclear
- Power
- Shipping
- Metals
- Gas

Source: S&P Global Commodity Insights

GE VERNOVA
Our portfolio of energy businesses

Cyberbezpieczeństwo Defense-in-Depth

Podejścia do Cyberobrony

GE VERNOVA
Our portfolio of energy businesses

Outside In

- Podkreśla ochronę obwodową
- Większy budżet na cyberbezpieczeństwo wydawany na zewnętrzne kręgi
- Założenie jest takie, że większość cyberataków pochodzi z zewnątrz, powstrzymaj je, zanim posuną się zbyt daleko

Inside Out

- Podkreśla wewnętrzną ochronę aktywów
- Greater cybersecurity budget spent protecting asset
- Zakłada się, że aktywa muszą być chronione za wszelką cenę lub że zagrożenia wewnętrzne mogą spowodować największe szkody

 21

7 Warstw Cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Warstwa	Nazwa Warstwy	Opis Warstwy
1	Edukacja/szkolenie użytkowników*	Szkolenie / Edukacja użytkowników w zakresie różnych „najlepszych praktyk” w zakresie cyberbezpieczeństwa, w tym różnych metod cybernetycznych ukierunkowanych na użytkowników.
2	Fizyczna / Kontrola dostępu*	Chociaż nie ma charakteru „cyber”, kluczowe znaczenie ma zapewnienie fizycznego dostępu do technologii, takich jak systemy sprzętowe i różne infrastruktury IT i OT.
3	Zabezpieczenia obwodowe	Ochrona i kontrola dostępu do sieci za pośrednictwem routerów, bram, przełączników i zapór sieciowych.
4	Bezpieczeństwo sieci	Ochrona rzeczywistej infrastruktury sieciowej i ruchu sieciowego (np. danych), który w niej przepływa.
5	Bezpieczeństwo punktów końcowych	Ochrona rzeczywistych urządzeń, w tym ich systemów operacyjnych (np. komputerów, urządzeń IoT/IIoT, urządzeń SCADA, urządzeń IED), które są podłączone do sieci.
6	Bezpieczeństwo aplikacji	Zabezpieczanie i ochrona różnych aplikacji oraz oprogramowania systemów działających w sieci.
7	Bezpieczeństwo danych	Ochrona i zabezpieczenie przechowywania i transmisji wszystkich typów i form danych przepływających przez sieć.

* = Nie specjalnie cyberbezpieczeństwo; ale krytycznie ważne i związane z cyberbezpieczeństwem.

 22


Defense-in-Depth - Przykład
GE VERNOVA
Our portfolio of energy businesses
OUTSIDE THREAT PROTECTION
Sieć Publiczna
Sieć Prywatna
HACKER
HACKER
PERIMETER SECURITY
DMZ
VPN
2FA/MFA
IDS/IPS
WAF
Web Content Filter
Honeypot
NETWORK SECURITY
VoIP Security
Wireless Security
Firewall
Virtual Patching
Mobile Security
External Vuln Scanning
Message Security
Internal IDS/IPS
ENDPOINT SECURITY
NAC
DLP
DDos Prevention
Internal Firewall
NGAV/EDR/MDR (malware/ransomware)
File Integrity Monitoring
Internal Vuln Scanning
Patch Management
Physical Security
ICAM/ZTA (2FA/MFA)
Network Device Hardening
Endpoint App White/Blacklist
APPLICATION SECURITY
Endpoint Disk Encryption
DLP
Endpoint Firewall
Application Vuln Scanning
Dynamic App Testing
Physical Security
Logging
ICAM/ZTA (2FA/MFA)
Endpoint Hardening
Database Security
DATA SECURITY
Static App Testing
DLP
Physical Security
Logging
WAF
ICAM/ZTA (2FA/MFA)
ICAM/ZTA (2FA/MFA)
Data Classification
DLP
Logging
CSIRT
ICAM/ZTA (2FA/MFA)
Data Integrity Monitoring
Logging
Focused Ops
SIEM
Continuous C&A
Data/Drive Encryption
Data Wiping
Security Dashboard
Digital Forensics
IT Security Governance
Security Plan
PKI
DLP
Logging
Vulnerability Assessment
Business Continuity Plan
SOC/NOC Monitoring (24x7)
Escalation Management
Security Awareness Training
IT Disaster Recovery Plan
Continuous Monitoring & Assessement
Situational Awareness
Security SLA/SLO Reporting
Security Architecture & Design
Risk Management
MISSION CRITICAL ASSETS
Security Policies & Compliance
Data Classification
Penetration Testing
Cyber Threat Intelligence
POLICY MANAGEMENT & PREVENTION
MONITORING & RESPONSE / OPERATIONS
-GE NON-PUBLIC-
Copyright 2024 © GE VERNOVA
Proprietary and confidential. Do not distribute.
23


GE VERNOVA
Our portfolio of energy businesses
Standardy Cyberbezpieczeńsywa
Standards
Copyright 2024 © GE VERNOVA
Proprietary and confidential. Do not distribute.
24

Najczęściej stosowane standardy

GE VERNOVA
Our portfolio of energy businesses

ISA / IEC
- ISA/IEC 62443 standard cyberbezpieczeństwa definiuje procesy, techniki i wymagania dla Industrial Automation and Control Systems (IACS)
- IEC 62351 seria norm obejmuje technologie cyberbezpieczeństwa dla protokołów komunikacyjnych zdefiniowanych przez IEC TC 57.

NERC CIP
- NERC 1300 od CIP-002-3 do CIP-009-3(CIP=Critical Infrastructure Protection). Standardy NERC CIP zostały opracowane w celu ochrony krytycznej infrastruktury sieci energetycznej Ameryki Północnej.

NIS 2
- Dyrektywa NIS 2 jest ogólnounijnym aktem prawnym dotyczącym bezpieczeństwa cybernetycznego. Przewiduje ona środki prawne mające na celu podniesienie ogólnego poziomu bezpieczeństwa cybernetycznego w UE.

NIST
- The NIST Cybersecurity Framework to zbiór wytycznych dla firm z sektora prywatnego, których należy przestrzegać, aby lepiej przygotować się do identyfikacji, blokowania, wykrywania, reagowania i usuwania/zmniejszania skutków ataków.

ISO / IEC
- ISO/IEC 27001 to zbiór regulacji do stosowania, których głównym celem jest zapewnienie zaimplementowania i późniejszego utrzymywania i doskonalenia w organizacji systemu zarządzania bezpieczeństwem, informacji .

 25

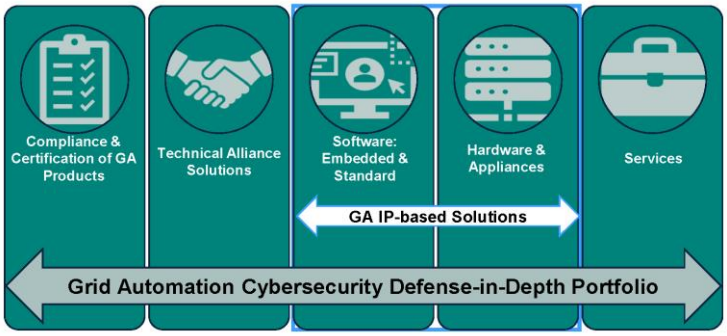
GE VERNOVA
Our portfolio of energy businesses

GE Grid Automation - Wizja Cyberbezpieczeństwa

 26

Grid Automation Defense-in-Depth

GE VERNOVA
Our portfolio of energy businesses



Ochrona cybernetyczna od krawędzi do rdzenia:

- Certyfikacja produktów Grid Automation pod kątem zgodności z cyberbezpieczeństwem
- Dostarczanie dojrzałych, sprawdzonych i solidnych rozwiązań w zakresie cyberbezpieczeństwa
- Innowacyjne rozwiązania z zakresu cyberbezpieczeństwa (Oprogramowanie i Sprzęt)
- Kompleksowe usługi w zakresie cyberbezpieczeństwa

 27

GA - Cyberbezpieczeństwo Aktualna oferta

GE VERNOVA
Our portfolio of energy businesses

Produkty i Rozwiązania:

- Next Generation Firewall (NGFW)
- Monitorowanie bezpieczeństwa sieci(aka: NIDS)
- Host Intrusion Detection & Prevention (HIDS/HIPS)
- Kontrola Dostępu & Autentykacja Multi-factor (MFA)
- Bezpieczny zdalny dostęp klasy przemysłowej
- Anti-Virus / Anti-Malware

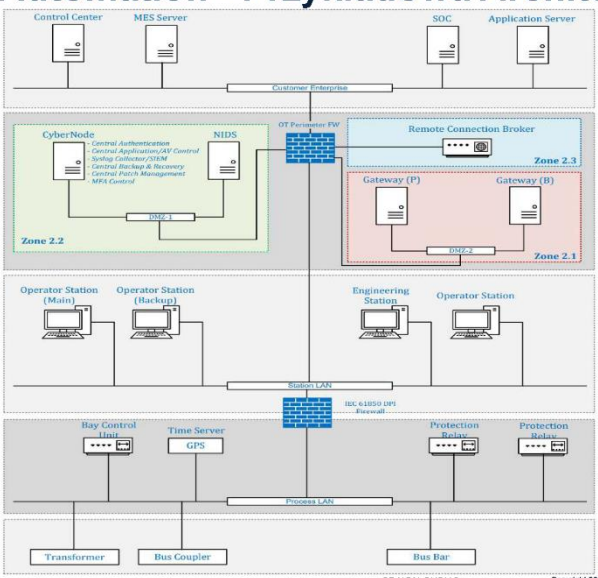
Usługi:

- Backup & Recovery
- Planowanie reakcji na incident
- Audyt cyberbezpieczeństwa i zgodności
- Analiza luk w cyberbezpieczeństwie przemysłowym i ocena ryzyka
- Ocena sieci przemysłowej pod kontem cyberbezpieczeństwa
- Opracowanie polityki i procedur
- Opracowanie “białej listy” dla aplikacji
- Hartowanie węzła końcowego
- Industrial Patching / Patch Management

 28

Grid Automation - Przykładowa Architektura

GE VERNOVA
Our portfolio of energy businesses



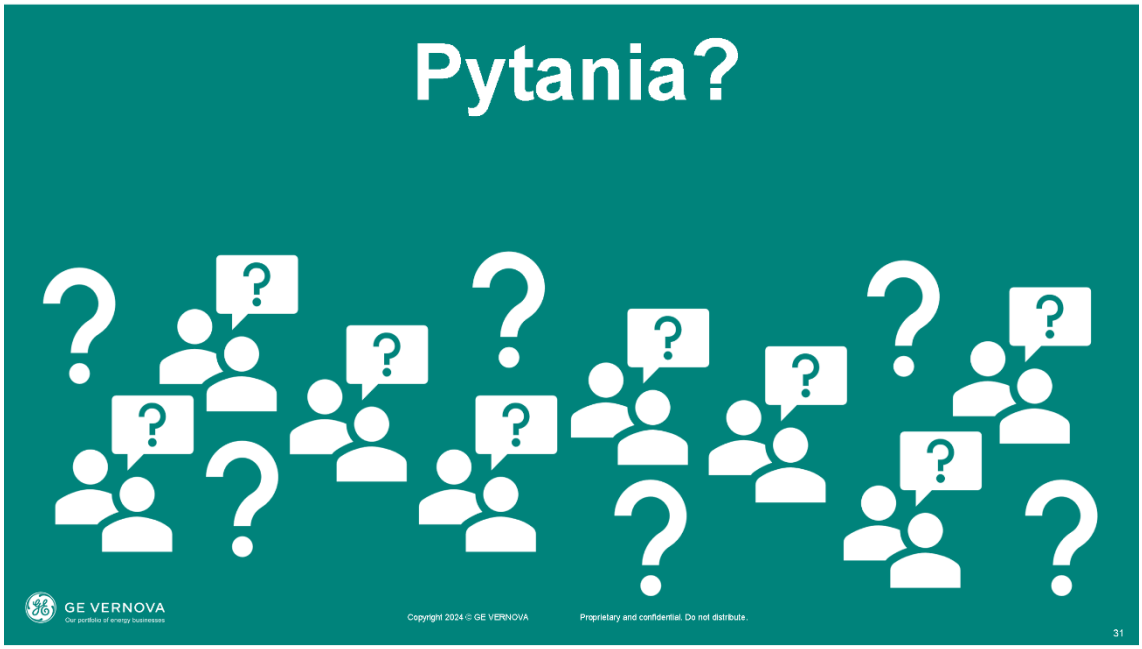
-GE NON-PUBLIC-

29

GE VERNOVA
Our portfolio of energy businesses

Cyberbezpieczeństwo a eksploatacja i zapewnienie wysokiej dostępności

30


Pytania?
GE VERNOVA
Our portfolio of energy businesses
Copyright 2024 © GE VERNOVA
Proprietary and confidential. Do not distribute.
31


GE VERNOVA
Our portfolio of energy businesses
Copyright © GE VERNOVA. Implementation of these plans is subject to information and/or consultation with appropriate employee representatives in accordance with local laws.

ROZWIĄZANIA LRW W STACJACH ELEKTROENERGETYCZNYCH Z DŁAWIKAMI WN

Jarosław Gandzel, Mateusz Szablicki (PSE)

| Spis treści

01

Wprowadzenie

Geneza i plan pracy badawczo-rozwojowej

PSE Innowacje

Wprowadzenie Geneza i plan pracy badawczo-rozwojowej

Awaria w polu dławika 400 kV
Eksplozja operatywnie wyłączonego wyłącznika w polu dławika 400 kV wskutek długotrwałego *łukowego* przepływu prądu przez otwarty wyłącznik w następstwie wtórnych zapłonów.

Wnioski poawaryjne
Standardowe rozwiązanie LRW nie gwarantuje rezerwowania wyłączników dławikowych w takich sytuacjach (zakłócenie *nie*-zwarciowe, poza zestawem zadziałań LRW).
Potrzeba wdrożenia **dedykowanego rozwiązania LRW dla pól dławika WN**.

Zlecenie pracy BiR
Uzgodnienie zakresu i formuły realizacji pracy BiR.
Motywacja: **mitygacja ryzyka** powtórzenia zdarzenia.

Bieżąca aplikacja wniosków z Pracy w działaniach operacyjnych PSE S.A.

Praca BiR | Opracowanie i weryfikacja nowego algorytmu działania układu LRW w stacjach elektroenergetycznych z zainstalowanym dławikiem WN

Operacjonalizacja wyników Pracy
Rekomendacje eksploatacyjne.
Rekomendacje standaryzacyjne.
Rekomendacje projektowe.

ETAP I | *Discovery* + koncepcje
ZAKRES: *Discovery* (przegląd wymagań i doświadczeń innych OSP, przegląd rozwiązań producentów) + zdefiniowanie koncepcji nowego rozwiązania LRW dla pól dławikowych + wstępna ocena koncepcji + wybór koncepcji do badań symulacyjnych.

ETAP II | Badania symulacje + selekcja
ZAKRES: Opracowanie modeli EMT koncepcji nowego rozwiązania LRW + badania symulacyjne koncepcji + opracowanie *matrycy wdrożeniowej* koncepcji + ocena potencjału aplikacji w stacjach PSE S.A. + wskazanie rozwiązania LRW rekomendowanego do wdrożenia.

ETAP III | Badania w LZ + rekomendacje
ZAKRES: Zbudowanie stanowiska laboratoryjnego w Laboratorium Zabezpieczeń PSE + testy laboratoryjne + zdefiniowanie rekomendacji aplikacyjnych nowego rozwiązania LRW.

PSE Innowacje Wprowadzenie 4

02

Charakterystyka *standardowego* rozwiązania LRW

Wymagania PSE S.A. dla LRW | *Casy study* wtórnych zapłonów

PSE Innowacje

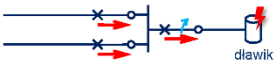
Charakterystyka *standardowego* rozwiązania LRW Wymagania PSE dla LRW

ŹRÓDŁO WYMAGAŃ DLA LRW | Standardowe Specyfikacje Techniczne: *Urządzenia elektroenergetycznej automatyki zabezpieczeniowej i układy z nią współpracujące, stosowane na stacjach WN i NN.* PSE-ST.EAZ.NN.WN/2021.

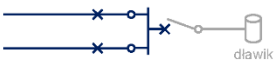
DEFINICJA LRW | **LRW (funkcja 50BF) jest układem umożliwiającym przerwanie prądu zwarciowego w przypadku, gdy zawiódł wyłącznik, który powinien wyłączyć element sieci, w którym wystąpiło zwarcie.**

OCZEKIWANE ZACHOWANIE LRW | Scenariusz wyłączenia wyłącznika podstawowego podczas zwarcia w dławiku.

1. Zwarcie → zadziałanie EAZ → sygnał *wyłącz* wyłącznika dławikowego

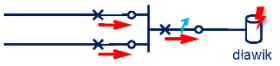


2. **Skuteczne** wyłączenie wyłącznika dławikowego (**podstawowego**)



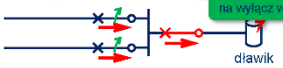
OCZEKIWANE ZACHOWANIE LRW | Scenariusz braku wyłączenia wyłącznika podstawowego podczas zwarcia w dławiku.

1. Zwarcie → zadziałanie EAZ → sygnał *wyłącz* wyłącznika dławikowego

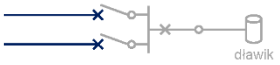


2. **Nieskuteczne** wyłączenie wył. dław.

ZADZIAŁANIE LRW | Impulsowanie na wyłącz wyłączników rezerw.



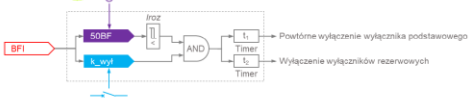
3. **Skuteczne** wyłączenie wyłączników **rezerwowych**



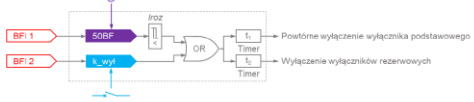
Charakterystyka *standardowego* rozwiązania LRW Wymagania PSE dla LRW

OPIS FUNKCJONALNY LRW | LRW pobudza się po zadziałaniu funkcji eliminacyjnych **EAZ** w polu, w którym wystąpiło zwarcie (sygnały BFI). Zadziałanie LRW nastąpi, jeśli kryteria decyzyjne LRW (kryterium prądowe **50BF**, kryterium wyłącznikowe **k_wył**) zidentyfikują brak skutecznego przerwania przepływu prądu przez wyłącznik podstawowy. Wówczas – po odliczeniu nastawionego opóźnienia czasowego t_1 – LRW wyśle sygnał *retrip* (powtórny sygnał na wyłączenie wyłącznika podstawowego) oraz – po odliczeniu nastawionego czasu t_2 – sygnał na wyłączenie wyłączników rezerwowych.

WARIANT **AND** |



WARIANT **OR** |

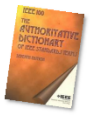


STANDARDOWA NASTAWA LRW | W LRW zainstalowanych w stacjach PSE S.A. najczęściej stosuje się ***wysoką* nastawę** kryterium prądowego 50BF **przekraczającą prąd znamionowy przekładnika** prądowego ← takie podejście gwarantuje wystarczającą czułość detekcji przepływu prądu zwarciowego (zgodnie z wytycznymi) i jednocześnie wyklucza ryzyko nadmiarowego zadziałania LRW.

POPRAWNOŚĆ DZIAŁANIA LRW | Dotychczasowa praktyka eksploatacyjna wskazuje, że LRW zapewnia **poprawną realizację rezerwowania wyłączników podstawowych** we wszystkich wymaganych sytuacjach związanych z niewyłączeniem tego wyłącznika **po zadziałaniu zabezpieczeń w następstwie zakłóceń zwarciowych**. Umożliwia to minimalizację ryzyka uszkodzenia chronionego obiektu KSE i ogranicza nadmiarową propagację skutków takich zakłóceń na otoczenie sieciowe obiektu.

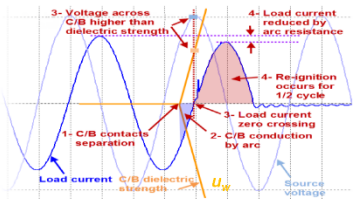
Charakterystyka *standardowego* rozwiązania LRW *Case study* wtórnych zapłonów

WTÓRNE ZAPŁONY W WYŁĄCZNIKU DŁAWIKOWYM | Przerywanie przepływu prądu dławika (uogólniając, prądu indukcyjnego) traktuje się jako ***trudną* operację łączeniową**, której mogą towarzyszyć m.in. **wtórne zapłony**.



DEFINICJA WTÓRNYCH ZAPŁONÓW (ang. *reignition*) | *Wtórny zapłon* jest definiowany jako **wznowienie przepływu prądu między stykami wyłącznika** podczas operacji jego wyłączania po **wcześniejszym przerwaniu tego przepływu**.

Wtórne zapłony mogą występować nawet podczas **operatywnego wyłączania wyłącznika** dławikowego, a mechanizm ich powstawania jest powiązany z *naturalnym przejściem sinusoidy wartości chwilowej prądu przez zero*. Podczas wyłączania wyłącznika dławikowego, w chwili *naturalnego* przerwania przepływu prądu, gdy wartość chwilowa prądu przyjmuje wartości bliskie zero, wartość chwilowa napięcia sieciowego jest bliska maksymalnej, tym samym wartość napięcia powrotnego u_p na rozchodzących się stykach tego wyłącznika skokowo zwiększa się do wartości bliskiej amplitudzie napięcia sieciowego (lub wyższej, jeśli podczas wyłączania występują przepięcia). **Zapłon wtórnego łuku nastąpi, jeśli krzywa u_p przetnie krzywą u_w** wytrzymałości izolacyjnej przerwy w wyłączniku powstałej między rozłączonymi stykami wyłącznika. Wtórny zapłon powoduje przepływ prądu przez wyłączony wyłącznik do ponownego przejścia wartości chwilowej prądu przez zero.



Wtórny zapłon podczas wyłączania wyłącznika

1- Otwarcie styków wyłącznika. **2-** Łuk pierwotny w wyłączniku. **3-** Przejście sinusoidy prądu przez zero i *naturalne* zgaszenie łuku w wyłączniku → skokowa zmiana $u_p \rightarrow u_p$ przekracza aktualną wytrzymałość $u_w \rightarrow$ następuje wtórny zapłon w wyłączniku. **4-** Przepływ prądu przez wyłączony wyłącznik.

Charakterystyka *standardowego* rozwiązania LRW *Case study* wtórnych zapłonów

SKUTKI WTÓRNYCH ZAPŁONÓW DLA WYŁĄCZNIKA | Wtórne zapłony implikują **trudne warunki pracy wyłączników dławikowych**. Powodują ponowny przepływ prądu przez wyłącznik, mimo otwarcia jego zestyków. Wpływa to na pogorszenie parametrów eksploatacyjnych tego wyłącznika, m.in przyspiesza degradację dysz, lub nawet – w skrajnej sytuacji przebicia dysz – powoduje jego trwałe uszkodzenie, w tym występowanie ryzyka eksplozji.

Zgodnie ze standardowym podejściem eksploatacyjnym, zaistnienie wtórnych zapłonów w wyłączniku wymusza podjęcie działań, których zakres zależy od liczby wtórnych zapłonów i standardowych wymagań producentów wyłączników:

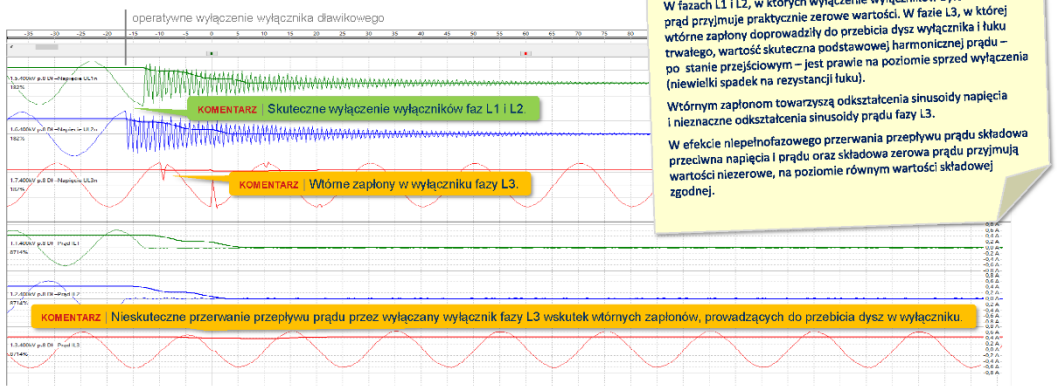
- jednokrotny wtórny zapłon | kontakt z producentem wyłącznika celem pozyskania opinii odnośnie możliwości dalszej eksploatacji → zwykle informacja zwrotna o **możliwej dalszej eksploatacji**;
- dwukrotny wtórny zapłon | kontakt z producentem wyłącznika celem pozyskania opinii odnośnie możliwości dalszej eksploatacji → zwykle informacja o **konieczności przeglądu wyłącznika** lub **konieczności wymiany wyłącznika**;
- przebicie dyszy | zwykle informacja o **konieczności wymiany wyłącznika**.

SKUTKI WTÓRNYCH ZAPŁONÓW DLA SIECI | Wtórne zapłony implikują powstanie **ryzyk aparaturowych i obiektowych dla otoczenia sieciowego** wyłącznika, ponieważ wtórne zapłony mogą wywoływać m.in. przepięcia w otoczeniu sieciowym wyłącznika (oddziałując m.in. na pogorszenie własności izolacji), a ewentualna eksplozja wyłącznika w następstwie wtórnych zapłonów może doprowadzić do uszkodzenia aparatów i obiektów.

WNIOSEK | Propagacja skutków zjawisk towarzyszących wtórnym zapłonom w operatywnie wyłączanych wyłącznikach stanowi silną przesłankę do poszukiwania rozwiązań rezerwowania wyłączników dławikowych w sytuacji zaistnienia w nich wtórnych zapłonów.

Charakterystyka *standardowego* rozwiązania LRW *Case*

STUDIUM PRZYPADKU – ANALIZA WARUNKÓW PODCZAS AWARII W POLU DŁAWIKA 400 kV



Wyłączenie wyłączników w fazach L1 i L2 nastąpiło w chwilach odpowiadających zerowej wartości chwilowej prądów w tych fazach.

Wtórne zapłony w wyłączniku fazy L3 pojawiają się w szczytach pierwszych półokresów sinusoidy napięcia.

W fazach L1 i L2, w których wyłączenie wyłączników było skuteczne, prąd przyjmuje praktycznie zerowe wartości. W fazie L3, w której wtórne zapłony doprowadziły do przebicia dysz wyłącznika i łuku trwałego, wartość skuteczna podstawowej harmonicznej prądu – po stanie przejściowym – jest prawie na poziomie sprzed wyłączenia (niewielki spadek na rezystancji łuku).

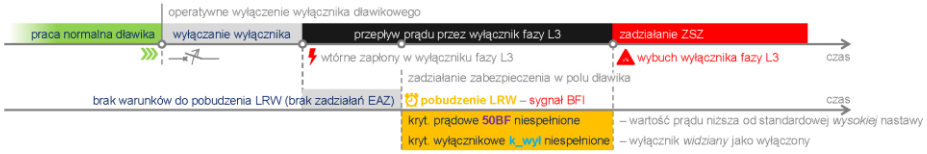
Wtórnym zapłonom towarzyszą odkształcenia sinusoidy napięcia i nieznaczne odkształcenia sinusoidy prądu fazy L3.

W efekcie niepełnofazowego przerwania przepływu prądu składowa przeciwna napięcia i prądu oraz składowa zerowa prądu przyjmują wartości niezerowe, na poziomie równym wartości składowej zgodnej.

Przebieg czasowy wartości chwilowej i skutecznej (**pogrubione przebiegi**) podstawowej harmonicznej napięć fazowych i prądów w polu dławika 400 kV podczas operatywnego wyłączania dławika

Charakterystyka *standardowego* rozwiązania LRW *Case study* wtórnych zapłonów

ANALIZA ZACHOWANIA LRW PODCZAS AWARII W POLU DŁAWIKA 400 kV | LRW zachowała się poprawnie dla przyjętej praktyki eksploatacyjnej nastawiania LRW – wtórne zapłony stanowią **niestandardowe zakłócenie**, wykraczająca poza zwarcia, dla których konfiguruje się LRW. Wznowiony przepływ prądu zwykle nie przekracza prądu znamionowego dławika (czyli nie przekracza *standardowej wysokiej* nastawy LRW) ← kryterium prądowe niespełnione, a wyłącznik jest „widziany” jako otwarty ← kryterium wyłącznikowe niespełnione. Niemniej wielokrotne wtórne zapłony mogą doprowadzić do przebicia dyszy tego wyłącznika i trwałej utraty jego zdolności do przerywania przepływu prądu, wskutek czego prąd nadal płynie przez wyłącznik mimo jego wyłączenia. Wówczas **uzasadnione byłoby zadziałanie LRW i wyłączenie wyłączników rezerwowych, mimo że jest to działanie operatywne**.



Ilustracja przebiegu czasowego działania dotychczasowego rozwiązania LRW w polu dławika 400 kV

NIESTANDARDOWE ZAKŁÓCENIE WYMAGAJĄCE REZERWOWANIA | **Wielokrotne wtórne zapłony podczas operatywnego wyłączania wyłącznika dławika** ← zdarzenie w polu dławika 400kV, które doprowadziło do eksplozji wyłącznika.

PSE Innowacje | Charakterystyka *standardowego* rozwiązania LRW | 11

03

Nowe rozwiązanie LRW dla stacji z dławikiem

Przegląd dostępnych rozwiązań | Koncepcje rozwiązania | Rozwiązanie rekomendowane | Rozwiązanie alternatywne

PSE Innowacje

Nowe rozwiązanie LRW dla stacji z dławikiem Przegląd dostępnych rozwiązań

CEL WYSZUKIWANIA | Przegląd **wymagań innych operatorów sieci przesyłowej dla LRW** dedykowanych dla stacji z dławikiem.

OSP	Informacje o LRW dla dławika	Informacje o LRW
Austria Power Grid AG (Austria)	NIE	NIE
Elia System Operator SA (Belgia)	NIE	NIE
Electricity System Operator (Bułgaria)	NIE	TAK
Swissgrid (Szwajcaria)	NIE	NIE
CEPS (Czechy)	NIE	NIE
TRANSNET BW (Niemcy)	NIE	NIE
TENNET (Niemcy)	NIE	NIE
AMPRION (Niemcy)	NIE	NIE
50hertz (Niemcy)	NIE	NIE
ENERGINET (Dania)	NIE	NIE
REN (Portugalia)	NIE	NIE
EirGrid (Irlandia)	NIE	TAK
Statnett (Norwegia)	NIE	TAK
National Grid (Wielka Brytania)	NIE	TAK

KOMENTARZ | Wymagania **zbieżne** ze stosowanymi w PSE.

PSE Innowacje Nowe rozwiązanie LRW dla stacji z dławikiem 13

Nowe rozwiązanie LRW dla stacji z dławikiem Przegląd dostępnych rozwiązań

CEL WYSZUKIWANIA | Przegląd **rynku w zakresie dostępności i sposobu realizacji LRW** dedykowanych dla stacji z dławikiem.

GE | Dialogi techniczne (kontakt mailowy + rozmowy z dedykowanym zespołem + dokumentacja).
Rekomendacja | Sugestia rozwiązania problemu przez zastosowanie zabezpieczenia do detekcji wtórnych zapłonów w wyłączniku.

HITACHI ABB | Dialogi techniczne (kontakt mailowy + rozmowy z dedykowanym zespołem + dokumentacja).
Rekomendacja | Sugestia rozwiązania problemu przez zastosowanie zabezpieczenia od martwej strefy w polu.

SEL | Dialogi techniczne (kontakt mailowy + wymiana mailowa z dedykowanym inżynierem + dokumentacja).
Rekomendacja | Sugestia rozwiązania problemu przez zastosowanie zabezpieczenia do detekcji wtórnych zapłonów w wyłączniku.

SIEMENS | Dialogi techniczne (kontakt mailowy + wymiana mailowa z dedykowanym zespołem + dokumentacja).
Rekomendacja | Sugestia rozwiązania problemu przez zastosowanie zabezpieczenia do detekcji wtórnych zapłonów w wyłączniku.

ZPAE | Dialogi techniczne (kontakt mailowy + wymiana mailowa + wizyta studialna).
Rekomendacja | Sugestia rozwiązania problemu przez zastosowanie *niskiej* nastawy kryterium prądowego dla wariantu *OR* LRW.

PSE Innowacje Nowe rozwiązanie LRW dla stacji z dławikiem 14

Nowe rozwiązanie LRW dla stacji z dławikiem Koncepcje rozwiązania

KONCEPCJE ZDEFINIOWANIE W PRACY

- KONCEPCJA 1 | *niska* nastawa kryterium prądowego LRW
- KONCEPCJA 2 | KONCEPCJA 1 + zdezaktywowanie kryterium wyłącznikowego dla wyłączeń operatywnych
- KONCEPCJA 3 | KONCEPCJA 1 + KONCEPCJA 2 + dodatkowe pobudzenie LRW dla wyłączeń operatywnych
- KONCEPCJA 4 | *niska* nastawa kryterium prądowego LRW ← równoważne koncepcji 1
- KONCEPCJA 5 | KONCEPCJA 5 + dodatkowe pobudzenie LRW dla wyłączeń operatywnych ← równoważne koncepcji 4
- KONCEPCJA 6 | KONCEPCJA 5 + pobudzenie LRW przez *niestandardowe* zabezpieczenia

WARIANTY |
a* – rozszerzenie zestawu sygnałów pobudzających LRW o sygnał zadziałania II stopnia zabezpieczenia ziemnozwarciowego zerowoprądowego w polu dławika (3I0 II)
b – rozszerzenie zestawu sygnałów pobudzających LRW o sygnał zadziałania I stopnia zabezpieczenia od asymetrii w polu dławika (I2 I)
c – rozszerzenie zestawu sygnałów pobudzających LRW o sygnał zadziałania zabezpieczenia do detekcji wtórnych zapłonów w wyłączniku (50RS)

- KONCEPCJA 7 | implementacja w LRW funkcji detekcji wtórnych zapłonów + dodatkowe pobudzenie LRW dla wyłączeń operatywnych;
- KONCEPCJA 8 | dedykowane zabezpieczenie do detekcji wtórnych zapłonów.
- KONCEPCJA 9 | KONCEPCJA 1 + połączenie zmodyfikowanych KONCEPCJI 2 i 6c

wariant AND LRW | wariant OR LRW | > LRW

* Zestaw pobudzeń LRW zgodny ze standardem PSE-ST.OW.NN.WN/2021 obowiązującym od sierpnia 2021 r.

Nowe rozwiązanie LRW dla stacji z dławikiem Koncepcje rozwiązania Wyniki wstępnej oceny eksperckiej

Kryteria oceny	Koncepcja nowego rozwiązania LRW 1	2	3	4	5	6	7	8
Zgodność z dotychczasową ideą LRW	znaczna	znaczna	średnia	znaczna	średnia	znaczna	niewielka	nie dotyczy
Zakres zmian w urządzeniu LRW	nie dotyczy	średni	średni	nie dotyczy	średni	niewielki	duży	nie dotyczy
Rekomendacja Producentów	brak	brak	brak	tak	brak	tak	tak	tak
Zakres zmian w obwodach wtórnych *ocena szacunkowa*	nie dotyczy	średni	duży	nie dotyczy	średni	duży	średni	duży
Zakres zmiany praktyki nastawiania LRW	niewielki	niewielki	średni	niewielka	średni	średni	duży	nie dotyczy
Skuteczność LRW podczas wtórnych zapł. *ocena ekspercka*	zerowa	niewielka	wysoka	niewielka	wysoka	wysoka	wysoka	wysoka
Wiarygodność decyzji LRW *ocena ekspercka*	nie dotyczy	średnia	niewielka	średnia	niewielka	wysoka	średnia	wysoka
Rekomendacja analiz szczegółowych koncepcji	NIE	NIE	NIE	TAK	NIE	TAK	NIE	TAK

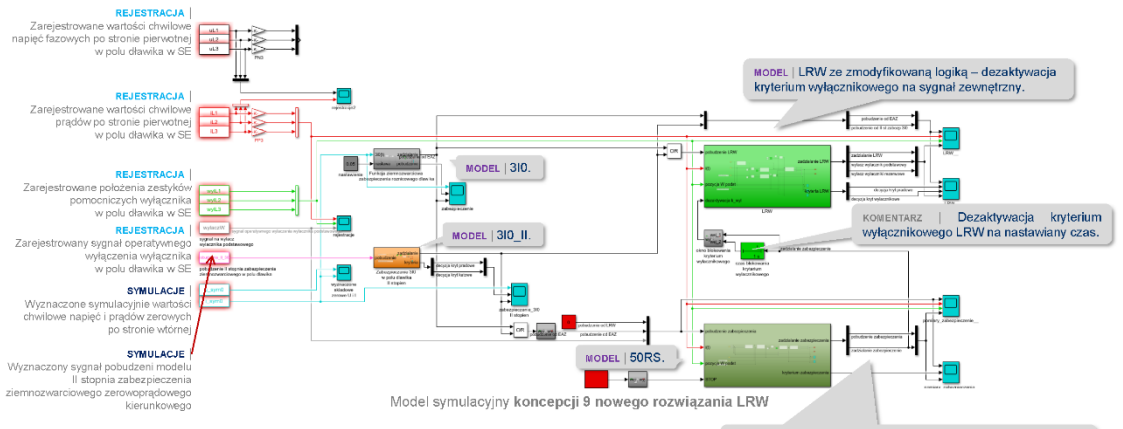
Perspektywa standardów/definicji | Perspektywa rynkowa | Perspektywa aplikacyjna | Perspektywa operacyjna

Nowe rozwiązanie LRW dla stacji z dławikiem Koncepcje rozwiązania Ocena symulacyjna

- Modele stanowiące „cyfrowego bliźniaka” cyfrowych układów EAZ.
- Dokładne odwzorowanie toru przetwarzania sygnałów, algorytmów wyznaczania wielkości kryterialnych i algorytmów decyzyjnych EAZ.
- Modele realizowane w programie MATLAB, z wykorzystaniem funkcji przeznaczonych do modelowania i symulacji układów ciągłych i dyskretnych.
- Użycie funkcji programu MATLAB umożliwiających wykonanie analiz EMT stanów przejściowych.
- Przygotowanie modeli do wczytywania sygnałów rzeczywistych przebiegów (zapisanych w plikach COMTRADE) zarejestrowanych w stacjach PSE S.A. podczas operatywnych łączeń wyłączników dławikowych, w tym zdarzeń z wtórnymi zapłonami, na potrzeby weryfikacji poprawności działania rozpatrywanych koncepcji nowego rozwiązania LRW (EAZ).

PSE Innowacje Nowe rozwiązanie LRW dla stacji z dławikiem 17

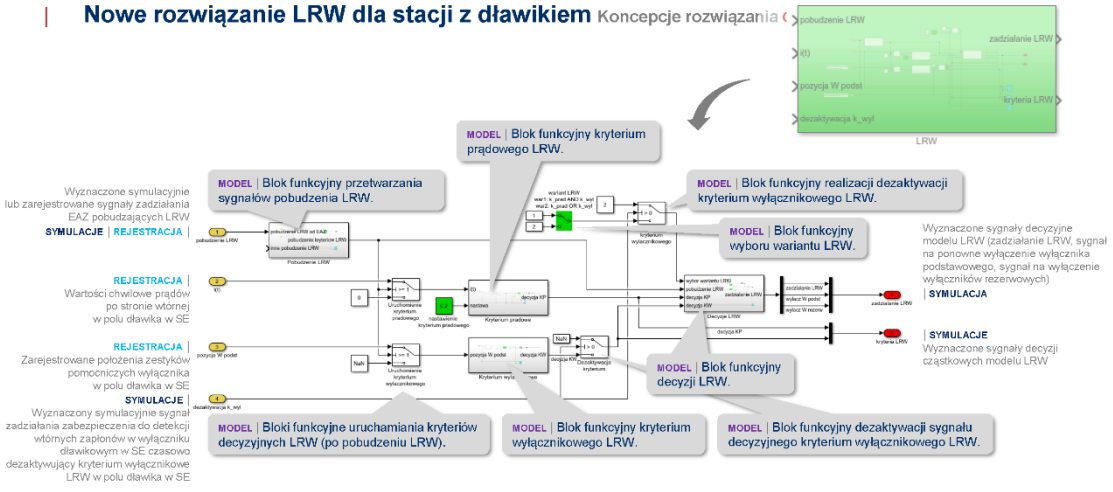
Nowe rozwiązanie LRW dla stacji z dławikiem Koncepcje rozwiązania Ocena symulacyjna



Model symulacyjny **koncepcji 9 nowego rozwiązania LRW**

PSE Innowacje Nowe rozwiązanie LRW dla stacji z dławikiem 18

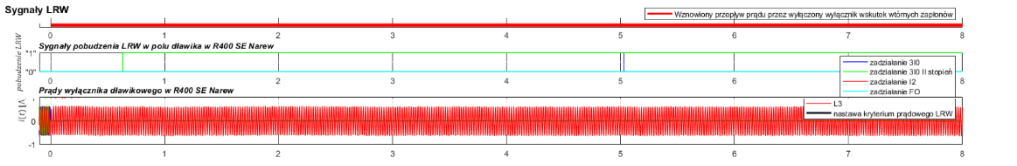
Nowe rozwiązanie LRW dla stacji z dławikiem Koncepcje rozwiązania



Model symulacyjny **LRW** (główny tor przetwarzania sygnałów) (dla koncepcji 9)

Nowe rozwiązanie LRW dla stacji z dławikiem Koncepcje rozwiązania Ocena symulacyjna

STUDIUM PRZYPADKU – ANALIZA WARUNKÓW WYSTĘPUJĄCYCH PODCZAS AWARII W POLU DŁAWIKA 400 kV

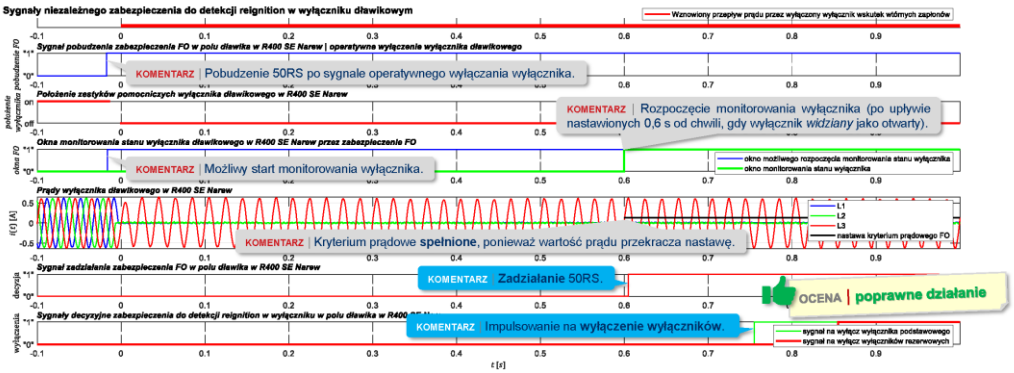


Ilustracja przebiegu czasowego działania ***starego*** **rozwiązania LRW**

Ilustracja przebiegu czasowego działania **rekomendowanego nowego rozwiązania LRW**

Nowe rozwiązanie LRW dla stacji z dławikiem Koncepcje rozwiązania Ocena pomiarowa

STUDIUM PRZYPADKU – ANALIZA WARUNKÓW WYSTĘPUJĄCYCH PODCZAS AWARII W POLU DŁAWIKA 400 kV



Ilustracja przebiegu czasowego działania elementu **alternatywnego nowego rozwiązania LRW**

Nowe rozwiązanie LRW dla stacji z dławikiem Koncepcje rozwiązania Wyniki oceny generalnej

Kryteria oceny		Koncepcja nowego rozwiązania LRW 4	6a	6b	6c	8	9
Zakres zmian projekt. w obw. wtórnych *ocena szczegółowa*		brak	niewielki	niewielki	średni	znaczny	znaczny
Poziom zaangażowania w instalację *ocena szczegółowa*		standardowy	standardowy	standardowy	znaczny	bardzo znaczny	znaczny
Czas zadziałania *ocena symulacyjna*		długi	krótki	krótki	krótki	krótki	krótki
Poprawność działania *ocena symulacyjna*	Operatywne wyłączenia z wielokrotnymi wtór. zapłonami	średnia	wysoka	wysoka	wysoka	wysoka	wysoka
	Operatywne wyłączenia z pojedynczymi wtór. zapłonami	wysoka	wysoka	średnia	wysoka	wysoka	wysoka
	Operatywne wyłączenia bez wtórnych zapłonów	wysoka	wysoka	średnia	wysoka	wysoka	wysoka
Ryzyko nieuzasadnionego zadziałania *ocena ekspercka*		nieznacznie wyższe	nieznacznie wyższe	wyższe	nieznacznie wyższe	nieznacznie wyższe	standardowe
Ryzyko nieuzasadnionego niezadziałania *ocena ekspercka*		niższe	niższe	niższe	niższe	wyższe	wyższe
Ryzyko nieuzasadnionego zadziałania podczas testowania EAZ *ocena ekspercka*		wysokie	wysokie	wysokie	wysokie	niskie	niskie
Zestaw koncepcji do aplikacji		NIE	TAK	NIE	NIE	NIE	TAK

PSE FZ

FZ | Firma Zewnętrzna.

Nowe rozwiązanie LRW dla stacji z dławikiem Rozwiązanie rekomendowane

6a KONCEPCJA 6a

KOMENTARZ | Ścieżka ewolucji, nie rewolucji!

wariant LRW — **OR**

Logika OR algorytmu działania LRW | Wtórne zapłony występują jedynie w otwierającym się wyłączniku – wówczas kryterium wyłącznikowe LRW nie może być spełnione, ponieważ wyłącznik jest *widziany* jako otwarty – zatem ewentualną decyzję o zadziałaniu LRW należy podejmować wyłącznie na podstawie decyzji kryterium prądowego LRW.

W PSE S.A. od dawna... Praktycznie wszystkie LRW zainstalowane w polach dławików są skonfigurowane w wariancie OR.

pobudzenie LRW — **3I0 *niska***

Funkcja zabezpieczenia zerowoprądowego w polu dławika o *niskiej* nastawie prądowej i czasowej | Wtórne zapłony wywołują wznowienie przepływu prądu przez operatywnie wyłączany wyłącznik – takie wznowienie przepływu prądu można szybko wykryć, kontrolując składową zerową prądu – zadziałanie zabezpieczenia zapewni oczekiwane pobudzenie LRW.

Niedawny wymóg... Wymóg stosowania przedmiotowych funkcji w polach dławików wprowadzony standardem PSE-ST.OW.NN.WN/2021.

UWAGA | Dwie powyższe cechy LRW – już stosowane w PSE S.A. – jeszcze nie zapewniają oczekiwanego zadziałania LRW w sytuacji zaistnienia wtórnych zapłonów podczas operatywnego wyłączania wyłącznika dławikowego. **Kluczowe jest wdrożenie trzeciej cechy** rekomendowanego rozwiązania LRW.

nastawa kryterium prądowego LRW — ***niska***

Nastawa kryterium prądowego LRW poniżej prądu znamionowego dławika | Podczas wtórnych zapłonów przez operatywnie wyłączany wyłącznik płynie prąd nieprzekraczający prądu znamionowego dławika, zatem obniżenie nastawy kryterium prądowego rozszerzy zakres prądowy „widziany” przez LRW, co umożliwi detekcję przepływu tego *małego* prądu i **oczekiwane zadziałanie LRW**.

Nowy wymóg!!! Dotychczas LRW w polach dławików w stacjach PSE S.A. nastawiano *wysoko* (dla innych zakłóceń taka nastawa jest wystarczająca, czego dowodzi praktyka) – **istotna zmiana dotychczasowej praktyki nastawiania LRW**.

Nowe rozwiązanie LRW dla stacji z dławikiem Rozwiązanie rekomendowane

***Niska* nastawa kryterium prądowego LRW**

SUGEROWANE PODEJŚCIE DO WYZNACZANIA *NISKIEJ* NASTAWY KRYTERIUM PRĄDOWEGO LRW | *Niska* nastawa wartości rozruchowej *Iroz* kryterium prądowego 50BF powinna zawierać się w przedziale: $Imin \le Iroz < Id$, gdzie *Imin* – wartość minimalna *Iroz* wymagana Standardem PSE-ST.EAZ.NN.WN/2021, *Id* – prąd znamionowy dławika.

KOMENTARZ | Dla dławika regulowanego jako *Id* należy przyjąć wartość prądu roboczego dławika dla minimalnego zaczepu.

GÓRNA GRANICA PRZEDZIAŁU WARTOŚCI *NISKIEJ* NASTAWY *Iroz* | CIGRE zaleca ustawianie *Iroz* na poziomie nieprzekraczającym **0,9·*Id***.
Jest to podyktowane koniecznością uwzględnienia zależności prądu roboczego dławika od wartości napięcia zasilania. Tym samym w sytuacji obniżenia napięcia w miejscu przyłączenia dławika wartość prądu płynącego przez nieskutecznie operatywnie wyłączony wyłącznik dławikowy może być niższa niż *Id*, co wpływa na warunki działania kryterium prądowego LRW. Podstawą szacowania rekomendowanej górnej granicy nastawiania *Iroz* jest założenie, że ruchowo wartość napięcia w stacji z dławikiem będzie nie niższa niż 0,95 napięcia znamionowego. Jeśli dopuszcza się większe odchylenie w dół napięcia, wówczas należy także obniżyć górną granicę nastawy, proporcjonalnie do kwadratu ilorazu napięcia spodziewanego i napięcia znamionowego (przykładowo, dla napięcia spodziewanego na poziomie 0,9 napięcia znamionowego – górna granica przedziału *niskiej* nastawy *Iroz* wynosi $(0,9)^2 \cdot Id \approx 0,8 \cdot Id$).

SUGEROWANA *NISKA* NASTAWA *Iroz* | **0,3·*Id*** – rekomendacja eksploatacyjna ABB

UWAGA | Zastosowanie *niskiej* nastawy kryterium prądowego LRW wymaga potwierdzenia braku lub pomijalnego ryzyka nasycenia rdzeni przekładników prądowych współpracujących z LRW w sytuacji silnych zwarć poza dławikiem – nasycenie przekładników powoduje, że po wyłączeniu wyłącznika podstawowego ewentualny prąd rozładowania obwodu wtórnego z przekładnikiem, „widziany” przez LRW, może przekraczać *niską* nastawę, co implikuje ryzyko nieuzasadnionego zadziałania LRW. W toku weryfikacji parametrów przekładników prądowych należy uwzględnić spodziewane maksymalne warunki zwarciowe w miejscu instalacji tych przekładników oraz ich rzeczywiste obciążenie. Najlepiej, gdyby weryfikacja objęła również przekładniki prądowe współpracujące z EAZ pobudzającymi LRW, aby wykluczyć ryzyko zbędnego zadziałania tych EAZ i zmitygować ryzyko zbędnego pobudzenia LRW w rozpatrywanej sytuacji nasycenia przekładników.

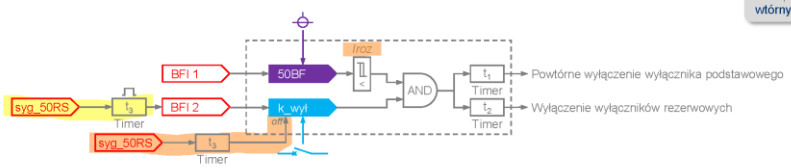
Nowe rozwiązanie LRW dla stacji z dławikiem Rozwiązanie alternatywne

KONCEPCJA 9

KOMENTARZ | **Ścieżka rewolucji!**

IDEA WYKORZYSTANIA FUNKCJI 50RS W KONCEPCJI NOWEGO ROZWIĄZANIA | Dla stacji PSE S.A. z LRW skonfigurowanym w **wariancie *AND*** (do zadziałania LRW niezbędne jest koincydencyjne spełnienie 50BF i k_wył), w których nie ma możliwości zmiany konfiguracji na **wariant *OR*** (do zadziałania LRW wystarczy spełnienie 50BF lub k_wył) rekomenduje się aplikację koncepcji 9 (*niska* nastawa 50BF, czasowa dezaktywacja lub czasowe spełnianie k_wył po odebraniu sygnału zadziałania zabezpieczenia 50RS syg_50RS).

50RS | Funkcja zabezpieczenia do detekcji wtórnych zapłonów w wyłącznikach.



Schemat ideowy alternatywnego rozwiązania LRW z zaznaczonym zakresem zmiany

04

Podsumowanie

Story | Najważniejsze osiągnięcia

PSE Innowacje

Podsumowanie *Story*

BYŁO

Eksplozja w polu dławika 400 kV

Eksplozja operatywnie wyłączanego wyłącznika dławikowego wskutek długotrwałego *łukowego* przepływu prądu przez otwarty wyłącznik w następstwie wtórnych zapłonów.

MOŻE BYĆ

Wyłączenie rezerwowe w polu dławika 400 kV

Detekcja nieskutecznego operatywnego wyłączenia wyłącznika dławikowego przez LRW oraz wyłączenie wyłączników rezerwowych.

DIAGNOZA

- Operatywnemu wyłączeniu wyłącznika dławikowego mogą towarzyszyć **wtórne zapłony**, których następstwem jest wznowienie przepływu prądu w wyłączanym wyłączniku, poprzez łuk między otwartymi stykami wyłącznika.
- Zwykle przerwanie *łukowego* przepływu prądu następuje *naturalnie* w chwili kolejnego przejścia sinusoidy wartości chwilowej prądu przez zero → zgodnie z praktyką i wymaganiami producentów po **zapłonach pojedynczych** możliwa jest dalsza eksploatacja wyłącznika.
- W rzadkich przypadkach wtórne zapłony przyjmują postać **zapłonów wielokrotnych** prowadzących do trwałej utraty zdolności wyłącznika do przerwania przepływu prądu → powinno to prowadzić do **wyłączenia wyłączników rezerwowych**.
- **Dotychczasowe rozwiązanie LRW nie gwarantuje oczekiwanego rezerwowania nieskutecznie operatywnie wyłączonych wyłączników dławikowych** → zakłócenie *nie*-zwarciowe wykraczające poza standardowy zestaw zadziałań LRW.
- W skrajnie niekorzystnym przypadku brak rezerwowego przerwania przepływu prądu może prowadzić do **eksplozji wyłącznika**.
- Opracowane **rekomendowane rozwiązanie LRW zapewni oczekiwane *pełne* rezerwowanie wyłączników dławikowych**.

Podsumowanie Wybrane osiągnięcia

Beneficjenci

ROZWIĄZANIE EAZ

Opracowanie rozwiązania LRW dedykowanego dla pól dławikowych

KORZYŚCI

- Minimalizacja ryzyk ludzkich i infrastrukturalnych wywołanych nieskutecznym operatywnym wyłączeniem wyłącznika dławikowego w niestandardowej sytuacji wielokrotnych wtórnych zapłonów prowadzących do trwałej utraty zdolności wyłącznika do przerwania przepływu prądu.
- Mitygacja ryzyka wystąpienia w przyszłości niepożądanego zdarzenia zaistniałego w polu dławika 400 kV – eksplozja wyłącznika.

WYTYCZNE EKSPLOATACYJNE

Opracowanie metodyki wyznaczania *niskiej* nastawy LRW dla pól dławikowych

KORZYŚĆ

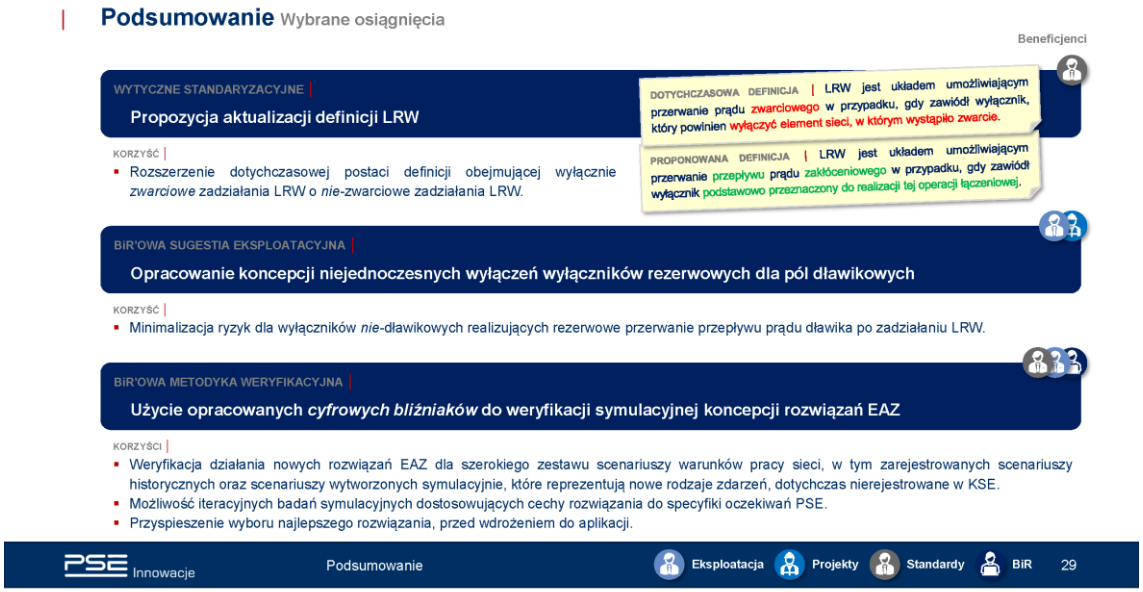
- Wsparcie wdrożenia opracowanego rozwiązania LRW dla pól dławikowych, poprzez ułatwienie doboru parametrów nastawczych LRW.

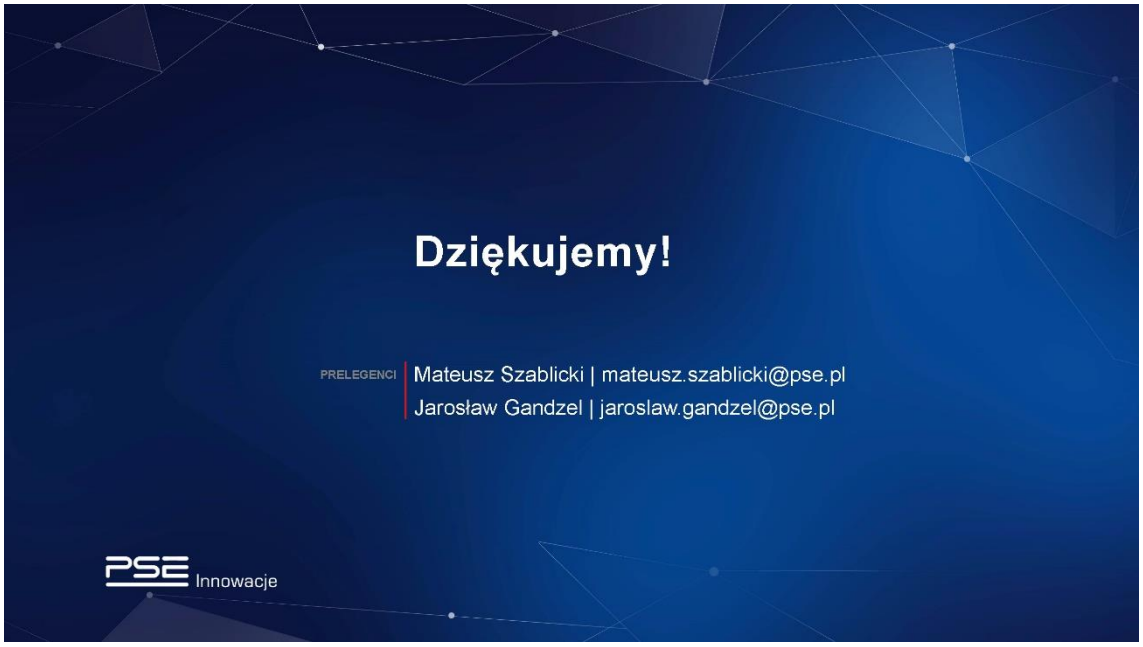
WYTYCZNE EKSPLOATACYJNE I PROJEKTOWE

Opracowanie ścieżki aplikacji rekomendowanego rozwiązania LRW

KORZYŚĆ

- Wsparcie wdrożenia opracowanego rozwiązania LRW dla pól dławikowych, poprzez zdefiniowanie kroków cząstkowych aplikacji rozwiązania.


Podsumowanie Wybrane osiągnięcia
Beneficjenci
WYTYCZNE STANDARYZACYJNE
Propozycja aktualizacji definicji LRW
DOTYCHCZASOWA DEFINICJA | LRW jest układem umożliwiającym przerwanie prądu zwarciowego w przypadku, gdy zawiódł wyłącznik, który powinien wyłączyć element sieci, w którym wystąpiło zwarcie.
PROPONOWANA DEFINICJA | LRW jest układem umożliwiającym przerwanie przepływu prądu zakłóceniowego w przypadku, gdy zawiódł wyłącznik podstawowo przeznaczony do realizacji tej operacji łączeniowej.
KORZYŚĆ
Rozszerzenie dotychczasowej postaci definicji obejmującej wyłącznie zwarciowe zadziałania LRW o nie-zwarciowe zadziałania LRW.
BiR'OWA SUGESTIA EKSPLOATACYJNA
Opracowanie koncepcji niejednoczesnych wyłączeń wyłączników rezerwowych dla pól dławikowych
KORZYŚĆ
Minimalizacja ryzyk dla wyłączników nie-dławikowych realizujących rezerwowe przerwanie przepływu prądu dławika po zadziałaniu LRW.
BiR'OWA METODYKA WERYFIKACYJNA
Użycie opracowanych cyfrowych bliźniaków do weryfikacji symulacyjnej koncepcji rozwiązań EAZ
KORZYŚCI
Weryfikacja działania nowych rozwiązań EAZ dla szerokiego zestawu scenariuszy warunków pracy sieci, w tym zarejestrowanych scenariuszy historycznych oraz scenariuszy wytworzonych symulacyjnie, które reprezentują nowe rodzaje zdarzeń, dotychczas nierejestrowane w KSE.
Możliwość iteracyjnych badań symulacyjnych dostosowujących cechy rozwiązania do specyfiki oczekiwań PSE.
Przyspieszenie wyboru najlepszego rozwiązania, przed wdrożeniem do aplikacji.
PSE Innowacje
Podsumowanie
Eksploatacja
Projekty
Standardy
BiR
29


Dziękujemy!
PRELEGENCI
Mateusz Szablicki | mateusz.szablicki@pse.pl
Jarosław Gandzel | jaroslaw.gandzel@pse.pl
PSE Innowacje

IDEA GRID FORMING CAPABILITY

Piotr Rzepka, Mateusz Szablicki (PSE)

GFC – *discovery* z perspektywy OSP | motywacje

Tło inicjatywy BiR

dziś

Rozwój SEE
Rosnące nasycenie SEE układami energoelektronicznymi w rozproszonych i wielkoskalowych obiektach elektroenergetycznych.

Wyzwanie dla operatorów
Utrzymanie stabilnej pracy SEE przy malejącym ilościowo i jakościowo zestawie dotychczas stosowanych środków regulacyjnych.

Ryzyko *systemowe*
Wzrost dynamiki stanów przejściowych i skrócenie dopuszczalnego czasu reakcji wskutek malejącej *naturalnej* inercji SEE.

Możliwe rozwiązanie
Wdrożenie GFC jako zdolności technicznej oczekiwanej od obiektów elektroenergetycznych z układami energoelektronicznymi.

Wyzwania dla PSE dt. GFC
Określenie zdolności technicznych klasyfikowanych jako GFC.
Wypracowanie jednolitego podejścia/standardu dla GFC w ENTSO-E.
Określenie krajowych wymagań dla GFC (jakościowe i ilościowe).

Motywacje *systemowe* potrzeby wdrożenia GFC

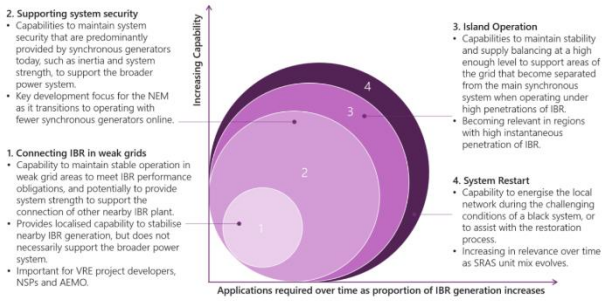
BYŁO | SEE *klasyczny*
Oczekiwane zachowanie OZE | **wyłączenie podczas zakłóceń w SEE**
Przełożenie na legislację | **nie dotyczy**

JEST | SEE *przejściowy*
Oczekiwane zachowanie OZE | ***Grid Following Converter***
Układy energoelektroniczne *nadążają* za sytuacją w SEE.
Przełożenie na legislację | **IRIESP** (m.in. funkcja przejścia przez zwarcie); **Kodeksy Sieci** (m.in. wymóg udziału w generacji prądu zwarciowego, wymóg inercji *syntetycznej*)

BĘDZIE | SEE *nasycony IBR*
Oczekiwane zachowanie obiektów z energoelektronicznych | ***Grid Forming Converter***
Układy energoelektroniczne (IBR) *kształtują* sytuację w SEE.
Przełożenie na legislację | **??**
GFC ma być zdefiniowane w aktualizowanych Kodeksach Sieci i objąć **moduły parku energii**, **systemy HVDC** i **magazyny energii**.

GFC | uzasadnienie idei

Zdolności techniczne wymagane od zasobów bazujących na przekształtnikach



Źródło: Application of Advanced Grid-scale Inverters in the NEM Agust 2021. White Paper An Engineering Framework report on design capabilities needed for the future National Electricity Market

Docelowo te usługi powinny być dostarczane przez urządzenia z GFC

GFC | uzasadnienie idei

Zjawiska warunkujące stabilność przyszłych SEE

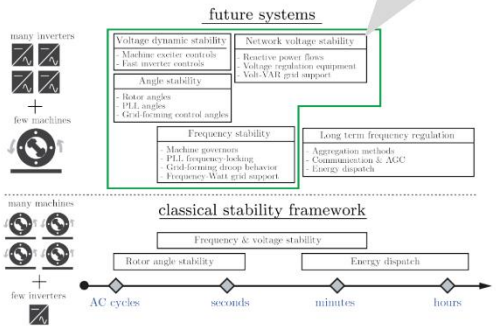
Potrzeby przyszłego SEE

Capability	Description	Purpose
System strength[A]	The ability to generate, maintain, and control the voltage waveform.	Support maintaining network synchronism during steady state operation, disturbances, and recovery after disturbances and supply enough fault current to ensure correct operation of network protection systems.
Disturbance withstand	Defined responses and ability to maintain stable operation during voltage, frequency, phase disturbances (fault ride-through), and to damp active power oscillations after a disturbance.	Maintain supply resources operating during and following a disturbance, to support power system recovery and stabilisation.
Inertia[C]	Instantaneous and inherent active power response, not dependant on measurement, to rapid changes in frequency.	Impede the system's rate of change of frequency (RoCoF) as a response to frequency disturbances.
Primary frequency response[C]	Locally controlled active power response to frequency change. Can include Fast Frequency Response (FFR)[B].	Maintain the network within a tight frequency band, manage intra-dispatch supply and demand variations, and arrest changes in power system frequency. In some cases, FFR can reduce system inertia requirements.
Support power system island	Manage active power output to support island operation over dispatch timescale.	Provide sufficient energy resources (dispatchability, ramp rate, and secondary frequency response) to maintain supply-demand balance within island boundaries.
Initiate or support system restoration	Bring plant online during system restoration process, including provision of necessary surge current and capability to remain online under adverse conditions.	Provision of SRAS during black start.

Źródło: Application of Advanced Grid-scale Inverters in the NEM Agust 2021. White Paper An Engineering Framework report on design capabilities needed for the future National Electricity Market

Kwestie warunkujące stabilność SEE

Kluczowe zdolności techniczne, które powinno obejmować GFC



Źródło: Research Roadmap on Grid-Forming Inverters. November 2020. Yashen Lin,1 Joseph H. Eto,2 Brian B. Johnson,3 Jack D. Flicker,4 Robert H. Lasseter,5 Hugo N. Villegas Pico,1 Gab-Su Seo,1 Brian J. Pierre,4 and Abraham Ellis4

Definicje

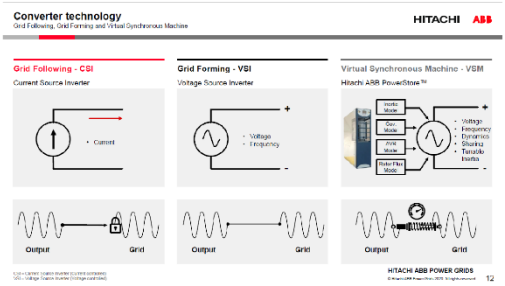
| Grid-following vs Grid-forming

PSE Innowacje

| GFC – *discovery* z perspektywy OSP | **czym jest GFC**

Technologie wysterowania przekształtników

Grid-following vs ***Grid-forming*** vs ***Virtual synchronous machine***



Definicje

Terminologia dotycząca GFC nie jest wpełni ustandaryzowana i zdefiniowana. Definicje przyjęte na potrzeby niniejszej prezentacji

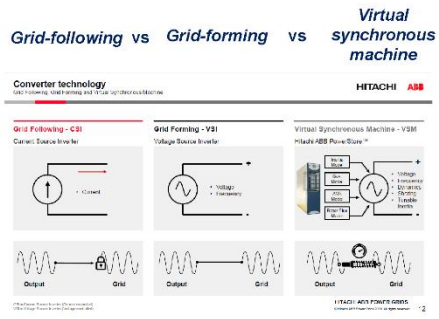
Definitons:

- **Grid-following inverters** synchronise to the grid voltage waveform, adjusting their output to track an external voltage reference.
- **Grid-forming inverters** set their own internal voltage waveform reference and can synchronise with the grid or operate independently of other generation

| GFC – *discovery* z perspektywy OSP | **czym jest GFC**

Technologie przekształtników

Grid-following vs ***Grid-forming*** vs ***Virtual synchronous machine***



Cechy *Grid-following* vs *Grid-forming*

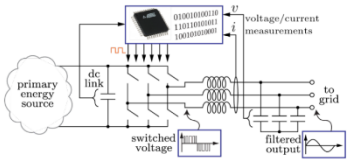
	Grid-Following	Grid-Forming
Functionality	Follow the grid voltage and frequency	Actively controls its voltage output and frequency
Mode of operation	Grid connected mode	Islanded and grid-connected mode
Stability	Vulnerable to grid disruptions and prone to tripping offline during faults	Robust and provide stability during grid faults

GFC | uzasadnienie idei

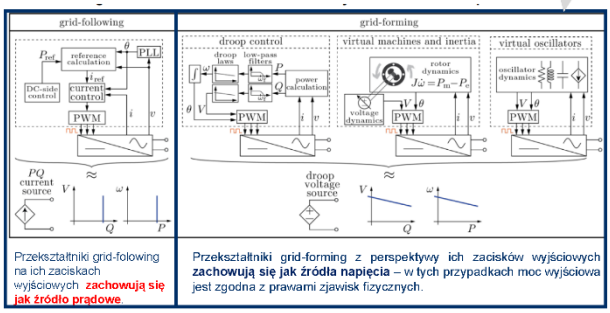
Strury przekształtników grid-following vs grid-forming

Struktura układu z grid-forming jest znacznie bardziej rozbudowana

Generalna struktura przekształtnika z closed-loop control



Schematy funkcjonalne przekształtników grid-followin oraz grid-forming



Przekształtniki grid-folowing na ich zaciskach wyjściowych **zachowują się jak źródło prądowe**

Przekształtniki grid-forming z perspektywy ich zacisków wyjściowych **zachowują się jak źródła napięcia** – w tych przypadkach moc wyjściowa jest zgodna z prawami zjawisk fizycznych.

Źródło: Research Roadmap on Grid-Forming Inverters. November 2020. Yashen Lin,1 Joseph H. Eto,2 Brian B. Johnson,3 Jack D. Flicker,4 Robert H. Lasseter,5 Hugo N. Villegas Pico,1 Gab-Su Seo,1 Brian J. Pierre,4 and Abraham Ellis4

Discovery

| Podejście do tematyki na świecie

PSE Innowacje

GFC – *discovery* z perspektywy OSP | postrzeganie GFC przez innych

GFC | aplikacje praktyczne

Podejście ENTSO-E

Tylko 3 strony treści !!!

Oczekiwana funkcjonalność GFC

- Creating (forming) system voltage.
- Contributing to fault level (short circuit power).
- Contributing to total system inertia (limited by energy storage capacity and the available power rating of the PPM or HVDC converter station).
- Supporting system survival to enable the effective operation of low frequency demand disconnection for rare system splits.
- Acting as a sink to counter harmonics and inter-harmonics in system voltage.
- Acting as a sink to counter any unbalance in system voltage.
- Preventing adverse control system interactions.

Źródło: Grid-Forming Capabilities: Towards System Level Integration 31 March 2021

Podejście brytyjskiego OSP

| National Grid ESO

PSE Innowacje

GFC | Podejście brytyjskiego operatora NG ESO

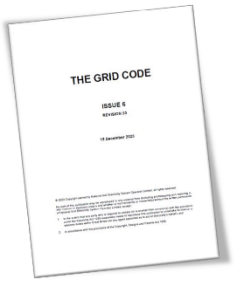
Podejście TSO do GFC

GC0137 Minimum Specifiaction Required for Provision of GB Grid Forming (GBGF) Capability (formerly Virtual Synchronou Machine/VSM Capability

Harmonogram prac NG-ESO GBGF

- 10 grudzień 2019 - Rozpoczęcie prac– pierwsza propozycja
- 14 luty 2022 - Zaimplementowane w Grid Code poprawki GC0137
- Kwiecień 2023 – Publikacja Great Britain Grid Forming
- Prace w toku – pogłębione rozpoznania GFC

NG-ESO - wymagania



THE GRID CODE (nationalgrideso.com)

NG-ESO - Najlepsze praktyki

Great Britain Grid Forming Best Practice Guide (nationalgrideso.com)

Najbardziej zaawansowane wymagania

PSE Innowacje PTPiRE | Idea Grid Forming Capability (GFC) 14

GFC | Podejście brytyjskiego operatora NG ESO

Podejście TSO do GFC

GC0137 Minimum Specifiaction Required for Provision of GB Grid Forming (GBGF) Capability (formerly Virtual Synchronou Machine/VSM Capability

Harmonogram prac NG-ESO GBGF

- 10 grudzień 2019 - Rozpoczęcie prac– pierwsza propozycja
- 14 luty 2022 - Zaimplementowane w Grid Code poprawki GC0137
- Kwiecień 2023 – Publikacja Great Britain Grid Forming
- Prace w toku – pogłębione rozpoznania GFC

nationalgridESO

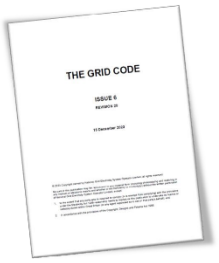
Final Modification Report GC0137
Published on 11 November 2021

Contents

GFC | Podejście brytyjskiego operatora NG ESO

Podstawowe definicje dt. GFC zawarte w The Grid Code

NG-ESO – Grid Code



THE GRID CODE (nationalgrideso.com)

Grid Forming Capability is (but not limited to) the capability a

- Power Generating Module,
- HVDC Converter (which could form part of an HVDC System),
- Generating Unit, Power Park Module,
- DC Converter,
- OTSDUW Plant and Apparatus,
- Electricity Storage Module,
- Dynamic Reactive Compensation Equipment
- or any Plant and Apparatus (including a smart load)

whose supplied Active Power is directly proportional to the difference between the magnitude and phase of its Internal Voltage Source and the magnitude and phase of the voltage at the Grid Entry Point or User System Entry Point and the sine of the Load Angle.

As a consequence, Plant and Apparatus which has a Grid Forming Capability has a frequency of rotation of the Internal Voltage Source which is the same as the System Frequency for normal operation, with only the Load Angle defining the relative position between the two.

In the case of a GBGF-I, a Grid Forming Unit forming part of a GBGF-I shall be capable of sustaining a voltage at its terminals irrespective of the voltage at the Grid Entry Point or User System Entry Point for normal operating conditions.

For GBGF-I, the control system, which determines the amplitude and phase of the Internal Voltage Source, shall have a response to the voltage and System Frequency at the Grid Entry Point or User System Entry Point) with a bandwidth that is less than a defined value as shown by the control system's NFP Plot.

Exceptions to this requirement are only allowed during transients caused by System faults, voltage dips/surges and/or step or ramp changes in the phase angle which are large enough to cause damage to the Grid Forming Plant via excessive currents.

OTSDUW - Offshore Transmission System Development User Works
In relation to a particular User where the OTSDUW Arrangements apply, means those activities and/or works for the design, planning, consenting and/or construction and installation of the Offshore Transmission System to be undertaken by the User as identified in Part 2 of Appendix I of the relevant Construction Agreement.

Jako GF może również świadczyć

- odbiór indywidualny

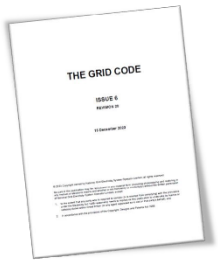
Wprowadzone dokumentem GC0137: "Minimum specification Required for provision of GB Grid Forming (GBGF) Capability (formerly Virtualn Synchronous Machine/VSM Capability)"

Wprowadzone dokumentem GC0137: "Minimum specification Required for provision of GB Grid Forming (GBGF) Capability (formerly Virtualn Synchronous Machine/VSM Capability)"

GFC | Podejście brytyjskiego operatora NG ESO

Podstawowe definicje dt. GFC zawarte w The Grid Code

NG-ESO – Grid Code



- **Grid Forming Plant**
  A site which contains Plant and Apparatus which is classified as either a GBGF-S or a GBGF-I
- **GB Grid Forming - Inverter or GBGF-I**
  Is any Power Park Module, HVDC System, DC Converter, OTSDUW Plant and Apparatus, Non-Synchronous Electricity Storage Module, Dynamic Reactive Compensation Equipment or any Plant and Apparatus (including a smart load) which is connected or partly connected to the Total System via an Electronic Power Converter which has a Grid Forming Capability (GBGF-I).
- **GB Grid Forming – Synchronous or GBGF-S**
  Is a Synchronous Power Generating Module, Synchronous Electricity Storage Module or Synchronous Generating Unit with a Grid Forming Capability.
- **Grid Forming Plant Owner**
  The owner or operator of a Grid Forming Plant
- **Grid Forming Unit**
  A Power Park Unit or Electricity Storage Unit or a Synchronous Power Generating Unit or Individual Load with a Grid Forming Capability.
- **Grid Forming Electronic Power Converter**
  A Grid Forming Plant whose output is derived from an Electronic Power Converter with a GBGF-I capability.
- **Internal Voltage Source**
  For a Grid Forming Synchronous Generating Unit a real magnetic field, that rotates synchronously with the System Frequency under normal operating conditions, which induces an Internal Voltage Source in the stationary generator winding that has a real impedance. For a Grid Forming Electronic Power Converter it uses switched power electronic devices to produce a real voltage waveform, with harmonics, that has a fundamental component that rotates synchronously with the System Frequency under normal operating conditions to produce the real Internal Voltage Source that is connected to a one or more real impedances.
- **Load Angle**
  The angle in radians between the voltage of the Internal Voltage Source and the voltage at the Grid Entry Point or User System Entry Point.

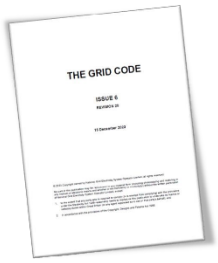
THE GRID CODE (nationalgrideso.com)

Jako GF może również świadczyć
- odbiór indywidualny

GFC | Podejście brytyjskiego operatora NG ESO

Podstawowe definicje dt. GFC zawarte w The Grid Code

NG-ESO – Grid Code



- **Grid Forming Active Power**
  Grid Forming Active Power is the inherent Active Power produced by Grid Forming Plant that includes Active Inertia Power plus Active Phase Jump Power plus Active Damping Power
- **Active Control Based Power**
  The Active Power output supplied by a Grid Forming Plant through controlled means (be it manual or automatic) of the positive phase sequence Root Mean Square Active Power produced at fundamental System Frequency by the control system of a Grid Forming Unit. For GBGF-I, this is equivalent to a Synchronous Generating Unit with a traditional governor coupled to its prime mover. Active Control Based Power includes Active Power changes that results from a change to the Grid Forming Plant Owners available set points that have a 5 Hz limit on the bandwidth of the provided response. Active Control Based Power also includes Active Power components produced by the normal operation of a Grid Forming Plant that comply with the Engineering Recommendation P28 limits. These Active Power components do not have a 5 Hz limit on the bandwidth of the provided response. Active Control Based Power does not include Active Power components proportional to System Frequency, slip or deviation that provide damping power to emulate the natural damping function provided by a real Synchronous Generating Unit.
- **Active Damping Power**
  The Active Power naturally injected or absorbed by a Grid Forming Plant to reduce Active Power oscillations in the Total System. More specifically, Active Damping Power is the damped response of a Grid Forming Plant to an oscillation between the voltage at the Grid Entry Point or User System Entry Point and the voltage of the Internal Voltage Source of the Grid Forming Plant. For the avoidance of doubt, Active Damping Power is an inherent capability of a Grid Forming Plant that starts to respond naturally, within less than 5ms to low frequency oscillations in the System Frequency.
- **Active Inertia Power**
  The injection or absorption of Active Power by a Grid Forming Plant to or from the Total System during a System Frequency change. The transient injection or absorption of Active Power from a Grid Forming Plant to the Total System as a result of the ROCOF value at the Grid Entry Point or User System Entry Point. This requires a sufficient energy storage capacity of the Grid Forming Plant to meet the Grid Forming Capability requirements specified in ECC.6.3.19. For the avoidance of doubt, this includes the rotational inertial energy of the complete drive train of a Synchronous Generating Unit. Active Inertia Power is an inherent capability of a Grid Forming Plant to respond naturally, within less than 5ms, to changes in the System Frequency. For the avoidance of doubt, the Active Inertia Power has a slower frequency response compared with Active Phase Jump Power
- **Active Phase Jump Power**
  The transient injection or absorption of Active Power from a Grid Forming Plant to the Total System as a result of changes in the phase angle between the Internal Voltage Source of the Grid Forming Plant and the Grid Entry Point or User System Entry Point. In the event of a disturbance or fault on the Total System, a Grid Forming Plant will instantaneously (within 5ms) inject or absorb Active Phase Jump Power to the Total System as a result of the phase angle change. For GBGF-I as a minimum value this is up to the Phase Jump Angle Limit Power. Active Phase Jump Power is an inherent capability of a Grid Forming Plant that starts to respond naturally, within less than 5 ms and can have frequency components of over 1000 Hz.
- **Active ROCOF Response Power**
  - The Active Inertia Power developed from a Grid Forming Plant plus the Active Frequency Response Power that can be supplied by a Grid Forming Plant when subject to a rate of change of the System Frequency.

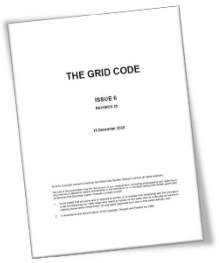
THE GRID CODE (nationalgrideso.com)

Wprowadzone dokumentem GC0137: "Minimum specification Required for provision of GB Grid Forming (GBGF) Capability (formerly Virtualn Synchronous Machine/VSM Capability)"

GFC | Podejście brytyjskiego operatora NG ESO

Podstawowe definicje dt. GFC zawarte w The Grid Code

NG-ESO – Grid Code



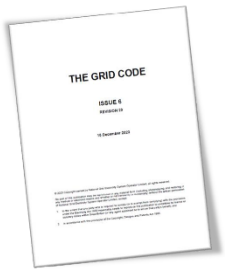
THE GRID CODE
(nationalgrideso.com)

- **Control Based Reactive Power**
  The Reactive Power supplied by a Grid Forming Plant through controlled means based on operator adjustment selectable setpoints (these may be manual or automatic).
- **GBGF Fast Fault Current Injection**
  The ability of a Grid Forming Plant to supply reactive current, that starts to be delivered into the Total System in less than 5ms when the voltage falls below 90% of its nominal value at the Grid Entry Point or User System Entry Point.
- **Voltage Jump Reactive Power**
  The transient Reactive Power injected or absorbed from a Grid Forming Plant to the Total System as a result of either a step or ramp change in the difference between the voltage magnitude and/or phase of the voltage of the Internal Voltage Source of the Grid Forming Plant and Grid Entry Point or User System Entry Point. In the event of a voltage magnitude and phase change at the Grid Entry Point or User System Entry Point, a Grid Forming Plant will instantaneously (within 5ms) supply Voltage Jump Reactive Power to the Total System as a result of the voltage magnitude change.

Wprowadzone dokumentem GC0137: "Minimum specification Required for provision of GB Grid Forming (GBGF) Capability (formerly Virtualn Synchronous Machine/VSM Capability)"

GFC | Podejście brytyjskiego operatora NG ESO

Podstawowe definicje dt. GFC zawarte w The Grid Code



THE GRID CODE
(nationalgrideso.com)

Definicje zmodyfikowane

- **Active Frequency Response Power**
  The injection or absorption of Active Power by a Grid Forming Plant to or from the Total System during a deviation of the System Frequency away from the Target Frequency. For a GBGF-I this is very similar to Primary Response but with a response time to achieve the declared service capability (which could be the Maximum Capacity or Registered Capacity) within 1 second. For GBGF-I this can rapidly inject or absorb Active Power in addition to the phase-based Active Inertia Power to provide a system with desirable NFP plot characteristics. Active Frequency Response Power can be produced by any viable control technology.
- **Active Control Based Droop Power**
  The Active Control Based Power output supplied by a Grid Forming Plant through controlled means (be it manual or automatic). For GBGF-I this is equivalent to a Synchronous Generating Unit with a traditional governor coupled to its prime mover. Active Control Based Droop Power is used by The Company to control System Frequency changes through the instruction of Primary Response and Secondary Response.
- **Control Based Real Power**
  Control Based Real Power output supplied by a Grid Forming Plant through controlled means (be it manual or automatic)
- **Fast Fault Current Injection**
  The ability of a Grid Forming Plant to supply reactive current, that starts to rise in less than 5 ms, into the Total System when the voltage falls below 90% of its nominal value.
- **Network Frequency Perturbation Plot**
  A form of Bode Plot which plots the amplitude (%) of the output oscillation and Phase (degrees) to the frequency of an applied input oscillation. The purpose of which is to assess the capability and performance of a Grid Forming Plant and to ensure it does not pose a risk to other Plant and Apparatus connected to the Total System. The input is oscillations in the System s Frequency and the output can either be oscillations in the System's power or oscillations in the Internal Voltage Source.
- **Control based**
  Control based are changes in the System's Real Power or Reactive Power produced by the control system of a Grid Forming Unit that occur due to changes in an external signal connected to the control system. These Control based changes have a bandwidth limited to 5 Hz

Dodatkowe definicje

- **Dynamic Reactive Compensation Equipment**
  Plant capable of supplying or absorbing Reactive Power in a controlled manner which could include but not limited to a Synchronous Compensator, Static Var Compensator (SVC), or STATCOM.
- **Electronic Power Converter**
  An electronic power converter which uses switched solid state power electronic devices to produce a real voltage waveform, with harmonics, that has a fundamental component that rotates to produce the real Internal Voltage Source

Podejście niemieckich OSP

50Hertz Transmission GmbH,
Transnet BW GmbH,
Amprion GmbH,
Tennet TSO GmbH

PSE Innowacje

GFC | Podejście niemieckich OSP

Dokument *4-TSO Paper on Requirements for Grid-Forming Converters*

Zakres

- przedstawia stanowisko niemieckich operatorów sieci przesyłowej do zagadnienia GFC.
- zawiera generalne wymagania jakim muszą sprostać przekształtniki energoelektroniczne w celu uzyskania tzw. „pełnego grid-formingu”.

Wymagania GFC

- Tworzenie napięcia systemowego (*Creating System Voltage*),
- Udział w poziomie zwarcia (*Contribution to Fault Level*),
- Zapewnienie inercji systemu (*Contribution to Inertia*),
- Zapobieganie niekorzystnym interakcjom sterowania (*Preventing adeverse control interaction*),
- Stabilność sterowania (*Controller stability*)

Podstawowe informacje	
Data/status	**10.05.2022 r - opublikowany**
Uczestnicy projektu	• 50Hertz Transmission GmbH, • Transnet BW GmbH, • Aprion GmbH, • Tennet TSO GmbH,
Cel	**Podstawowe wymagania dla przekształtników GFC**
Źródło	4-TSO Paper on Requirements for Grid-Forming Converters

4 TSO zamierzają wypracować definicję wymagań dla przekształtników typu GFC w niemieckiej sieci przesyłowej na poziomie krajowym do kolejnej rewizji *Technical Application Rules* (TAR).

Data publikacji: **10.05.2022 r.**

Źródło: 4-TSO Paper on Requirements for Grid-Forming Converters

PSE Innowacje PTPiRE | Idea Grid Forming Capability (GFC) Źródło: 4-TSO Paper on Requirements for Grid-Forming Converters 22

GFC | Podejście niemieckich OSP

Dokument *4-TSO Paper on Requirements for Grid-Forming Converters*

Publikacja ogólnych wymagań

German transmission grid at national level for the next revision of the Technical Application Rules (TAR) right now

Źródło: 4-TSO Paper on Requirements for Grid-Forming Converters

Projekt *GFM-Benchmark*

Źródło: GFM-Benchmark – Measurements of Grid Forming Converters

Normy VDE

Technical Connection Rules
- VDE-AR-N 4120 (TAR High Voltage)
- VDE-AR-N 4130 (TAR Extra High Voltage)
- VDE-AR-N 4131 (TAR HVDC)

Źródło: Technical Connection Rules

Grid connection regulations

Grid Connection Rules (NAR)

The VDE technical requirements:
- VDE-AR-N 4120:2018-11 (TCR HV);
- VDE-AR-N 4130:2018-11 (TCR EHV);
- VDE-AR-N 4131:2019-03 (TCR HVDC);

are an integral part of these NAR and shall be complied with insofar as they apply.

Są wstępne zapisy dt. GFC dla NC HVDC
- Requirements for HVDC-Stations System Studies | Grid forming control study
- Requirements for offshore grid connection | System Studies | Grid forming control study

Dokument z: 24th July 2023

Źródło: Grid connection Regulation

GFC | Podejście niemieckich OSP

GFM-Benchmark

- Projekt GFM-Benchmark skupia się na wytworzeniu nowych metod weryfikacji spełnienia wymagań dotyczących stabilnej pracy systemu we wszystkich stanach sieci.
- Fraunhofer ISE opracowuje odpowiednią procedurę weryfikacji i testuje ją z różnymi urządzeniami grid-forming. Projekt ten zapewni przegląd działania GFC i interpretacji implementacji dokonywanych przez różnych producentów.

Podstawowe informacje	
Data/status	**06.2023 - 05.2024** – w trakcie realizacji
Uczestnicy projektu	• Fraunhofer ISE • 50Hertz Transmission GmbH, • Transnet BW GmbH, • Aprion GmbH, • Tennet TSO GmbH,
Cel projektu	**Opracowanie procedury weryfikacji i testowania urządzeń z GFC**
Źródło	https://www.ise.fraunhofer.de/en/research-projects/gfm-benchmark.html

Źródło: GFM-Benchmark – Measurements of Grid Forming Converters

Cele projektu

- Analiza aktualnego stanu wiedzy w zakresie wydajności i wdrażania przetworników energoelektronicznyc typu GFC
- Szeroko zakrojone gromadzenie doświadczeń i wiedzy w zakresie weryfikacji i testowania zgodności przetworników typu grid-forming GFC
- Określenie niezbędnego dalszego potencjału rozwojowego dla przetworników sieciowych do stabilizacji systemu

GFC | Podejście niemieckich OSP

Dokument *4-TSO Paper on Requirements for Grid-Forming Converters*

Zakres:
- przedstawia stanowisko niemieckich operatorów sieci przesyłowej do zagadnienia GFC.
- zawiera generalne wymagania jakim muszą sprostać przekształtniki energoelektroniczne w celu uzyskania tzw. „pełnego grid-formingu”.

4 TSO zamierzają wypracować definicję wymagań dla przekształtników typu GFC w niemieckiej sieci przesyłowej na poziomie krajowym do kolejnej rewizji *Technical Application Rules* (TAR).

Wymagania:

Tworzenie napięcia systemowego
Każdy przekształtnik powinien zachowywać się jak źródło napięcia, które jest w stanie ograniczyć oscylacje napięcia w zakresie krótkotrwałym (kilka okresów po zakłóceniu sieci). W konsekwencji stabilizujące prądy wyrównawcze wystąpią między napięciem przyłączeni do sieci, a napięciem zasilającym.

Udział w poziomie zwarcia
W przypadku zwarcia krótkotrwałego stała czasowa, położenie fazy i amplituda prądu zwarciowego określane są przez impedancję sieci, impendancję zwarcia oraz inne impedancje całego systemu. Dodatnia sekwencja prądu przekształtnika dla zwarć długotrwałych powinna zostać zapewniona w sposób kontrolowany zgodnie z krzywą charakterystyki lub charakterystyką systemu.

Zapewnienie inercji systemu
W przypadku zmiany obciążenia lub zasilania w systemie, prąd kompensacji prowadzi do udziału w rezerwie chwilowej. Przy ciągłej zmianie kąta poza zakres krótkotrwały, prąd kompensacji prowadzi do składowej skutecznej proporcjonalnej do gradientu częstotliwości. Ograniczenie prądu i mocy w celu ochrony instalacji, jest dopuszczalne i nie może prowadzić do utraty synchronizmu

Zapobieganie niekorzystnym interakcjom sterowania
Przekształtnik powinien zachowywać się pasywnie dla składowych częstotliwości nie równych częstotliwości podstawowej i przyczyniać się do stabilnego połączenia równoległego kilku przekształtników i innych elementów sieci.

Stabilność sterowania
Stabilność sterownika (oparta na pracy w wirtualnej wyspie) jest wymagana w przypadku obiektów wytwórczych tworzących sieć, a także tworzących sieć systemów HVDC

GFC | Podejście niemieckich OSP

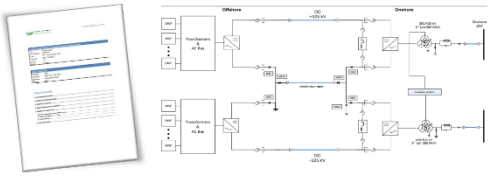
T14 – Grid Forming OWF | Position paper | TenneT

Dokumencie opisano, w jaki sposób TenneT, jako operator odpowiedzialny za przyłączenie do sieci MFW, proponuje wypracowanie możliwość implementację funkcjonalności GFC w MFW (morskich turbinach wiatrowych) i świadczenia usługi blackstart.

Zawartość:

- ogólne warunki jakie muszą być spełnione że by MFW z GFC mogła świadczyć usługę blackstart – w tym podkreślenie potrzebęykoordynacji tej zdolności z systemem HVDC układu eksportowego;
- kolejne kroki uruchamiania MFW i poszczególnych elementów układu wyprowadzenia mocy,
- ramową ocenę wpływu tej funkcjonalności na strukturę MFW, m.in. w zakresie:
  - magazynowania energii,
  - skoordynowania sterowania,
- ramową ocenę wpływu tej funkcjonalności na system HVDC będący głównym elementem układu eksportowego:
  - wymagania dotyczące zasilania pomocniczego,
  - wymagania dotyczące kontroli i zabezpieczeń.

Podstawowe informacje	
Data/status	**06.2023 - 05.2024** – w trakcie realizacji
Uczestnicy	TENNET
Cel	Wypracowanie ogólnej metodyki koordynacji implementacji GFC w MFW (przyłączanych przez HVDC)
Źródło	https://offshore-documents.tennet.eu/fileadmin/offshore_document_uploads/Consultation_documents/15._Grid_Forming_OWF/ONL_TTB-05442_T14_Grid_Forming_OWF_v1.0.pdf



Źródło: T14- Grid Forming OWF | Position paper | TenneT

Podsumowanie

Implementacja GFC w KSE

PSE Innowacje

GFC | NC

GFC w kodeksach sieci 2.0. – NC RfG

Article Y

(new article, to be placed before current Article 20):

Requirements for type A power park modules (type B, C, D)

[…]

6. The relevant TSO shall have the right to request grid forming capability from type A PPM at its connection point as defined by the following paragraphs:

a. Within the power park module current limits, the power park module shall be capable of behaving at its connection point as a voltage source behind an internal impedance (Thevenin source), during the normal operating conditions (non-disturbed grid conditions) and quasi immediately after a grid disturbance (including voltage, frequency and voltage phase angle disturbance). The Thevenin source is characterized by its voltage amplitude, voltage phase angle, frequency and internal impedance.

b. During the first instant following a grid disturbance and while the power park module capabilities and current limits are not exceeded:

(i) the instantaneous AC voltage characteristics of the Thevenin source according to paragraph (a) shall be capable of not changing its amplitude and voltage phase angle while voltage phase angle steps or voltage magnitude steps (in positive and in negative sequence) are occurring at the connection point (grid side). The positive and the negative sequence current exchanged between the power park module (power park module side) at the connection and AC grid shall flow naturally according to grid and converter impedances.

(ii) The relevant system operator shall specify a minimum time dependent current profile for which the grid forming capability of the power park module is required.

c. During the disturbance period (voltage magnitude, frequency and voltage phase angle disturbance) and after the first instant,

(iii) The internal voltage magnitude and voltage phase angle of the power park module shall be adapted according to a predefined dynamic performance.

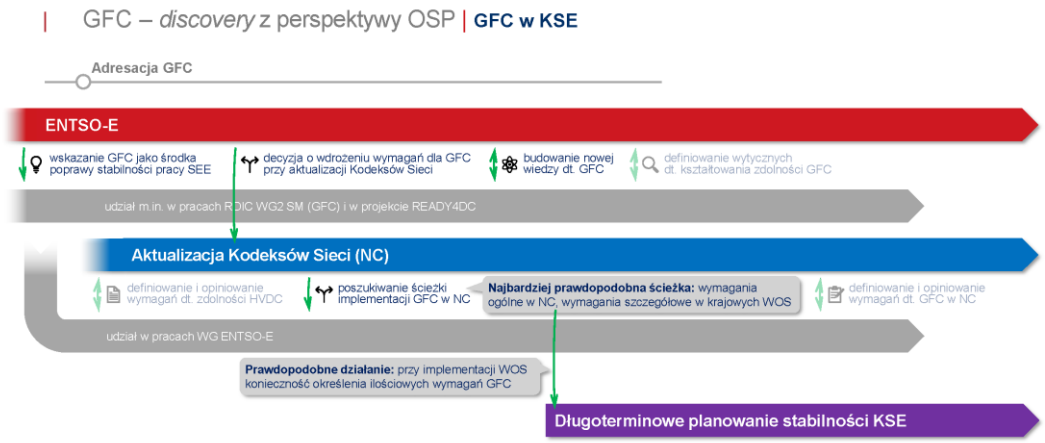
(iv) The power park module active and reactive current adjustment shall always respect the minimum and maximum power park module capability and current limits.

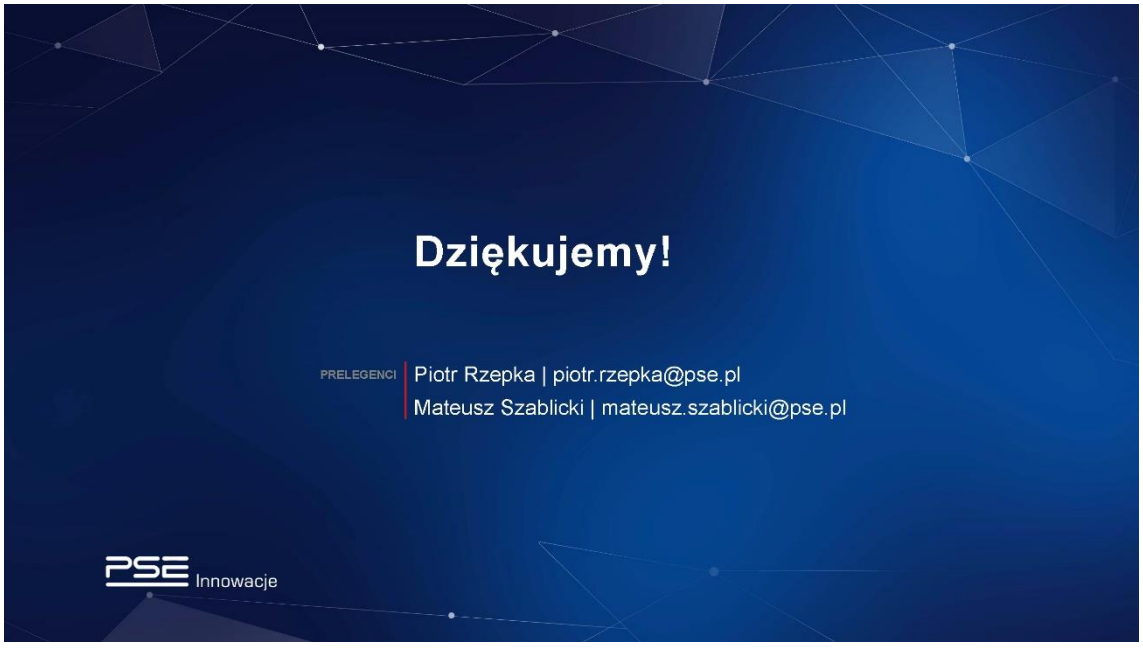
(v) The TSO may specify additional requirements in the case that current limitation is necessary.

(vi) The power park module shall be capable of stable and smooth transition when reaching the power park module current limits, without interruption, in a continuous manner and returning to the behaviour described in paragraph (b)(ii) as soon as the limitations are no more active.

d. The required energy to deliver the minimum capability in paragraph (a) to (b) shall be ensured through the whole active power operating range of power park module.

e. The required dynamic performance of the power park module for the paragraphs (a) to (d) and its associated performance parameters shall be specified by the relevant TSO.


GFC – discovery z perspektywy OSP | GFC w KSE
Adresacja GFC
ENTSO-E
wskazanie GFC jako środka poprawy stabilności pracy SEE
decyzja o wdrożeniu wymagań dla GFC przy aktualizacji Kodeksów Sieci
budowanie nowej wiedzy dt. GFC
definiowanie wytycznych dt. kształtowania zdolności GFC
udział m.in. w pracach RDIC WG2 SM (GFC) i w projekcie READY4DC
Aktualizacja Kodeksów Sieci (NC)
definiowanie i opiniowanie wymagań dt. zdolności HVDC
poszukiwanie ścieżki implementacji GFC w NC
Najbardziej prawdopodobna ścieżka: wymagania ogólne w NC, wymagania szczegółowe w krajowych WOS
definiowanie i opiniowanie wymagań dt. GFC w NC
udział w pracach WG ENTSO-E
Prawdopodobne działanie: przy implementacji WOS konieczność określenia ilościowych wymagań GFC
Długoterminowe planowanie stabilności KSE


Dziękujemy!
PRELEGENCI
Piotr Rzepka | piotr.rzepka@pse.pl
Mateusz Szablicki | mateusz.szablicki@pse.pl
PSE Innowacje

WYBRANE ASPEKTY DOBORU I NASTAWIANIA ZABEZPIECZEŃ W SIECI 110 KV

Jacek Floryn (Tauron Dystrybucja SA)

Dobór nastawień zabezpieczeń linii 110 kV na ogół wykonywany jest przez służby Operatora Przesyłowego. Jednak szczegółowa znajomość zasad wyliczeń wspomnianych nastawień w OSD ma bardzo istotne znaczenie dla optymalnej pracy automatyki zabezpieczeniowej w poszczególnych sieciach. Umiejętność i zrozumienie w tym zakresie jest też nieodzowne w procesie analizy działania zabezpieczeń i badania awarii prowadzonych w OSD. Wnioski wynikające z wyliczeń nastawień mają też istotne znaczenie w obszarach, które wydają się niezwiązane i odległe od tego zagadnienia, np. w procesie rozwoju sieci.

W materiale przedstawiono wybrane przykłady uwarunkowań doboru nastawień. Część z nich mocno związana jest ze specyfiką sieci 110 kV: układami sieci i wyposażeniem stacji odmiennych niż w sieci przesyłowej NN. Biorąc również pod uwagę szereg analizowanych awarii w sieci 110 kV, odpowiedzialność za nastawienia zabezpieczeń zdaniem autora powinna ciążyć w największym wymiarze na OSD.

Wiele zagadnień dotyczących nastawiania zabezpieczeń linii 110 kV jest szeroko opisanych w literaturze. Niektóre z nich zasługują na przypomnienie i wyeksponowanie.

Sieć 110 kV ma cechy, których zazwyczaj nie spotyka się w sieciach NN. Niejednorodność struktury i parametrów linii, szczególnie w obszarach zurbanizowanych, jest powszechna. Linie na swej długości zmieniają przekrój, sylwetki słupów. Są prowadzone na wspólnych słupach z innymi liniami niekoniecznie o tym samym poziomie napięcia i tylko na części swej długości. Linie 110 kV są często częściowo kablowane. Kablowanie, które głównie służy uwalnianiu terenu i eliminowaniu kolizji z projektami infrastrukturalnymi czy deweloperskimi, wykonywane jest w środkowych fragmentach linii. Często w linii danej relacji dokonuje się kilka kablowań – autorowi znane są przypadki skablowani linii 110 kV w sześciu odcinkach. Dużo częściej niż w sieciach przesyłowych w sieci 110 kV napotyka się układy odczepowe - aktywne i pasywne. W ciągach liniowych pomiędzy stacjami systemowymi powstają linie o bardzo zróżnicowanej długości – choć biorąc pod uwagę linie kablowe 110 kV - reaktancji. Zdarza się, że kolejne stacje 110 kV połączone są liniami o reaktancji wieloomowej oraz krótkimi liniami o reaktancji mniejszej niż 0,2 oma. W sieciach 110 kV często do stacji mających jedynie dwa powiązania z innymi stacjami przyłącza się elektrownie lokalne o stosunkowo dużej mocy, będące źródłami prądu zwarciowego i nieodporne na łączenia asynchroniczne. Należy jeszcze pamiętać o dużo większym prowdopodobieństwie niż w sieciach przesyłowych powstawania zwarć oporowych. Związane jest to oczywiście z wysokością linii oraz sposobem i zakresem prowadzonych wycinek. Dodając do tego zróżnicowane wyposażenie poszczególnych stacji 110 kV w automatykę zabezpieczeniową, wszystko to powoduje, że dobór nastawień zabezpieczeń linii 110 kV jest złożonym zagadnieniem.

Niejednorodność budowy linii 110 kV nie tylko utrudnia precyzyjne wyliczenia parametrów linii ale również powoduje, że wyniki działania lokalizatorów miejsca zwarcia zaszytych w zabezpieczeniach odległościowych są obarczone dużymi błędami i mniej przydatne. Zabezpieczenia odległościowe używane w OSD zazwyczaj nie umożliwiają zaprogramowania niejednorodnej struktury linii dla potrzeb działania lokalizatorów. Biorąc pod uwagę

niejednorodność oraz fakt, że cześć linii ma budowę niestandardową - sylwetki słupów są odmienne od znanych typów – rośnie rola wyznaczania pomiarowego podstawowych parametrów elektrycznych linii. Zdaniem autora wymagania dotyczące pomiarów X1, R1, X0, RO powinno być stawiane przy każdej budowie i przebudowie linii 110 kV. Wyniki rzetelnie wykonanych pomiarów powinny być podstawą obliczeń, w szczególności współczynników korekcyjnych.

Różnorodność budowy poszczególnych linii, a zatem ich parametrów elektrycznych może być źródłem pewnych niedogodności. Jako przykład przedstawia się linie w ciągu o tak odmiennej budowie, że kąty charakterystyczne linii różnią się nawet o 10 stopni. Jeśli takie wartości kątów zostaną przyjęte jako kąty nachylenia charakterystyk poligonalnych zabezpieczeń odległościowych (co zazwyczaj ma miejsce), to okazuje się, że zasięgi takich zabezpieczeń nieco się różnią. W przypadku zwarć oporowych może dojść do nieselektywnego wyłączenia zwarcia mimo, że nastawy zasięgów rezystancyjnych są jednakowe.

Jak już wspomniano, zdarza się, że w ciągu linii 110 kV powstaje linia krótka, mająca nawet mniej niż kilka kilometrów. Jeśli przy okazji jest to linia kablowa, okazuje się, że reaktancja takiej linii wynosi kilka dziesiątek omów. Zabezpieczenia takiej linii buduje się aby zapewnić właściwą eliminację zakłóceń dla linii krótkiej. Jednak problemem staje się zapewnienie szybkiej i selektywnej eliminacji zakłóceń w z całym ciągu. Szczególnie jest to wyraźne, gdy w ciągu o wieloomowej reaktancji kolejnych linii powstaną pod rząd dwie linie o reaktancjach kilkunastokrotnie mniejszych. Aby myśleć o szybkim i selektywnym działaniu zabezpieczeń, należy sąsiednie linii (w stosunku do linii krótkiej), wyposażyć w zabezpieczenia odcinkowe oraz uwspółbieżnione, a szyny stacji objąć układami zabezpieczeń szyn. Na podobne problemy można się natknąć w układach odczepowych linii. Nie do końca jest prawdą, że panaceum w zakresie eliminacji zakłóceń w liniach z odczepami (aktywnymi i biernymi) jest zastosowanie zabezpieczeń różnicowych dla linii o wielu końcach. Nie rozwiązują one problemu zmienności zasięgów dalszych stref zabezpieczeń odległościowych w zależności stanu pracy sieci.

W sieci dystrybucyjnej 110 kV stosunkowo często dochodzi do sytuacji, kiedy do stacji pracującej w układzie H na napięciu 110 kV dołącza się źródło wytwórcze. Taka elektrownia ma jedynie dwa powiązania z systemem elektroenergetycznym. OSD określa wymagania techniczne również dotyczące EAZ. Dotyczą one rozwiązań przyłączanej stacji, zabezpieczeń linii łączącej GPZ z GPO, oraz ewentualnie pracy współbieżnej zabezpieczeń i kontroli synchronizmu linii bezpośrednio związanych z GPZ. Problem, nad którym warto się szczególnie pochylić dotyczy sytuacji, kiedy stacja z przyłączoną generacją jest w ciągu wielu stacji pomiędzy stacjami systemowymi, a sam ciąg zostaje przerwany. Dzieje się to wskutek konieczności wprowadzenia podziału sieci dla potrzeb eksploatacyjnych czy serwisowych. Czas utrzymywania takiego nienormalnego układu bywa całkiem długi, a ryzyko niepomijalne. Problem powstaje w sytuacji, kiedy dojdzie do zwarcia w odległej linii pomiędzy stacją systemową, a źródłem wytwórczym. Wyłączone zwarcie od strony systemu, niekoniecznie jest wyłączane od strony źródła. Jeśli źródło nie zostanie dostatecznie szybko wyłączone, utrudnić może dejonizacje przestrzeni połukowej uniemożliwiając skuteczne działanie SPZ. Ale załączenie w cyklu SPZ, zazwyczaj bez kontroli synchronizmu, może spowodować asynchroniczne podanie napięcia na generator. Oczywiście radą na to miałoby być odstawienie w całym przerwanym ciągu automatyki SPZ we wszystkich stacjach. Ale z punktu widzenia zapewnienia ciągłości dostaw energii jest to sytuacja w oczach OSD nieakceptowalna. Należałoby raczej budować układy kontroli synchronizmu we wszystkich stacjach ciągu, nawet pozornie odległych od elektrowni. Natomiast samą elektrownię wyposażać w zabezpieczenia od utraty połączenia z siecią działające z czasem znacznie krótszym niż czas przerwy beznapięciowej w cyklu SPZ.

Większa samodzielność OSD w zakresie doboru nastawień sprzyja tworzeniu algorytmów działania zabezpieczeń, które wykraczają poza typowe rozwiązania. Istnieje większa elastyczność w doborze schematów funkcjonowania telezabezpieczeń. Wykorzystywane są różne schematy funkcjonowania telezabezpieczeń adekwatnie do lokalnych uwarunkowań również w sytuacji utraty transmisji pomiędzy zabezpieczeniami odległościowymi. W liniach mieszanych, wykorzystując dostępne strefy zabezpieczeń odległościowych, próbuje się identyfikować i odróżniać zwarcie w części kablowej linii, uzależniając od tego działanie automatyki SPZ. W wyjątkowych układach sieci 110 kV, opierając się na działaniu zabezpieczeń i teletransmisji, realizuję się układy automatyk restytucyjnych wykraczających poza typowy SPZ i SZR.

Od dziesięcioleci obserwuje się pozytywne wyniki w zakresie działania zabezpieczeń ziemnozwarciowych linii nastawianych według zasad, które nie są obecnie powszechnie praktykowane. Mianowicie, tam gdzie warunki zwarciowe na to pozwalają, jeden stopień zabezpieczenia ziemnozwarciowego kierunkowego nastawia się bezzwłocznie, a drugi odpowiednio nisko prądowo – tak aby zapewnić reakcję zabezpieczenia przy zwarciach wysokooporowych. Pierwszy wysokonastawiony stopień pobudza automatykę SPZ. W ten sposób nastawiając zabezpieczenie ziemnozwarciowe, można uzyskać dwa niezależne zabezpieczenia działające bezzwłocznie: podstawowe - odległościowe oraz rezerwowe - ziemnozwarciowe. Niedogodnością tej metody jest konieczność monitorowania zmian w rozpływach prądów ziemnozwarciowych i ewentualne korygowanie progów rozruchowych zabezpieczeń ziemnozwarciowych. Zasada ta przestaje mieć uzasadnienie w polach linii wyposażonych w zabezpieczenia różnicowe i odległościowe.

Ramy organizacyjne są źródłem pewnych ewidentnych problemów dotyczących nastawień zabezpieczeń linii. Otóż w wielu przypadkach, otrzymane nastawienia są wprowadzane do zabezpieczeń bez jakiejkolwiek analizy i uzupełnienia. Unika się wręcz współdzielenia odpowiedzialności za poprawność materiałów. Dane pozyskiwane od OSP nie zawsze zawierają wszystkie istotne parametry nastawcze. Również nie zawsze są one wykonane w oparciu o najaktualniejsze dane i szczegóły wyposażenia i rozwiązań w poszczególnych stacjach. W procesach inwestycyjnych obserwowany jest mechanizm przekazywania danych pozyskanych od OSP wykonawcom bez jakiejkolwiek analizy czy uzupełnienia w celach konfiguracji i nastawiania. Prowadzi to, jak pokazuje praktyka, do wielu nieoczekiwanych sytuacji i zdarzeń. Niekiedy niezdefiniowane parametry nastawcze pozostawiane są na wartościach fabrycznych.

I tak znane są przypadki nieprawdopodobnych zdarzeń, które jednak stały się faktami np. pobudzania automatyki SPZ w innych strefach niż pierwsza czy pierwsza wydłużona. Ustawiania czułości napięciowej zabezpieczenia ziemnozwarciowego na poziomie charakterystycznym dla sieci skompensowanych i wyższych (nawet 30V!), działanie bezkierunkowe zabezpieczenia ziemnozwarciowego. Pozostawienie (nie wyłączenie) niechcianych i zbędnych zabezpieczeń np. nadprądowych bezkierunkowych. Takie sytuacje mogą wychodzić na jaw niestety dopiero po zaistniałych zdarzeniach i nieprawidłowej eliminacji zakłóceń oraz podczas przeglądów okresowych pól. Służby serwisu powinny mieć bezpośredni codzienny kontakt z inżynierami kompetentnymi z zakresu nastaw zabezpieczeń w celu szybkiego bezpośredniego wyjaśniania sytuacji tego wymagających.

Zdaniem autora OSD powinny w większym stopniu poczuwać się do odpowiedzialności za nastawienia linii 110 kV. Aby to skutecznie realizować muszą być wprowadzone odpowiednie mechanizmy i procedury. Posiadana w przeszłości w poszczególnych spółkach dystrybucyjnych wiedza i umiejętności w zakresie doboru nastawień powinny być wzmocnione bądź na nowo zbudowane.

Niektóre wnioski wynikające z doboru nastawień zabezpieczeń powinny być uwzględniane w procesie tworzenia planów pracy sieci, budowania planów inwestycyjnych, wydawania warunków przyłączenia i przebudowy. Oczywiście wiele ze wskazanych wyżej problemów mogłoby być złagodzone, gdyby wszystkie stacje były odpowiednio wyposażone w zakresie elektroenergetycznej automatyki zabezpieczeniowej.

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