Niezależność sprzętu i oprogramowania jako kierunek rozwoju zabezpieczeń stacyjnych

Niezależność sprzętu i oprogramowania jako kierunek rozwoju zabezpieczeń stacyjnych

Krzysztof Kulski – GE Vernova

Streszczenie

Referat przedstawia rozwój automatyki zabezpieczeniowej stacji energetycznych – od tradycyjnych, sprzętowo zorientowanych przekaźników do nowoczesnego podejścia *software-defined*, w którym funkcje zabezpieczeniowe są oddzielone od konkretnego sprzętu. Główne czynniki tej zmiany to starzejąca się infrastruktura, rosnąca liczba urządzeń EAZ, nowe wymagania regulacyjne i cyberbezpieczeństwa oraz niedobór doświadczonych kadr. Artykuł wskazuje, że tradycyjne systemy, choć niezawodne, są mało elastyczne, kosztowne w utrzymaniu i trudne do aktualizacji. W odpowiedzi przedstawiono koncepcję *software-defined protection* oraz rozwiązanie GridBeats™ APS firmy GE Vernova, które umożliwia uruchamianie wielu funkcji na jednej platformie sprzętowej, zdalne aktualizacje, łatwiejsze zarządzanie cyberbezpieczeństwem i uproszczenie eksploatacji.

1. Wstęp

Automatyka zabezpieczeniowa stacji energetycznych stanowi kluczowy element bezpieczeństwa i niezawodności nowoczesnych sieci elektroenergetycznych. Jej zadaniem jest szybkie wykrywanie i izolowanie zakłóceń, minimalizowanie skutków awarii, ochrona urządzeń oraz utrzymanie jakości i ciągłości dostaw energii.

Przez dziesięciolecia dominowało podejście oparte na dedykowanym sprzęcie – przekaźnikach zabezpieczeniowych, w których algorytmy ochronne były ściśle powiązane z fizyczną warstwą urządzenia. Rozwój technologii cyfrowych, rosnąca złożoność systemu elektroenergetycznego oraz nowe wymagania w obszarze cyberbezpieczeństwa sprawiły jednak, że ta tradycyjna architektura zaczęła osiągać swoje granice. Odpowiedzią na te wyzwania stały się koncepcje architektury definiowanej programowo (*software-defined*), które stopniowo zmieniają sposób projektowania, wdrażania i utrzymania automatyki zabezpieczeniowej.

2. Wyzwania współczesnej energetyki

Sektor energetyczny stoi dziś przed szeregiem poważnych wyzwań strukturalnych i operacyjnych, które wymuszają głęboką transformację podejścia do automatyki zabezpieczeniowej. Wyzwania te nie są od siebie niezależne – wzajemnie się wzmacniają i tworzą złożone środowisko, w którym tradycyjne metody zarządzania infrastrukturą przestają być wystarczające.

2.1 Starzejąca się infrastruktura i rosnąca liczba urządzeń

Znaczna część infrastruktury elektroenergetycznej – zarówno w Polsce, jak i w innych krajach europejskich – pochodzi z lat 70., 80. i 90. XX wieku. Urządzenia te były projektowane z myślą o scentralizowanym, stosunkowo prostym systemie wytwarzania i dystrybucji energii. Współcześnie muszą jednak funkcjonować w zupełnie innym środowisku.

Problemy związane ze starzeniem się infrastruktury:

- Wiele przekaźników zabezpieczeniowych osiągnęło lub przekroczyło zakładany okres eksploatacji (typowo 20–30 lat), co zwiększa ryzyko awarii i pogarsza parametry niezawodnościowe.
- Producenci stopniowo wycofują wsparcie techniczne dla starszych modeli urządzeń, ograniczając dostępność części zamiennych i aktualizacji oprogramowania.
- Dokumentacja techniczna starszych instalacji jest często niekompletna, nieaktualna lub niedostępna w formie cyfrowej, co utrudnia planowanie modernizacji.
- Koszty utrzymania starzejącej się infrastruktury rosną nieproporcjonalnie szybko w stosunku do wartości, jaką ta infrastruktura dostarcza.

Wzrost liczby urządzeń EAZ i złożoności systemu:

Równolegle do problemu starzenia się istniejących instalacji, w sieciach energetycznych gwałtownie rośnie liczba nowych urządzeń elektroenergetycznej automatyki zabezpieczeniowej (EAZ). Jest to efekt kilku nakładających się trendów:

- **Rozwój odnawialnych źródeł energii (OZE)** – przyłączanie farm wiatrowych, fotowoltaicznych i innych rozproszonych źródeł wytwarzania wymaga instalacji dodatkowych układów zabezpieczeniowych dostosowanych do specyfiki tych źródeł (m.in. ochrona przed wyspowaniem, zabezpieczenia interfejsu sieciowego).
- **Rozbudowa sieci dystrybucyjnych** – modernizacja i rozbudowa sieci średnich i niskich napięć, budowa nowych stacji transformatorowych oraz linie kablowe zastępujące napowietrzne generują potrzebę instalacji kolejnych urządzeń EAZ.
- **Elektromobilność i nowe obciążenia** – dynamiczny wzrost liczby stacji ładowania pojazdów elektrycznych oraz inne nowe kategorie odbiorników wprowadzają nowe wymagania w zakresie ochrony sieci.
- **Cyfryzacja stacji** – przejście na komunikację cyfrową (IEC 61850, magistrale procesowe) wiąże się z instalacją *merging units*, bram komunikacyjnych i innych urządzeń pośredniczących, które również wymagają nadzoru i zabezpieczenia.

Efektem jest sytuacja, w której operatorzy sieci muszą jednocześnie zarządzać starzejącą się infrastrukturą i obsługiwać rosnącą liczbę nowych urządzeń – przy niezmienionych lub nawet ograniczonych zasobach ludzkich i finansowych.

Tabela 1. Wyzwania systemu elektroenergetycznego

2.2. Nowe regulacje prawne i rosnące ryzyka - cyberbezpieczeństwo

Sektor energetyczny jest uznawany za infrastrukturę krytyczną, co sprawia, że podlega coraz bardziej rozbudowanym regulacjom prawnym – zarówno na poziomie krajowym, jak i unijnym. Jednocześnie dynamicznie zmienia się krajobraz zagrożeń, z jakimi muszą mierzyć się operatorzy sieci.

Nowe ramy regulacyjne:

Dyrektywa NIS2 (Network and Information Security Directive 2) nakłada na operatorów infrastruktury krytycznej, w tym energetycznej, obowiązek wdrożenia kompleksowych środków zarządzania ryzykiem cyberbezpieczeństwa, raportowania incydentów oraz zapewnienia ciągłości działania.

Rozporządzenie DORA (Digital Operational Resilience Act) – choć skierowane pierwotnie do sektora finansowego, wyznacza kierunek dla regulacji odporności cyfrowej w innych sektorach krytycznych.

Regulacje NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) – standardy obowiązujące w Ameryce Północnej, stanowiące punkt odniesienia dla regulacji europejskich w zakresie cyberbezpieczeństwa systemów sterowania i automatyki.

Krajowe regulacje – w Polsce ustawa o krajowym systemie cyberbezpieczeństwa oraz wymagania URE i PSE nakładają konkretne obowiązki na operatorów systemów elektroenergetycznych.

Spełnienie tych wymagań w środowisku złożonym z setek lub tysięcy różnorodnych urządzeń, działających na przestarzałych platformach z ograniczoną możliwością aktualizacji, stanowi poważne wyzwanie operacyjne i finansowe.

Cyberbezpieczeństwo jako nowa kategoria ryzyka:

Rosnąca łączność urządzeń EAZ z systemami nadrzędnymi (SCADA, EMS, systemy zarządzania majątkiem) oraz z sieciami korporacyjnymi zwiększa powierzchnię potencjalnych ataków.

Incydenty takie jak ataki na ukraińską sieć energetyczną (2015, 2016) czy atak ransomware na Colonial Pipeline (2021) pokazały, że infrastruktura energetyczna jest realnym celem dla cyberprzestępców i podmiotów państwowych.

Długi cykl życia urządzeń EAZ sprawia, że wiele z nich pracuje z oprogramowaniem, które nie było projektowane z myślą o współczesnych zagrożeniach i nie może być łatwo zaktualizowane.

Podatności w protokołach komunikacyjnych (np. starsze wersje protokołów przemysłowych bez mechanizmów uwierzytelniania) stanowią potencjalne wektory ataku.

Kluczowy wniosek: Zarządzanie cyberbezpieczeństwem w środowisku zróżnicowanych urządzeń EAZ wymaga nie tylko technicznych rozwiązań, ale także nowych procesów, procedur i kompetencji organizacyjnych.

2.3. Odchodzenie pracowników na emeryturę i złożoność procesów operacyjnych

Obok wyzwań technicznych i regulacyjnych, sektor energetyczny stoi przed poważnym wyzwaniem kadrowym, które w perspektywie najbliższych lat może stać się jednym z kluczowych ograniczeń operacyjnych.

Kryzys demograficzny w energetyce:

Znaczna część doświadczonych inżynierów i techników specjalizujących się w automatyce zabezpieczeniowej osiąga wiek emerytalny. Wiedza tych pracowników – często nieustrukturyzowana, przekazywana w formie praktycznego doświadczenia – jest trudna do skodyfikowania i przeniesienia na młodsze pokolenia.

Złożoność i specjalistyczny charakter systemów EAZ sprawiają, że wykształcenie nowego specjalisty wymaga wielu lat praktyki. Uczelnie techniczne nie zawsze nadążają z programami kształcenia dostosowanymi do szybko zmieniających się potrzeb sektora.

Konkurencja o wykwalifikowanych inżynierów ze strony innych sektorów (IT, telekomunikacja, przemysł) utrudnia pozyskiwanie i utrzymanie kompetentnych kadr.

W wielu organizacjach następuje utrata wiedzy instytucjonalnej – odchodzący pracownicy zabierają ze sobą znajomość nieudokumentowanych konfiguracji, nieformalnych procedur i historii decyzji projektowych.

Rosnąca złożoność procesów operacyjnych:

- **Heterogeniczność środowiska** – różne generacje urządzeń, różni producenci, różne protokoły komunikacyjne i interfejsy konfiguracyjne wymagają od operatorów utrzymywania szerokiej i zróżnicowanej wiedzy technicznej.
- **Złożone procedury testowe** – każda zmiana konfiguracji lub wymiana urządzenia wymaga przeprowadzenia szczegółowych testów odbiorczych, których zakres i pracochłonność rosną wraz ze złożonością systemu.
- **Zarządzanie dokumentacją** – utrzymywanie aktualnej, spójnej dokumentacji technicznej dla setek lub tysięcy urządzeń, schematów i konfiguracji jest zadaniem wymagającym znacznych nakładów pracy.
- **Koordynacja między działami** – procesy związane z zabezpieczeniami angażują wiele jednostek organizacyjnych (służby eksploatacyjne, IT, bezpieczeństwo, planowanie), co zwiększa ryzyko błędów wynikających z błędnej komunikacji i nieskoordynowanych działań.
- **Presja czasowa** – rosnące wymagania dotyczące czasu przywracania zasilania po awarii (regulowane wskaźnikami SAIDI/SAIFI) zwiększają presję na szybkie i bezbłędne działanie służb eksploatacyjnych.

Kluczowy wniosek: Wszystkie te wyzwania łącznie tworzą środowisko, w którym tradycyjne podejście do automatyki zabezpieczeniowej – oparte na dedykowanym sprzęcie, ręcznych procedurach i wiedzy ekspertów – przestaje być wystarczające. To właśnie w tym kontekście koncepcja *software-defined protection* nabiera szczególnego znaczenia jako odpowiedź na rzeczywiste potrzeby operacyjne sektora energetycznego.

3. Tradycyjna struktura automatyki zabezpieczeniowej

3.1. Sprzętowe sieci przekaźnikowe

Klasyczne systemy zabezpieczeń opierały się na sprzętowych przekaźnikach, w których każda funkcja ochronna – nadprądowa, różnicowa, odległościowa czy częstotliwościowa – była realizowana w dedykowanym module.

Charakterystyczne cechy tego podejścia: ścisłe powiązanie algorytmów zabezpieczeniowych z konkretną platformą sprzętową, ograniczona możliwość modyfikacji logiki działania i parametrów poza zakresem przewidzianym przez producenta, konieczność fizycznej wymiany urządzenia lub jego części przy wprowadzaniu istotnych zmian funkcjonalnych.

W praktyce oznaczało to, że cykl życia funkcji zabezpieczeniowej był nierozerwalnie związany z cyklem życia samego przekaźnika.

3.2. Ograniczenia tradycyjnego podejścia

Choć klasyczne rozwiązania przekaźnikowe zapewniały wysoki poziom niezawodności, w obliczu współczesnych wymagań ujawniło się szereg ich ograniczeń.

Niski poziom elastyczności

- Każda modyfikacja funkcji zabezpieczeniowej, dodanie nowego algorytmu lub obsługa nowych protokołów komunikacyjnych wymagały modyfikacji oprogramowania układowego (firmware).
- Często konieczna była fizyczna wymiana urządzeń lub ich gruntowna modernizacja, co wiązało się z wyłączeniami i długotrwałymi testami.

Wysokie koszty eksploatacji

- Duża różnorodność typów i modeli przekaźników w jednej stacji wymuszała utrzymywanie szerokiego asortymentu części zamiennych.
- Złożone i czasochłonne procedury testowe oraz odbiorowe zwiększały nakłady pracy technicznej.
- Różne generacje urządzeń i interfejsów utrudniały standaryzację i automatyzację procesów serwisowych.

Wyzwania związane z cyberbezpieczeństwem

- Aktualizacje firmware'u były wykonywane rzadko i często wymagały planowanych wyłączeń oraz obecności personelu na miejscu.
- Długie odstępy między aktualizacjami powiększały lukę bezpieczeństwa wobec dynamicznie rozwijających się zagrożeń cybernetycznych.
- Ryzyko błędów podczas ręcznych aktualizacji mogło negatywnie wpływać na ciągłość ochrony.

4. Koncepcja software-defined protection

W odpowiedzi na ograniczenia tradycyjnych systemów pojawiła się koncepcja *software-defined protection* (SDP)–automatyki zabezpieczeniowej, w której kluczową rolę odgrywa oprogramowanie, a logika zabezpieczeniowa jest w znacznym stopniu niezależna od konkretnej platformy sprzętowej.

Istota podejścia SDP polega na:

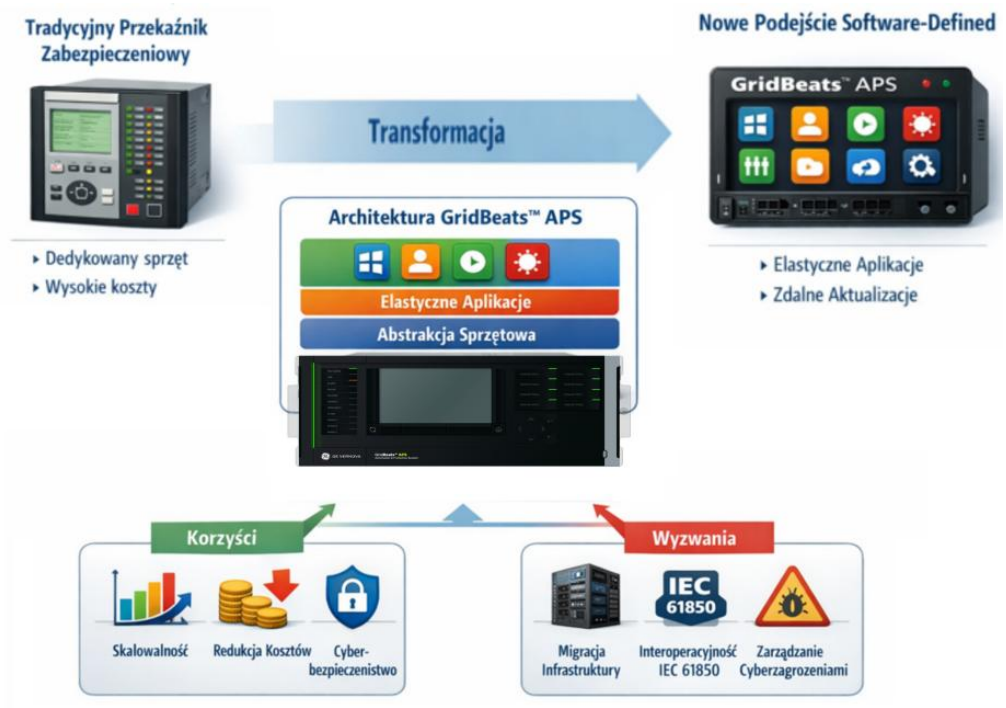
- uniezależnieniu aplikacji zabezpieczeniowych od konkretnego modelu przekaźnika,
- przeniesieniu części inteligencji z warstwy sprzętowej do warstwy programowej,
- umożliwieniu wdrażania i aktualizacji funkcji zabezpieczeniowych poprzez zmiany w oprogramowaniu, bez konieczności wymiany urządzeń.

Taka zmiana paradygmatu – od funkcji sprzętowo zorientowanych do architektury definiowanej programowo – otwiera drogę do:

- większej elastyczności konfiguracji i modyfikacji systemu,
- skrócenia czasu wdrożenia nowych rozwiązań,
- lepszej integracji z zaawansowanymi narzędziami analitycznymi i systemami nadrzędnymi,
- wdrożenia strategii cyberbezpieczeństwa w sposób spójny i centralnie zarządzany.

5. Koncepcja software-defined protection

Poniższy schemat ilustruje przejście od tradycyjnego przekaźnika zabezpieczeniowego do nowego podejścia *software-defined* oraz miejsce systemu GridBeats™ APS w tej transformacji.



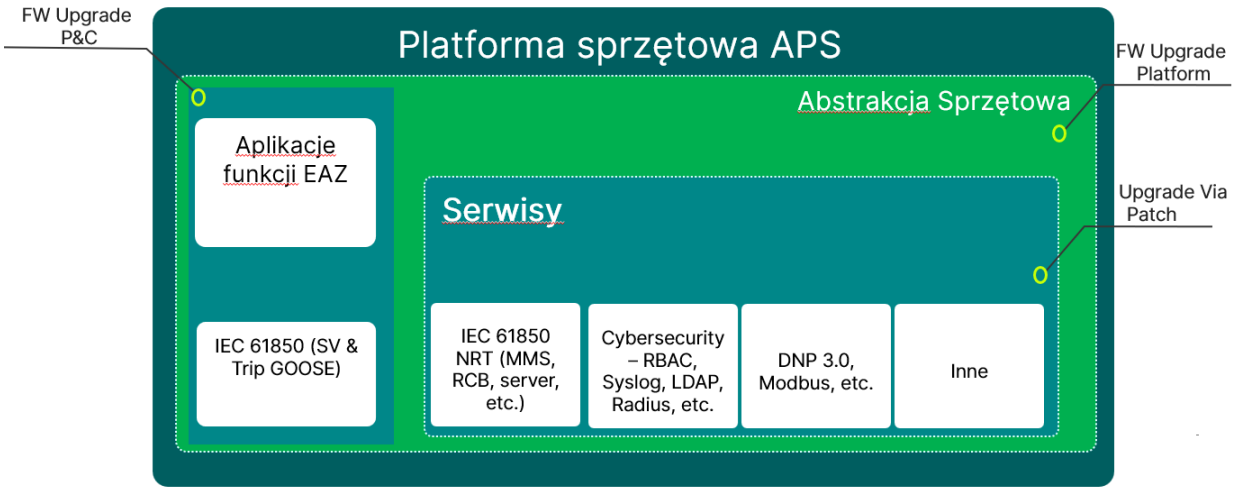
Rys. 1. Transformacja

Schemat przedstawia:

- **po lewej** – tradycyjny przekaźnik zabezpieczeniowy oparty na dedykowanym sprzęcie, charakteryzujący się ograniczoną elastycznością i wysokimi kosztami utrzymania,
- **po prawej** – nowe podejście *software-defined* z systemem GridBeats™ APS, umożliwiające uruchamianie niezależnych aplikacji na jednej platformie sprzętowej oraz wykonywanie zdalnych aktualizacji,
- **poniżej** – architekturę GridBeats™ APS z abstrakcją sprzętową i elastycznymi aplikacjami, a także obszary korzyści (skalowalność, redukcja kosztów, cyberbezpieczeństwo) oraz wyzwań (migracja infrastruktury, interoperacyjność IEC 61850, zarządzanie cyberzagrożeniami).

6. GridBeats™ - przykład nowej generacji automatyki zabezpieczeniowej

Jednym z przykładów praktycznego wdrożenia podejścia *software-defined* w automatyce stacyjnej jest GridBeats™ APS (Automation & Protection System) – rozwiązanie z portfolio oprogramowania GridBeats™ firmy GE Vernova. System ten redefiniuje klasyczne podejście do zabezpieczeń i sterowania w stacjach, łącząc funkcje ochronne, komunikacyjne i cyberbezpieczeństwa w ramach jednej, spójnej platformy.



Rys. 2. Struktura systemu GridBeats™ APS

6.1. Architektura i kluczowe cechy

Separacja aplikacji od sprzętu

GridBeats™ APS umożliwia oddzielenie aplikacji typu *Protection & Control* (P&C) od fizycznej warstwy przekaźnika. W praktyce oznacza to, że:

- różne funkcje – ochrona, komunikacja, cyberbezpieczeństwo, monitorowanie – mogą być uruchamiane na jednej, wspólnej platformie urządzenia,
- ten sam sprzęt może obsługiwać różne zestawy funkcji w zależności od konfiguracji oprogramowania,
- rola sprzętu ewoluuje w kierunku uniwersalnej platformy wykonawczej.

Technologia abstrakcji sprzętowej

Dzięki opatentowanej technologii abstrakcji sprzętowej:

- możliwe jest uruchamianie wielu aplikacji na jednym urządzeniu,
- aktualizacje oraz rozbudowa funkcjonalności odbywają się bez fizycznej ingerencji w warstwę sprzętową,
- ustandaryzowane interfejsy między oprogramowaniem a sprzętem upraszczają integrację i migrację.

Niezależność warstwy aplikacyjnej od firmware'u platformy

Kluczowe elementy funkcjonalne są odseparowane od *firmware*'u platformy:

- aktualizacje dotyczące komunikacji (np. nowe protokoły, kolejne wersje standardów) oraz bezpieczeństwa (np. łatanie podatności, nowe mechanizmy uwierzytelniania) mogą być wprowadzane bez naruszania podstawowych algorytmów zabezpieczeniowych,
- ogranicza to konieczność przeprowadzania pełnego, powtarzanego testowania algorytmów P&C po każdej zmianie w warstwie systemowej,
- zwiększa stabilność i przewidywalność działania całego systemu.

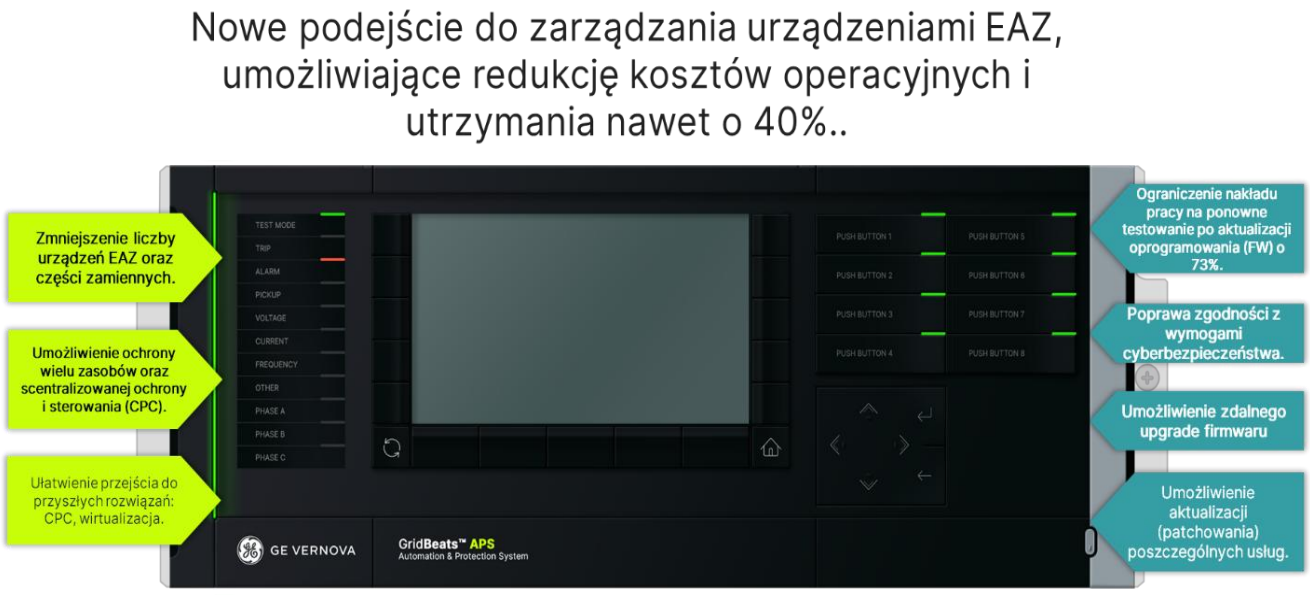
6.2. Korzyści operacyjne

Obszar korzyści	Tradycyjne podejście	GridBeats™ APS (software-defined)
Elastyczność	**Zmiany wymagają wymiany sprzętu**	**Zmiany przez aktualizację oprogramowania**
Aktualizacje bezpieczeństwa	**Zwykle wymagają wyłączeń**	**Zdalne, bez przerywania pracy**
Różnorodność sprzętu	**Wiele typów urządzeń**	**Jedna ujednolicona platforma**
Szkolenia personelu	**Wiele platform – złożone szkolenia**	**Jedno środowisko – uproszczone szkolenia**
Koszty eksploatacji	**Wysokie – duży asortyment części**	**Niższe – ujednolicony sprzęt i procedury**
Czas wdrożenia zmian	**Długi – testy po każdej zmianie sprzętu**	**Krótki – separacja warstw ogranicza retesty**

Tabela. 2. Korzyści operacyjne

Odpowiedź na wyzwania kadrowe

- Ujednolicone środowisko programowe obniża próg wejścia dla nowych pracowników – zamiast znajomości dziesiątek różnych platform sprzętowych wystarczy opanowanie jednego, spójnego środowiska.
- Narzędzia do zdalnego zarządzania i monitorowania zmniejszają potrzebę częstych wizyt serwisowych w terenie, co pozwala efektywniej wykorzystać ograniczone zasoby ludzkie.
- Automatyzacja procesów konfiguracyjnych i testowych redukuje zależność od wiedzy eksperckiej i ogranicza ryzyko błędów wynikających z czynnika ludzkiego.



Rys. 3. Korzyści operacyjne

7. Perspektywy rozwoju automatyki zabezpieczeniowej

7.1. Nowe modele architektur sieciowych

Przejście do platformy *software-defined* otwiera drogę do coraz bardziej zaawansowanych modeli realizacji funkcji P&C:

- **Częściowa lub pełna centralizacja logiki zabezpieczeniowej** – część funkcji może być realizowana w sposób rozproszony (bliżej pola), a część – w jednostkach centralnych, z wykorzystaniem szybkich i niezawodnych kanałów komunikacyjnych.
- **Ścisła integracja z narzędziami analitycznymi** – dane z systemów zabezpieczeń mogą być przekazywane w czasie zbliżonym do rzeczywistego do platform analitycznych wspierających diagnostykę, prognozowanie awarii i optymalizację pracy sieci.
- **Adaptacyjność sieci** – możliwość dynamicznej zmiany parametrów i algorytmów zabezpieczeń w odpowiedzi na aktualny stan systemu (np. zmienne warunki pracy, wysoki udział OZE, zmiany topologii).
- **Zwiększona odporność na zakłócenia cyber-fizyczne** – dzięki spójnemu zarządzaniu oprogramowaniem, mechanizmami bezpieczeństwa i monitorowaniem integralności systemu.

W dłuższej perspektywie ewolucja w kierunku *software-defined* sprzyja budowie „inteligentnych" stacji, które mogą być łatwiej integrowane z koncepcją sieci inteligentnych (*smart grids*) i systemami zarządzania zasobami rozproszonymi (DER).

8. Wyzwania i kierunki dalszego rozwoju

Pomimo znaczących korzyści, wdrażanie systemów zabezpieczeń definiowanych programowo wiąże się z nowymi wyzwaniami.

Migracja istniejącej infrastruktury

- Znaczna część infrastruktury pracuje w oparciu o tradycyjne przekaźniki; przejście do nowej architektury wymaga starannego planowania, etapowania i testów.
- Konieczne jest zapewnienie kompatybilności nowych rozwiązań z istniejącymi systemami, zarówno na poziomie technicznym, jak i organizacyjnym (procedury, kompetencje personelu).

Interoperacyjność i akceptacja standardów

- Kluczową rolę odgrywa wsparcie dla międzynarodowych standardów, takich jak IEC 61850, które ułatwiają integrację urządzeń różnych producentów.
- Interoperacyjność staje się warunkiem nie tylko wymiany danych, ale także spójnego zarządzania funkcjami P&C w złożonym środowisku wielodostawczym.

Niezbędna jest współpraca producentów, operatorów i organizacji standaryzacyjnych na rzecz wypracowania wspólnych modeli i najlepszych praktyk

Bezpieczeństwo cybernetyczne

- Wzrost roli oprogramowania i łączności sieciowej zwiększa powierzchnię potencjalnych ataków.
- Wymagane są zaawansowane strategie ochrony, obejmujące m.in. segmentację sieci, uwierzytelnianie, szyfrowanie oraz zarządzanie tożsamością i uprawnieniami.
- Kluczowe znaczenie ma ciągłe monitorowanie, szybka reakcja na incydenty oraz regularne aktualizacje zabezpieczeń – przy jednoczesnym zachowaniu stabilności funkcji ochronnych.

Dalszy rozwój będzie prawdopodobnie obejmował:

- większą automatyzację testów i walidacji oprogramowania zabezpieczeniowego,
- wykorzystanie sztucznej inteligencji i uczenia maszynowego do wykrywania anomalii oraz wsparcia decyzji operatorów,
- rozwój modeli typu *protection as a service*, w których część funkcji jest dostarczana i zarządzana centralnie.

9. Podsumowanie

Automatyka zabezpieczeniowa stacji energetycznych przechodzi głęboką transformację – od klasycznych, sprzętowo zorientowanych rozwiązań do elastycznych, programowo definiowanych platform. U źródeł tej transformacji leżą rzeczywiste, pilne wyzwania: starzejąca się infrastruktura i rosnąca liczba urządzeń EAZ, zaostrzające się regulacje i nowe zagrożenia cybernetyczne oraz presja demograficzna wynikająca z odchodzenia doświadczonych specjalistów na emeryturę.

Koncepcja *software-defined protection* pozwala uniezależnić funkcje zabezpieczeniowe od konkretnego sprzętu, przyspieszyć wdrażanie innowacji oraz skuteczniej odpowiadać na rosnące wymagania w zakresie niezawodności, skalowalności i cyberbezpieczeństwa.

Rozwiązania takie jak GridBeats™ APS firmy GE Vernova pokazują, że możliwe jest połączenie:

- wysokiej elastyczności konfiguracji,
- uproszczonej architektury sprzętowej,
- zaawansowanych mechanizmów bezpieczeństwa,
- narzędzi ułatwiających pracę w warunkach ograniczonych zasobów kadrowych,

bez kompromisów w zakresie jakości i niezawodności działania zabezpieczeń. Ewolucja w kierunku systemów definiowanych programowo staje się jednym z kluczowych kierunków rozwoju automatyki stacyjnej i – szerzej – nowoczesnych sieci elektroenergetycznych.

Literatura

[1] IEC 61850: Communication networks and systems for power utility automation, International Electrotechnical Commission.

[2] IEEE Power System Relaying Committee, IEEE Guide for Protective Relay Applications to Transmission Lines, IEEE Std C37.113.

[3] G. Ziegler, Numerical Distance Protection: Principles and Applications, Publicis Publishing.

[4] P. M. Anderson, Power System Protection, Wiley-IEEE Press.

[5] ENTSO-E, Cybersecurity for Power System Operations, ENTSO-E Report.

[6] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS2).

[7] NERC CIP Standards, Critical Infrastructure Protection, North American Electric Reliability Corporation.

[8] Materiały produktowe GE Vernova – Grid Automation & Grid Software (GridBeats™ APS, broszury i karty katalogowe). Dostępne: https://*gevernova.com/grid-solutions/gridbeats/gridbeats-aps*