**Tomasz Grudniewski**[1]
Akademia Bialska im. Jana Pawła II, Biała Podlaska

https://doi.org/10.29316/9788368103373_14

# BEZPIECZEŃSTWO ENERGETYCZNE PAŃSTWA W ERZE DECENTRALIZACJI DOSTAW

## NATIONAL ENERGY SECURITY IN THE ERA OF DECENTRALISED SUPPLIES

**Streszczenie**

Bezpieczeństwo energetyczne państwa coraz silniej zależy od zdolności systemu elektroenergetycznego do integrowania rozproszonych źródeł energii (distributed energy resources – DER), elastyczności popytu oraz magazynów energii w warunkach rosnącej zmienności generacji i narastających ryzyk zakłóceniowych. Wirtualne elektrownie (Virtual Power Plants – VPP) stanowią warstwę agregacji i koordynacji wielu rozproszonych zasobów, umożliwiając ich udział w rynkach energii oraz świadczenie usług systemowych. W rozdziale przedstawiono ramy analityczne łączące wymiary bezpieczeństwa energetycznego (4A: availability, accessibility, affordability, acceptability) oraz odporność (resilience) z architekturą VPP i warstwami ICT (HEMS/EMS, DERMS, ADMS/SCADA, EMS/TSO). Zastosowano ustrukturyzowany przegląd literatury (2018-2026) oraz mapowanie funkcji VPP na mechanizmy wpływu na bezpieczeństwo energetyczne, uzupełnione perspektywą cyberbezpieczeństwa DER. Wynikiem jest (1) typologia mechanizmów

[1] https://doi.org/0000-0003-3394-8992 , e-mail: gisbourne2@gmail.com

wzmacniania bezpieczeństwa przez VPP, (2) propozycja zestawu wskaźników KPI oraz procesu oceny wkładu VPP w bezpieczeństwo energetyczne i (3) rekomendacje wdrożeniowe akcentujące interoperacyjność danych, koordynację DSO-TSO, pomiar i weryfikację (M&V) oraz podejście security-by-design. Wykazano, że VPP może wzmacniać adekwatność mocy, stabilność operacyjną i przystępność cenową, ale jednocześnie wprowadza zależności cyfrowe, które muszą być zarządzane jako element bezpieczeństwa dostaw.

**Słowa kluczowe:** bezpieczeństwo energetyczne, wirtualna elektrownia, agregacja DER, elastyczność, DERMS, ADMS, cyberodporność, zarządzanie popytem

**Abstract**

A country's energy security increasingly depends on its power system's ability to integrate distributed energy resources (DER), demand flexibility, and energy storage in the face of growing generation variability and increasing disruption risks. Virtual power plants (VPPs) provide a layer of aggregation and coordination for multiple distributed resources, enabling them to participate in energy markets and provide system services. The article author presents the dimensions of energy security (4A: availability, accessibility, affordability, acceptability) and resilience with the VPP architecture and ICT layers (HEMS/EMS, DERMS, ADMS/SCADA, EMS/TSO). A structured literature review (2018-2026) and mapping of VPP functions to mechanisms influencing energy security, supplemented by a DER cybersecurity perspective, were used. The result is (1) a typology of mechanisms for strengthening security through VPPs, (2) a proposal for a set of KPIs and a process for assessing the contribution of VPPs to energy security, and (3) implementation recommendations emphasising data interoperability, DSO-TSO coordination, measurement and verification (M&V), and a security-by-design approach. It has been shown that VPPs can enhance capacity adequacy, operational stability, and affordability, but at the same time introduce digital dependencies that must be managed as part of security of supply.

**Keywords:** energy security, virtual power plant, DER aggregation, flexibility, DERMS, ADMS, cyber resilience, demand management

## Wstęp

Bezpieczeństwo energetyczne jest pojęciem wielowymiarowym i silnie zależnym od kontekstu technologicznego, gospodarczego i instytucjonalnego. W literaturze często przywołuje się podejście „4A" – availability (dostępność), accessibility (dostęp), affordability (przystępność cenowa)

i acceptability (akceptowalność środowiskowo-społeczna) – jako podstawę budowy wskaźników i ram oceny (Siksnelyte-Butkiene i in., 2024). Współczesne ujęcia podkreślają jednak, że same „4A" nie domykają problemu, ponieważ rośnie znaczenie odporności (resilience), rozumianej jako zdolność systemu do absorpcji zakłóceń, adaptacji oraz odtworzenia funkcji krytycznych (Schmitz i in., 2025). Transformacja elektroenergetyki – wzrost udziału OZE, elektryfikacja transportu i ciepłownictwa, rozwój prosumeryzmu, magazynów i ładowania pojazdów elektrycznych – przenosi ciężar bezpieczeństwa z dużych, sterowalnych jednostek wytwórczych na zdolność systemu do elastycznego bilansowania i koordynacji zasobów rozproszonych. Wysoka zmienność generacji i popytu zwiększa wartość prognozowania, automatyzacji i zarządzania w czasie rzeczywistym, co oznacza, że bezpieczeństwo energetyczne państwa staje się w coraz większym stopniu „cyfrowe" (data-driven). Przeglądy dotyczące zastosowań AI i IoT w programach demand response wskazują, że cyfryzacja poprawia zdolność do predykcji i sterowania, ale równocześnie wymaga dojrzałego zarządzania jakością danych i cyberochrony (Algburi i in., 2025).

Wirtualna elektrownia (VPP) jest jednym z kluczowych rozwiązań organizacyjno-technicznych w tym krajobrazie. W sensie funkcjonalnym VPP agreguje heterogeniczne zasoby DER (generacja rozproszona, magazyny, pojazdy elektryczne, elastyczne obciążenia) i koordynuje je tak, aby zachowywały się jak jedna jednostka zdolna do: (a) sprzedaży energii (rynki day-ahead/intraday), (b) świadczenia usług bilansujących i rezerw, oraz (c) wsparcia pracy sieci (np. zarządzania ograniczeniami i redukcji curtailmentu OZE). Przeglądy pokazują jednocześnie szybkie dojrzewanie modeli VPP: rośnie zakres rynków, stopień automatyzacji, a także nacisk na wykonalność praktyczną, interoperacyjność i skalowalność (Esfahani i in., 2025; Roozbehani i in., 2022; Zare, Shafiyi, 2025). Jednocześnie VPP – jako platforma cyfrowa sterująca potencjalnie tysiącami urządzeń – zwiększa zależność systemu elektroenergetycznego od warstwy ICT oraz powiększa powierzchnię ataku. Koordynacja DER wymaga telemetrii, kanałów sterowania i integracji API w architekturze wielostronnej (agregator, operator, dostawcy technologii, właściciele urządzeń). Przeglądy cyberbezpieczeństwa DER podkreślają, że rosnąca skala i heterogeniczność urządzeń wprowadzają ryzyka fałszowania danych (false data injection), przejęć sterowania, a także

kaskadowych konsekwencji incydentów w systemie fizycznym (Chen i in., 2025; Hasan i in., 2022). W tym sensie VPP, choć wzmacnia elastyczność i odporność operacyjną, jednocześnie wymusza systemowe podejście do cyberodporności jako warunku bezpieczeństwa dostaw (Leszczyna, 2018).

## Problem badawczy i cel

W literaturze VPP dominują dwa nurty: (1) modelowanie i optymalizacja udziału w rynkach (strategie ofertowania, zarządzanie niepewnością, value stacking) oraz (2) metody sterowania i integracji DER (architektury scentralizowane i zdecentralizowane). Mniej prac łączy te zagadnienia z wymiarami bezpieczeństwa energetycznego państwa w sposób operacjonalizowany (KPI, proces oceny, warunki brzegowe wdrożenia), szczególnie z uwzględnieniem cyberodporności jako integralnej części bezpieczeństwa dostaw. Równolegle literatura o systemach zarządzania DER (HEMS/EMS, DERMS, ADMS/SCADA) bywa analizowana „w oderwaniu" od ram bezpieczeństwa energetycznego.

Celem rozdziału jest: (1) zaproponowanie ram analitycznych łączących wymiary bezpieczeństwa energetycznego z architekturą VPP i systemami ICT, (2) zmapowanie funkcji VPP oraz warstw informatycznych na mechanizmy wzmacniania bezpieczeństwa, (3) zaproponowanie zestawu KPI i procesu oceny wkładu VPP w bezpieczeństwo energetyczne państwa z uwzględnieniem cyberryzyk. Pytania badawcze sformułowano następująco:
RQ1 – które mechanizmy VPP najsilniej wspierają poszczególne wymiary 4A + odporność?
RQ2 – jakie warstwy ICT (HEMS/EMS, DERMS, ADMS/SCADA, EMS/TSO) są krytyczne dla bezpiecznego skalowania VPP?
RQ3 – jakie ryzyka cyberfizyczne towarzyszą VPP i jak włączyć je do oceny bezpieczeństwa energetycznego?

## Metody

## Projekt badania

Zastosowano podejście mieszane: ustrukturyzowany przegląd literatury (scoping review) oraz analizę konceptualną opartą na mapowaniu funkcji i zależności. Przyjęto, że dla oceny bezpieczeństwa energetycznego

państwa istotna jest nie tylko poprawność modeli optymalizacyjnych VPP, lecz także zdolność do skalowania, interoperacyjności, weryfikowalności (measurement & verification – M&V) i odporności na ryzyka (w tym cybernetyczne). Z tego powodu analizą objęto prace z trzech obszarów: (a) VPP i agregacja DER, (b) systemy zarządzania zasobami rozproszonymi po stronie operatorów (DERMS/ADMS/EMS), (c) cyberbezpieczeństwo DER i systemów smart grid.

## Dobór literatury i kryteria włączenia

Publikacje identyfikowano dla lat 2018-2026, ze szczególnym naciskiem na prace po 2021 r. Włączano materiały spełniające łącznie kryteria: (a) bezpośrednie odniesienie do VPP, agregacji DER, elastyczności, DERMS/ADMS/EMS lub cyberbezpieczeństwa DER, (b) możliwość powiązania z co najmniej jednym wymiarem bezpieczeństwa energetycznego (4A, resilience/cyber), (c) dostępny identyfikator DOI. Wykluczano publikacje bez DOI, czysto opisowe bez implikacji dla funkcji systemu lub niewystarczająco związane z elektroenergetyką.

## Procedura analityczna

Dla każdej publikacji kodowano: (1) wymiar bezpieczeństwa energetycznego (availability, accessibility, affordability, acceptability, resilience/cyber), (2) funkcje VPP (prognozowanie, optymalizacja, dyspozycja, udział w rynkach, usługi systemowe, M&V), (3) warstwę systemów ICT (HEMS/EMS, DERMS, ADMS/SCADA, EMS/TSO), (4) typ ryzyka i środki kontroli (np. szyfrowanie, uwierzytelnianie, segmentacja, monitoring, ocena ryzyka). Następnie przeprowadzono syntezę tematyczną i opracowano mapowanie mechanizmów (Tabela 1) oraz porównanie warstw ICT (Tabela 2), a także dwa schematy koncepcyjne (Rysunki 1-2).

## Wyniki

## Mechanizmy, przez które VPP wzmacniają bezpieczeństwo energetyczne

Synteza literatury pozwala wyróżnić sześć klas mechanizmów łączących funkcje VPP i systemów ICT z bezpieczeństwem energetycznym państwa.

1. Adekwatność mocy i bilansowanie (availability). VPP zwiększa „efektywną" dyspozycyjność poprzez agregację wielu małych jednostek i zasobów elastyczności. Kluczowa jest zdolność sterowania w krótkim horyzoncie: strategie agregacji i dyspozycji w czasie rzeczywistym podnoszą zdolność regulacyjną i elastyczność VPP (Liu i in., 2024). Dla państwa oznacza to potencjał redukcji ryzyka niedoborów mocy w sytuacjach krytycznych – pod warunkiem, że elastyczność jest kontraktowalna, dostępna i zweryfikowana (M&V).
2. Usługi systemowe i stabilność (frequency/voltage). Integracja magazynów i elastycznych obciążeń umożliwia świadczenie usług regulacji częstotliwości i rezerw, a w pewnych konfiguracjach także wsparcie parametrów lokalnych (napięcia, przeciążenia). Przykładowo, mechanizmy zdecentralizowane mogą ograniczać zależność od jednego centrum sterowania oraz zmniejszać wąskie gardła obliczeniowe, co sprzyja odporności operacyjnej, pokazują to m.in. prace dotyczące zdecentralizowanego świadczenia regulacji częstotliwości przez VPP (Sun i in., 2023).
3. Redukcja kosztów i ryzyk cenowych (affordability). VPP umożliwia optymalizację portfela zasobów w wielu segmentach rynku („value stacking") oraz ograniczanie kosztów bilansowania i rezerw przez wykorzystanie elastyczności. Przeglądy VPP akcentują, że nowoczesne modele obejmują coraz szerszy zakres rynków i usług oraz łączą cele ekonomiczne z ograniczeniami technicznymi (Esfahani i in., 2025; Zare, Shafiyi, 2025). Dla państwa efekt jest pośredni: niższe koszty systemowe mogą stabilizować ceny energii i zmniejszać ekspozycję gospodarki na szoki, ale wymaga to poprawnego projektowania bodźców i zasad rozliczeń.
4. Dywersyfikacja i dostęp (accessibility). Agregacja rozproszona zmniejsza koncentrację ryzyka w pojedynczych punktach i technologiach. VPP może koordynować zasoby prosumenckie i lokalne magazyny, zwiększając udział energii lokalnej w bilansie oraz umożliwiając priorytetyzację odbiorów w sytuacjach kryzysowych (np. utrzymanie zasilania infrastruktury krytycznej na poziomie dystrybucji). W tym wymiarze krytyczne są rejestry zasobów, mechanizmy kwalifikacji urządzeń, a także integracja z DERMS, które „pilnuje" ograniczeń sieci.

5. Akceptowalność transformacji (acceptability). VPP ułatwia integrację OZE poprzez sterowanie popytem, magazyny i redukcję kosztów zmienności. Ograniczenie redukcji generacji OZE (curtailment) oraz poprawa wykorzystania lokalnych zasobów mogą zmniejszać potrzebę utrzymywania wysokoemisyjnych rezerw i ograniczać koszty społeczne transformacji. W ujęciu bezpieczeństwa energetycznego oznacza to jednoczesne wsparcie celów środowiskowych i kosztowych. W praktyce mechanizm ten jest wzmacniany przez narzędzia prognozowania i optymalizacji, które – jak wskazują przeglądy AI/IoT w DR – stają się coraz bardziej dostępne, ale wymagają nadzoru jakości danych i cyberochrony (Algburi i in., 2025).
6. Odporność i cyberbezpieczeństwo (resilience/cyber). Cyfrowa koordynacja zasobów zwiększa możliwości reagowania na zakłócenia (rekonfiguracja portfela, aktywacja DR, przejście w tryby awaryjne), ale jednocześnie powiększa powierzchnię ataku: urządzenia IoT i firmware, kanały łączności, interfejsy API, protokoły OT/IT, a także zależności w łańcuchu dostaw oprogramowania. Wzrost skali VPP oznacza, że incydent cybernetyczny może mieć konsekwencje systemowe, dlatego cyberodporność musi być traktowana jako część bezpieczeństwa dostaw (Schmitz i in., 2025). Przeglądy cyberbezpieczeństwa DER identyfikują zestaw środków obrony: segmentację stref OT/IT, zarządzanie tożsamością i uprawnieniami (IAM), szyfrowanie i uwierzytelnianie komunikacji, monitoring (SOC/IDS) oraz procedury reagowania na incydenty, uwzględniające współdziałanie wielu interesariuszy (Chen i in., 2025; Hasan i in., 2022). Ramy i standardy sektorowe stanowią w tym kontekście „szkielet" wymagań bezpieczeństwa (Leszczyna, 2018; Ustun, 2022), a adaptacje kryteriów oceny ryzyka do środowisk VPP są rozwijane także w pracach dotyczących oceny ryzyka dla wirtualnych elektrowni (Gkoktsis i in., 2023).

Poniżej (Tabela 1) przedstawiono mapę: wymiary bezpieczeństwa energetycznego, mechanizmy VPP/ICT oraz przykładowe KPI.

**Tabela 1.** Mapowanie wymiarów bezpieczeństwa energetycznego na funkcje VPP i systemów ICT

| Wymiar bezpieczeństwa | Przykładowe ryzyko systemowe | Mechanizmy VPP (funkcje) | Warstwa ICT (przykłady) | Przykładowe KPI do oceny |
|---|---|---|---|---|
| Dostępność / adekwatność (availability) | Niedobór mocy, wysoki EENS/ LOLE, ograniczenia bilansowania | Agregacja DER, prognozy, optymalizacja portfela, dispatch w RT, rezerwy | Platforma VPP, integracja z EMS/TSO, DERMS/ADMS | LOLE, EENS, margines rezerw, dostępna elastyczność (MW/MWh), ramp rate (MW/ min), niezawodność aktywacji (%) |
| Stabilność operacyjna (frequency/voltage) | Odchylenia f/U, przeciążenia, ograniczenia OZE | Usługi regulacyjne, sterowanie magazynem i obciążeniem, lokalne wsparcie napięcia | ADMS/SCADA, DERMS, VPP | Czas i liczba naruszeń limitów f/U, wolumen usług pomocniczych, redukcja curtailment, liczba interwencji DSO |
| Przystępność cenowa (affordability) | Zmienność cen, koszty bilansowania, ubóstwo energetyczne | Value stacking, DR, arbitraż magazynem, optymalizacja kosztów | EMS/HEMS, VPP, rozliczenia/M&V | Koszt bilansowania i rezerw, zmienność cen (quantyle), koszty krańcowe elastyczności, oszczędność u odbiorców |
| Dostęp i dywersyfikacja (accessibility) | Zależność importowa, awarie punktów, wąskie gardła | Rozproszenie zasobów, lokalne bilansowanie, priorytetyzacja odbiorów | DERMS/ADMS, HEMS, rejestry | Udział energii lokalnej, dywersyfikacja portfela (HHI), czas przywrócenia, liczba krytycznych węzłów |
| Akceptowalność (acceptability) | Emisyjność rezerw, konflikty środowiskowe | Integracja OZE, redukcja emisji, ograniczenie pracy źródeł szczytowych | EMS/planowanie, analityka VPP | Emisje CO2e (kg/MWh), redukcja curtailment OZE, odsetek odbiorców w DR, proxy jakości powietrza |
| Odporność i cyber (resilience/cyber) | Blackout, incydent cyber, awaria łączności, manipulacja danymi | Rekonfiguracja portfela, tryby awaryjne, monitoring, M&V | SOC/monitoring, IAM, segmentacja, IDS, audyty | MTTR/MTBF usług cyfrowych, czas detekcji/reakcji, liczba incydentów, zgodność ze standardami, dostępność łączności |

Źródło: opracowanie własne.

## Warstwy informatyczne zarządzania a VPP: rola DERMS i ADMS

VPP nie działa w próżni: jej bezpieczeństwo i użyteczność zależą od integracji z warstwami sterowania i danych po stronie odbiorców (HEMS/EMS), operatorów dystrybucyjnych (DERMS + ADMS/SCADA) i operatora przesyłowego (EMS/TSO). W praktyce DERMS pełni rolę „tłumacza" między światem zasobów rozproszonych a wymaganiami bezpiecznej pracy sieci: łączy rejestr zasobów, obserwację stanu, zarządzanie ograniczeniami, a także interfejsy do agregatorów/VPP (Strezoski, 2023). ADMS/SCADA dostarcza obraz stanu sieci i narzędzia automatyki (np. rekonfiguracja), ważne dla odtwarzania zasilania.

Z perspektywy bezpieczeństwa energetycznego (Tabela 2) kluczowe są trzy konsekwencje tej architektury. Po pierwsze, aktywacja usług przez VPP musi uwzględniać ograniczenia sieci dystrybucyjnej (constraints), w przeciwnym razie elastyczność może generować lokalne ryzyka. Po drugie, parametry telemetrii i sterowania (czas reakcji, rozdzielczość danych, dostępność łączności) stają się elementem krytycznymi dla niezawodności usług. Po trzecie, integracja danych i interfejsów oznacza nowe wektory ataku, dlatego minimalne wymagania cyberbezpieczeństwa powinny obejmować cały łańcuch (urządzenia, łączność, VPP, integracje z DSO/TSO).

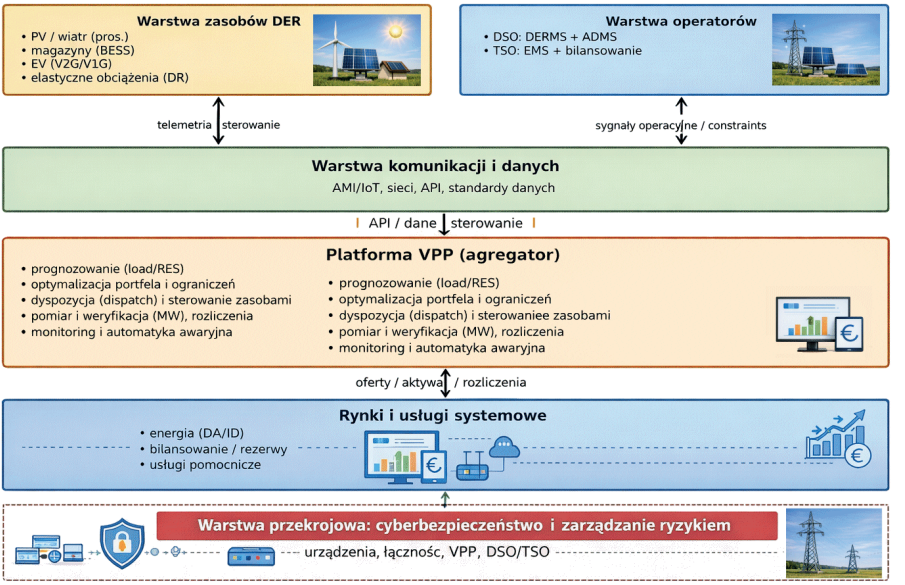
**Tabela 2.** Porównanie funkcji warstw ICT istotnych dla VPP i bezpieczeństwa energetycznego

| Warstwa/system | Główny cel | Horyzont sterowania | Dane wejściowe (przykłady) | Kluczowe punkty integracji | Typowe ryzyka i kontrole |
|---|---|---|---|---|---|
| HEMS/EMS (budynek/zakład) | Optymalizacja lokalna (koszt/komfort), sterowanie urządzeniami | sekundy-godziny | smart meter, czujniki, taryfy, prognoza PV, stan magazynu/EV | integracja z VPP (API), lokalna automatyka | prywatność, błędy sterowania, uwierzytelnianie, aktualizacje, segmentacja sieci lokalnej |
| Platforma VPP (agregator) | Agregacja, prognozowanie, optymalizacja, udział w rynkach/usługach | minuty-dni | profile zasobów, prognozy, ograniczenia, ceny, sygnały TSO/DSO | integracja z DERMS/ ADMS i rynkami, M&V | single point of failure, manipulacja danymi, redundancja, audyt algorytmów, SOC, testy |
| DERMS (operator DSO) | Bezpieczna integracja DER z siecią, zarządzanie ograniczeniami | sekundy-godziny | topologia sieci, pomiary, zdolności elastyczności, constraints | integracja z ADMS/ SCADA i VPP | ataki na telemetrię, błędna estymacja, segmentacja OT/IT, monitoring, polityki dostępu |
| ADMS/SCADA (sieć dystrybucyjna) | Nadzór i automatyka sieci, przywracanie zasilania | sekundy-minuty | pomiary, stany łączników, sygnały zabezpieczeń, prognozy | współpraca z DERMS, interfejsy OT | incydenty cyber-fizyczne OT, hardening, separacja stref, testy, procedury IR |
| EMS/TSO (system przesyłowy) | Bilansowanie krajowe, usługi systemowe, bezpieczeństwo KSE | minuty-dni | prognozy obciążenia/ generacji, rezerwy, constraints | integracja z rynkami i agregatorami | błędy koordynacji, procedury operacyjne, rezerwy manualne, redundancja |

Źródło: opracowanie własne.

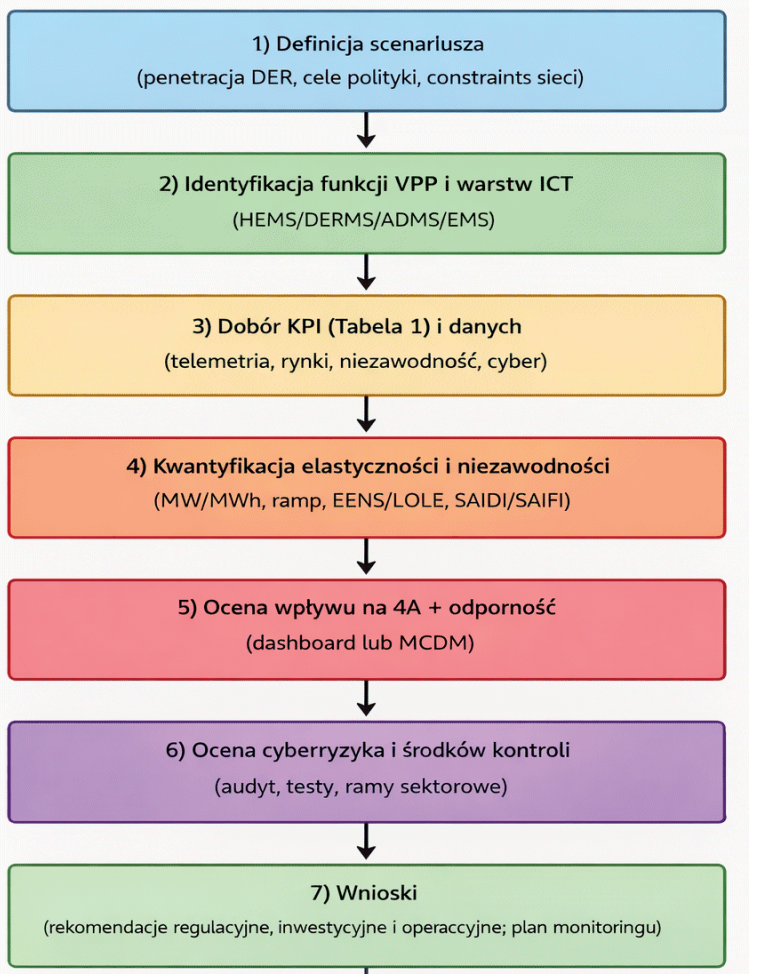
## Modele graficzne: architektura i proces oceny

Poniżej przedstawiono dwa rysunki koncepcyjne: architekturę przepływów danych (Rysunek 1) oraz proces oceny wkładu VPP w bezpieczeństwo energetyczne (Rysunek 2).




**Rysunek 1.** Architektura VPP i systemów ICT w relacji do operatorów oraz rynków

Źródło: opracowanie własne.




**Rysunek 2.** Proces oceny wkładu VPP w bezpieczeństwo energetyczne
Źródło: opracowanie własne.

## Dyskusja

### VPP jako instrument bezpieczeństwa energetycznego

Wyniki sugerują, że VPP i systemy ICT mogą stać się narzędziem polityki bezpieczeństwa energetycznego, ale tylko wtedy, gdy są traktowane jako element ekosystemu operacyjnego i regulacyjnego, a nie wyłącznie jako rozwiązanie rynkowe. Włączenie VPP do planowania bezpieczeństwa wymaga powiązania wskaźników technicznych (EENS/LOLE, stabilność),

ekonomicznych (koszty bilansowania, zmienność cen) i środowiskowych (emisje) z odpornością cyfrową (czas detekcji, gotowość procedur, dostępność łączności). W praktyce państwo (regulator, operatorzy, instytucje ds. cyber) powinno traktować platformy VPP jako element infrastruktury krytycznej „z funkcji", nawet jeśli są własnością podmiotów komercyjnych.

Poziom techniczny. Aktywacja elastyczności przez VPP musi uwzględniać ograniczenia sieci dystrybucyjnej, w przeciwnym razie działania rynkowe mogą być technicznie niebezpieczne (np. kumulacja ładowania EV w słabym węźle). Dlatego rozwój VPP powinien iść w parze z rozwojem DERMS/ADMS, automatyki i procedur koordynacji DSO-TSO (Strezoski, 2023). Poziom ekonomiczny. Korzyści dla przystępności cenowej zależą od projektowania rynków elastyczności, transparentności rozliczeń i właściwej alokacji ryzyk, bez tego elastyczność może istnieć „na papierze", ale nie być dostępna w godzinach krytycznych (Esfahani i in., 2025).

## Rekomendacje wdrożeniowe w skali państwa

Na podstawie syntezy można wskazać cztery grupy rekomendacji zwiększających prawdopodobieństwo, że VPP wzmocnią bezpieczeństwo energetyczne:

1. Interoperacyjność i governance danych: standardy danych, minimalna telemetria, rejestry zasobów, wymagania dla API oraz zasady jakości danych (kompletność, spójność, czasowość). W praktyce chodzi o to, by zasoby były „adresowalne" i „mierzalne" oraz by możliwy był audyt.
2. Koordynacja DSO-TSO: reguły priorytetyzacji (bezpieczeństwo sieci przed rynkiem), platformy wymiany constraints i mechanizmy unikania sprzecznych sygnałów do tych samych zasobów. W państwach o rosnącej penetracji DER koordynacja ta staje się warunkiem wykorzystania elastyczności bez pogorszenia niezawodności.
3. M&V jako filar bezpieczeństwa: weryfikacja wolumenów, parametrów dynamicznych (czas reakcji, ramp) i niezawodności usług, logowanie decyzji i ścieżek audytu (auditability). Im większy wpływ VPP na bilansowanie systemu, tym większa potrzeba formalizacji M&V.
4. Security-by-design: minimalne wymagania bezpieczeństwa dla urządzeń końcowych, łączności i platform, obejmujące m.in. segmentację

OT/IT, IAM, monitoring (SOC) i procedury IR obejmujące cały łańcuch interesariuszy. Przeglądy podkreślają, że bezpieczeństwo smart grid nie jest możliwe bez spójnych standardów i praktyk wdrażanych end-to-end (Chen i in., 2025; Leszczyna, 2018).

Rozdział ma charakter konceptualno-przeglądowy. Ograniczeniem jest brak empirycznej weryfikacji na danych krajowych oraz fakt, że literatura techniczna często opiera się na modelach testowych. Dalsze badania powinny łączyć: (a) analizę niezawodności i odporności (EENS/LOLE, scenariusze szoków i procesów długotrwałych), (b) modelowanie ekonomiczne rynków elastyczności oraz (c) ocenę cyberryzyka w architekturach wielostronnych, w tym wpływu pojedynczych platform na ryzyko systemowe. Szczególnie potrzebne są studia przypadków dużych VPP, które pokażą, w jakim stopniu „cyfrowe" KPI (dostępność łączności, jakość danych, dojrzałość SOC) korelują z KPI energetycznymi (np. niezawodność dostaw usług bilansujących).

## Wnioski

VPP i powiązane systemy ICT mogą wzmacniać bezpieczeństwo energetyczne państwa w wielu wymiarach: od adekwatności mocy i stabilności pracy systemu, przez przystępność cenową i dywersyfikację, po akceptowalność środowiskową. Warunkiem jest jednak traktowanie VPP jako elementu infrastruktury krytycznej, w którym elastyczność jest mierzalna, weryfikowalna i bezpieczna cyfrowo. Proponowane w rozdziale mapowanie mechanizmów, KPI oraz proces oceny mogą stanowić podstawę do projektowania programów elastyczności i cyfryzacji w taki sposób, aby były one jednocześnie efektywne kosztowo i odporne na ryzyka zakłóceniowe.

## Literatura

1. Algburi, S., Abed Al Kareem, S. S., Sapaev, I. B., Mukhitdinov, O., Hassan, Q., Khalaf, D. H., Jabbar, F. I. (2025). The role of artificial intelligence in accelerating renewable energy adoption for global energy transformation. *Unconventional Resources, 8*, 100229. https://doi.org/10.1016/j.uncres.2025.100229

2. Chen, J., Yan, J., Kemmeugne, A., Kassouf, M., Debbabi, M. (2025). Cybersecurity of distributed energy resource systems in the smart grid: A survey. *Applied Energy, 383*, 125364. https://doi.org/10.1016/j.apenergy.2025.125364
3. Esfahani, M., Alizadeh, A., Cao, B., Kamwa, I., Xu, M. (2025). Bridging theory and practice: A comprehensive review of virtual power plant technologies and their real-world applications. *Renewable and Sustainable Energy Reviews, 222*, 115929. https://doi.org/10.1016/j.rser.2025.115929
4. Gkoktsis, G., Lauer, H., Jäger, L. (2023). Risk assessments in virtual power plants with NESCOR criteria, practical application, advantages and disadvantages. ARES 2023: *Proceedings of the 18Th International Conference on Availability, Reliability and Security*, 1-11. https://doi.org/10.1145/3600160.3605179
5. Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., Razzaque, M. A. (2022). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of Network and Computer Applications, 209*, 103540. https://doi.org/10.1016/j.jnca.2022.103540
6. Leszczyna, R. (2018). Standards and frameworks for cybersecurity in smart grid. *Computers Security, 79*, 1-15. https://doi.org/10.1016/j.cose.2018.03.011
7. Liu, X., Li, Y., Wang, L., Tang, J., Qiu, H., Berizzi, A., Valentin, I., Gao, C. (2024). Dynamic aggregation strategy for a virtual power plant to improve flexible regulation ability. *Energy, 297*, 131261. https://doi.org/10.1016/j.energy.2024.131261
8. Roozbehani, M. M., Heydarian-Forushani, E., Hasanzadeh, S., Elghali, S. B. (2022). Virtual power plant operational strategies: Models, markets, optimization, challenges, and opportunities. *Sustainability, 14*(19), 12486. https://doi.org/10.3390/su141912486
9. Schmitz, R., Flachsbarth, F., Plaga, L. S., Braun, M., Härtel, P. (2025). Energy security and resilience: Revisiting concepts and advancing planning perspectives for transforming integrated energy systems. *Energy Policy, 207*, 114796. https://doi.org/10.1016/j.enpol.2025.114796

10. Siksnelyte-Butkiene, I., Streimikiene, D., Lekavicius, V., Balezentis, T. (2024). Comprehensive analysis of energy security indicators and measurement of their integrity. *Technological Forecasting and Social Change, 200*, 123167. https://doi.org/10.1016/j.techfore.2023.123167
11. Strezoski, L. (2023). Distributed energy resource management systems (DERMS): State of the art and how to move forward. *WIREs Energy and Environment, 12*(1), e460. https://doi.org/10.1002/wene.460
12. Sun, X., Xie, H., Qiu, D., Xiao, Y., Bie, Z., Strbac, G. (2023). Decentralized frequency regulation service provision for virtual power plants: A best response potential game approach. *Applied Energy, 352*, 121987. https://doi.org/10.1016/j.apenergy.2023.121987
13. Ustun, T. S. (2022). Cybersecurity for smart grids. *Energies, 15*(15), 5458. https://doi.org/10.3390/en15155458
14. Zare, A., Shafiyi, M. A. (2025). Virtual power plant models and market participation: A deep dive into optimization and real-world applications. *Results in Engineering, 26*, 105548. https://doi.org/10.1016/j.rineng.2025.105548