# Architektura odporności ewoluujących sieci elektroenergetycznych: od teorii sieci złożonych do predykcji kaskad i sterowania AI w ujęciu Donga Liu


**AUTOR**

Fundacja Dobre Państwo



## STRESZCZENIE / ABSTRACT

Artykuł analizuje ewolucję sieci elektroenergetycznych z perspektywy systemów złożonych, odchodząc od prostego rozumienia wytrzymałości materiałowej na rzecz globalnej odporności strukturalnej. Autorzy, opierając się na pracach Donga Liu i współpracowników, wskazują na konieczność integracji trzech porządków: topologicznego (grafy i centralność), fizycznego (prawa Kirchhoffa, rozpływy mocy) oraz dynamicznego. Kluczowym zagadnieniem jest mechanizm awarii kaskadowych, gdzie lokalne zabezpieczenia mogą paradoksalnie prowadzić do globalnej katastrofy poprzez redystrybucję obciążeń. Tekst podkreśla, że nowoczesna architektura odporności wymaga zaawansowanego modelowania stochastycznego i sterowania AI, aby skutecznie zarządzać infrastrukturą krytyczną w obliczu nieprzewidywalnych zdarzeń.

The article analyzes the evolution of power grids from the perspective of complex systems, moving away from a simple understanding of material strength toward global structural resilience. Drawing on the work of Dong Liu and colleagues, the authors highlight the necessity of integrating three dimensions: the topological (graphs and centrality), the physical (Kirchhoff's laws, power flows), and the dynamic. A key issue is the mechanism of cascading failures, where local protections can paradoxically lead to global catastrophe through load redistribution. The text emphasizes that a modern resilience architecture requires advanced stochastic modeling and AI control to effectively manage critical infrastructure in the face of unpredictable events.

Artykuł analizuje ewolucję odporności sieci elektroenergetycznych, argumentując, że w dobie transformacji cyfrowej i energetycznej tradycyjne podejście oparte na fizycznej wytrzymałości komponentów (logika N-1) jest niewystarczające. Autor stawia tezę, że współczesna odporność musi być rozumiana jako dynamiczna synteza teorii sieci złożonych, praw fizyki przepływów oraz zaawansowanej analityki AI. Tekst dowodzi, że przejście od statycznego planowania infrastruktury do predykcyjnego zarządzania systemem cyberfizycznym pozwala na wczesne rozpoznawanie tzw. węzłów niezbędnych i hamowanie kaskad awarii, zanim osiągną one punkt krytyczny. Poprzez przywołanie narzędzi takich jak grafowe sieci uwagowe (GAT) czy głębokie uczenie ze wzmocnieniem (DRL), artykuł ukazuje sieć nie jako zbiór przewodów, lecz jako geometrię zależności, w której bezpieczeństwo przestaje być cechą pojedynczego urządzenia, a staje się funkcją relacji i jakości poznawczej systemu. Jest to studium przejścia od infrastruktury liniowej do organicznej, gdzie technologia AI wspiera ludzką odpowiedzialność w zarządzaniu ryzykiem cywilizacyjnym.

**SŁOWA KLUCZOWE**

odporność sieci elektroenergetycznych | teoria sieci złożonych | awarie kaskadowe | Deep Reinforcement Learning | Proximal Policy Optimization | kryterium N-1 | topologia sieci | centralność pośrednictwa | systemy cyberfizyczne | modelowanie stochastyczne | rozpływy mocy AC/DC | architektura odporności | sterowanie AI w energetyce | sieci małego świata | zarządzanie infrastrukturą krytyczną

# Od infrastruktury materialnej do geometrii zależności

Sieć, która przestała być siecią. Od infrastruktury przewodów do organizmu zależności

Nowoczesna sieć elektroenergetyczna jest jednym z najdoskonalszych, a zarazem najbardziej kruchych wytworów cywilizacji technicznej. Na pierwszy rzut oka wydaje się materialna i ciężka, niemal archaiczna: elektrownie, transformatory, linie przesyłowe, izolatory, stacje, rozdzielnie, kable czy aparatura zabezpieczeniowa. Jest w niej coś z pejzażu przemysłowego poprzedniej epoki, z wielkiej żelaznej składni XX wieku.

Pod tą widzialną warstwą pracuje jednak system zupełnie innego rodzaju: sieć pomiarów, algorytmów i sterowania, automatycznych zabezpieczeń, danych w czasie rzeczywistym, prognoz pogody, rynku mocy, falowników, źródeł rozproszonych oraz cybernetycznych zależności. To już nie tylko maszyneria. To środowisko sprzężonych decyzji.

Kategoria odporności (ang. robustness) nie może być rozumiana banalnie jako wytrzymałość pojedynczego elementu. W klasycznym myśleniu technicznym łatwo ulec pokusie prostego obrazowania: jeśli coś pęka, należy to pogrubić; jeśli linia się przeciąża, trzeba zbudować drugą; jeśli transformator jest krytyczny, warto kupić większy. Taka intuicja bywa użyteczna, lecz w systemach złożonych okazuje się niewystarczająca. System może składać się z mocnych komponentów, a mimo to zachowywać się krucho. Może posiadać elementy lokalnie zabezpieczone, pozostając globalnie podatnym. Może wyglądać bezpiecznie w tabeli inżyniera, by w godzinie próby zareagować jak tłum na stadionie po fałszywym alarmie: każdy ruch pojedynczo racjonalny, całość katastrofalna.

Teza oparta na książce „Robustness of Evolving Power Grids: Modeling and Analysis" Donga Liu, Xi Zhanga i Chi Konga Tse prowadzi właśnie ku takiemu rozumieniu odporności. Sieć elektroenergetyczna zostaje tam przedstawiona jako system ewoluujący, w którym tradycyjne zagadnienia inżynierii mocy spotykają się z teorią sieci złożonych, uczeniem maszynowym, analizą awarii kaskadowych i problemem sterowania w czasie rzeczywistym. Autorzy nie redukują sieci do diagramu technicznego; traktują ją jako strukturę, której zachowanie zależy od topologii, fizyki przepływów, dynamiki zabezpieczeń, dostępności obserwacji, a coraz częściej również od odporności warstwy cybernetycznej. Pierwszym krokiem jest modelowanie.

Sieć elektroenergetyczną można opisać jako graf: węzły reprezentują elektrownie, stacje i centra obciążeniowe, a krawędzie odpowiadają liniom przesyłowym, dystrybucyjnym oraz transformatorom. Taki obraz jest atrakcyjny, gdyż pozwala wykorzystać aparat teorii sieci złożonych: stopień węzła, najkrótszą ścieżkę, centralność pośrednictwa, współczynnik grupowania czy koncepcję sieci małego świata. W tej perspektywie system elektroenergetyczny przestaje być mapą przewodów, a staje się geometrią zależności. Można pytać, które punkty są hubami, które pełnią funkcję mostów, gdzie sieć posiada nadmiarowość, a gdzie wystarczy jedno cięcie, aby rozdzielić całość na bezradne wyspy.

Sama topologia jednak kłamie, jeśli uzna się ją za jedyną prawdę. To kłamstwo eleganckie, matematyczne i kuszące – a przez to szczególnie niebezpieczne. Graf wskazuje, że dwa węzły są połączone, lecz nie mówi nic o impedancjach, limitach termicznych, rozpływach mocy, profilach napięć, rezerwach stabilności czy zachowaniu zabezpieczeń. W sieci społecznej informacja może

krążyć wieloma drogami, lecz w sieci elektroenergetycznej prąd nie wybiera ścieżki według ludzkiej intuicji ani życzeń operatora.

## Fizyka przepływów a mechanika awarii kaskadowych

System podlega prawom fizyki. Dlatego słusznie podkreśla się różnicę między modelem czysto topologicznym a elektrycznym, w którym należy uwzględnić prawa Kirchhoffa, przepływy AC lub DC, ograniczenia przepustowości oraz realne parametry elementów.

W tym miejscu pojawia się zasadnicza lekcja: w systemie złożonym mapa nigdy nie jest terytorium, lecz zła mapa może stać się narzędziem katastrofy. Jeśli analityk dostrzega jedynie liczbę połączeń, ryzykuje przecenienie odporności sieci. Jeśli skupia się wyłącznie na fizyce pojedynczego przepływu, może przeoczyć znaczenie struktury globalnej. Z kolei ufność w historyczne scenariusze awarii sprawia, że można przegapić zdarzenie bez precedensu, które jest już wpisane w architekturę systemu jak pęknięcie w szkle.

Nowoczesna ocena odporności wymaga zatem integracji trzech porządków: topologicznego, fizycznego i dynamicznego. Awaria kaskadowa stanowi najlepszy dowód na to, że systemu nie wolno opisywać wyłącznie przez stan lokalny. Mechanizm kaskady wydaje się prosty: jeden element wypada, przepływy mocy rozkładają się inaczej, kolejne linie zostają przeciążone, a zabezpieczenia odłączają je dla ochrony sprzętu, przenosząc obciążenie dalej. Ta prostota jest jednak złudna. Kaskada nie jest zwykłą sumą usterek; to proces, w którym każda decyzja automatyki zmienia warunki kolejnej.

Zabezpieczenie lokalne może uratować urządzenie, jednocześnie pogarszając sytuację systemową. Automat działa poprawnie według instrukcji, a mimo to przyczynia się do globalnego rozpadu. Oto biurokracja maszyn: każdy przekaźnik ma rację w swoim okienku, ale państwo elektryczne idzie w ciemność.

W tradycyjnym języku bezpieczeństwa infrastruktury długo dominowała logika kryterium N-1. System powinien przetrwać utratę jednego istotnego elementu bez naruszenia dopuszczalnych limitów pracy. Założenie to jest rozsądne i pozostaje kluczowe, lecz w świecie rosnącej złożoności staje się warunkiem koniecznym, a nie wystarczającym. Katastrofy rzadko są grzeczne. Nie pytają operatora, czy wolno im wystąpić pojedynczo. Zdarzenia pogodowe, błędy ludzkie, cyberataki, awarie aparatury, niestabilność źródeł opartych na falownikach i reakcje automatyki mogą złożyć się w sekwencję, której nie obejmuje komfortowa wyobraźnia pojedynczej usterki. Kryterium N-1

jest jak pas bezpieczeństwa: należy go mieć, ale nie wolno sądzić, że unieważnia on fizykę zderzenia.

Przykład brytyjskiego blackoutu z 9 sierpnia 2019 roku pokazuje, że współczesne awarie nie muszą przypominać filmowej eksplozji elektrowni. Według raportów technicznych zdarzenie rozpoczęło się od zaburzenia w systemie, po którym nastąpiła utrata generacji i automatyczne odłączenie części odbiorców; zasilanie straciło około milion klientów.

Znaczenie tego przypadku nie polega wyłącznie na liczbie poszkodowanych. Istotniejsze jest to, że w systemach wysokiej techniki niewielkie opóźnienia, brak koordynacji i gwałtowna zmiana bilansu mocy błyskawicznie przekładają się na skutki społeczne: paraliż transportu, łączności, usług publicznych oraz utratę zaufania do instytucji. Elektryczność jest tak oczywista, że politycznie widzialna staje się dopiero wtedy, gdy jej brakuje. Jeszcze większą skalę miało zaciemnienie północnoamerykańskie z 14 sierpnia 2003 roku. Oficjalny raport U.S.-Canada Power System Outage Task Force wskazywał, że blackout objął około 50 milionów ludzi oraz dziesiątki tysięcy megawatów obciążenia.

Zdarzenie to ma klasyczne znaczenie dla teorii odporności: dowiodło, że katastrofa nie musi wynikać z jednego monumentalnego błędu. Może powstać z sekwencji zaniedbań, ograniczonej świadomości sytuacyjnej, niewłaściwie przyciętej roślinności, awarii systemów alarmowych i braku koordynacji. System nie upadł dlatego, że nikt nic nie robił. Upadł między innymi dlatego, że lokalne działania i lokalna niewiedza nie złożyły się w adekwatną inteligencję całości.

To prowadzi do kluczowego rozróżnienia: odporność nie jest wyłącznie właściwością infrastruktury, lecz także właściwością poznania. System jest tak odporny, jak dobre są jego czujniki, modele, prognozy, procedury i zdolność decyzyjna. Jeśli operator widzi zbyt mało, reaguje za późno. Jeśli model upraszcza zbyt mocno, reaguje błędnie. Jeśli automatyka działa szybko, lecz ślepo na konsekwencje systemowe, staje się akceleratorem kaskady. Jeżeli zaś sztuczna inteligencja działa szybko, lecz bez kontroli i zrozumiałości, może stworzyć nową klasę ryzyka: algorytmiczną pewność w warunkach, które wymagają sceptycyzmu.

## Teoria sieci złożonych a architektura odporności

Książka Liu, Zhanga i Tse to nie tylko opowieść o energetyce. To studium współczesnej cywilizacji infrastrukturalnej. Nasze społeczeństwa chętnie mówią o innowacjach, transformacji i zielonej energii, lecz rzadziej pytają o architekturę odporności. Dodajemy źródła odnawialne, elektryfikujemy transport, przenosimy sterowanie do warstwy cyfrowej i splatamy zależności

między sektorem energetycznym, telekomunikacyjnym, finansowym oraz publicznym. Każdy z tych kroków może być racjonalny, jednak razem tworzą system, w którym lokalne optimum staje się globalną pułapką. Technokratyczny optymizm bez teorii kaskady jest jak projektowanie mostu przez człowieka zakochanego w widoku rzeki, ale obojętnego na ciężar ciężarówek.

Należy odrzucić dwa skrajne złudzenia. Pierwsze to wiara w proste wzmacnianie: przekonanie, że wystarczy dobudować więcej infrastruktury, zwiększyć rezerwy, położyć więcej kabli i wylać więcej betonu. Drugie to złudzenie algorytmicznego zbawienia: przekonanie, że sztuczna inteligencja sama rozwiąże problem dzięki swojej szybkości, adaptacyjności i pozornej bezsenności. W rzeczywistości odporność wymaga syntezy. Potrzebuje właściwej topologii, realistycznych modeli fizycznych, precyzyjnych pomiarów, automatyki, ludzkiej odpowiedzialności, planowania inwestycyjnego oraz procedur odbudowy – a także algorytmów, które wspierają decyzje, lecz nie unieważniają polityki bezpieczeństwa. Tu wchodzi teoria sieci złożonych i pytanie o to, dlaczego struktura jest losem systemu.

Teoria ta zaczyna się od gestu pozornie prostego: przekłada rozległą rzeczywistość materialną na język grafu. Tam, gdzie inżynier widzi elektrownię, stację transformatorową, odbiorcę przemysłowego czy rozdzielnię, teoria sieci widzi węzeł. Gdzie technik dostrzega linię przesyłową, transformator lub łącznik systemowy, teoria sieci widzi krawędź. Z tego uproszczenia rodzi się ogromna siła analityczna. System przestaje być katalogiem urządzeń, a staje się strukturą relacji: kto z kim jest połączony, przez kogo musi przejść przepływ, gdzie istnieje nadmiarowość, a gdzie jeden element staje się wąskim gardłem całej cywilizacji elektrycznej. Ta abstrakcja jest konieczna; współczesna sieć elektroenergetyczna jest zbyt obszerna i dynamiczna, by rozumieć ją wyłącznie przez pryzmat pojedynczych części. Można znać parametry każdego transformatora i moc każdego bloku wytwórczego, a mimo to nie rozumieć, co stanie się po utracie jednego węzła w krytycznym momencie.

Wiedza o częściach nie sumuje się automatycznie w wiedzę o całości. W systemach złożonych całość bywa bardziej kapryśna niż jej elementy, gdyż jej zachowanie wynika z relacji, sprzężeń i redystrybucji obciążeń. Dlatego teoria sieci złożonych jest w energetyce kluczowa: pozwala dostrzec formę zależności, zanim dojdzie do dramatu fizycznego przeciążenia.

Stopień węzła określa liczbę jego bezpośrednich połączeń z innymi punktami. Węzeł o wysokim stopniu staje się hubem – miejscem kluczowym dla spójności sieci. Potocznie mówimy, że to punkt, przez który „wszyscy przechodzą”, choć w energetyce wymaga to ostrożności: nie każdy punkt o dużej liczbie połączeń jest równie krytyczny elektrycznie. Sama liczba relacji nie mówi nic o przepływach mocy, impedancjach czy limitach termicznych. Mimo to stopień węzła pozostaje pierwszym sygnałem, że istnieją miejsca, których utrata boli bardziej niż innych. Demokracja grafu

jest fikcją. Węzły nie są równe, choć w arkuszach kalkulacyjnych często wyglądają równie schludnie.

Drugą miarą jest najkrótsza ścieżka – minimalna liczba połączeń potrzebna do przejścia między węzłami. Średnia długość tej ścieżki opisuje ogólną „bliskość" elementów systemu. Intuicja podpowiada, że im krótsze ścieżki, tym lepiej: energia dociera sprawniej, a sieć jest bardziej zintegrowana. Jednak w elektroenergetyce intuicja bywa zdradliwa.

Zbyt silnie skrócone ścieżki i topologia typu „małego świata" mogą paradoksalnie zmniejszać odporność, gdy ograniczone marginesy bezpieczeństwa przyspieszają przenoszenie przeciążeń. Krótka droga sprzyja komunikatowi, ale nie zawsze kaskadzie. To ironia infrastruktury: system świetnie połączony potrafi znakomicie rozprowadzać nie tylko energię, lecz i awarię. Trzecią istotną miarą jest centralność pośrednictwa. Określa ona, jak często dany węzeł lub krawędź leży na najkrótszych ścieżkach między innymi elementami. Taki punkt wcale nie musi mieć największej liczby połączeń; może być skromny i niewidoczny, a jednak pełnić funkcję mostu między fragmentami sieci. Jest to miara szczególnie cenna, gdyż wiele katastrof zaczyna się nie od upadku centrum, lecz od utraty elementu spajającego dwa światy. Mosty mają tę niewdzięczną cechę, że zauważamy je dopiero wtedy, gdy ich brakuje.

W systemie elektroenergetycznym element o wysokim pośrednictwie może przejąć krytyczne przepływy zastępcze po awarii innej linii. Jeśli zostanie przeciążony i odłączony przez zabezpieczenia, sieć nie tylko dozna uszkodzenia, ale zmieni swoją geometrię w sposób katastrofalny.

## Topologie sieci a odporność strukturalna

Czwarta miara, współczynnik grupowania, opisuje stopień, w jakim sąsiedzi danego węzła są połączeni również między sobą. Wysoki wskaźnik oznacza istnienie lokalnych klastrów, czyli zagęszczeń relacji. W systemach elektroenergetycznych przekłada się to na lokalną strukturę połączeń, która z jednej strony może zwiększać dostępność alternatywnych ścieżek, z drugiej zaś – zamykać część dynamiki w obszarze lokalnym. Nie ma tu jednej, prostej reguły.

Wysokie klastrowanie pomaga, gdy zapewnia nadmiarowość, lecz szkodzi, jeśli sprzyja lokalnym przeciążeniom lub utrudnia kontrolowane rozproszenie przepływów. Teoria sieci daje język, ale nie zwalnia z myślenia. Kto bierze wskaźnik za wyrocznię, ten tylko zamienia dawną magię w nowszą tabelę.

Klasyczne modele sieciowe pozwalają uchwycić różne typy organizacji strukturalnej. Sieci losowe Erdősa-Rényiego powstają poprzez przypadkowe tworzenie połączeń między węzłami i cechują się relatywnie homogenicznym rozkładem stopni – większość punktów posiada podobną liczbę powiązań. Z kolei sieci bezskalowe Barabásiego-Alberta opierają się na mechanizmie preferencyjnego przyłączania: nowe węzły chętniej łączą się z tymi, które już dysponują wieloma połączeniami. W efekcie powstaje niewielka liczba potężnych hubów oraz duża liczba punktów peryferyjnych. Taka struktura bywa odporna na awarie przypadkowe, gdyż losowo uszkodzony element rzadko okazuje się kluczowy, jednak pozostaje skrajnie podatna na celowe ataki wymierzone w huby. To zjawisko ma znaczenie nie tylko techniczne; stanowi przypomnienie starej prawdy instytucjonalnej: centralizacja daje sprawność, ale produkuje zakładników własnej sprawności.

Szczególnie istotne są sieci małego świata, opisane modelem Wattsa-Strogatza. Łączą one krótką średnią długość ścieżki z wysokim współczynnikiem grupowania. Cechy te odnajdujemy w wielu rzeczywistych systemach elektroenergetycznych. Jest to struktura kusząca, gdyż pozwala na wydajne połączenie lokalnej gęstości i globalnej bliskości. W energetyce oznacza to topologię zdolną do sprawnego przesyłu, lecz jednocześnie specyficznie podatną na szybkie przenoszenie skutków zakłóceń. Należy tu zwrócić uwagę na subtelność: sieci o cechach małego świata bywają odporniejsze od sieci regularnych, jednak w warunkach ograniczonych marginesów pojemnościowych zbyt krótka średnia ścieżka może obniżać odporność na kaskady.

Tu właśnie przebiega granica między wiedzą popularną o „sieciach” a poważną analizą systemową. W uproszczonych narracjach sieć jest dobra, gdy jest gęsta, połączona, szybka i bezpośrednia.

## Topologia sieci a fizyka przepływów

W rzeczywistości należy pytać: połączona jak, czym, przy jakich limitach i z jaką rezerwą? Jaka jest dynamika awaryjna i jak działa automatyka zabezpieczeń? Połączenie nie jest wartością samą w sobie. Nadmiarowość staje się wartością tylko wtedy, gdy nie zamienia się w kanał propagacji przeciążenia. Krótka droga jest zaletą, o ile system potrafi absorbować nagłe przepływy. Hub jest użyteczny, dopóki jego utrata nie rozrywa organizmu. Most zaś okazuje się zbawienny wtedy, gdy nie staje się jedyną drogą ewakuacji prądu z płonącego miasta zależności.

Klasyczna teoria sieci złożonych dostarcza energetyce potężnego narzędzia do rozpoznawania podatności. Pozwala identyfikować elementy topologicznie kluczowe, porównywać architektury sieci, badać skutki losowych awarii i celowych ataków oraz mierzyć konsekwencje usuwania kolejnych węzłów lub krawędzi. Dzięki niej możemy pytać nie tylko o to, co stanie się po awarii

konkretnego elementu, ale jaka klasa komponentów jest strukturalnie niebezpieczna. Czy groźniejsza jest utrata hubów, mostów i linii o wysokiej centralności, czy elementów łączących klastry? Czy sieć rozpada się stopniowo, czy istnieje punkt krytyczny prowadzący do nagłej fragmentacji? I wreszcie: czy awarie losowe i ataki celowe ujawniają te same słabości, czy zupełnie różne?

W elektroenergetyce samo pytanie o spójność grafu jest niewystarczające. Sieć może pozostać topologicznie połączona, a jednocześnie być fizycznie niezdolna do bezpiecznej pracy. To jedna z najważniejszych lekcji dla tych, którzy chcieliby przenosić pojęcia z informatyki czy socjologii sieci bez korekty inżynieryjnej. Jeśli w mediach społecznościowych ścieżka informacyjna zostanie przeciążona, użytkownik odczuje opóźnienie, zobaczy błąd serwera lub – co gorsza – komentarz eksperta od wszystkiego. W sieci elektroenergetycznej przeciążenie oznacza wzrost temperatury przewodów, naruszenie limitów stabilności i zadziałanie zabezpieczeń, co zmienia rozpływ mocy i może zainicjować kaskadę. Graf jest szkieletem, ale fizyka jest krwią i ciśnieniem tego organizmu.

Współczesne badania nad odpornością łączą teorię sieci z modelami przepływu mocy. Modele DC upraszczają rzeczywistość, analizując rozpływy mocy czynnej przy pewnych założeniach dotyczących napięć i kątów fazowych. Modele AC są bardziej realistyczne – uwzględniają napięcia, moc bierną i pełniejszą dynamikę elektryczną – lecz są bardziej złożone obliczeniowo. Wybór modelu nie jest kwestią matematycznej elegancji, lecz kompromisem między szybkością a dokładnością decyzyjną. W fazie planowania można pozwolić sobie na głębokie symulacje; w trakcie rozwijającej się awarii liczą się sekundy, a czasem ułamki sekund. Model idealny, który odpowiada po katastrofie, jest epistemologicznie ciekawy, ale operacyjnie bezużyteczny – przypomina lekarza, który wygłasza perfekcyjną diagnozę już po pogrzebie.

Awarie kaskadowe pokazują, że struktura jest losem systemu. Gdy jedna linia zostaje odłączona, prąd nie znika, lecz szuka nowych dróg zgodnie z prawami fizyki. Linie sąsiednie przejmują obciążenie i jeśli ich marginesy są zbyt małe, mogą przekroczyć limity termiczne lub stabilnościowe. Zabezpieczenia odłączą je, by chronić sprzęt, co ponownie zmieni topologię i wymusi kolejną redystrybucję. W ten sposób lokalna usterka przeobraża się w proces samowzmacniający. Nie chodzi o to, że system „chce” upaść, lecz o to, że poprawne lokalnie reakcje mogą utworzyć globalnie niszczącą sekwencję. W systemach złożonych tragedia często nie wynika z braku reguł, lecz z faktu, że każda z nich działa w zbyt wąskim horyzoncie.

Wyróżnia się deterministyczne i stochastyczne modelowanie kaskad. Podejście deterministyczne uznaje element przekraczający próg za uszkodzony i usuwa go z sieci; jest to metoda przejrzysta, szybka i użyteczna w badaniu scenariuszy granicznych. Modelowanie stochastyczne uwzględnia losowość czasu awarii, opóźnienia zabezpieczeń oraz zmienne warunki środowiskowe. Jest bliższe

rzeczywistości, bo realne systemy nie psują się z elegancją podręcznika. Dwa podobne przeciążenia mogą przynieść różne skutki w zależności od temperatury, stanu aparatury czy kolejności zdarzeń. Katastrofa ma gramatykę, ale nie zawsze ma scenariusz.

Warto zwrócić uwagę na aspekt „ewoluujący" w tytule analizowanej koncepcji. Sieci elektroenergetyczne przestały być stabilnymi, hierarchicznymi strukturami opartymi na kilku wielkich elektrowniach i biernych odbiorcach. Rosnący udział odnawialnych źródeł energii, generacji rozproszonej, magazynów, prosumentów oraz cyfrowych systemów zarządzania zmienia zarówno topologię, jak i dynamikę systemu. Tradycyjna elektrownia synchroniczna dostarczała nie tylko moc, ale i inercję stabilizującą częstotliwość. Źródła oparte na falownikach, choć sterowalne szybciej, nie oferują tej samej fizycznej bezwładności. Transformacja energetyczna to zatem nie tylko podmiana paliwa, lecz przebudowa dynamiki systemu.

Tu pojawia się problem często pomijany w debacie publicznej. Politycy i komentatorzy mówią o megawatach mocy zainstalowanej, jakby system był prostym koszykiem, do którego wrzuca się kolejne źródła. Ale sieć nie jest koszykiem – jest układem równowagi. Liczy się nie tylko to, ile energii można wytworzyć, lecz gdzie, kiedy i z jaką przewidywalnością, przy jakiej rezerwie i z jakim wpływem na częstotliwość oraz napięcie. Megawat megawatowi nierówny, tak jak obietnica wyborcza nie równa się ustawie, choć obie bywają drukowane podobną czcionką.

## Od statycznej analizy do predykcji dynamicznej

Teoria sieci złożonych pozwala uporządkować pierwszy poziom problemu: kto jest połączony z kim i jakie są strukturalne konsekwencje tych powiązań. Prawdziwa ocena odporności musi jednak iść dalej. Musi pytać, jak zachowa się system po utracie elementu, jak szybko przeciążenie rozprzestrzeni się w strukturze, które węzły są niezbędne w danych warunkach operacyjnych, gdzie nastąpi gwałtowne przyspieszenie kaskady oraz jakie decyzje sterujące mogą zatrzymać ten proces, zanim przejdzie on z fazy ostrzeżenia w fazę katastrofy. Tu właśnie pojawia się sztuczna inteligencja: nie jako magiczny kapłan nowej techniki, lecz jako narzędzie do rozpoznawania wzorców zbyt złożonych, szybkich i wielowymiarowych dla klasycznego nadzoru ręcznego.

Zanim przejdziemy do GAT, Attention-LSTM i DRL, należy jasno nazwać zmianę paradygmatu. Dawniej ocena bezpieczeństwa opierała się przede wszystkim na zaplanowanych scenariuszach, statycznych marginesach i regułach operacyjnych. Dziś niezbędna jest predykcja dynamiczna: nie tylko pytanie „czy system wytrzyma utratę tego elementu?", lecz „jak rozwinie się sekwencja po jego utracie w tej konkretnej konfiguracji, przy tych przepływach, tej generacji odnawialnej, tej częściowej obserwowalności i tej odpowiedzi zabezpieczeń?". To różnica między fotografią a

filmem. Statyczna analiza pokazuje kadr; awaria kaskadowa jest ruchem. Kto widzi tylko kadr, może starannie opisać pierwszy akt tragedii, kompletnie przegapiając trzeci.

Ocena odporności staje się więc sztuką przewidywania przyszłości systemu na podstawie jego aktualnej struktury i stanu. Nie jest to wróżbiarstwo – choć w instytucjach publicznych bywa ono czasem tańsze od rzetelnej analityki – lecz próba przekształcenia złożonej dynamiki w konkretne metryki, ostrzeżenia i decyzje. Właśnie dlatego kluczowe są tutaj grafowe sieci uwagowe, modele Attention-LSTM, klasyfikatory onset time, drzewa decyzyjne i głębokie uczenie ze wzmocnieniem.

Każde z tych narzędzi odpowiada na inny fragment problemu. GAT wskazuje, które węzły są niezbędne i groźne w razie utraty. Attention-LSTM analizuje kierunek biegu kaskady. Klasyfikacja onset time określa moment przejścia awarii z fazy powolnej do gwałtownej. DRL zaś podpowiada, jaką akcję podjąć, gdy system już płonie, a czas na narady właśnie się skończył.

Teoria sieci złożonych pełni funkcję fundamentu, a nie sufitu. Dostarcza pojęć pozwalających zrozumieć architekturę podatności, lecz sama w sobie nie wystarcza do sterowania realnym systemem. Jej największa wartość polega na tym, że wymusza myślenie relacyjne. Nie pyta wyłącznie o wytrzymałość danego elementu, ale o miejsce, jakie zajmuje on w całości. Nie bada tylko istnienia połączenia, lecz skutki jego zniknięcia. Nie analizuje jedynie aktualnego przepływu prądu, ale to, gdzie popłynie on po pierwszej usterce. To zmiana intelektualna o znaczeniu wykraczającym poza energetykę: w świecie systemów złożonych bezpieczeństwo przestaje być cechą rzeczy, a staje się cechą relacji.

Ocena odporności sieci elektroenergetycznej jest próbą odpowiedzi na pytanie pozornie proste, a w istocie cywilizacyjnie ciężkie: ile zakłócenia może znieść system, zanim lokalna usterka przejdzie w awarię kaskadową? Nie chodzi tu o ciekawość akademicką ani elegancką zabawę wskaźnikami, lecz o zdolność przewidzenia, czy państwo, region, aglomeracja albo infrastruktura krytyczna przejdą przez zaburzenie z raną, czy z zapaścią. Robustness assessment jest poznawczym odpowiednikiem medycyny intensywnej: mierzy parametry organizmu, zanim niewydolność jednego narządu pociągnie za sobą niewydolność całego ciała. W klasycznym ujęciu analiza ta skupiała się na skutkach hipotetycznej awarii – sprawdzano utracony procent obciążenia, liczbę odizolowanych regionów czy konsekwencje usunięcia konkretnej linii, transformatora albo generatora.

## Od statycznej oceny do dynamicznej predykcji

Takie podejście pozostaje niezbędne, zwłaszcza w fazie planowania. Pozwala ono rozpoznać topologiczne słabości, wskazać miejsca wymagające modernizacji, zaplanować rezerwy,

przebudować połączenia i sensownie alokować środki inwestycyjne. Jednak w obliczu realnej awarii sama wiedza o końcowych stratach jest spóźnioną mądrością. Operator nie potrzebuje jedynie informacji, że pożar strawi pół miasta; musi wiedzieć, którą ulicą ogień pójdzie za trzy minuty.

Nowoczesna ocena odporności przesuwa się zatem od statycznego pomiaru ku dynamicznej predykcji. Nie wystarczy zapytać, jak system wygląda jako graf – trzeba zapytać, jak będzie się zachowywał po inicjalnym zakłóceniu. Wskazanie elementów centralnych w topologii to za mało; należy ustalić, które komponenty są niezbędne w konkretnym stanie operacyjnym, przy określonych przepływach, obciążeniach, generacji, rezerwach, dostępności danych i konfiguracji zabezpieczeń.

Nie wystarczy policzyć średniej długości ścieżki. Trzeba zrozumieć, czy ta ścieżka stanie się drogą ratunkową, czy autostradą dla przeciążenia. Źródło trafnie odróżnia ocenę odporności od jej zwiększania. Pierwsza polega na rozpoznawaniu i kwantyfikowaniu podatności systemu; druga jest już ingerencją: zmianą topologii, wzmacnianiem komponentów, rekonfiguracją, sterowaniem, odłączaniem czy odbudową. Ocena jest diagnozą, zwiększanie odporności – terapią. W sprawnym systemie jedno poprzedza drugie. W tym wadliwym terapia zaczyna się od konferencji prasowej, czyli wtedy, gdy pacjent już leży na podłodze, a komisja ustala, czy grawitacja miała podstawę prawną.

W ujęciu Donga Liu i współautorów ocena odporności operuje na dwóch poziomach czasowych. W fazie planowania służy do mierzenia statycznych skutków hipotetycznych kaskad, takich jak utrata obciążenia czy izolacja fragmentów sieci. W fazie operacyjnej musi natomiast śledzić dynamiczny rozwój zakłóceń, by umożliwić operatorom szybką interwencję. Planowanie pyta: jak zbudować system, który wytrzyma? Operacja pyta: co zrobić teraz, skoro system właśnie przestaje wytrzymywać?

Nowoczesna ocena odporności korzysta z metod sztucznej inteligencji nie dlatego, że klasyczne podejścia są bezużyteczne, lecz ponieważ złożoność i wielowymiarowość współczesnych sieci przekraczają granice tradycyjnej analizy ręcznej. Klasyczna symulacja awarii kaskadowej bywa dokładna, ale jest czasochłonna. Algorytm predykcyjny może być mniej kompletny fizycznie, lecz staje się użyteczny operacyjnie, jeśli dostarcza szybkie ostrzeżenie. W bezpieczeństwie infrastruktury czas nie jest dodatkiem do jakości modelu – on stanowi o tej jakości. Prawda dostarczona po blackoutcie ma wartość raportu, a nie zabezpieczenia.

Pierwszym z narzędzi wskazanych w notatce są grafowe sieci uwagowe (Graph Attention Networks). Ich znaczenie wynika z samej natury danych elektroenergetycznych. Sieć przesyłowa jest grafem wyposażonym w konkretne cechy: kąty fazowe napięcia, moce, stany węzłów,

obciążenia czy parametry linii. Zwykłe modele uczenia maszynowego często gubią strukturę relacyjną, traktując dane jak płaską tabelę. GAT natomiast uczy się bezpośrednio na grafie, co oznacza, że model widzi nie tylko cechy pojedynczego węzła, lecz także relacje między nimi i znaczenie sąsiedztwa. W systemie, w którym los jednego punktu zależy od zachowania pozostałych, jest to przewaga zasadnicza, a nie kosmetyczna. Kluczowym elementem GAT jest mechanizm uwagi.

Podczas gdy tradycyjna grafowa sieć konwolucyjna agreguje informacje od sąsiadów w sposób jednolity, GAT pyta subtelniej: który sąsiad jest w tej chwili ważniejszy? Którego głos powinien ważyć więcej i która relacja ma większe znaczenie dla oceny ryzyka? Dzięki temu model przypisuje różne wagi poszczególnym węzłom, zamiast traktować ich jak równoprawnych statystów w wielkim przedstawieniu przepływów. W realnej sieci jest to kluczowe, gdyż fizyczna bliskość nie zawsze oznacza równą istotność. Sąsiedztwo jest faktem, ale jego znaczenie pozostaje zmienne.

## Narzędzia AI w predykcji awarii kaskadowych

GAT stanowi fundament modelu NIE, czyli Node Indispensability Estimation. Jego zadaniem jest identyfikacja węzłów niezbędnych – takich, których awaria w konkretnych warunkach operacyjnych mogłaby natychmiast wywołać groźne przeciążenia w innych częściach systemu i naruszyć kryterium bezpieczeństwa N-1. To istotne przesunięcie od abstrakcyjnej centralności ku operacyjnej niezbędności. Węzeł nie musi być najbardziej efektowny topologicznie, aby stać się krytyczny; może zyskać na znaczeniu dlatego, że aktualny układ przepływów, obciążeń i rezerw czyni go punktem, którego utrata uruchomi redystrybucję przekraczającą marginesy bezpieczeństwa. Przypomina to różnicę między formalną rangą a realnym wpływem.

W strukturze organizacyjnej najwyżej sytuuje się prezes, minister lub dyrektor generalny, jednak paraliż instytucji może wywołać księgowa znająca jedyne hasło, informatyk zarządzający systemem albo urzędnik, który „od zawsze wiedział, gdzie leży segregator”. W sieci elektroenergetycznej jest podobnie: najważniejszy nie zawsze okazuje się ten element, który wygląda najpoważniej na schemacie. Krytyczność jest funkcją relacji, stanu i czasu.

Ogromną zaletą GAT, podkreśloną w książce, jest zdolność do działania przy częściowych obserwacjach. To nie drobny dodatek techniczny, lecz kluczowy warunek praktycznej użyteczności. Rzeczywiste systemy SCADA i aparatura pomiarowa nie zawsze dostarczają pełnego, idealnego i aktualnego obrazu każdego węzła; dane bywają opóźnione, niepełne lub kosztownie ograniczone. Klasyczny model wymagający pełnej obserwowalności może prezentować się pięknie na konferencji, pozostając bezradnym w dyspozytorni. Model GAT, dzięki uczeniu się relacji

grafowych i mechanizmowi uwagi, potrafi wnioskować o zagrożeniach nawet przy niepełnym wglądzie w system.

W tym miejscu pojawia się głębsza lekcja epistemologiczna: odporność systemu zależy nie od wszechwiedzy, lecz od jakości wnioskowania przy niepełnej wiedzy. Operator nigdy nie działa w świecie absolutnego poznania, lecz w rzeczywistości opóźnień, uproszczeń, alarmów i presji czasu. W takim środowisku inteligencja polega na rozpoznawaniu wzorców mimo luk. To właśnie próbuje robić GAT – zamiast czekać na idealny obraz całości, wydobywa znaczenie z częściowo widzialnej struktury. Dobra analityka jest więc sztuką widzenia przez mgłę, a nie narzekaniem, że mgła nie podpisała protokołu ustąpienia.

Drugim narzędziem jest Attention-LSTM, czyli połączenie sieci rekurencyjnej LSTM z mechanizmem uwagi. Tutaj problem jest inny. O ile GAT wskazuje węzły niezbędne i ryzykowne w strukturze grafowej, o tyle Attention-LSTM ma przewidywać pełne ścieżki propagacji awarii kaskadowych. Pyta nie tylko „co jest krytyczne?", lecz „co zepsuje się potem?". Awaria kaskadowa jako sekwencja zdarzeń musi być traktowana jak proces czasowy: jeden element wypada, drugi zostaje przeciążony, trzeci reaguje na nowy rozkład przepływów, a czwarty zostaje odłączony przez zabezpieczenia.

To nie jest zwykła lista usterek, lecz narracja systemowa. LSTM (Long Short-Term Memory) powstało po to, by radzić sobie z długimi zależnościami w sekwencjach. Standardowe sieci rekurencyjne zawodzą przy pamięci odległych zdarzeń, gdyż informacja może zanikać lub eksplodować w procesie uczenia. LSTM wykorzystuje komórki pamięci oraz bramki zapominania, wejściową i wyjściową, dzięki czemu model uczy się selekcji informacji. W kontekście kaskady jest to kluczowe – pierwsze zdarzenie może wpływać na rozwój procesu długo po tym, jak w szeregu czasowym pojawią się kolejne stany. Początek kaskady nie znika wraz z upływem kilku kroków; w systemach złożonych przeszłość ma długi ogon.

Ponieważ standardowy LSTM może osłabiać informację przy bardzo długich sekwencjach, do modelu dodaje się mechanizm uwagi (Attention). Pozwala on sieci „spojrzeć wstecz" i dynamicznie ustalić, które wcześniejsze zdarzenia są najważniejsze dla bieżącej predykcji. Nie każde zdarzenie z przeszłości ma tę samą wagę – niektóre są szumem, inne zaś zapalnikiem, którego skutki ujawniają się dopiero teraz.

Mechanizm uwagi umożliwia przypisanie wag stanom historycznym, tworząc kontekst predykcyjny oparty na selektywnej pamięci. To niepokojąca analogia do życia instytucji. Wiele kryzysów publicznych rozwija się jak kaskada: drobne zaniedbanie, niepełna informacja, zła procedura, opóźniona reakcja i wreszcie paniczna decyzja. Gdy katastrofa staje się widzialna, uwaga skupia się

na ostatnim elemencie, bo ten pęka najgłośniej, choć przyczyna leżała znacznie wcześniej. Attention-LSTM uczy maszynę, że nie każde „wczoraj” jest równe; niektóre wczoraj nadal sterują dzisiejszym upadkiem.

Wskazano, że model Attention-LSTM, trenowany na dużych zbiorach symulowanych scenariuszy, osiąga dokładność przewidywania ścieżek awarii przekraczającą 85 procent. Liczba ta nie powinna być traktowana magicznie – skuteczność zależy od jakości danych i reprezentatywności warunków. Ważny jest jednak kierunek: zamiast uruchamiać kosztowne symulacje w chwili kryzysu, system korzysta z modelu, który zna typowe wzorce propagacji i szybko wskazuje prawdopodobną sekwencję zdarzeń.

Trzecim elementem oceny odporności jest przewidywanie onset time, czyli momentu gwałtownego przyspieszenia awarii. Wiele kaskad ma fazę początkową, w której usterki narastają wolno, po czym następuje punkt przełomowy i liczba awarii rośnie lawinowo. Przewidzenie tego momentu ma znaczenie decyzyjne: pozwala odróżnić przypadek pilny (wymagający ostrych działań ochronnych) od stosunkowo pilnego lub niepilnego, co zapobiega nadmiernej reakcji, która sama mogłaby stworzyć nowe ryzyko. Bezpieczeństwo systemu to nie tylko unikanie zbyt słabej odpowiedzi, ale i unikanie reakcji zbyt silnej i źle skalibrowanej.

W energetyce odłączenie obciążenia czy kontrolowane wyspowanie są działaniami poważnymi – mogą uratować system, ale uderzają w gospodarkę. Predykcja pilności jest więc formą racjonalizacji dramatu. Pozwala odróżnić konieczność natychmiastowego cięcia od potrzeby korekty punktu pracy. Bez takiej klasyfikacji operator mógłby zachowywać się jak lekarz, który każdemu pacjentowi na kaszel proponuje amputację – stanowczo i z godną podziwu konsekwencją, lecz jednak niepokojąco.

Czwartym elementem są drzewa decyzyjne służące do oceny krytyczności i wskaźników odporności. Ich wartość tkwi w wydobywaniu relacji między właściwościami sieci a jej stabilnością. Wskazano trzy kluczowe cechy: średnią długość najkrótszej ścieżki, średni współczynnik grupowania oraz średnią efektywną odległość elektryczną do najbliższego generatora. Ten ostatni wskaźnik przekracza czystą topologię – nie pyta o liczbę krawędzi, lecz o właściwości elektryczne połączenia. W systemie energetycznym bliskość nie jest kwestią geograficzną ani wyłącznie grafową.

Wskaźnik dostępności generatorów oddaje znaczenie zdecentralizowanego rozmieszczenia źródeł energii. Krótsza efektywna droga do generacji może odciążyć długie linie przesyłowe i poprawić zniesienie zakłóceń. Nie oznacza to jednak, że rozproszenie jest zawsze lepsze; wymaga ono precyzyjnego sterowania, koordynacji i odporności cybernetycznej. Topologia generacji ma znaczenie: centralizacja bywa efektywna ekonomicznie, lecz tworzy długie zależności przesyłowe,

podczas gdy rozproszenie poprawia dostępność lokalną kosztem złożoności koordynacji. Nie ma darmowego obiadu, zwłaszcza gdy obiad gotuje sieć synchroniczna pod presją falowników.

Wszystkie te metody – GAT, Attention-LSTM, klasyfikacja onset time i drzewa decyzyjne – łączy ambicja przekształcenia niewidzialnej dynamiki ryzyka w informację operacyjną. System nie może czekać, aż awaria wyjaśni swoje intencje; musi rozpoznawać sygnały wstępne i prognozować propagację. Nowoczesna ocena odporności jest sztuką wcześniejszego zrozumienia, której celem nie jest estetyczna mapa zagrożeń, lecz dodatkowy czas na decyzję.

Warto jednak zachować sceptycyzm: sztuczna inteligencja nie rozwiązuje problemu odpowiedzialności. Modele uczą się na danych, które są wersją przeszłości lub symulacji. Jeśli scenariusze treningowe są niepełne, model może być pewny tam, gdzie powinien być pokorny. Jeśli dane są systematycznie stronnicze, predykcja dziedziczy ich ślepotę. Jeśli operatorzy potraktują wynik modelu jak rozkaz, a nie wsparcie decyzji, inteligencja zamieni się w automatyzm – który jest świetny do czasu zdarzenia nieprzewidzianego, gdy komisja od wyjątków ma akurat szkolenie z procedur standardowych.

Ocena odporności musi być więc pojmowana jako układ człowiek-model-procedura-infrastruktura. AI może wskazać węzeł niezbędny i oszacować pilność kaskady, ale decyzje o zrzucie obciążenia czy wyspowaniu niosą skutki społeczne, ekonomiczne i polityczne.

## Architektura obrony i ochrona prewencyjna

Odporność sieci nie jest wyłącznie techniczną optymalizacją; to także zarządzanie stratą. To wybór, komu chwilowo odebrać zasilanie, by reszta systemu nie pogrążyła się w ciemności. Ten brutalny wymiar bezpieczeństwa infrastruktury sprawia, że w chwilach kryzysu system nie pyta, czy wystąpi strata, lecz czy będzie ona kontrolowana, czy totalna.

Ocena odporności stanowi pomost między poznaniem a działaniem. Sama predykcja kaskady nie wystarczy, jeśli brakuje mechanizmów ochrony. Wczesne ostrzeżenie bez procedury jest tylko elegancką paniką. Wykrycie węzła krytycznego bez możliwości rekonfiguracji staje się wiedzą tragiczną. Przewidzenie onset time bez narzędzi interwencji przypomina słyszenie tykania zegara w pomieszczeniu bez drzwi. Prawdziwa wartość oceny odporności ujawnia się dopiero wtedy, gdy zostanie połączona z ochroną prewencyjną, awaryjną i naprawczą.

Architektura obrony systemu – obejmująca te trzy etapy – nie jest pojedynczą funkcją ani jedną procedurą. To struktura rozciągnięta w czasie: system broni się przed awarią, w trakcie jej trwania oraz po niej. Każdy z tych momentów wymaga innej wiedzy, szybkości działania i odwagi

decyzyjnej. Przed awarią kluczowa jest przezorność; w trakcie – szybkość i selektywność; po niej – cierpliwość, dyscyplina sekwencji i zdolność odbudowy bez pychy. W energetyce pycha operacyjna bywa szczególnie kosztowna: zbyt szybkie włączenie nadmiaru elementów może w jednej chwili zniweczyć godziny mozolnej pracy.

Logika ta dzieli się na trzy podstawowe kategorie: ochronę prewencyjną, awaryjną i naprawczą. Ten podział to nie tylko klasyfikacja techniczna, lecz filozofia zarządzania systemem złożonym, gdzie każdy etap odpowiada innemu stanowi organizmu. Ochrona prewencyjna działa, gdy system funkcjonuje normalnie lub w pobliżu tej normy. Ochrona awaryjna uruchamia się, gdy zakłócenie już wystąpiło i należy zatrzymać przejście od zaburzenia do katastrofy. Ochrona naprawcza zaczyna się w momencie rozległej utraty zasilania, by przywrócić system do życia.

Ochrona prewencyjna jest sztuką niedopuszczania do sytuacji, w której pojedyncza usterka mogłaby uruchomić kaskadę. Jej podstawowym narzędziem jest utrzymywanie marginesów bezpieczeństwa, w tym spełnianie kryterium N-1. System powinien być planowany tak, aby utrata jednego istotnego elementu – linii, transformatora czy generatora – nie doprowadziła do przekroczenia limitów fizycznych ani przerwy w dostawach. Kryterium to ma charakter cywilizacyjnie trzeźwy: przyznaje, że awarie będą się zdarzać, ale wymaga, by pojedyncza usterka nie stała się katastrofą.

Prewencja nie polega jedynie na biernym sprawdzaniu formalnych kryteriów, lecz na aktywnym sterowaniu punktem pracy sieci. Operatorzy monitorują przepływy mocy, napięcia, częstotliwość, rezerwy wirujące oraz obciążenia linii. Jeśli analiza wykaże, że utrata jednej linii przeciąży inną, można z wyprzedzeniem zmienić rozdział generacji, ograniczyć przepływ na krytycznej trasie lub skorygować konfigurację sieci. Prewencja jest zatem inteligencją przed zdarzeniem. Jej sukces polega na tym, że nic spektakularnego się nie dzieje – co czyni ją politycznie niewdzięczną formą sukcesu, gdyż najlepiej wykonana praca wygląda jak brak wydarzenia.

Przykładem może być linia X przesyłająca 480 MW przy limicie 500 MW. Jeśli symulacja wykaże, że po utracie równoległej linii Y przepływ na X wzrośnie do 560 MW, operator może prewencyjnie obniżyć bazowy przepływ do 400 MW, by po awarii pozostać w granicach bezpieczeństwa. To istotą prewencji: działanie teraz, aby późniejszy wstrząs nie przekroczył zdolności absorpcji systemu. Podobnie działa rezerwa wirująca – jeśli operator przewiduje spadek marginesu poniżej minimum podczas wieczornego szczytu, może wcześniej uruchomić dodatkową turbinę gazową. Rezerwa wirująca jest jednym z najbardziej eleganckich pojęć energetyki; przypomina, że bezpieczeństwo to nie to, co wykorzystujemy, lecz to, czego jeszcze nie musimy wykorzystać. Nadmiar w systemie nie zawsze jest marnotrawstwem – często jest polisą przeciwko katastrofie. Ochrona prewencyjna opiera się także na zabezpieczeniach przekaźnikowych i lokalnej automatyce, które wykrywają

anomalie elektryczne i izolują uszkodzone elementy, podczas gdy regulatory napięcia korygują lokalne wahania.

## Ochrona prewencyjna a mechanizmy ochrony awaryjnej

Narzędzia typu SCED, czyli ekonomiczne dysponowanie z ograniczeniami bezpieczeństwa, pozwalają prowadzić system efektywnie, nie zbliżając się przy tym do granic operacyjnych. To kluczowe rozróżnienie: efektywność bez bezpieczeństwa jest w energetyce fałszywą oszczędnością. Można przez pewien czas pracować taniej i bliżej limitów, lecz system zaczyna wtedy przypominać księgowego, który uznał poduszkę finansową za „nieproduktywny kapitał", by później dziwić się, że pierwsza większa faktura wywołuje zapaść płynności.

Ochrona prewencyjna ma jednak swoje granice. Nie każde zdarzenie da się przewidzieć, nie każdą kombinację awarii objąć standardem N-1 i nie każdy stan sieci można utrzymać w komfortowym marginesie. Ekstremalne warunki pogodowe, cyberataki, nagła utrata dużego źródła, jednoczesne uszkodzenia wielu elementów czy nieoczekiwana reakcja źródeł odnawialnych mogą wypchnąć system poza obszar, w którym prewencja wystarcza. Wtedy uruchamia się drugi etap: ochrona awaryjna.

Ochrona awaryjna opiera się na logice działania w stanie bezpośredniego zagrożenia stabilności. Zakłócenie już wystąpiło, marginesy zostały naruszone, a system może tracić częstotliwość, napięcie lub synchronizm. Tu nie chodzi już o elegancką optymalizację, lecz o powstrzymanie rozpadu. Jeśli prewencja jest sztuką unikania pożaru, to ochrona awaryjna jest sztuką odcięcia części budynku, aby nie spłonęło całe miasto. Jej cel bywa brutalny, ale racjonalny: poświęcić mniej, aby uratować więcej.

Kluczowym mechanizmem ochrony awaryjnej jest zrzucanie obciążenia. Gdy w systemie dochodzi do gwałtownej nierównowagi między generacją a zapotrzebowaniem i częstotliwość zaczyna spadać poniżej ustalonych progów, automatyczne systemy UFLS (Under Frequency Load Shedding) odłączają część odbiorców. Analogicznie, w przypadku zagrożenia napięciowego, stosuje się UVLS (Under Voltage Load Shedding). Dla odbiorcy końcowego jest to porażka – brak prądu. Z perspektywy systemu to jednak amputacja ratująca życie; częściowe odłączenie odbiorców może zapobiec całkowitemu blackoutowi.

Rozważmy system pracujący z obciążeniem 10 000 MW przy częstotliwości 50 Hz. Nagła utrata bloku o mocy 1500 MW powoduje 15-procentowy deficyt. Rezerwy wirujące pokrywają jedynie część braku, a częstotliwość gwałtownie spada w stronę wartości krytycznych. System UFLS odłącza

etapowo odbiorców o łącznej mocy 900 MW, dzięki czemu równowaga zostaje przywrócona, a reszta systemu ocalona. To przykład decyzji społecznie nieprzyjemnej i technicznie koniecznej, lecz moralnie łatwiejszej do obrony niż bierność prowadząca do powszechnej ciemności.

## Warstwy ochrony awaryjnej i naprawczej

Kolejnym mechanizmem ochrony awaryjnej są specjalne schematy zabezpieczeń, określane jako SPS lub RAS. To przygotowane wcześniej automatyczne algorytmy, które reagują na ściśle określone warunki w systemie. Wykorzystując dane z rozległych systemów pomiarowych, SCADA lub WAMS, podejmują one działania w ułamkach sekund – szybciej, niż człowiek byłby w stanie w ogóle zdiagnozować problem. Działania te mogą obejmować zrzut generacji, rekonfigurację sieci lub inne środki zapobiegające przeciążeniom i utracie synchronizmu. Siłą tych systemów jest szybkość; ryzykiem zaś fakt, że operują one w ramach przewidzianej logiki, a rzeczywistość ma niekiedy paskudny zwyczaj nie czytać instrukcji.

Rozważmy sytuację, w której kompleks elektrowni o mocy 1000 MW przesyła energię dwiema liniami 400 kV. Po awarii jednej z nich cały przepływ trafia na drugą. Choć fizycznie linia mogłaby chwilowo wytrzymać takie obciążenie, gwałtowny skok mocy wywołuje groźne oscylacje elektromechaniczne. SPS reaguje natychmiast, zrzucając generator o mocy 300 MW. Redukuje to przesył do stabilnego poziomu i pozwala zachować spójność systemu bez konieczności odcinania odbiorców domowych. Przykład ten obrazuje różnicę między mechanicznym trzymaniem się limitów a dynamicznym rozumieniem stabilności: linia może nie być jeszcze „spalona”, ale system może już zmierzać ku utracie synchronizmu.

Ochrona awaryjna obejmuje również dynamiczne sterowanie stabilnością, mające na celu tłumienie oscylacji i zapobieganie rozsynchronizowaniu generatorów. Stosuje się tu m.in. dynamiczne rezystory hamujące lub gwałtowne zwiększanie wzbudzenia generatora. W systemach synchronicznych utrata synchronizmu jest jednym z najgroźniejszych zjawisk, gdyż oznacza, że elementy systemu przestają pracować we wspólnym rytmie. Sieć elektroenergetyczna jest w pewnym sensie ogromnym chórem fizyki. Gdy część śpiewaków wypada z rytmu, nie wystarczy poprosić o ciszę – trzeba natychmiast przywrócić warunki wspólnej pracy lub podzielić chór na mniejsze zespoły.

Tym motywem kieruje się ostatni środek awaryjny: kontrolowane tworzenie wysp. Gdy utrata synchronizmu w dużym systemie staje się nieunikniona, można celowo podzielić sieć na mniejsze, niezależne obszary, z których każdy posiada zbilansowaną generację i obciążenie. Wyspowanie jest środkiem drastycznym, lecz niekiedy niezbędnym. Lepiej mieć kilka stabilnych wysp niż jeden

tonący kontynent. W skali państwa przypominałoby to regionalizację kryzysu: odcięcie uszkodzonych zależności w celu ochrony funkcjonujących obszarów i niedopuszczenie do kaskadowego upadku całości.

Jeżeli ochrona awaryjna zawiedzie, system przechodzi w stan ochrony naprawczej. To etap po rozległej awarii, gdy znaczne części sieci są pozbawione zasilania, odbiorcy zostali odłączeni, a infrastruktura utraciła referencyjne wartości napięcia i częstotliwości. Ochrona naprawcza nie jest prostym „ponownym włączeniem prądu", lecz skomplikowanym procesem odbudowy porządku elektrycznego z ruin. Zbyt szybkie przywracanie obciążeń grozi wtórnym blackoutem, zbyt wolne zaś przedłuża dotkliwe skutki społeczne i gospodarcze.

Wymagana jest tu dyscyplina sekwencji. Pierwszym etapem jest czarny start (black start). Większość dużych elektrowni konwencjonalnych nie może uruchomić się samodzielnie, gdyż ich systemy pomocnicze – pompy, wentylatory czy układy wzbudzenia – wymagają energii z zewnątrz. Proces odbudowy zaczyna się więc od jednostek zdolnych do startu autonomicznego, takich jak małe elektrownie wodne, turbiny gazowe lub układy wspierane magazynami energii. Tworzą one pierwsze wyspy napięcia, które następnie zasilają urządzenia pomocnicze większych jednostek.

Przykład obrazuje to najlepiej: po blackoutcie mała elektrownia wodna o mocy 30 MW uruchamia się z pomocą lokalnego banku baterii. W ciągu kilku minut osiąga nominalne obroty i napięcie, zasila lokalną stację 110 kV, a następnie dostarcza energię do dużej elektrowni cieplnej o mocy 500 MW. Dzięki temu kolos może uruchomić własne systemy pomocnicze. W ciemności systemowej hierarchia mocy zostaje na chwilę odwrócona: wielki obiekt potrzebuje małego startera.

Drugim etapem ochrony naprawczej jest sekwencyjne przywracanie obciążenia i rekonfiguracja sieci. Operatorzy stopniowo podłączają odbiorców, lecz nie mogą robić tego dowolnie. Odbudowywany system cechuje się niską inercją i wąskimi marginesami stabilności; każde nowe obciążenie obniża częstotliwość. W pierwszej kolejności zasilanie przywraca się infrastrukturze krytycznej: szpitalom, wodociągom, łączności i systemom bezpieczeństwa. Nie jest to biurokracja, lecz konieczność fizyczna. Jeśli wyspa dysponuje 200 MW generacji i 20 MW rezerwy wirującej, operator podłącza obciążenia w małych krokach: np. 5 MW dla szpitala, potem 10 MW dla pomp wodociągowych. Częstotliwość spada nieznacznie i stabilizuje się. Gdyby jednak od razu podłączyć dzielnicę o poborze 30 MW, rezerwa zostałaby przekroczona, a spadek częstotliwości mógłby uruchomić zabezpieczenia, niwecząc cały proces odbudowy.

Ta lekcja wykracza poza energetykę. Odbudowa każdego złożonego systemu – państwa po kryzysie, firmy po awarii czy gospodarki po szoku – wymaga sekwencji i uznania realnych rezerw. Najgorszym błędem jest żądanie pełnej wydolności natychmiast po upadku tylko dlatego, że „ludzie

czekają”. Ludzie rzeczywiście czekają, ale fizyka nie głosuje w sondażach. Przeciążenie systemu ponad jego aktualną rezerwę doprowadzi do ponownego, być może głębszego upadku.

Trzecim etapem jest synchronizacja wysp. Gdy poszczególne fragmenty sieci zostaną ustabilizowane, należy je połączyć w jeden spójny system. Wymaga to precyzyjnego zrównania napięć, częstotliwości i kątów fazowych; zamknięcie wyłącznika bez właściwej synchronizacji mogłoby wywołać gwałtowne przepływy wyrównawcze i kolejną awarię. Odbudowa kończy się nie w momencie pojawienia się prądu, lecz gdy system odzyskuje wspólny rytm.

Wszystkie trzy warstwy – prewencyjna, awaryjna i naprawcza – tworzą architekturę odporności. Nie są one alternatywami. Twierdzenie, że dobra ochrona awaryjna pozwala zaniedbać prewencję, byłoby jak uznanie, że posiadanie oddziału intensywnej terapii w szpitalu zdejmuje obowiązek zapinania pasów bezpieczeństwa. Z kolei wiara, że doskonała prewencja eliminuje potrzebę planowania odbudowy, to administracyjne zaklinanie losu. Dojrzały system zakłada możliwość awarii i opiera swoją siłę na wielowarstwowej odpowiedzi.

Odporność jest funkcją czasu. Przed awarią liczy się przewidywanie i utrzymywanie marginesów; w trakcie – szybkie ograniczanie szkód; po niej – sekwencyjne przywracanie funkcji. System działający tylko w jednym z tych wymiarów pozostaje niebezpiecznie niepełny: sama prewencja może zostać zaskoczona, sama reakcja awaryjna bywa brutalna, a sama odbudowa staje się heroicznym naprawianiem skutków zaniedbań. Dopiero ich integracja tworzy dojrzałą obronę.

Współczesne AI wzmacnia każdy z tych poziomów. W prewencji pomaga identyfikować węzły krytyczne i stany naruszające kryterium N-1. W ochronie awaryjnej wspiera wybór działań w czasie rzeczywistym, tam gdzie sztywne schematy RAS nie nadążają za złożonością sytuacji. W ochronie naprawczej zaś optymalizuje sekwencję przywracania obciążeń, dobór zasobów black start oraz proces synchronizacji wysp.

## Planowanie strukturalne a dynamiczne sterowanie siecią

Należy jednak powtórzyć: AI nie jest osobnym poziomem zbawienia. To warstwa poznawczo-decyzyjna, która musi zostać osadzona w procedurach, odpowiedzialności i inżynierskiej fizyce systemu. Szczególne znaczenie ma tu przejście od sztywnych schematów do sterowania adaptacyjnego. Tradycyjne systemy RAS i SPS są potężne, lecz działają według logiki przygotowanych reakcji. W świecie dynamicznych zmian, gdzie źródła odnawialne, magazyny, prosumenci i warstwa cybernetyczna mnożą liczbę możliwych stanów, sztywne tabele mogą okazać

się niewystarczające. Nie dlatego, że są błędne, lecz ponieważ rzeczywistość ma więcej kombinacji niż cierpliwość projektantów.

Tu otwiera się przestrzeń dla DRL, czyli głębokiego uczenia ze wzmocnieniem. Zanim jednak przejdziemy do techniki, warto zauważyć, że architektura obrony sieci elektroenergetycznej jest także lekcją myślenia instytucjonalnego. Każdy poważny system publiczny powinien opierać się na ochronie prewencyjnej, awaryjnej i naprawczej; powinien pilnować marginesów, reagować na kryzys i potrafić się odbudować. Tymczasem wiele instytucji funkcjonuje jedynie w dwóch trybach: samozadowolenia przed kryzysem i improwizacji po nim. Brakuje im realnej prewencji, automatyzmów awaryjnych i planów odbudowy. Energetyka, przez swoją bezlitosną fizykę, nie znosi takiej teatralności. Tu nie wystarczy stwierdzić, że „sytuacja jest monitorowana". Sieć pyta brutalniej: monitorowana – czyli czym, jak szybko i jaka decyzja zapadnie po alarmie?

System Planning i System Control: od projektowania odporności do decyzji w czasie rzeczywistym. O ile ochrona prewencyjna, awaryjna i naprawcza opisują trzy momenty obrony systemu, o tyle system planning i system control definiują dwa wielkie tryby budowania odporności. Pierwszy należy do czasu długiego: projektowania, inwestycji, modernizacji i zmiany architektury sieci. Drugi to czas krótki, niemal natychmiastowy: reagowanie na rozwijającą się awarię, zanim lokalne uszkodzenie przejdzie w lawinę odłączeń. W pierwszym przypadku decyzje mierzy się latami i budżetami; w drugim – sekundami i ułamkami sekund, których skutki będą później liczone w raportach, odszkodowaniach, politycznych konferencjach i społecznym gniewie. System planning jest więc odpornością wpisaną w strukturę – momentem, w którym można jeszcze działać bez presji alarmu.

Można badać topologię, symulować scenariusze, identyfikować słabe punkty, planować rozmieszczenie źródeł energii i zwiększać głębię obronną infrastruktury. W ujęciu Liu planowanie systemu jest długoterminową, proaktywną strategią projektową, stosowaną przed wystąpieniem zakłóceń. Jej celem jest stworzenie architektury, która wytrzyma losowe usterki i zdarzenia ekstremalne, nie zamieniając jednocześnie odporności w ekonomicznie niemożliwy kult pancerności. W systemach infrastrukturalnych nie istnieje bowiem absolutne bezpieczeństwo. Można marzyć o sieci z pełną redundancją każdego elementu, gdzie każdy transformator ma zastępstwo, a każda linia jest podwojona, lecz taka fantazja szybko zderza się z kosztami, przestrzenią i zwykłą racjonalnością.

Odporność nie polega na tym, aby wzmacniać wszystko jednakowo, lecz na wiedzy, co wzmacniać najpierw i jakim kosztem. Bez tej hierarchii bezpieczeństwo staje się księgą pobożnych życzeń pisaną językiem przetargów publicznych. Pierwszym obszarem system planning jest optymalizacja topologii sieci. Fizyczny układ połączeń decyduje o tym, którędy płyną moce i jakie powstaną

ścieżki alternatywne po awarii. Topologia nie jest tłem pracy systemu – jest warunkiem jego zachowania.

Źle zaprojektowana sieć może wyglądać poprawnie w stanie normalnym, by ujawnić kruchość dopiero po zakłóceniu. To typowy dramat systemów złożonych: prawdziwa natura architektury wychodzi na jaw nie w dniu spokojnym, lecz w dniu odchylenia. Autor wskazuje dwa kluczowe parametry topologiczne: dostępność do generatorów oraz średnią długość najkrótszej ścieżki. Dostępność ta mierzona jest przez średnią efektywną odległość rezystancyjną konsumentów do najbliższego źródła. Im bardziej zdecentralizowane rozmieszczenie generacji, tym krótsze dystanse elektryczne i większa zdolność systemu do przetrwania zakłóceń. To dowód na to, że lokalizacja źródeł nie jest wyłącznie sprawą rynku, lecz elementem odporności państwa.

Decentralizacja nie jest jednak magicznym słowem rozwiązującym wszystkie problemy. Rozproszone źródła wymagają koordynacji, sterowania i odporności cybernetycznej. Mogą skracać dystanse elektryczne, ale zwiększają liczbę punktów sterowania; ograniczają skutki awarii dużego źródła, lecz wprowadzają zmienność pogodową. System odporny nie powstaje przez prostą zamianę centralizacji w jej odwrotność, lecz przez mądrą architekturę relacji między źródłami centralnymi, rozproszonymi i magazynami. W energetyce, jak w państwie, najgorsze reformy zaczynają się od wiary, że wystarczy odwrócić dawny błąd, by otrzymać mądrość.

Drugim parametrem jest średnia długość najkrótszej ścieżki. Intuicyjnie można sądzić, że krótsza ścieżka zawsze wzmacnia system, poprawiając łączność i dostępność dróg alternatywnych. Jednak w warunkach ograniczonych marginesów pojemnościowych topologia o zbyt krótkiej średniej ścieżce – zwłaszcza o cechach sieci małego świata – może obniżać odporność na awarie kaskadowe. Zbyt sprawna łączność może bowiem równie sprawnie przenosić przeciążenia. System nie powinien być ani labiryntem, ani autostradą dla katastrofy. To jedna z najcenniejszych lekcji teorii sieci: efektywność i odporność nie zawsze są tym samym. Wydajny w normalnych warunkach system może być kruchy w kryzysie, jeśli brakuje mu redundancji i zdolności izolacji. W logice rynku premiuje się wykorzystanie zasobów blisko granic opłacalności; w logice bezpieczeństwa trzeba utrzymywać przestrzeń niewykorzystaną, która w zwykły dzień wygląda jak nadmiar, a w dniu kryzysu okazuje się powodem, dla którego światło nadal świeci. Rezerwa jest nieatrakcyjna tylko do momentu, gdy staje się ostatnim mostem.

Drugim narzędziem planowania jest hardening, czyli fizyczne wzmacnianie komponentów krytycznych. Problem polega na tym, że przy ograniczonym budżecie nie da się wzmocnić wszystkiego. Źle dobrana selekcja tworzy paradoks: wydajemy środki na elementy spektakularne, pomijając te, których awaria uruchomi realną kaskadę. Tak powstaje infrastrukturalna wersja

polityki pomnikowej: dużo betonu, mało odporności. Rozwiązaniem proponowanym przez Liu i współautorów jest gradientowa strategia celowej alokacji zasobów.

Najpierw, za pomocą symulacji Monte Carlo, oblicza się metrykę krytyczności odporności, wskazującą wpływ usterki danego komponentu na sumaryczne straty. Następnie algorytm k-means grupuje elementy w klastry o różnym stopniu ważności, a budżety rozdzielane są gradientowo: elementy w tym samym klastrze otrzymują poziom ochrony proporcjonalny do ich znaczenia. Zamiast tworzyć kilka niezniszczalnych punktów, strategia podnosi odporność całego systemu równomiernie i efektywnie kosztowo. Podejście to odrzuca dwa naiwne modele: egalitarny (wszystkim po równo) oraz heroiczny (ochrona tylko symboli infrastruktury). Gradientowe wzmacnianie sugeruje coś subtelniejszego: system ma różne poziomy krytyczności, więc ochrona powinna być różnicowana, ale nie skrajnie skoncentrowana. To logika portfela odporności, a nie jednego sejfu. W systemach złożonych jeden pancerny punkt nie wystarczy, jeśli reszta sieci pęka jak cienkie szkło.

Planowanie obejmuje również rozmieszczanie rozproszonych źródeł energii i rezerw regulacyjnych, co jest kluczowe przy transformacji w stronę OZE. Źródła odnawialne zmieniają profile generacji i przepływy, ale wprowadzają zmienność wymagającą bilansowania. Planowanie musi więc uwzględniać nie tylko ilość energii, lecz także jej lokalizację, czas powstania i koszt dla sterowalności systemu. W przeciwnym razie transformacja może przypominać dekorowanie domu bez sprawdzenia fundamentów: ładnie, zielono, medialnie – aż do pierwszego trzasku.

System planning to jednak tylko połowa opowieści. Nawet najlepiej zaprojektowana sieć może wejść w stan awaryjny. Wtedy decyduje system control – zdolność do szybkiego sterowania i zabezpieczania sieci w trakcie rozwijającej się kaskady. Czas długi ustępuje miejsca czasowi krótkiemu. Nie chodzi już o planowanie inwestycji, lecz o natychmiastową akcję; nie o statyczne skutki hipotetycznych awarii, lecz o dynamiczną interwencję w proces, który właśnie trwa.

Tradycyjne schematy RAS (Remedial Action Schemes) opierają się na przygotowanych tabelach i wytycznych, co zapewnia szybkość i przewidywalność. Jednak przy rosnącej złożoności sieci stają się one niewystarczające. Liczba kombinacji awarii i konfiguracji źródeł OZE sprawia, że ręczne przygotowanie reakcji dla każdego scenariusza jest nierealne. Tradycyjny schemat przypomina mapę drogową w mieście, które codziennie przebudowuje własne ulice.

Tu pojawia się DRL (Deep Reinforcement Learning). W koncepcji Liu i współautorów DRL służy do sterowania systemem w czasie rzeczywistym podczas awarii kaskadowej. Agent uczy się podejmować działania metodą prób i błędów w środowisku symulacyjnym, maksymalizując funkcję

nagrody. Nie jest to bierna klasyfikacja danych, lecz uczenie działania – model nie tylko przewiduje zdarzenia, ale uczy się, jak ograniczyć straty.

Problem sformułowano jako proces decyzyjny Markowa. Stan obejmuje znormalizowane parametry sieci: fazy napięcia, przepływy mocy i wskaźniki awaryjności. Akcją naprawczą jest celowe, prewencyjne odcięcie wybranej linii przesyłowej, aby przerwać propagację awarii. Przejście oznacza nowy stan sieci po akcji, symulowany modelem stochastycznym, a nagroda promuje minimalizację utraty mocy. Agent uczy się zatem sztuki kontrolowanego cięcia: odłączyć tak, aby ocalić jak najwięcej.

Choć brzmi to paradoksalnie, w systemie kaskadowym pewne połączenie może stać się kanałem propagacji przeciążenia. Celowe rozłączenie służy izolacji uszkodzonego procesu – podobnie jak kontrolowane wyspowanie czy pasy przeciwpożarowe w lesie. Czasem trzeba przerwać ciągłość, aby ocalić całość. W normalnej sytuacji połączenie jest zasobem; w awaryjnej może stać się przewodem katastrofy. Inteligencja operacyjna polega na rozpoznaniu momentu tej zmiany.

Do trenowania agenta zastosowano PPO (Proximal Policy Optimization) w architekturze actor-critic: sieć aktora wybiera akcje, a krytyka ocenia ich wartość. PPO wykorzystuje obciętą funkcję celu, co stabilizuje trening i zapobiega chaotycznym zmianom strategii pod wpływem pojedynczych doświadczeń – zbyt nerwowa inteligencja w systemach bezpieczeństwa byłaby jedynie wyrafinowaną formą paniki.

Wyniki symulacji są znaczące. Agent DRL podejmował decyzje niemal natychmiastowo, poniżej 0,01 sekundy, podczas gdy klasyczne algorytmy przeszukujące (np. branch exclusion) potrzebowały od 0,36 do 0,73 sekundy. W zwykłej rozmowie ta różnica jest nieistotna; w awarii kaskadowej może być granicą między kontrolą a spóźnionym raportem. Systemy elektroenergetyczne rozchodzą się w czasie fizycznym, nie urzędowym.

Skuteczność mierzono zachowaną dostawą mocy: model PPO utrzymał średnio 81,16% w systemie IEEE 39 Bus i 67,08% w IEEE 57 Bus. Bez algorytmów RAS wartości te wynosiły odpowiednio 67,98% i 63,11%. Różnica ta pokazuje, że adaptacyjne sterowanie nie tylko przyspiesza reakcję, ale realnie ogranicza rozmiar blackoutu. Nie jest to dowód na bezkrytyczne wdrażanie DRL wszędzie, lecz potwierdzenie, że klasyczna logika tabelaryczna ma konkurenta zdolnego uczyć się nieliniowej dynamiki kaskad. Pozostaje jednak pytanie o granice zaufania: agent DRL może być szybki i skuteczny, ale szybkość nie jest tym samym co odpowiedzialność.

# Od sterowania AI do odporności cyberfizycznej

System control oparty na AI musi być osadzony w rygorystycznym środowisku testowania, walidacji i audytu, obejmującym symulacje skrajne, ochronę przed błędami danych oraz nadzór operatorów. Jeśli agent uczy się w symulacji, należy pytać, jak wiernie odwzorowuje ona rzeczywistość. Gdy podejmuje decyzje o odcinaniu elementów sieci, trzeba określić granice jego autonomii. A jeśli maksymalizuje zachowaną moc, kluczowe jest pytanie, czy funkcja nagrody uwzględnia wszystkie istotne koszty społeczne, techniczne i kwestie bezpieczeństwa.

Funkcja nagrody stanowi jeden z najważniejszych problemów filozoficznych sztucznej inteligencji stosowanej w infrastrukturze krytycznej. To, co zdefiniujemy jako cel, stanie się kierunkiem działania agenta. Jeśli nagroda minimalizuje utratę generowanej mocy, model będzie optymalizował system pod ten konkretny wskaźnik. Tymczasem system elektroenergetyczny opiera się na wielu wartościach: stabilności częstotliwości i napięcia, bezpieczeństwie sprzętu, zasilaniu infrastruktury krytycznej, minimalizacji liczby odbiorców pozbawionych prądu, sprawiedliwym rozkładzie obciążeń, zdolności do odbudowy czy ograniczeniu ryzyka wtórnych awarii. Każda funkcja celu jest uproszczeniem świata, a w systemie krytycznym takie uproszczenie może komuś wyłączyć światło.

Nie oznacza to jednak konieczności odrzucenia DRL. Przeciwnie – należy traktować tę technologię poważnie, czyli bez technoentuzjastycznego kadzidła i bez konserwatywnego odruchu „zawsze robiliśmy inaczej”. DRL może stać się narzędziem szczególnie przydatnym w scenariuszach, w których tradycyjne schematy nie nadążają za liczbą możliwych stanów. Może wspierać operatora, proponować ranking działań, symulować skutki odcięć czy uczyć się strategii minimalizacji kaskady. Powinno być jednak elementem architektury obrony, a nie jej suwerenem. Sztuczna inteligencja w energetyce powinna pełnić rolę bardzo szybkiego doradcy w sztabie kryzysowym, a nie jako nieodwoływalny monarcha ciemności i światła.

Różnica między system planning a system control jest zatem różnicą między odpornością zaprojektowaną a odpornością wykonaną w chwili próby. Planowanie tworzy topologię, rezerwy, wzmocnienia oraz rozmieszczenie źródeł i warunki, w których awaria ma mniejsze szanse stać się kaskadą. Sterowanie przejmuje rolę wtedy, gdy mimo tych zabezpieczeń awaria się rozwija. Jedno bez drugiego jest niepełne.

Najlepszy system control nie naprawi lat złego planowania, choć może ograniczyć skutki. Z kolei najlepsze planowanie nie zwalnia z potrzeby szybkiej reakcji, gdyż świat nie ma obowiązku trzymać się scenariuszy projektowych. Odporność rodzi się z ich połączenia: długiej mądrości struktury i krótkiej mądrości działania.

W ten sposób model zaczyna tworzyć spójną całość. Teoria sieci złożonych pozwala zrozumieć architekturę relacji, a ocena odporności wskazuje podatności, węzły krytyczne, ścieżki kaskady i momenty przyspieszenia. Ochrona prewencyjna utrzymuje marginesy, awaryjna ogranicza katastrofę w trakcie jej rozwoju, a naprawcza podnosi system po upadku. System planning zmienia strukturę, natomiast system control ingeruje w dynamikę. AI przenika te poziomy jako narzędzie rozpoznawania i decyzji. Nie ma tu jednego cudownego elementu – jest ekologia odporności.

Sieć cyberfizyczna: kiedy awaria płynie nie tylko przez przewody, lecz także przez dane. Współczesna sieć elektroenergetyczna nie jest już wyłącznie systemem fizycznym. To system cyberfizyczny, w którym infrastruktura materialna i informacyjna tworzą jeden sprzężony organizm. Linie przesyłowe, transformatory czy generatory nadal podlegają prawom elektrotechniki, lecz ich praca zależy coraz silniej od sensorów, systemów SCADA, automatyki zabezpieczeniowej, komunikacji cyfrowej, algorytmów predykcyjnych, sterowania rozproszonego, danych meteorologicznych, rynków bilansujących i decyzji podejmowanych w czasie rzeczywistym. Prąd płynie przewodami, ale decyzja o tym, jak ma płynąć, coraz częściej płynie przez dane.

Ta zmiana ma charakter głęboki. Dawna sieć była hierarchiczna: duże elektrownie wytwarzały moc, sieć przesyłowa transportowała ją na odległość, a dystrybucja dostarczała energię odbiorcom, którzy zasadniczo jedynie ją pobierali. Choć obraz ten był uproszczeniem, dobrze oddawał ówczesny kierunek myślenia. Współczesny system staje się wielokierunkowy. Pojawiają się prosumenci, magazyny energii, źródła odnawialne, mikrosieci, instalacje sterowane falownikami, agregatory elastyczności, inteligentne liczniki i automatyczne systemy zarządzania popytem. Odbiorca przestaje być tylko końcem przewodu – staje się elementem gry systemowej.

W takim świecie odporność nie może oznaczać wyłącznie wytrzymałości linii na przeciążenie czy transformatora na uszkodzenie. Musi obejmować także odporność komunikacji, danych, algorytmów, systemów sterowania oraz odporność organizacyjną operatorów. Jeśli system błędnie odczytuje swój stan, może podjąć złą decyzję. Jeśli dane są opóźnione, reakcja nastąpi zbyt późno. Błędny odczyt czujnika może sprawić, że zabezpieczenie zadziała niepotrzebnie lub zawiedzie w krytycznym momencie. Z kolei malware zakłócający warstwę komunikacyjną może wprowadzić fizyczną sieć w stan ryzyka poprzez zdarzenie, które nie zaczęło się od przeciążenia przewodu, lecz od naruszenia integralności informacji.

Ewoluujące sieci elektroenergetyczne należy zatem rozumieć jako złożone systemy cyberfizyczne, w których obok modelowania infrastruktury fizycznej pojawia się problem powiązania z sieciami cybernetycznymi oraz scenariuszami propagacji złośliwego oprogramowania. Jest to istotne uzupełnienie klasycznej teorii awarii kaskadowych. Kaskada nie musi już oznaczać wyłącznie sekwencji przeciążeń linii; może obejmować również ciąg błędów informacyjnych, fałszywych

pomiarów, sygnałów i niedostępności komunikacji oraz nieadekwatnych decyzji automatyki. To przesunięcie komplikuje pojęcie podatności.

W tradycyjnej analizie pytaliśmy, który węzeł jest topologicznie krytyczny, która krawędź ma wysoką centralność i gdzie przepływ po awarii przekroczy limit. W analizie cyberfizycznej trzeba pytać także: które sensory są kluczowe dla świadomości sytuacyjnej, które kanały komunikacyjne stanowią pojedynczy punkt awarii, które systemy sterowania mają uprawnienia do działań automatycznych, jakie dane karmią algorytm predykcyjny, jaki błąd pomiaru może zmienić decyzję i czy system potrafi odróżnić prawdziwe zakłócenie fizyczne od zakłócenia informacyjnego.

## Cyberfizyczny układ nerwowy i problem obserwowalności

Można powiedzieć, że dawniej sieć miała ciało, a dziś ma także układ nerwowy. Linie, generatory i transformatory stanowią mięśnie i kości systemu; sensory, SCADA, WAMS, algorytmy oraz telekomunikacja są jego nerwami, zaś operatorzy i procedury pełnią rolę mózgu instytucjonalnego. Problem polega na tym, że układ nerwowy zwiększa sprawność, ale jednocześnie wprowadza nową klasę chorób. Organizm pozbawiony nerwów jest powolny i prymitywny; organizm z nerwami może reagować błyskawicznie, lecz bywa podatny na paraliż, drgawki lub halucynacje. W cyberfizycznej energetyce halucynacja danych nie jest metaforą literacką – to potencjalne źródło realnej awarii.

W tym kontekście kluczowe staje się pojęcie obserwowalności. Operator nie zarządza rzeczywistością bezpośrednio, lecz jej modelem budowanym przez pomiary, estymację stanu, wizualizacje, alarmy i analitykę. Jeśli model jest niepełny, operator może nie dostrzec narastającego ryzyka. Jeśli jest zbyt obciążony alarmami, krytyczny sygnał może zginąć w szumie. Gdy zaś model fałszywie uspokaja, organizacja może trwać w złudzeniu pełnej kontroli. To problem tyleż ludzki, co techniczny: system informacyjny potrafi nie tylko informować, ale i usypiać.

Dlatego modele takie jak GAT są istotne przy częściowych obserwacjach. W rzeczywistych systemach SCADA często brakuje pełnego monitorowania wszystkich stacji ze względu na koszty i ograniczenia techniczne. Grafowe sieci uwagowe pozwalają wnioskować o zagrożeniach mimo braków w danych, ponieważ uczą się relacji między węzłami i potrafią odtworzyć znaczenie informacji z kontekstu sąsiedztwa. Jest to narzędzie niezbędne tam, gdzie pełna wiedza jest luksusem, a decyzja koniecznością.

Zdolność działania przy niepełnych danych nie powinna być jednak mylona z nieomylnością. Model wnioskujący z luk może zostać zwiedziony przez braki nietypowe, systematyczne lub złośliwie

spreparowane. O ile przy losowych ograniczeniach pomiarowych model radzi sobie dobrze, o tyle w przypadku skoordynowanego ataku, celowego maskowania zdarzeń czy awarii komunikacyjnej w elementach krytycznych, ryzyko gwałtownie rośnie. W systemie cyberfizycznym nie wystarczy pytać, czy model jest trafny przy niepełnej obserwacji; trzeba zapytać, czy jest odporny na obserwację zmanipulowaną.

Tu pojawia się napięcie między automatyzacją a odpowiedzialnością. Im bardziej złożony system, tym silniej potrzebuje automatyzacji, gdyż człowiek nie jest w stanie analizować wszystkich stanów w czasie rzeczywistym. Jednak większa automatyzacja to większe ryzyko, że błędna informacja zostanie błyskawicznie przełożona na błędną akcję. Automatyka ma tę zaletę, że nie panikuje. Ma też tę wadę, że nie zawstydza się swojej pomyłki.

Działa zgodnie z nadaną jej logiką, nawet gdy świat przesunął się poza jej ramy. W klasycznych zabezpieczeniach elektroenergetycznych szybkość jest cnotą: zwarcie należy usunąć natychmiast, przeciążenie ograniczyć przed uszkodzeniem elementu, a spadek częstotliwości powstrzymać przed zapaścią systemu. Jednak w warstwie cyberfizycznej szybkość musi iść w parze z walidacją informacji. Fałszywy sygnał wywołujący szybkie odłączenie może sam zainicjować kaskadę, a fałszywy brak alarmu pozwoli awarii rozwinąć się bez przeszkód. W obu przypadkach problemem nie jest fizyka, lecz relacja między informacją a działaniem.

Odporność cyberfizyczna wymaga zatem redundancji poznawczej. Nie chodzi jedynie o rezerwową linię czy dodatkowy transformator, lecz o alternatywne źródła danych, krzyżową walidację pomiarów, detekcję anomalii i segmentację systemów sterowania, a także procedury pracy przy utracie komunikacji, możliwość manualnego przejęcia sterowania oraz algorytmy sygnalizujące niepewność. System mówiący wyłącznie „tak” lub „nie” bywa zbyt pewny siebie. System dojrzały powinien umieć stwierdzić: „widzę sprzeczność”, „mam niepełny obraz”, „to predykcja poza znanym zakresem” lub „wymagana weryfikacja operatora”. Pokora algorytmiczna nie jest ozdobą etyczną.

## Od inercji fizycznej do odporności instytucjonalnej

Kwestia ta jest funkcją bezpieczeństwa.

Kluczowe znaczenie ma tu rosnąca rola źródeł odnawialnych opartych na falownikach. Tradycyjne maszyny synchroniczne wnosiły do systemu fizyczną inercję, która stabilizowała częstotliwość po nagłych zaburzeniach. Źródła falownikowe mogą reagować szybko i elastycznie, jednak ich zachowanie zależy od sterowania, oprogramowania oraz parametrów pracy. Transformacja

energetyczna przesuwa zatem część stabilności z fizycznej bezwładności maszyn do warstwy kontroli.

Nie jest to argument przeciw OZE, lecz przeciw infantylnej opowieści, że system energetyczny da się przebudować poprzez samo dodawanie mocy zainstalowanej, bez równoległej reformy sterowania, rezerw, magazynowania, sieci i ochrony systemowej. W systemie o dużym udziale generacji rozproszonej i falownikowej zmienia się także pojęcie awarii. Dawniej centralnym problemem była utrata dużego bloku wytwórczego albo linii przesyłowej. Dziś znaczenie mają także skoordynowane zachowania wielu mniejszych źródeł, gwałtowne zmiany generacji zależnej od pogody, reakcje falowników na zaburzenia napięcia i częstotliwości oraz interakcje między lokalnymi automatykami.

Mały element nie jest już nieważny tylko dlatego, że jest mały. W systemie złożonym wiele drobnych elementów może zachować się jak jeden duży problem. Demokracja urządzeń nie gwarantuje demokracji skutków. Prowadzi to do problemu koordynacji. Rozproszone zasoby energetyczne mogą wzmacniać odporność lokalną, zwłaszcza gdy są dobrze zintegrowane z magazynami energii, mikrosieciami i systemami zarządzania popytem; mogą także umożliwiać wyspową pracę fragmentów systemu i szybszą odbudowę po awarii. Jednak bez właściwej koordynacji mogą zwiększać nieprzewidywalność przepływów, utrudniać działanie zabezpieczeń, pogarszać profile napięciowe i komplikować estymację stanu. Nie jest to spór między „starą" a „nową" energetyką, lecz między transformacją systemową a transformacją życzeniową. Pierwsza przebudowuje architekturę bezpieczeństwa; druga dopisuje do slajdu słowo „smart" i liczy, że rzeczywistość poczuje się zobowiązana. Warstwa cyberfizyczna sprawia ponadto, że granica między awarią techniczną a atakiem staje się mniej oczywista. Zaburzenie może wynikać z pogody, błędu człowieka, awarii sprzętu, wadliwej konfiguracji oprogramowania, błędnej aktualizacji, ataku cybernetycznego albo kombinacji tych czynników.

Z punktu widzenia systemu pierwsze pytanie brzmi nie tyle „kto zawinił?", ile „jak zatrzymać propagację?". Jednak z perspektywy państwa pytanie o przyczynę jest równie konieczne, gdyż od niego zależą procedury bezpieczeństwa, odpowiedzialność, regulacje, inwestycje i współpraca międzysektorowa. Odporność operacyjna i odporność instytucjonalna muszą więc iść w parze. System musi umieć działać natychmiast i uczyć się później. To „uczenie się później" jest jednym z najważniejszych, a często lekceważonych elementów odporności. Każda poważna awaria powinna stać się źródłem wiedzy: o błędach pomiaru, lukach komunikacyjnych, złych nastawach zabezpieczeń, niewłaściwych procedurach, niedostatecznym szkoleniu, nadmiernej centralizacji decyzji, braku rezerw albo źle zaprojektowanych bodźcach rynkowych. System, który po awarii

tylko szuka winnego, ale nie zmienia architektury, ćwiczy rytuał oczyszczenia zamiast uczenia. Winny bywa potrzebny prawu, ale odporność potrzebuje przyczyny.

Energetyka cyberfizyczna wymaga kultury organizacyjnej zbliżonej do kultur wysokiej niezawodności. Trzeba zakładać, że błąd jest możliwy, dane są niepełne, alarmy bywają mylące, automatyka może wejść w nieprzewidzianą interakcję, a człowiek pod presją czasu może uprościć obraz sytuacji. Dobre organizacje nie budują swojej dumy na haśle „u nas awarie się nie zdarzają", lecz na zdolności do wcześniejszego wykrywania słabych sygnałów, swobodnego raportowania nieprawidłowości, ćwiczenia scenariuszy granicznych i korygowania procedur. W bezpieczeństwie infrastruktury samozadowolenie jest miękką nazwą twardej podatności.

## Aksjologia i etyka odporności cyberfizycznej

Sztuczna inteligencja może tu pełnić podwójną rolę. Po pierwsze, wzmacniać percepcję systemu: wykrywać anomalie, przewidywać ścieżki kaskad, identyfikować węzły krytyczne czy wspierać estymację stanu przy częściowej obserwowalności. Po drugie, wspierać proces decyzyjny: proponować działania sterujące, symulować skutki odłączeń i optymalizować sekwencje odbudowy. Ta dwoistość funkcji niesie jednak ze sobą podwójne ryzyko.

Jeżeli AI błędnie interpretuje dane, może źle doradzić. Jeśli zaś dysponuje zbyt dużą autonomią, błąd w rekomendacji przełoży się na błędne działanie. W infrastrukturze krytycznej nie wolno zatem oddzielać skuteczności modelu od warunków jego nadzoru. Kluczowe pytanie nie brzmi: czy używać AI w systemach elektroenergetycznych? Przy obecnej skali złożoności odpowiedź jest oczywista: tak, i to w coraz większym stopniu. Prawdziwym wyzwaniem jest kwestia tego, jak jej używać, aby nie zamienić złożoności fizycznej w złożoność algorytmicznie nieprzejrzystą. Model wspierający bezpieczeństwo musi być testowany nie tylko pod kątem średniej trafności, ale przede wszystkim w rzadkich scenariuszach, pod kątem odporności na dane odstające, stabilności przy zmianie warunków systemowych, interpretowalności sygnałów ostrzegawczych oraz zgodności z procedurami operatora.

W przeciwnym razie otrzymamy nowy rodzaj czarnej skrzynki zarządzającej czarnym startem – co brzmi jak żart złośliwego inżyniera, zatwierdzony przez dział PR. Cyberfizyczna odporność jest bowiem problemem regulacyjnym i politycznym. Operatorzy sieci, wytwórcy, dostawcy technologii, agregatorzy, właściciele źródeł rozproszonych, instytucje państwowe i regulatorzy muszą dzielić odpowiedzialność za standardy danych, bezpieczeństwo komunikacji, interoperacyjność, testowanie urządzeń, reagowanie kryzysowe oraz ochronę infrastruktury krytycznej. Jeśli każdy

podmiot będzie optymalizował jedynie własny fragment, system jako całość może stracić odporność. To klasyczny konflikt między racjonalnością lokalną a bezpieczeństwem globalnym.

Rynek potrafi precyzyjnie wyceniać energię w danej godzinie, lecz rzadko wycenia milczenie awarii, która nie nastąpiła dzięki utrzymanej rezerwie. Prowadzi to do szerszej tezy: odporność elektroenergetyczna jest dobrem publicznym. Jej brak dotyka wszystkich, także osób niezainteresowanych energetyką. Szpital, bankomat, wodociąg, serwer, kolej, telefonia, sklep, administracja czy gospodarstwo domowe – wszystko opiera się na założeniu dostępności prądu. Nowoczesne społeczeństwo zbudowano na niewidzialnej obietnicy ciągłości zasilania. Gdy ta obietnica pęka, okazuje się, że cyfrowa cywilizacja ma bardzo analogiczny problem: bez elektryczności jej chmura jest tylko cudzym komputerem, który również potrzebuje gniazdka.

Modelowanie cyberfizyczne nie jest zatem luksusem badawczym, lecz koniecznością strategiczną. Należy modelować nie tylko przepływy mocy, ale i informacji; nie tylko przeciążenia linii, lecz także systemów alarmowych; nie tylko awarie transformatorów, ale i komunikacji między urządzeniami. Złośliwe oprogramowanie nie może być traktowane wyłącznie jako problem informatyczny, lecz jako potencjalny czynnik fizycznej destabilizacji sieci. W świecie cyberfizycznym nie istnieje już czyste „IT" i czyste „OT". Istnieje wspólny organizm, w którym błąd bitu może mieć zapach spalonego izolatora. Nie unieważnia to klasycznej energetyki – przeciwnie, czyni ją jeszcze ważniejszą.

Prawa Kirchhoffa nie zostały anulowane przez algorytmy. Częstotliwość nie negocjuje z aplikacją. Transformator nie interesuje się narracją o innowacyjności. Fizyczna warstwa systemu pozostaje nieubłagana. Nowością jest fakt, że coraz więcej decyzji dotyczących tej warstwy zależy od cyfrowej percepcji i sterowania. Kto rozumie tylko przewody, nie zrozumie współczesnej sieci. Kto rozumie tylko dane – tym bardziej jej nie pojmie. Trzeba widzieć oba porządki jednocześnie.

Aksjologia odporności to technika jako praktyczna filozofia dobra wspólnego. Sieć elektroenergetyczna wydaje się domeną inżynierów, operatorów, automatyków i informatyków, lecz w istocie jest także instytucją moralną. Nie dlatego, że przewody mają sumienie, a transformatory prowadzą życie duchowe – tu nawet najbardziej ambitna rozdzielnia zachowuje stosowną skromność – lecz dlatego, że decyzje o projektowaniu, zabezpieczaniu i odbudowie sieci rozdzielają ryzyko, koszty oraz ciągłość życia społecznego. Tam, gdzie trzeba zdecydować, które elementy wzmacniać, których odbiorców chronić w pierwszej kolejności, jakie obciążenia zrzucić, jaki poziom rezerw finansować i jaką autonomię powierzyć algorytmom, technika staje się praktyczną filozofią dobra wspólnego.

Odporność nie jest wartością neutralną. Jest wyborem przeciwko krótkowzrocznej efektywności i złudzeniu, że system można prowadzić stale na granicy wytrzymałości tylko dlatego, że wczoraj się udało. To wybór na rzecz rezerw, redundancji, procedur, testów i inwestycji, których pełna wartość ujawnia się dopiero wtedy, gdy zdarzenie nie zamienia się w katastrofę. Jest to trudna wartość polityczna, gdyż jej sukces jest niewidzialny. Gdy dzięki prewencji nie dochodzi do blackoutu, społeczeństwo nie urządza owacji na cześć marginesu bezpieczeństwa. Nikt nie pisze pieśni pochwalnych o poprawnie zachowanej rezerwie wirującej – a szkoda, bo niejedna rezerwa zasłużyła na więcej wdzięczności niż niejeden komitet.

W logice gospodarczej odporność bywa traktowana jako koszt. Dodatkowe linie, zapasy transformatorów, systemy black start czy cyberbezpieczeństwo w normalnym dniu mogą wyglądać jak nadmiar. W dniu kryzysu okazują się warunkiem przetrwania. Największy spór toczy się więc nie między techniką a nietechniką, lecz między dwiema racjonalnościami: krótkookresową kosztową i długookresową systemową. Pierwsza pyta, ile oszczędzimy, przycinając marginesy; druga – ile stracimy, gdy tych marginesów zabraknie.

System planning opiera się na próbie zachowania równowagi między kosztem a odpornością. Nie można wzmocnić wszystkiego, dlatego niezbędna jest identyfikacja komponentów krytycznych, symulacje Monte Carlo i gradientowa strategia hardeningu. Model ten ma znaczenie aksjologiczne: odrzuca zarówno beztroskę („jakoś to będzie”), jak i paranoję („opancerzmy wszystko”). Odpowiedzialność nakazuje rozpoznać, gdzie interwencja daje największy wzrost odporności przy ograniczonym budżecie.

Odporność wymaga hierarchii priorytetów. W czasie odbudowy po blackoucie zasilanie przywraca się najpierw infrastrukturze krytycznej: szpitalom, wodociągom i służbom bezpieczeństwa. Nie jest to przywilej arbitralny, lecz uznanie, że pewne funkcje podtrzymują życie i możliwość dalszej odbudowy. Bez nich awaria energetyczna staje się awarią społeczną. Ochrona naprawcza pokazuje więc, że system ma wbudowaną etykę kolejności. W kryzysie równość potrzeb zderza się z nierównością funkcji krytycznych.

Podobny problem pojawia się przy awaryjnym zrzucaniu obciążenia. Mechanizmy UFLS i UVLS ratują system, ale ich skutki ponoszą konkretni odbiorcy. Pytania o to, kto traci zasilanie i czy rozkład strat jest społecznie akceptowalny, są kluczowe. W najprostszym modelu zrzut obciążenia jest automatyczny; w szerszym – jest decyzją o kontrolowanej dystrybucji niedoboru. Technika wykonuje to, co aksjologia powinna wcześniej przemyśleć.

Nie chodzi o to, by każdy przekaźnik konsultował się z komisją etyczną przed zadziałaniem – taki pomysł zabiłby system szybciej niż przeciążenie. Chodzi o to, by wartości zostały wpisane w projekt:

w progi zabezpieczeń, plany odłączeń i standardy infrastruktury krytycznej. Etyka nie powinna przychodzić po awarii z miną zatroskanego komentatora; powinna być zakodowana w architekturze działania.

Z tego punktu widzenia kluczowa jest funkcja nagrody w systemach DRL. Agent uczący się sterowania maksymalizuje cel, który mu zadano. Jeśli funkcja nagrody promuje minimalizację utraty mocy poprzez odcięcie linii w celu przerwania kaskady, ma to sens techniczny. Jednak każda funkcja celu jest aktem wyboru wartości. Licząc tylko zachowaną moc, możemy pominąć znaczenie odbiorców krytycznych czy społeczną akceptowalność decyzji.

Algorytmiczne sterowanie infrastrukturą krytyczną nie może być zatem neutralną optymalizacją. Optymalizacja zawsze odbywa się względem czegoś. Pytanie brzmi: czy to „coś" reprezentuje wartości systemu? Czy funkcja celu uwzględnia bezpieczeństwo publiczne, sekwencję odbudowy i różnice w skutkach społecznych podobnych strat megawatów?

Tutaj energetyka spotyka się z filozofią instytucji. Systemy publiczne często udają neutralność, posługując się liczbami, lecz liczba jest uczciwa tylko wtedy, gdy wiemy, co pomija. Megawat nie opisuje osoby podłączonej do respiratora, a procent obciążenia nie oddaje hierarchii funkcji społecznych. Metryki są konieczne, ale nigdy niewinne; ich ryzyko polega na tym, że po redukcji złożoności ktoś zapomina o świecie, który został zredukowany.

Odporność jako dobro publiczne wymaga sprawiedliwego finansowania. Rezerwy i modernizacja kosztują, a ich korzyści są rozproszone – każdy korzysta z braku blackoutu, lecz nie każdy chce za tę zdolność płacić. To klasyczny problem dóbr wspólnych. Rynek premiuje najtańszą energię „tu i teraz", podczas gdy odporność wymaga opłacenia niewidzialnej gotowości. Bez właściwych regulacji operatorzy mogą być popychani ku krótkoterminowej efektywności zamiast systemowej odporności.

Transformacja energetyczna musi być zatem oceniana nie tylko przez wskaźniki emisyjne, lecz także przez wskaźniki odporności. OZE i magazyny wzmacniają system, jeśli towarzyszy im modernizacja sterowania i rezerw. W przeciwnym razie zwiększają jedynie złożoność operacyjną. Polityka energetyczna nie powinna pytać wyłącznie o to, ile mocy zainstalowaliśmy, lecz jak ta moc zachowuje się w systemie, gdy coś pójdzie źle.

## Nowy paradygmat odporności cyberfizycznej

Prawdziwa transformacja nie polega na tym, że w dobry dzień wszystko wygląda nowocześnie. Polega na tym, że w zły dzień system nadal działa. Aksjologia odporności dotyczy również wiedzy i

jawności. Społeczeństwo nie musi znać wszystkich technicznych szczegółów zabezpieczeń, a część informacji o infrastrukturze krytycznej musi pozostać chroniona. Ale społeczeństwo ma prawo do wiedzy o standardach bezpieczeństwa, planach reagowania, odpowiedzialności instytucji i wnioskach z awarii. Tajemnica bezpieczeństwa nie może stać się zasłoną dla zaniedbań. Z kolei pełna jawność szczegółów operacyjnych nie może ułatwiać ataków. Tu również potrzebna jest równowaga: transparentność co do zasad i odpowiedzialności, ostrożność co do podatnych szczegółów technicznych. Kultura odporności wymaga ponadto uczciwego raportowania błędów. Systemy wysokiego ryzyka nie uczą się, jeśli każda nieprawidłowość jest natychmiast tłumaczona wizerunkowo albo personalizowana wyłącznie jako wina jednostki. Oczywiście jednostki mogą popełniać błędy i ponosić odpowiedzialność. Ale awarie systemowe rzadko mają jednego ojca. Częściej są dziećmi wielu drobnych zaniedbań, złych bodźców, milczących kompromisów, nieaktualnych procedur i opóźnionych inwestycji. W tym sensie kultura winy bywa wrogiem kultury uczenia się. Jeśli każdy boi się zgłosić słaby sygnał, system dowie się o problemie dopiero wtedy, gdy problem zgłosi się sam - zwykle dość efektownie. Lektura o awariach kaskadowych pokazuje, że lokalnie poprawne reakcje mogą globalnie pogarszać sytuację. Zabezpieczenie odłącza przeciążony element, chroniąc go przed uszkodzeniem, ale jednocześnie zmienia rozpływy i może przeciążyć kolejne linie. To znakomita metafora problemów instytucjonalnych. Każdy dział chroni własny zakres odpowiedzialności, każdy urząd działa według swojej procedury, każdy podmiot rynku optymalizuje swój wynik, a całość traci odporność. W systemach złożonych dobro wspólne nie powstaje automatycznie z lokalnych racjonalności. Musi być projektowane. To projektowanie wymaga regulatora i instytucji publicznych zdolnych do myślenia systemowego. Regulacja nie może ograniczać się do wymuszania minimalnych standardów technicznych ani do reakcji po awarii. Musi tworzyć warunki dla inwestycji w sieci, premiować elastyczność, wspierać cyberbezpieczeństwo, określać wymagania wobec źródeł falownikowych, wymuszać testy black start, zapewniać koordynację między operatorami i przeciwdziałać przerzucaniu ryzyka na niewidzialne marginesy systemu. Najgorsza regulacja to taka, która mierzy to, co łatwe do zmierzenia, i ignoruje to, co naprawdę utrzymuje system przy życiu. pojawia się jeszcze jedna wartość: pokora wobec złożoności. Nowoczesne systemy elektroenergetyczne są tak złożone, że żadna instytucja, żaden algorytm i żaden ekspert nie posiada pełnej kontroli w sensie absolutnym. Można zwiększać obserwowalność, poprawiać modele, automatyzować reakcje i wzmacniać komponenty, ale nie można unieważnić niepewności. Pokora nie oznacza bierności. Oznacza projektowanie z założeniem, że nasze modele są ograniczone, dane niepełne, scenariusze nie wyczerpują rzeczywistości, a system może zaskoczyć. W bezpieczeństwie infrastruktury pycha jest błędem technicznym przebranym za pewność siebie. Ta pokora jest szczególnie potrzebna wobec sztucznej inteligencji. GAT, Attention-LSTM i DRL są narzędziami imponującymi. Pozwalają oceniać niezbędność węzłów, przewidywać ścieżki kaskad, klasyfikować pilność i wybierać działania

sterujące w czasie rzeczywistym. Ale ich użycie musi być powiązane z walidacją, interpretowalnością, testowaniem, audytem, procedurami awaryjnymi i możliwością ludzkiego nadzoru. W infrastrukturze krytycznej nie wystarczy, że model działa dobrze średnio. Trzeba wiedzieć, jak zachowa się w warunkach rzadkich, granicznych, sprzecznych i złośliwie zakłóconych. Średnia trafność bywa pocieszająca - aż do momentu, gdy akurat mieszkamy w ogonie rozkładu. Aksjologia odporności prowadzi więc do wniosku, że technika musi być sprzężona z instytucjonalną odpowiedzialnością. Nie można pozostawić odporności wyłącznie inżynierom, choć bez inżynierów nie ma odporności. Nie można pozostawić jej wyłącznie rynkowi, choć bez ekonomicznej racjonalności nie ma skalowalnych inwestycji. Nie można pozostawić jej wyłącznie politykom, bo wtedy margines bezpieczeństwa zacznie zależeć od cyklu medialnego. Potrzebny jest układ: wiedza techniczna, regulacja, finansowanie, audyt, kultura raportowania, zdolność operacyjna i społeczna świadomość, że bezpieczeństwo infrastruktury jest kosztem wolności od chaosu. sieć elektroenergetyczna jest jedną z najważniejszych lekcji o państwie. Państwo również jest siecią zależności. Ma węzły krytyczne, przepływy, przeciążenia, rezerwy, procedury awaryjne i zdolność odbudowy. Państwo, które oszczędza na odporności, może wyglądać sprawnie w normalnym dniu, ale ujawnia prawdę o sobie w dniu kaskady. Podobnie firma, samorząd, system ochrony zdrowia czy administracja. Każda struktura złożona potrzebuje prewencji, reakcji i recovery. Każda potrzebuje planowania i sterowania. Każda musi wiedzieć, które połączenia wzmacniać, a które w kryzysie przeciąć. techniczna analiza robustness of evolving power grids ma wartość znacznie większą niż energetyczna specjalizacja. Uczy myślenia o odporności jako zdolności do życia z niepewnością. Nie obiecuje świata bez awarii. Obiecuje lepsze rozpoznanie, mądrzejsze marginesy, szybsze interwencje i bardziej uporządkowaną odbudowę. To wystarczająco ambitne. System, który twierdzi, że nigdy nie upadnie, zwykle nie ma planu, jak wstać. System dojrzały wie, że upadek jest możliwy, więc projektuje sposób, by nie był końcem. Nowy paradygmat odporności. Od grafu do cywilizacji zdolnej przetrwać własną złożoność Nowoczesna analiza odporności sieci elektroenergetycznych prowadzi do wniosku, który wykracza poza samą energetykę: im bardziej system staje się złożony, tym mniej wolno ufać prostym obrazom jego bezpieczeństwa. Nie wystarczy już powiedzieć, że mamy elektrownie, linie, transformatory, rezerwy i procedury. Nie wystarczy narysować schemat sieci, policzyć liczbę połączeń i uznać, że nadmiarowość załatwia sprawę. Nie wystarczy też przywołać sztucznej inteligencji niczym nowego zaklęcia technokratycznego. Odporność współczesnej sieci rodzi się dopiero ze złączenia kilku porządków: topologii, fizyki przepływów, predykcji algorytmicznej, automatyki zabezpieczeń, planowania inwestycyjnego, cyberbezpieczeństwa, regulacji i kultury odpowiedzialności. książkowy aparat pojęciowy dotyczący evolving power grids należy czytać jako opis przejścia od infrastruktury liniowej do infrastruktury organicznej. Dawna wyobraźnia energetyczna była hierarchiczna: źródło, przesył, dystrybucja, odbiorca. Nowa wyobraźnia musi być sieciowa: źródła centralne i

rozproszone, magazyny, prosumenci, falowniki, automatyka, systemy SCADA, predykcja AI, rynek bilansujący, komunikacja cyfrowa, zabezpieczenia lokalne i globalne, procedury odbudowy. Sieć elektroenergetyczna nie jest już tylko systemem dostarczania energii. Jest systemem utrzymywania ciągłości cywilizacji. Pierwszy filar nowego paradygmatu to rozumienie sieci jako grafu, ale grafu niewystarczającego bez fizyki. Teoria sieci złożonych pozwala rozpoznać węzły, krawędzie, huby, mosty, centralność, klastrowanie, średnią długość ścieżki i podatność na fragmentację. Pozwala zobaczyć, że struktura nie jest dekoracją, lecz przeznaczeniem systemu w chwili zakłócenia. Jednak sama topologia nie powie, jak rozpłynie się prąd, gdzie przekroczone zostaną limity termiczne, jak zachowa się napięcie, co zrobią zabezpieczenia i czy system utrzyma synchronizm. Dlatego nowy paradygmat nie odrzuca teorii grafów, lecz ją dyscyplinuje. Graf jest szkieletem. Fizyka jest krwią. Automatyka jest odruchem. Operator jest świadomością - czasem czujną, czasem zmęczoną, a czasem niestety zastępowaną przez procedurę pisaną w czasach, gdy rzeczywistość była mniej złośliwa. Drugi filar to myślenie kaskadowe. Awaria kaskadowa nie jest "dużą awarią" w banalnym sensie. Jest procesem, w którym jedno uszkodzenie zmienia warunki pracy kolejnych elementów. Linia wypada, przepływy się redystrybuują, inne elementy przejmują obciążenie, zabezpieczenia odłączają przeciążone komponenty, a każde odłączenie tworzy nową topologię i nowy rozkład ryzyka. W ten sposób system może przejść od lokalnego problemu do globalnej katastrofy. Najważniejsze jest tu zrozumienie, że kaskada nie potrzebuje złej woli. Wystarczy sekwencja lokalnie racjonalnych reakcji, które globalnie tworzą zapaść. To wielka lekcja systemowa: całość nie jest sumą poprawnych lokalności. Trzeci filar to przejście od oceny statycznej do predykcji dynamicznej. Dawna ocena odporności mogła pytać, ile obciążenia zostanie utracone po danym scenariuszu. Nowa musi pytać, jak szybko awaria będzie się rozprzestrzeniać, które węzły są niezbędne w danym stanie operacyjnym, którędy pobiegnie propagacja, kiedy nastąpi onset time, czyli moment gwałtownego przyspieszenia, oraz jakie działanie może zatrzymać proces. To przesunięcie od fotografii do filmu. Statyczny obraz mówi, jak wygląda system. Predykcja dynamiczna mówi, jak system może zacząć umierać - i gdzie należy przerwać ten proces. pojawia się rola GAT, Attention-LSTM i innych modeli AI. Grafowe sieci uwagowe pozwalają oceniać niezbędność węzłów, ucząc się znaczenia relacji sąsiedzkich i pracując także przy częściowych obserwacjach. Attention-LSTM pozwala przewidywać ścieżki propagacji awarii, traktując kaskadę jako sekwencję czasową, w której niektóre dawne zdarzenia mają większe znaczenie niż inne. Klasyfikatory onset time pomagają rozpoznać pilność interwencji. Drzewa decyzyjne wydobywają związki między cechami strukturalnymi sieci a odpornością. Te narzędzia nie są ozdobą cyfrową. Są próbą zwiększenia świadomości sytuacyjnej w systemie, który stał się zbyt szybki i zbyt złożony dla czysto ręcznego nadzoru. Czwarty filar to wielowarstwowa ochrona: prewencyjna, awaryjna i naprawcza. Prewencja utrzymuje marginesy, pilnuje kryterium N-1, redysponuje generację, utrzymuje rezerwy i nie pozwala systemowi zbliżyć się do granicy, za którą pojedyncze zdarzenie

uruchamia lawinę. Ochrona awaryjna działa, gdy zakłócenie już uderzyło: zrzuca obciążenie, zrzuca generację, tłumi oscylacje, tworzy wyspy, izoluje proces rozpadu. Ochrona naprawcza zaczyna się po utracie zasilania: uruchamia black start, buduje pierwsze wyspy napięcia, sekwencyjnie przywraca obciążenie i synchronizuje fragmenty systemu. Każda z tych warstw ma inną logikę czasową. Kto myli prewencję z reakcją, reakcję z odbudową, a odbudowę z pośpiesznym włączaniem wszystkiego naraz, ten nie zarządza systemem, tylko negocjuje z katastrofą na jej warunkach. Piąty filar to rozróżnienie między system planning a system control. Planowanie systemu jest długoterminową architekturą odporności. Obejmuje optymalizację topologii, rozmieszczanie generatorów, analizę efektywnej odległości elektrycznej, wzmacnianie komponentów krytycznych, alokację budżetów hardeningu, planowanie rezerw i projektowanie zdolności odbudowy. Sterowanie systemem jest natomiast zdolnością działania w czasie rzeczywistym. Gdy awaria już się rozwija, nie ma czasu na wieloletni program inwestycyjny. Trzeba zdecydować, co odłączyć, co zachować, jak zatrzymać kaskadę i jak ograniczyć stratę. To różnica między architektem twierdzy a dowódcą w chwili szturmu. Obaj są potrzebni. Jeden bez drugiego produkuje albo piękne plany, albo bohaterską improwizację. W tym obszarze szczególne znaczenie ma DRL, czyli głębokie uczenie ze wzmocnieniem. W ujęciu notatki agent DRL uczy się sterowania siecią podczas awarii kaskadowej przez modelowanie problemu jako procesu decyzyjnego Markowa. Stan obejmuje parametry sieci, akcją jest celowe odcięcie wybranej linii, przejście prowadzi do nowego stanu, a funkcja nagrody premiuje zachowanie jak największej ilości dostępnego zasilania. Zastosowanie PPO, czyli Proximal Policy Optimization, pozwala trenować agenta w architekturze actor-critic i ograniczać niestabilność procesu uczenia. Wyniki symulacyjne opisane w notatce pokazują szybkość reakcji poniżej 0,01 sekundy oraz wyższą skuteczność ograniczania strat niż w scenariuszach bez takiego wsparcia. trzeba zachować najwięcej intelektualnej dyscypliny. Sztuczna inteligencja w systemie elektroenergetycznym nie jest magią, lecz narzędziem optymalizacji pod zadany cel. Jeżeli cel jest wąski, model będzie inteligentnie realizował wąskość. Jeżeli dane treningowe są niepełne, model może nie rozpoznać zdarzeń rzadkich. Jeżeli symulacja nie oddaje rzeczywistej dynamiki, agent nauczy się świata, który istnieje tylko w laboratorium. Jeżeli system dopuści zbyt dużą autonomię bez walidacji, może otrzymać błyskawiczną decyzję, której nikt nie zdążył zrozumieć. W infrastrukturze krytycznej nie wystarczy, by algorytm miał rację statystycznie. Musi być osadzony w odpowiedzialnej architekturze decyzyjnej. Szósty filar to cyberfizyczność. Współczesna sieć nie jest tylko przewodem i transformatorem. Jest również systemem danych. Sensor widzi, SCADA zbiera, algorytm klasyfikuje, automatyka działa, operator interpretuje, rynek wysyła bodźce, a komunikacja cyfrowa spina całość. To zwiększa sprawność, ale tworzy nową podatność. Błąd danych, opóźnienie komunikacji, fałszywy pomiar, złośliwe oprogramowanie, wadliwa aktualizacja albo niewłaściwie zaprojektowany interfejs operatorski mogą stać się elementem awarii równie realnym jak

przeciążona linia. W XXI wieku blackout może zacząć się od pioruna, ale może też zacząć się od informacji, która wyglądała jak prawda i została potraktowana jak rozkaz. Siódmy filar to aksjologia odporności. Nie da się mówić o bezpieczeństwie systemu elektroenergetycznego bez pytań o koszty, priorytety, sprawiedliwość strat i odpowiedzialność publiczną. Kto ma być zasilany pierwszy po blackoucie? Które obciążenia można zrzucić? Jak chronić szpitale, wodociągi, łączność i infrastrukturę krytyczną? Ile społeczeństwo powinno zapłacić za rezerwy, których wartość ujawnia się dopiero wtedy, gdy nie dochodzi do katastrofy? Jakie cele wpisujemy w funkcje nagrody algorytmów?

## Nowy paradygmat odporności cyberfizycznej

Czy minimalizujemy utraconą moc, liczbę odbiorców, czas odbudowy i ryzyko wtórnej awarii, czy skupiamy się na ochronie funkcji krytycznych? Technika nie znika w tych pytaniach – staje się ich wykonawczą gramatyką.

Nowy paradygmat odporności jest interdyscyplinarny. Inżynieria mocy dostarcza praw fizycznych, teoria sieci złożonych języka struktury, a sztuczna inteligencja narzędzi predykcji i sterowania. Cyberbezpieczeństwo zapewnia ochronę warstwy informacyjnej.

Ekonomia wnosi refleksję o kosztach, bodźcach i inwestycjach. Prawo i regulacje wyznaczają ramy odpowiedzialności, natomiast socjologia organizacji dostarcza wiedzy o błędach instytucjonalnych, kulturze raportowania i koordynacji. Filozofia dobra wspólnego przypomina z kolei, że system nie istnieje dla samego zachowania parametrów, lecz dla ochrony życia społecznego. Bez tej syntezy każda dziedzina będzie miała własną rację i wspólną ślepotę.

Przeciwnikiem odporności nie jest brak technologii, lecz często błędne wyobrażenie o stabilności. Stabilność bywa mylona z brakiem widocznych awarii, tymczasem ich brak może oznaczać dojrzałą odporność, ale równie dobrze szczęście, niewykryte napięcia albo życie na kredyt marginesów. System może przez długi czas działać poprawnie, choć narasta w nim podatność. Linie są przeciążane blisko limitów, rezerwy przycinane, procedury nieaktualizowane, cyberbezpieczeństwo traktowane jako koszt, a modernizacja odkładana. Potem nadchodzi zdarzenie, które nie „tworzy" katastrofy, lecz ujawnia tę wcześniej przygotowaną. Awaria często jest tylko premierą sztuki pisanej latami.

Nowoczesna odporność wymaga kultury wcześniejszego niepokoju. Nie chodzi o histerię, alarmizm czy widowiskowe czarnowidztwo, lecz o profesjonalną nieufność wobec łatwych zapewnień. Trzeba pytać: co się stanie po utracie tego elementu? Co pokażą dane, jeśli część sensorów zawiedzie? Czy

model AI wie, że nie wie? Czy black start był ćwiczony? Czy plan zrzutu obciążenia chroni funkcje krytyczne? Czy topologia nie przenosi przeciążeń zbyt szybko? Czy źródła falownikowe zachowają się stabilnie przy zaburzeniu? Czy operator widzi system, czy tylko interfejs?

Czy regulacja premiuje odporność, czy jedynie tanią normalność? To sceptyczne pytanie jest jednym z najważniejszych narzędzi bezpieczeństwa. W systemach złożonych niebezpieczne są nie tylko błędne odpowiedzi, lecz także pytania, których nikt nie zadaje, bo „dotąd działało". Historia awarii infrastrukturalnych uczy, że katastrofy rzadko zaczynają się od jednego spektakularnego błędu. Częściej wynikają z normalizacji odchyleń. Coś przekracza próg, ale nieznacznie. Alarm pojawia się, lecz bywa uznany za fałszywy. Procedura jest nieaktualna, ale wciąż „się przydaje". Rezerwa jest mniejsza, ale statystycznie wystarcza. Jeden wyjątek staje się praktyką, praktyka kulturą, a kultura podatnością. A potem przychodzi zdarzenie, które nie szanuje kultury organizacyjnej.

Z tej perspektywy „robustness" oznacza zdolność do opierania się własnej skłonności do samozadowolenia. System odporny nie ufa temu, że jutro będzie podobne do wczoraj. Nie traktuje optymalizacji kosztowej jako najwyższej cnoty i nie wierzy, że automatyka zawsze uratuje człowieka przed skutkami złego projektu. Nie oddaje AI decyzji bez pytań o dane, cele i granice; nie odkłada odbudowy procedur na czas po katastrofie. Wie, że bezpieczeństwo jest praktyką codzienną, a nie deklaracją po zdarzeniu.

Jednocześnie nowy paradygmat odporności nie jest pesymistyczny – przeciwnie, jest realistycznie obiecujący. Teoria sieci pozwala lepiej identyfikować podatności, modele AI szybciej przewidywać kaskady, a DRL wspierać decyzje w ułamkach sekund. Lepsze planowanie topologii może zmniejszać przeciążenia, a gradientowe wzmacnianie komponentów sensowniej alokować ograniczone budżety. Rozproszone źródła i magazyny mogą wspierać lokalną odporność, o ile są dobrze zintegrowane. Cyberbezpieczeństwo chroni układ nerwowy sieci, a kultura organizacyjna przyspiesza uczenie się z błędów.

To nie jest opowieść o bezradności, lecz o tym, że złożoność wymaga dojrzałości. Mówiąc syntetycznie: przyszła sieć elektroenergetyczna musi być jednocześnie mocna, elastyczna, obserwowalna, przewidywalna, sterowalna, odbudowywalna i instytucjonalnie odpowiedzialna. Mocna, bo komponenty krytyczne muszą wytrzymywać zakłócenia. Elastyczna, bo przepływy, generacja i popyt będą zmienne. Obserwowalna, bo bez dobrych danych nie ma dobrej decyzji. Przewidywalna, bo kaskada musi być rozpoznana przed punktem przyspieszenia. Sterowalna, bo samo ostrzeżenie bez akcji nie wystarcza. Odbudowywalna, bo żadna prewencja nie gwarantuje świata bez upadków. Odpowiedzialna, bo decyzje techniczne niosą realne skutki społeczne.

Odporność ewoluujących sieci elektroenergetycznych jest jednym z najważniejszych testów cywilizacji technologicznej. Pokazuje, czy potrafimy zarządzać systemami, których nie jesteśmy już w stanie ogarnąć prostą intuicją. Czy umiemy połączyć algorytmy z pokorą, efektywność z rezerwą, decentralizację z koordynacją, automatyzację z odpowiedzialnością i transformację energetyczną z bezpieczeństwem operacyjnym. Pokazuje wreszcie, czy rozumiemy, że światło w gniazdku nie jest banałem codzienności, lecz końcowym efektem ogromnej, kruchej i nieustannie bronionej architektury.

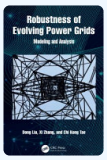
Blackout jest negatywną epifanią nowoczesności. W jednej chwili odsłania, ile instytucji, usług, obietnic i wygód było podłączonych do tej samej niewidzialnej podstawy. Dlatego analiza odporności sieci nie jest wąską specjalizacją techniczną, lecz nauką o tym, jak społeczeństwo może nie rozpaść się pod ciężarem własnych zależności. W epoce transformacji energetycznej, cyfryzacji i rosnących ryzyk klimatycznych pytanie nie brzmi już, czy sieć będzie bardziej złożona – bo będzie. Pytanie brzmi: czy będzie mądrzejsza od własnej złożoności.

Tym samym zamyka się sens wywodu. Modelowanie sieci i awarii kaskadowych, teoria sieci złożonych, GAT, Attention-LSTM, DRL, ochrona prewencyjna, awaryjna i naprawcza oraz system planning i system control nie są osobnymi szufladkami wiedzy. Są częściami jednej architektury myślenia.

Uczą one, że odporność nie jest stanem, lecz procesem; nie rzeczą, lecz relacją; nie deklaracją, lecz zdolnością do działania pod presją. Sieć elektroenergetyczna przetrwa przyszłość nie dlatego, że będzie idealna, lecz dlatego, że będzie umiała przewidywać własne pęknięcia, ograniczać ich propagację i wracać do życia po ciosie. To jest najważniejsza definicja odporności również poza energetyką: nie obietnica, że nigdy nie zgaśnie światło, lecz kompetencja, by ciemność nie stała się systemem.

> W świecie ekstremalnej złożoności prawdziwa odporność nie jest obietnicą wiecznego światła, lecz kompetencją szybkiego powrotu z ciemności. Pytanie brzmi zatem: czy nasze systemy staną się mądrzejsze od własnej architektury, czy pozostaną jedynie zakładnikami swojej sprawności? Ostatecznie to nie brak awarii świadczy o sile systemu, lecz zdolność do tego, by pojedynczy błąd bitu lub piorun nie zamienił nowoczesnej cywilizacji w analogiczny pomnik własnej kruchości.

## Inspiracje

[1] 

**"Robustness of Evolving Power Grids"** Dong Liu

*2026 | CRC Press | ISBN: 9781041030744*

**Dong Liu** jest inżynierem elektrykiem i badaczem akademickim, obecnie związanym z Uniwersytetem Metropolitalnym w Hongkongu. Jego badania koncentrują się na inżynierii energetycznej, ze szczególnym uwzględnieniem modelowania i analizy złożonych systemów sieci energetycznych. Jego praca dotyczy kluczowych wyzwań współczesnej infrastruktury energetycznej, w tym modelowania kaskadowych awarii, systemów cyberfizycznych oraz zastosowania uczenia maszynowego do oceny i poprawy odporności ewoluujących sieci energetycznych. Wniósł wkład w rozwój tej dziedziny poprzez recenzowane artykuły w czasopismach naukowych i książki naukowe, które integrują teorię sieci, zmienne elektryczne i strategie sterowania systemami w celu poprawy odporności sieci na awarie i ataki. Jego badania wpisują się również w globalne cele zrównoważonego rozwoju, szczególnie w obszarze niedrogiej i czystej energii.

***Dong Liu** is an electrical engineer and academic researcher currently affiliated with Hong Kong Metropolitan University. His research focuses on power engineering, with specific expertise in the modeling and analysis of complex power grid systems. His work addresses critical challenges in modern energy infrastructure, including cascading failure modeling, cyber-physical systems, and the application of machine learning to assess and enhance the robustness of evolving power grids. He has contributed to the field through peer-reviewed journal articles and academic books that integrate network theory, electrical variables, and system control strategies to improve grid resilience against faults and attacks. His research also aligns with global sustainability goals, particularly in the area of affordable and clean energy.*

*Hong Kong Metropolitan University*

## Literatura uzupełniająca

### Książki

#### Książki autorów przywoływanych i literatura pokrewna:

[1] **"Network science"**

Albert-László Barabási

[2] **"Linked: The New Science of Networks"**
Albert-László Barabási

[3] **"The Formula: the science behind why people succeed or fail"**
Albert-László Barabási

[4] **"Basic dimensions for a general psychological theory"**
Réka Albert

[5] **"Financial Inclusion"**
Tyler Girard

[6] **"Leading Change With a New Preface by the Author"**
John P Kotter

[7] **"Conflict Security Foreign Policy and International Political Economy"**
Michael Brecher

[8] **"Normal Accidents"**
Charles Perrow

## Artykuły naukowe

### Prace autorów przywoływanych w tekście:

[1] **"Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling"**
Jun-Young Chung, Çağlar Gülçehre, Kyunghyun Cho, Yoshua Bengio
2014 | arXiv (Cornell University) | DOI: 10.48550/arxiv.1412.3555
Źródło

[2] **"Complex Behavior of Switching Power Converters"**
Chi K. Tse
2003 | DOI: 10.1201/9780203494554
Źródło

[3] **"Design for Efficiency Optimization and Voltage Controllability of Series–Series Compensated Inductive Power Transfer Systems"**
Wei Zhang, Siu-Chung Wong, Chi K. Tse, Qianhong Chen
2013 | IEEE Transactions on Power Electronics | DOI: 10.1109/tpel.2013.2249112
Źródło

[4] **"Complex behavior in switching power converters"**
Chi K. Tse, Mario di Bernardo
2002 | Proceedings of the IEEE | DOI: 10.1109/jproc.2002.1015006
Źródło

[5] **"A network perspective of the stock market"**
Chi K. Tse, Jing Liu, Francis C. M. Lau
2010 | Journal of Empirical Finance | DOI: 10.1016/j.jempfin.2010.04.008
Źródło

[6] **"2. Introduction to Network Analysis"**
Jörg Menche, Albert - László Barabási
2017 | Network Medicine | DOI: 10.4159/9780674545533-003
Źródło

[7] **"Predicting perturbation patterns from the topology of biological networks"**
Marc Santolini, Albert-László Barabási
2018 | DOI: 10.1101/349324
Źródło

[8] **"Dynamics of Complex Systems: Scaling Laws for the Period of Boolean Networks"**
Réka Albert, Albert-László Barabási
2000 | Physical Review Letters | DOI: 10.1103/physrevlett.84.5660
Źródło

[9] **"Emergence of Scaling in Random Networks"**
Albert-Ĺaszló Barabási, Réka Albert
1999 | Science | DOI: 10.1126/science.286.5439.509
Źródło

[10] **"Statistical mechanics of complex networks"**
Réka Albert, Albert-Ĺaszló Barabási
2002 | Reviews of Modern Physics | DOI: 10.1103/revmodphys.74.47
Źródło

[11] **"Near linear time algorithm to detect community structures in large-scale networks"**
Usha Nandini Raghavan, Réka Albert, Soundar Kumara
2007 | Physical Review E | DOI: 10.1103/physreve.76.036106
Źródło

**[12] "Mean-field theory for scale-free random networks"**

Albert-Ĺaszló Barabási, Réka Albert, Hawoong Jeong

1999 | Physica A Statistical Mechanics and its Applications | DOI: 10.1016/s0378-4371(99)00291-5

Źródło

**[13] "Exploring Limits to Prediction in Complex Social Systems"**

Travis Martin, Jake M. Hofman, Amit Sharma, Ashton Anderson, Duncan J. Watts

2016 | Proceedings of the 25th International Conference on World Wide Web | DOI: 10.1145/2872427.2883001

Źródło

**[14] "Nominal-scale Evolving Connectionist Systems"**

M.J. Watts

The 2006 IEEE International Joint Conference on Neural Network Proceedings | DOI: 10.1109/ijcnn.2006.1716364

Źródło

**[15] "Does psychopathy manifest divergent relations with components of its nomological network depending on gender?"**

Joshua D. Miller, Ashley Watts, Shayne E. Jones

2011 | Personality and Individual Differences | DOI: 10.1016/j.paid.2010.11.028

Źródło

**[16] "J.H. Hubbard and B.H. West, Differential Equations. A Dynamical Systems Approach. Part I, Springer-Verlag, New York (1991)."**

S STROGATZ

1992 | Bulletin of Mathematical Biology | DOI: 10.1016/s0092-8240(05)80099-0

Źródło

**[17] "Designing temporal networks that synchronize under resource constraints"**

Yuanzhao Zhang, S. Strogatz

2021 | Nature Communications | DOI: 10.1038/s41467-021-23446-9

Źródło

**[18] "Modeling the Interplay Between Seasonal Flu Outcomes and Individual Vaccination Decisions"**

Irena Papst, K. O'Keeffe, S. Strogatz

2021 | Bulletin of Mathematical Biology | DOI: 10.1007/s11538-021-00988-z

Źródło

**[19] "Synchronization in random networks of identical phase oscillators: A graphon approach"**

Shriya V. Nagpal, Gokul G. Nair, S. Strogatz, Francesca Parise

2024

Źródło

**[20] "A behavioural approach to port-controlled systems"**

Jonas Kirchhoff

2024 | IFAC-PapersOnLine | DOI: 10.1016/j.ifacol.2024.10.220

Źródło

Treść tworzy Fundacja Dobre Państwo.
Redaguje i publikuje APA ONE, autorski system redakcyjny Fundacji oparty na AI.
APA ONE Publishing System
Fundacja Dobre Państwo © 2026
Article ID: a22f84f9-bd9a-4546-b3db-ca7371d470f6