NATO OTAN
This project is supported by: The NATO **Science** for **Peace** and **Security** Programme

IDEAS NCBR

SEBOR'26

System Elektroenergetyczny: Bezpieczeństwo Operacyjne i Rynkowe

PTBN
Polskie Towarzystwo Bezpieczeństwa Narodowego

R - GRID - OCENA PODATNOŚCI SIECI WN I NN NA AWARIE I ATAKI Z UWZGLĘDNIENIEM MOŻLIWOŚCI REKONFIGURACJI

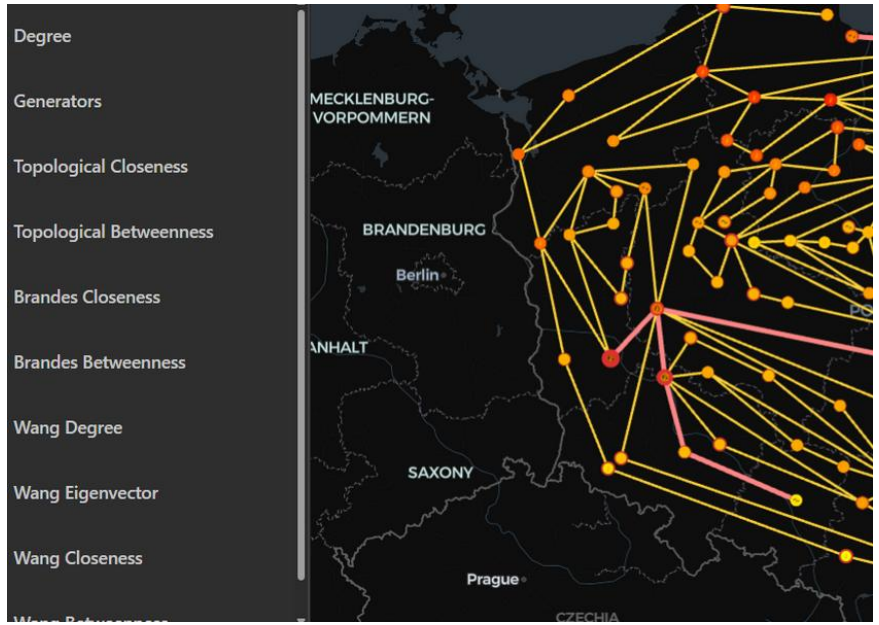
Krzysztof Łowczowski PTBN / PUT

LAUREA

Ukrainian Institute for the Future

Kazimierz Dolny, 17–19 marca 2026 r.

Wybrane możliwości RGRID



- RGRID służy do analiz zagrożeń pracy systemu elektroenergetycznego. Scenariusze zagrożeń przenoszone są do postaci użytecznej dla obliczeń rozpływowych. Obliczenia rozpływów mocy ujmują ograniczenia techniczne sterowania oraz sposób działania układów automatyki zabezpieczeniowej.
- Program RGRID jest na etapie prototypu i jest w trakcie prac rozwojowych.
- Program wykorzystuje dodatkowo miary centralności oraz inne narzędzia np. teorie gier pozwalających na dodatkowe analizy zagrożeń np. typowanie celów ataku z wykorzystaniem danych topologicznych.

Wybrane sposoby identyfikacji zagrożeń

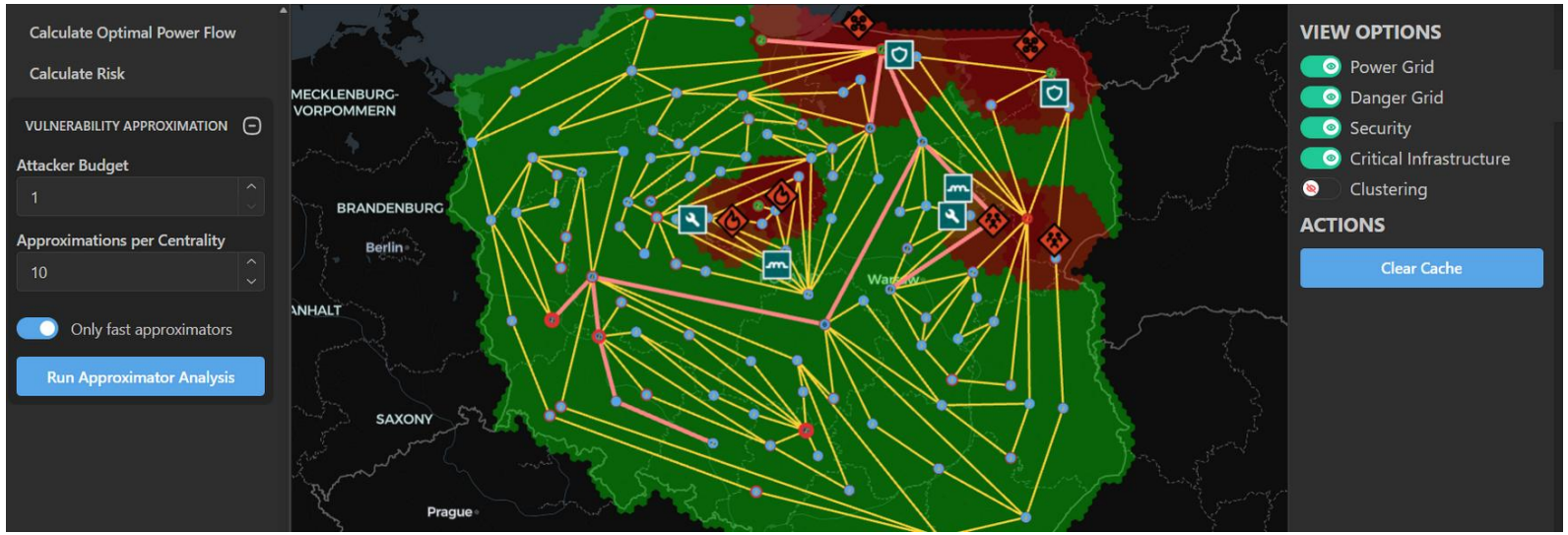
Zagrożenie	Sposoby identyfikacji
Awarie kaskadowe	Identyfikacja zmieniających się warunków pracy i wprowadzanie działań prewencyjnych np. ograniczenia generacji mocy biernej kompensatorów w celu ograniczenia przepięć po zadziałaniu zabezpieczeń bloków
Ataki cybernetyczne	Analiza podatnych elementów np. wyłączenie wentylatorów nowoczesnych transformatorów skutkujących znacznym ograniczeniem dopuszczalnej mocy lub symulacje gwałtownych wyłączeń inwerterów określonych producentów
Zakłócenia komunikacji	Zablokowanie możliwości zmiany punktów pracy elektrowni w celu oszacowania wpływu na odchylenia poziomu napięć itp. Baza powiązań między źródłem zasilania, a ważnymi dla sieci elektroenergetycznych stacjami telekomunikacyjnymi
Skutki awarii	Diagnostyka – nowe technologie wykrywające ukryte awarie oraz ewentualny sabotaż

Wybrane sposoby identyfikacji zagrożeń

Zagrożenie	Sposoby identyfikacji
Ataki z wykorzystaniem środków rażenia i lub BSP	Analiza dodatkowych danych związanych z podatnością na ataki np. wykonanie podziemne (dodatkowo informacje o przejściu w otwarty teren), ukształtowanie terenu
Wtargnięcia na teren stacji	Opracowanie bazy możliwych działań sabotażowych lub błędów eksploatacyjnych np. brak działania zabezpieczeń podstawowych na terenie stacji
Starzenie infrastruktury np. wzrost zawilgocenia	Wykorzystanie symulacji rozpływowych do określenia znaczenia ratingu i zdolności przeciążeniowych w sytuacjach awaryjnych – risk based maintenance (RBM); analogicznie zaleca się integracje informacji o indeksach zdrowia (HI)
Przerwy zasilania	Dodatkowe dane np. informacje o układach zasilania rezerwowego współpracującego z siecią lub układach zasilania odłączających odbiór od sieci w warunkach niedoboru mocy np. agregaty wojska Ocena możliwości podtrzymania zasilania w przypadku określenia SOC magazynów
Ograniczenia logistyczne	Baza części zamiennych i ograniczenia środków naprawczych np. limit roboczogodzin, czas przywiezienia części itp.

Model ryzyka

Prawdopodobieństwo zagrożenia x **Podatność na uszkodzenia** x **Konsekwencje ataku**



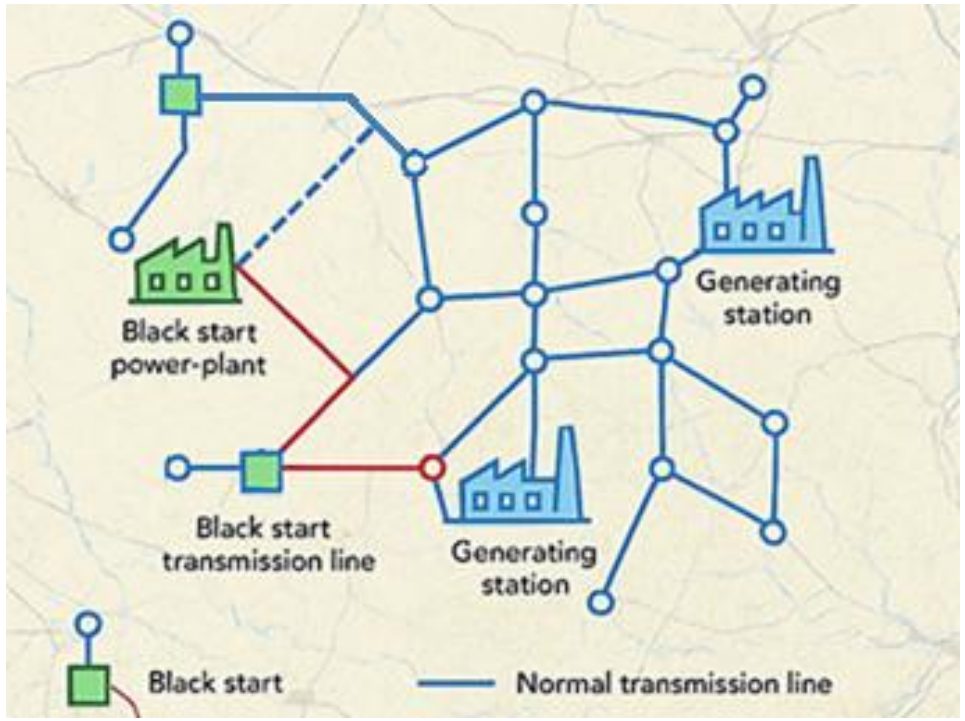
Proponowana ogólna metodologia analiz

1. Wykorzystanie AI (np. LLM) do pozyskania aktualnych tabeli ryzyka z określonych, wiarygodnych źródeł np. w zasięgu broni i celności dla aktualnych warunków pola walki np. ograniczenie skuteczności ochrony przeciwlotniczej przez pogodę lub środki zagłuszania;
2. Określenie aktualnych podatności dla ryzyka w oparciu o zadeklarowane wartości eksperckie, docelowo AI analizuje cyfrowego bliźniaka i/lub model 3d/VR stacji np. czy w stacji jest ochrona przed zwierzętami (normalne zagrożenia lub zwiększone np. szczury w pobliżu linii frontu)
3. Na podstawie ryzyka i podatności AI wspomaga lub samodzielnie inicjuje obliczenia rozpływowe dla założonych stanów awaryjnych, następnie aktualizuje ryzyka, podatności i efektywności w oparciu o aktualne informacje
4. Określenie skutków ataku (np. dla określonego obszaru, dla elementów dużego ryzyka lub iloczynu ryzyka i podatności) poprzez wykonanie obliczeń rozpływowych, a następnie analizy wyników obliczeń rozpływowych.
5. Analiza profili mocy generowanej i pobieranej oraz współczynników czułości (opcjonalnie w przypadku dostępu do danych)
6. Dobór środków zaradczych z uwzględnieniem optymalizacji lokalnej i/lub globalnej

Wybrane możliwości rekonfiguracji sieci

- Rekonfiguracja w oparciu o automatykę zabezpieczeniową
- Możliwość oceny czasu potrzebnego na wykonanie rekonfiguracji w celu wspomagania decyzji o budowie automatyki specjalnej (SPS)
- Doraźne działania np. eksploatacja linii 400 na napięciu 220 kV (warunki wojenne), mobilne stacje transformatorowe lub linie
- Pominiecie stacji i zwarcie przewodów (roboczogodziny i materiały (utrata możliwości rekonfiguracji)
- Przenoszenie mocy między stacjami WN liniami SN (dodatkowe dane – lista połączeń i przepustowość)
- Alternatywne możliwości np. moc bierna transformatorów przemysłowych pracujących równolegle,
- Prewencyjne wydzielanie wysp lub izolowanie fragmentów sieci (w oparciu o wielkości wyznaczone z symulatorów dynamicznych np. PSE) np. linii przed nieuniknionym zwarciem (np. obraz kamer) – wstępna klasyfikacja w oparciu o wiedzę ekspercką i wyniki symulacji
- Integracja z innymi programami np. SCC (układy zwarciowe i dodatkowe informacje np. linie wielotorowe) lub synchrosoft w celu uwzględniania realistycznych, możliwych z technicznego punktu widzenia rekonfiguracji sieci
- Zmiana lokalizacji punktu rozcięcia sieci 110 kV lub zmiana ilości punktów rozcięć np. w przypadku awarii AT i zmniejszeniu mocy zwarciowej możliwe jest zamykanie wyłączników 110 kV

Tory rozruchowe - koncepcja



Tory rozruchowe w Polsce są dobrze rozwinięte, ale tradycyjne tory rozruchowe cechują często znaczne długości i złożone procedury konfiguracji np. kilkaset km długości i wiele stacji. Niestety w warunkach zagrożeń hybrydowych, wojennych lub awarii katastrofalnych przekłada się to na duże ryzyko nieprawidłowości.

Istnieje możliwość automatycznego wyznaczania możliwych torów rozruchowych w oparciu o bazę sprawnych źródeł black start oraz prawidłowo funkcjonujących linii.

Duża ilość możliwych torów rozruchowych przekłada się na znaczne ograniczenie skuteczności ewentualnych ataków.

Proponowana procedura:

- etap identyfikacji powiązań między źródłami black start, a elektrowniami z uwzględnieniem technicznych możliwości (poziomy napięć w warunkach normalnych oraz rozruchu dla określonej wielokrotności prądu znamionowego)
- Opcjonalnie możliwość parowania źródeł black start do pracy równoległej w oparciu o dopuszczalną odległość od głównego toru
- Określanie kolejności uruchomień w przypadku powiązania 1go źródła black start z wieloma elektrowniami (np. priorytety ze względu na infrastrukturę krytyczną oraz kryteria techniczne – możliwość bilansowania sieci)

Synchronizacja wysp i odbudowa sieci wymaga dodatkowych danych i dalszych analiz.

Rekonfiguracja w przypadku awarii AT - koncepcja

Zaatakowane stacje [Reuters]

- w przypadku awarii AT podejmowana jest próba załączenia kolejnego AT znajdującego się w stacji i zamknięcia sprzęgła lub zamknięcia sprzęgła w przypadku braku AT
- Dla obszaru objętego przerwą zasilania analizowane są quasi ustalone stany przejściowe:
  - zwiększony pobór ze względu na wyłączoną generacje (opóźnione wznowienie pracy) w celu weryfikacji obecności ewentualnych przeciążeń (maksymalizacja ilości zasilonych odbiorów lub źródeł w przypadku zagrożenia systemu),
  - stan po wznowieniu pracy źródeł OZE (szybki powrót)
  - stan po wznowieniu konwencjonalnych źródeł energii
- w przypadku braku AT podejmowana jest próba określenia czasu dostarczenia rezerwowego AT z zapasów lub ocenia się możliwość przeniesienia AT pracującego w innej lokalizacji
- Istnieje możliwość wspomagania pracy obszaru sieci 110 kV dzięki wykorzystaniu magazynów energii zasilanych poprzez sieć SN – zaleca się wprowadzenie mechanizmów wspierania kluczowych dla bezpieczeństwa sieci lokalizacji magazynów energii

Izolowanie fragmentów sieci i wysp przed nieuniknioną awarią - koncepcja

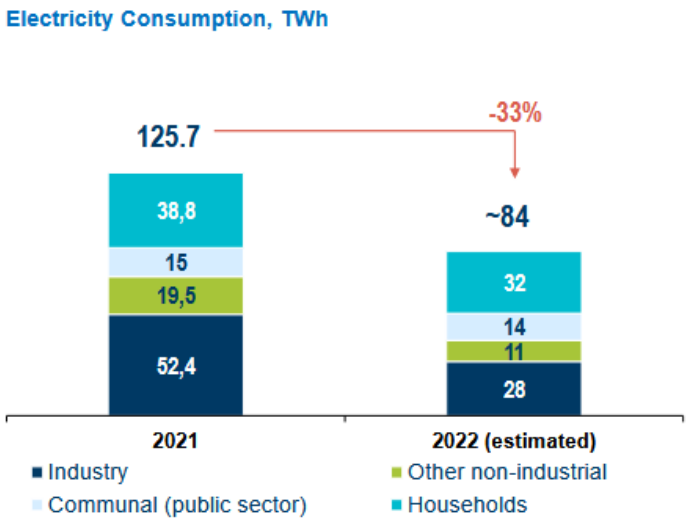
Izolowanie wysp

- Rozcinanie połączeń w określonej kolejności np. linia o największej impedancji odłączana jako ostatnia w celu ograniczenia udaru mocy czynnej lub odwrotnie – linia o najmniejsze impedancji w celu ograniczenia udaru napięcia wynikającego z mocy naturalnej linii oraz Q(P)
- Kryteria działania zbliżone do automatyki synchro-check (planowany artykuł)

Izolowanie fragmentów sieci np. linii

- Możliwość etapowania izolowania w zależności od prawdopodobieństwa zdarzenia np. odłączenie 1 go z 3 połączeń, 2 z 3 lub wszystkich połączeń

Podsumowanie



Zmiana mocy pobieranej – Ukraina

https://www.jvi.org/fileadmin/tx_abaeasydownloads/L-11_Piddubnyi_Energy_resilience_in_times_of_war.pdf

- W trakcie realizacji prac przeanalizowano scenariusze zagrożeń pracy sieci, możliwości ograniczania podatności sieci na skutki awarii i zaproponowano alternatywne możliwości poprawy
- Opracowano metodologie analiz z uwzględnieniem opcjonalnych źródeł danych
- Warto podkreślić, że punktu widzenia teorii gier atakujący i broniący mają dostęp do tych samych informacji. Należy dążyć nie tylko do ochrony najważniejszej infrastruktury, ale również do wyeliminowania słabych ‚ogniw' ponieważ np. skuteczny atak na 5 mało istotnych obiektów może prowadzić do poważniejszych skutków niż 1 skuteczny i 4 nieskuteczne ataki na ważny obiekt.
- Prace nad symulatorem trwały kilkanaście miesięcy i program jest na etapie prototypu – zaleca się kontynuacje prac analitycznych oraz wdrożeniowych
- Analizy wymagają przyjęcia założeń opisujących zachowania odbiorów, co wymaga ciągłego gromadzenia danych i analiz

Dziękuję za uwagę

dr inż. Krzysztof Łowczowski
krzysztof.lowczowski@put.poznan.pl