ChatGPT

# Ataki kaskadowe w systemach sieciowych i infrastrukturze krytycznej

## Streszczenie wykonawcze i abstrakt

**Streszczenie wykonawcze.** Ataki kaskadowe to szczególna klasa oddziaływań (cybernetycznych, fizycznych lub hybrydowych), których skutki rozchodzą się w czasie i przestrzeni poprzez zależności sieciowe, mechanizmy redystrybucji obciążeń oraz sprzężenia zwrotne sterowania, prowadząc do nieproporcjonalnie dużej degradacji funkcji systemu (np. rozległe przerwy w dostawie energii, utrata usług krytycznych, awarie bezpieczeństwa funkcjonalnego). Kluczowa cecha odróżniająca „atak kaskadowy" od pojedynczego incydentu polega na tym, że celem (lub przewidywalnym następstwem) jest uruchomienie propagacji awarii w sieci – w tym w sieciach współzależnych (np. IT–OT, energetyka–telekomunikacja), które mogą ulec gwałtownemu, nieliniowemu załamaniu nawet po małej inicjacji. Teoretyczne narzędzia opisu obejmują: modele progowe i dynamikę na grafach, modele przeciążeniowe (redystrybucja „load"), perkolację i przejścia fazowe w sieciach, modele epidemiologiczne (SIR) oraz formalizmy stabilności (np. równanie wahadłowe w energetyce). Wątki historyczne z badań nad łańcuchami reakcji i krytycznością – rozwijane m.in. w okresie wojennym w kontekście obliczeń procesów multiplikatywnych i metod probabilistycznych – przenikają do współczesnych ujęć kaskad jako zjawisk progowych z parametrem „reprodukcji" awarii > 1. [1]

Analiza czterech zdarzeń pokazuje różne mechanizmy kaskady: (i) blackout 14.08.2003 w USA/Kanadzie – sekwencja błędów sytuacyjnych, niedoborów mocy biernej i kolejnych wyłączeń linii doprowadziła do szybkiej propagacji w systemie przesyłowym; (ii) awaria w elektrowni Fukushima Daiichi Nuclear Power Plant [2] – katastrofa naturalna uruchomiła kaskadę utraty zasilania i funkcji chłodzenia; (iii) incydent TRITON/TRISIS – przykład ukierunkowania na warstwę bezpieczeństwa (SIS), gdzie kaskada ma charakter cyber–fizyczny i dotyczy dezaktywacji bariery ostatniej instancji; (iv) infekcja SQL Slammer w sieci zakładu Davis–Besse Nuclear Power Station [3] – ekstremalnie szybka propagacja złośliwego kodu (kaskada komunikacyjna) skutkująca utratą dostępności wybranych funkcji wspierających bezpieczeństwo. Wspólny mianownik stanowią: (a) ukryte współzależności, (b) ograniczona obserwowalność i błędy estymacji stanu, (c) automatyka zabezpieczeniowa, która w warunkach skrajnych może przyspieszać fragmentację, oraz (d) brak wystarczającej separacji domen (organizacyjnej i technicznej). [4]

**Abstrakt.** Artykuł przedstawia rygorystyczną, wielomodelową analizę „ataków kaskadowych" w systemach złożonych, ze szczególnym uwzględnieniem sieci energetycznych, infrastruktury krytycznej i kontekstu energetyki jądrowej. Zaproponowano praktyczną klasyfikację ataków kaskadowych według typu inicjacji, mechanizmu propagacji i topologii współzależności, a następnie zestawiono formalizmy matematyczne: (1) dynamikę progową na grafach (global cascades), (2) modele przeciążeniowe redystrybucji obciążeń, (3) perkolację i generujące funkcje, (4) modele epidemiologiczne i procesy rozgałęziające, (5) analizę stabilności (DC/AC power flow, równanie wahadłowe), (6) podejścia probabilistyczne (Monte Carlo, drzewa zdarzeń). Część historyczna syntetyzuje ewolucję idei multiplikacji i krytyczności – od obliczeń procesów łańcuchowych i stochastycznych w połowie XX wieku do współczesnej nauki o sieciach współzależnych. Część empiryczna prezentuje studia przypadków (blackout 2003, Fukushima, TRITON, Davis-Besse/SQL Slammer) z mechanizmami kaskady i wnioskami projektowymi. Praca kończy się rekomendacjami dla operatorów infrastruktury krytycznej, obejmującymi monitorowanie synchrofazorowe, odporne projektowanie (redundancja i różnorodność),

kontrolę zmian, segmentację IT/OT oraz ramy zgodności regulacyjnej w obszarze cyberbezpieczeństwa i bezpieczeństwa jądrowego. [5]

# Wprowadzenie

Systemy krytyczne (energetyka, woda, transport, telekomunikacja, przemysł procesowy, infrastruktura jądrowa) są dziś z natury sieciowe: składają się z węzłów (zasobów) i powiązań (przepływów energii, informacji, sterowania, logistyki). Ta sieciowość zwiększa efektywność, ale wprowadza ryzyko nieliniowych reakcji na zakłócenia: mała, lokalna inicjacja może uruchomić przejście fazowe od funkcjonowania globalnego do fragmentacji lub załamania usług. W literaturze naukowej opisuje się to jako kaskady awarii (cascading failures) oraz kaskady w sieciach współzależnych (interdependent networks), gdzie uszkodzenia w jednej warstwie (np. komunikacja) generują wtórne uszkodzenia w innej (np. elektroenergetyka), które wracają jako kolejne impulsy degradacji. [6]

W ujęciu bezpieczeństwa państwa i gospodarki kluczowe jest odróżnienie dwóch klas zdarzeń: (a) kaskad jako niezamierzonych awarii (błędy techniczne, pogoda, błędy procedur), oraz (b) ataków kaskadowych, w których inicjacja ma charakter umyślny (cybernetyczny, fizyczny lub hybrydowy), a krytycznym elementem jest wykorzystanie architektury sieci i automatyki do wzmocnienia skutków. Formalne modele kaskad dostarczają języka do oceny podatności i projektowania odporności, ale mają ograniczenia: uproszczenia topologiczne, brak pełnego odwzorowania sterowania, słaba identyfikowalność parametrów oraz trudność walidacji na rzadkich, skrajnych zdarzeniach. Z tego powodu w praktyce stosuje się triangulację: modele analityczne + symulacje (w tym Monte Carlo) + ćwiczenia i testy + mechanizmy monitoringu w czasie rzeczywistym. [7]

W niniejszym tekście zachowano ograniczenia bezpieczeństwa informacji: modele i mechanizmy opisano jako narzędzia analityczne i projektowe; pominięto szczegóły operacyjne, które mogłyby ułatwiać prowadzenie szkodliwych działań (np. konfiguracje podatności, procedury obejścia zabezpieczeń). [8]

# Definicja i klasyfikacja ataków kaskadowych

**Definicja robocza.** Atak kaskadowy jest inicjacją (lub sekwencją inicjacji) w systemie sieciowym, zaprojektowaną lub dobraną tak, aby uruchomić propagację wtórnych degradacji poprzez mechanizmy zależności (przepływy, sterowanie, zależności funkcjonalne), prowadząc do skutku globalnego nieproporcjonalnego do rozmiaru inicjacji. W tym sensie „atak kaskadowy" jest pojęciem nadrzędnym wobec: (i) ataków na węzły/łącza o wysokim znaczeniu dla przepływu i (ii) ataków na warstwy współzależne (IT→OT→fizyczne konsekwencje), które wzmacniają się w pętli sprzężenia. [9]

**Kluczowe osie klasyfikacji (praktyczne dla infrastruktury krytycznej):**

1) **Warstwa inicjacji i skutku** - *czysto fizyczna*: inicjacja w infrastrukturze materialnej, skutki przez redystrybucję obciążeń (np. sieć przesyłowa). [10]
- *czysto cybernetyczna*: kaskada w domenie informacyjnej (np. gwałtowna propagacja robaka) wpływająca na dostępność/obserwowalność, a pośrednio na bezpieczeństwo. [11]
- *cyber–fizyczna*: inicjacja cyber w systemach OT/SIS skutkująca potencjalnym zagrożeniem procesowym i awaryjnym. [12]

2) **Mechanizm propagacji** - *progowy (threshold)*: element przechodzi w stan awarii po przekroczeniu progu wpływu sąsiadów; typowe dla global cascades. [13]
- *przeciążeniowy (load redistribution)*: po awarii komponentu obciążenie jest redystrybuowane, co może

indukować kolejne przeciążenia. [14]
- *perkolacyjny/fragmentacyjny*: sieć traci spójność, pojawia się gwałtowny spadek rozmiaru składowej olbrzymiej. [15]
- *epidemiczny*: propagacja na grafie z parametrem transmisji i „usuwania", formalnie analogiczna do SIR. [16]
- *rozgałęziający*: każdy „aktywny" element może generować pewną liczbę wtórnych zdarzeń (reprodukcja). [17]

3) **Szybkość i sterowalność kaskady** - *szybka kaskada dynamiczna* (sekundy–minuty): typowa dla systemów energetycznych przy utracie synchronizmu i lawinowych wyłączeniach zabezpieczeń. [18]
- *wolna kaskada operacyjno-organizacyjna* (godziny–dni): rozchodzenie się skutków przez zależności logistyczne, utrzymaniowe, komunikacyjne i decyzyjne. [19]

4) **Topologia celu** - *atak ukierunkowany na „wąskie gardła"* (wysokie obciążenie/pośrednictwo), zwiększający ryzyko przeciążenia. [20]
- *atak na warstwy zależności* (interdependent links), gdzie zniszczenie relacji zależności może wywołać przejście do gwałtownej kaskady. [21]

# Modele matematyczne i teoretyczne

## Aparat ogólny: graf i stan elementów

System sieciowy formalizuje się jako graf $G = (V, E)$, gdzie $V$ to zbiór węzłów, $E$ – krawędzi; macierz sąsiedztwa $A = [a_{ij}]$ koduje połączenia, a stan węzła $i$ oznacza się np. $x_i(t) \in \{0, 1\}$ (sprawny/uszkodzony) lub ciągle (poziom sprawności). Dynamikę kaskady opisuje się regułą przejścia:

$$x_i(t+1) = F_i\big(x(t),\, \theta_i,\, \eta(t)\big),$$

gdzie $\theta_i$ to parametry (progi, pojemności), a $\eta(t)$ – wymuszenia/zakłócenia losowe. Takie ujęcie jest wspólnym rdzeniem modeli progowych, epidemiologicznych i przeciążeniowych; różni je definicja funkcji $F_i$ oraz interpretacja $x$. [22]

## Model progowy kaskad globalnych

W modelu progowym (w duchu „global cascades") każdy węzeł $i$ przyjmuje aktywację/awarię, gdy frakcja jego sąsiadów w stanie awarii przekroczy próg $\phi_i$:

$$x_i(t+1) = 1\left(\frac{\sum_{j\in\mathcal{N}(i)} x_j(t)}{k_i} \geq \phi_i\right),$$

gdzie $\mathcal{N}(i)$ to sąsiedzi, $k_i$ – stopień węzła. Model pokazuje, że duże kaskady mogą być rzadkie, ale możliwe w określonych reżimach parametrów (rozkład stopni, rozkład progów, gęstość sieci). Ograniczenia: brak jawnego przepływu (mocy, danych), brak opóźnień i sterowania, a także uproszczona topologia (często losowa). Zaletą jest analityczna przejrzystość i przydatność do oceny podatności na efekt „mała inicjacja → duża kaskada". [23]

## Model przeciążeniowy redystrybucji obciążeń

W modelu przeciążeniowym typu Motter–Lai obciążenie węzła $L_i$ interpretuje się np. jako miarę pośrednictwa (betweenness) w przepływie po najkrótszych ścieżkach, a pojemność jako

$$C_i = (1+\alpha)L_i^{(0)},$$

gdzie $L_i^{(0)}$ jest obciążeniem w stanie bazowym, a $\alpha > 0$ – margines nadmiarowości. Po usunięciu węzła/łącza obciążenia przeliczane są na nowo; węzły z $L_i > C_i$ ulegają awarii, wywołując kaskadę. Kluczowa intuicja: heterogeniczność obciążeń i istnienie węzłów krytycznych pozwala, by pojedyncza inicjacja powodowała nieproporcjonalny zanik funkcji sieci. Ograniczenia: obciążenie liczone na najkrótszych ścieżkach jest przybliżeniem realnych przepływów fizycznych, a mechanizmy sterowania/lokalnych zabezpieczeń nie są jawnie modelowane. [24]

## Perkolacja i przejścia fazowe w sieciach

Perkolacyjne ujęcie odporności opisuje, czy po usunięciu frakcji węzłów/krawędzi pozostaje składowa olbrzymia (giant component). Dla sieci losowych i modeli epidemicznych/propagacyjnych narzędziem są funkcje tworzące i mapowanie na perkolację, co pozwala wyznaczać progi krytyczne (np. warunki na średnie stopnie i rozkłady stopni). W praktyce interpretacja jest następująca: istnieje parametr krytyczny (np. „gęstość funkcjonalnych zależności"), poniżej którego system traci zdolność do utrzymania globalnej łączności/świadczenia usługi. Ograniczenia: w sieciach infrastrukturalnych topologia jest silnie nielosowa, obciążenia są przepływowe, a awarie zależą od stanów fizycznych, nie tylko od łączności. [25]

## Modele epidemiologiczne na sieciach

W klasycznym modelu SIR na grafie stany węzła to: podatny $S$, zakaźny $I$, usunięty $R$. W ujęciu ciągłym:

$$\frac{dS}{dt} = -\beta\frac{SI}{N}, \quad \frac{dI}{dt} = \beta\frac{SI}{N} - \gamma I, \quad \frac{dR}{dt} = \gamma I.$$

Na sieciach parametry transmisji mogą zależeć od krawędzi i stopni; formalny aparat łączy SIR z perkolacją poprzez prawdopodobieństwa transmisji i rozkłady stopni. Dla analizy ataków kaskadowych SIR jest użyteczny jako model propagacji „zdarzeń szkodliwych" (np. złośliwego kodu lub błędnych stanów informacyjnych), ale nie opisuje bezpośrednio przeciążeń fizycznych (mocy) ani działania automatyki zabezpieczeniowej. [26]

## Sieci współzależne i kaskady wielowarstwowe

W modelu sieci współzależnych rozważa się co najmniej dwie sieci $A$ i $B$ oraz relacje zależności: awaria węzła w $A$ może wymuszać awarię węzła zależnego w $B$. Proces ma charakter iteracyjny: usuwanie w jednej warstwie → wtórne usuwanie w drugiej → dalsza fragmentacja itd. Wynik fundamentalny: dla pewnych parametrów sprzężenia i topologii przejście od sprawności do załamania może być gwałtowne (przypominające „pierwszego rzędu"), a system bywa mniej odporny niż pojedyncza sieć o podobnej charakterystyce. Ta obserwacja jest szczególnie obciążająca dla infrastruktury krytycznej, która realnie jest wielowarstwowa (energia–telekomunikacja–IT–logistyka–ludzie). [27]

## Modele elektroenergetyczne: przepływy i stabilność

W energetyce kluczowe są modele przepływowe. W uproszczonym DC power flow (często stosowanym w analizach kontyngencji i szybkich symulacjach) zakłada się m.in. małe kąty i pomija straty, otrzymując zależność aktywnych mocy od kątów fazowych:

$$\mathbf{P} = \mathbf{B}\boldsymbol{\theta},$$

gdzie $\mathbf{B}$ jest macierzą susceptancji (zredukowaną). Przepływ na linii $(i,j)$ jest proporcjonalny do różnicy kątów $\theta_i - \theta_j$. Kaskada przeciążeniowa w sieci przesyłowej bywa modelowana jako: (1) kontyngencja

(utrata elementu), (2) recomputacja przepływów, (3) wyłączenia elementów przekraczających limity termiczne/ochronne, (4) powtórzenie. Ograniczenie: DC nie odwzorowuje wrażliwości napięciowej i mocy biernej, które w realnych blackoutach odgrywają rolę krytyczną. [28]

Stabilność dynamiczna dotyczy utrzymania synchronizmu generatorów. Klasyczny model „swing equation" (dla uproszczonego generatora synchronicznego) ma postać:

$$M\frac{d^2\delta}{dt^2} + D\frac{d\delta}{dt} = P_m - P_e(\delta),$$

gdzie $\delta$ to kąt wirnika względem układu odniesienia, $P_m$ – moc mechaniczna, $P_e$ – moc elektryczna (często $P_e = P_{\max}\sin\delta$ w modelu SMIB), $M$ – bezwładność, $D$ – tłumienie. W kaskadach blackoutów istotne są szybkie zmiany przepływów i częstotliwości, które mogą uruchamiać automatyczne odciążenia i wyłączenia, a następnie tworzenie wysp (islanding) i dalszą fragmentację. [29]

## Procesy rozgałęziające, krytyczność i wątki historyczne

Proces rozgałęziający (branching) jest naturalnym formalizmem kaskad: pojedyncze zdarzenie może generować losową liczbę zdarzeń wtórnych. Jeśli średnia liczba „potomków" $\mathbb{E}[Z] = R$ przekracza 1, proces ma dodatnie prawdopodobieństwo niezaniknięcia (superkrytyczność); dla $R < 1$ typowo wygasa (subkrytyczność). Ten język krytyczności jest głęboko związany z analizą łańcuchów reakcji i multiplikacji w fizyce jądrowej: warunek „reprodukcji" > 1 oznacza wzrost lawinowy, a ≈1 – stan krytyczny. W połowie XX wieku powstawały formalizmy stochastyczne dla procesów multiplikatywnych (w tym jako abstrakcje proliferacji neutronów), które wprost używały aparatu rozgałęzień i prawdopodobieństw. [30]

W kontekście Projekt Manhattan [31] oraz pracy środowiska Los Alamos National Laboratory [32] istotne jest, że koncepcje multiplikacji, krytyczności i probabilistycznych metod obliczeń stały się narzędziami inżynierii ryzyka skrajnego. Prace Stanisław Ulam [33] nad procesami multiplikatywnymi (ujęcie rozgałęziające) oraz rozwój metod probabilistycznych i symulacyjnych (Monte Carlo) są historycznie ważne nie jako „model ataku", lecz jako fundament nowoczesnego rozumienia kaskad: (i) małe fluktuacje w pobliżu progu krytycznego mogą dawać ogromne rozrzuty rozmiarów kaskady, (ii) symulacje losowe są narzędziem oceny zdarzeń rzadkich w systemach o ogromnej złożoności. [34]

## Tabela porównawcza modeli matematycznych

| Model | Równania kluczowe | Założenia | Zastosowania | Ograniczenia |
|---|---|---|---|---|
| Model progowy (global cascades) | $x_i(t+1) = 1\left(\frac{\sum_{j\in\mathcal{N}(i)} x_j}{k_i} \geq \phi_i\right)$ | Awaria zależy od frakcji sąsiadów; topologia często losowa | Analiza podatności na rzadkie, duże kaskady; zjawiska progowe | Brak jawnych przepływów; brak sterowania i opóźnień |
| Model przeciążeniowy Motter–Lai | $C_i = (1+\alpha)L_i^{(0)}$, awaria gdy $L_i > C_i$ po redystrybucji | Obciążenie ≈ pośrednictwo; przepływ po ścieżkach | Wrażliwość na inicjację w węzłach krytycznych; analogie do sieci energetycznych/ Internetu | Obciążenie jako proxy; uproszczenie fizyki i zabezpieczeń |

| Model | Równania kluczowe | Założenia | Zastosowania | Ograniczenia |
|---|---|---|---|---|
| Perkolacja / generujące funkcje | Próg spójności (giant component) zależne od rozkładu stopni | Skupienie na łączności, nie na przepływach | Ocena fragmentacji; mapowanie epidemii na perkolację | Nie opisuje przeciążeń i napięć; ograniczona realizm topologii |
| SIR na sieciach | $\dot{S} = -\beta SI/N$, $\dot{I} = \beta SI/N - \gamma I$ | Transmisja i „usuwanie”; czas infekcyjny | Propagacja malware/zdarzeń; analiza skutków transmisji | Słaba reprezentacja fizyki OT/ energetyki; parametry trudne do kalibracji |
| Sieci współzależne | Iteracja: usunięcia w A → zależne usunięcia w B → fragmentacja | Jawne relacje zależności między warstwami | Analiza kaskad IT–OT, energia–telekom; ryzyko gwałtownego załamania | Duża wrażliwość na definicję zależności; trudna walidacja |
| DC power flow + reguła wyłączeń | $\mathbf{P} = \mathbf{B}\boldsymbol{\theta}$, iteracja kontyngencji i odcięć | Małe kąty; pomija napięcia i straty | Szybkie testy N-1; symulacje kaskad przeciążeniowych | Brak pełnej dynamiki i mocy biernej; ograniczona zgodność z blackoutami napięciowymi |
| Równanie wahadłowe (stabilność) | $M\ddot{\delta} + D\dot{\delta} = P_m - P_e(\delta)$ | Uproszczony generator; analiza synchronizmu | Ocena stabilności przejściowej i ryzyka rozspojenia | Wymaga rozszerzeń do sieci wielowęzłowych; parametracja |
| Proces rozgałęziający (krytyczność) | $R = \mathbb{E}[Z]$ (reprodukcja wtórnych zdarzeń) | Zdarzenia wtórne jako „potomkowie” | Analiza rozkładu rozmiarów kaskad; zdarzenia rzadkie | Uproszczenie struktury zależności i czasów; brak sterowania |

```
flowchart TD
  A[Inicjacja: incydent/atak] --> B[Uszkodzenie lokalne lub utrata
obserwowalności]
  B --> C[Redystrybucja obciążenia / zmiana przepływów]
  C --> D{Czy przekroczono progi?}
  D -- nie --> E[Stabilizacja / degradacja ograniczona]
  D -- tak --> F[Zadziałanie automatyki / odcięcia / przełączenia]
  F --> G[Nowe przeciążenia i wtórne awarie]
  G --> C
  F --> H[Fragmentacja systemu / praca wyspowa]
```

```
H --> I[Utrata usług krytycznych]
I --> J[Skutki wtórne: społeczne, gospodarcze, bezpieczeństwa]
```

## Analiza przypadków

**Studium przypadku: blackout 14 sierpnia 2003 (USA/Kanada).** Oficjalny raport powypadkowy wskazuje, że zdarzenie było kaskadą wieloetapową, w której faza „przedkaskadowa" obejmowała narastające obciążenia i problemy z mocą bierną, a faza kaskadowa – gwałtowne, sekundowe wyłączenia linii, tworzenie wysp i utratę generacji. Raport podkreślał również rolę niewystarczającej świadomości sytuacyjnej i problemów narzędziowych (estymacja stanu / analiza kontyngencji). [36]

**Chronologia (wybrane punkty, skrót):**
– Ok. 13:31 czasu lokalnego: utrata jednostki wytwórczej Eastlake 5 (raport określa ją jako krok krytyczny w sekwencji zdarzeń). [37]
– Ok. 15:39–15:59: seria wyłączeń linii 138 kV w północnej części stanu Ohio [38] prowadząca do osłabienia układu; następnie awaria wyłącznikowa na szynie 138 kV (West Akron) powoduje kolejne odcięcia. [39]
– Ok. 16:05–16:06: wyłączenie Dale–West Canton 138 kV i następnie Sammis–Star 345 kV; raport wskazuje to jako punkt zwrotny inicjujący kaskadę obejmującą rozległy obszar. [39]
– Ok. 16:10: dynamiczny „power swing", szybkie zmiany przepływów (rzędu tysięcy MW), kolejne wyłączenia i utrata generacji; raport wskazuje równocześnie automatyczne odciążenia (under-frequency load shedding) oraz odcięcia kolejnych elementów. [40]

**Mechanizm kaskady.** W wymiarze sieciowym zdarzenie można interpretować jako przejście z reżimu lokalnie zarządzalnego do reżimu superkrytycznego (w sensie rozgałęzień/rozmiarów wtórnych awarii): utrata elementów przesyłu i wytwarzania wymusza redystrybucję przepływów, zwiększa prądy i obciążenia termiczne oraz pogarsza parametry napięciowe; automatyka zabezpieczeniowa, działając poprawnie lokalnie, kumulatywnie przyspiesza fragmentację (odcinanie przeciążonych elementów, separacje wyspowe). Raport pokazuje także, że znaczna część sekwencji opierała się na utracie skutecznej „pętli sterowania" na poziomie operatorskim (brak adekwatnej diagnozy i reakcji w czasie). [41]

**Wniosek operacyjny.** W blackoutach sieciowych kaskada jest nie tylko zjawiskiem topologicznym („kto z kim jest połączony"), lecz przepływowo-sterowniczym: to, jak obciążenia zmieniają się po inicjacji, decyduje o wczesnym wejściu w strefę progową. Z tego powodu monitorowanie i szybkie obliczenia kontyngencji (w tym oparte o DC power flow) są narzędziami redukcji ryzyka, lecz muszą uwzględniać ograniczenia uproszczeń i rolę mocy biernej. [42]

**Studium przypadku: awaria jądrowa Fukushima (kaskada utraty zasilania i funkcji chłodzenia).** Raport niezależnej komisji parlamentarnej (NAIIC) stwierdza, że choć inicjacja była katastrofą naturalną (trzęsienie ziemi i tsunami), samej awarii w elektrowni nie należy traktować wyłącznie jako „naturalnej" – wskazano na deficyty przygotowania, nadzoru i kultury bezpieczeństwa. [43]

**Mechanizm kaskady (model barier i sprzężeń):**
(1) bodziec ekstremalny → (2) ubytek zasilania i/lub infrastruktury pomocniczej → (3) degradacja chłodzenia i instrumentacji → (4) eskalacja zdarzeń do stanów awaryjnych reaktora i obudowy bezpieczeństwa → (5) skutki wtórne dla środowiska i zarządzania kryzysowego. Komisja NAIIC podkreśla niedostateczną „wytrzymałość" (yield strength) w aspekcie odporności na tak silne zdarzenie i powiązane braki w założeniach projektowych i wytycznych. [43]

**Materiały operatora (TEPCO) i ryzyko tsunami.** W dokumentach analitycznych operatora wskazywano na wyniki obliczeń wysokości tsunami i zalania terenu zakładu (wartości liczbowe i szczegółowe parametry są w tej pracy nieprzytaczane), co jest istotne jako ilustracja, że w kaskadach naturalno-technicznych („Natech") kluczowa jest nie sama inicjacja, lecz odporność infrastruktury wspierającej bezpieczeństwo (zasilanie, pompy, rozdzielnie, komunikacja). [44]

**Wniosek projektowy.** Fukushima jest przykładem kaskady wielobarierowej, w której awaria wspólnej przyczyny (common-cause) może naruszyć wiele niezależnie projektowanych funkcji naraz (np. zasilanie zewnętrzne i źródła rezerwowe), a następnie wymuszać działania awaryjne w warunkach obniżonej obserwowalności. To bezpośrednio uzasadnia w standardach bezpieczeństwa wymagania odporności na zdarzenia zewnętrzne i poprawę przygotowania do reakcji awaryjnej niezależnie od przyczyny inicjacji. [45]

**Studium przypadku: TRITON/TRISIS (kaskada cyber–fizyczna na warstwę bezpieczeństwa).** Według komunikatu Federal Bureau of Investigation (FBI) [46] (IC3) z 2022 r. złośliwe oprogramowanie TRITON zostało użyte przeciwko systemowi bezpieczeństwa (SIS) w obiekcie petrochemicznym na Bliskim Wschodzie w 2017 r. Cechą wyróżniającą była orientacja na warstwę, której funkcją jest inicjowanie bezpiecznego wyłączenia w sytuacjach awaryjnych. Dokument odnotowuje, że instalacja doprowadziła do wejścia obiektu w stan bezpieczny po wykryciu anomalii, a śledztwo ujawniło obecność atakującego i malware. [47]

**Mechanizm kaskady (bez szczegółów operacyjnych).** TRITON ilustruje wzorzec: przeniesienie wpływu z warstwy IT do OT, następnie do SIS, co potencjalnie przekształca incydent cybernetyczny w ryzyko fizyczne. W ujęciu kaskadowym „zdarzeniem wtórnym" nie jest tylko awaria kolejnego urządzenia, lecz degradacja bariery bezpieczeństwa: jeśli SIS nie zadziała w sytuacji procesu niebezpiecznego, skutki mogą eskalować do rozległych strat (ludzie, środowisko, infrastruktura). [12]

**Wniosek dla infrastruktury krytycznej.** Komunikat IC3 wskazuje także, że podobny schemat koncepcyjny dotyczy systemów bezpieczeństwa niezależnie od producenta: odporność wymaga izolacji, silnego zarządzania zmianą, kontroli dostępu i monitorowania – przy zachowaniu zasady minimalnej ekspozycji systemów bezpieczeństwa na sieci zewnętrzne. [48]

**Studium przypadku: infekcja SQL Slammer i efekt kaskady komunikacyjnej (Davis-Besse, 2003).** Analiza przypadku programu CyOTE (bazująca na informacjach publicznych) opisuje infekcję robakiem SQL Slammer, który w krótkim czasie zainfekował dużą część podatnych hostów na świecie; w przypadku Davis-Besse propagacja doprowadziła do zatorów sieciowych i utraty dostępności wybranych funkcji monitorowania przez ograniczony czas, przy czym zakład był w stanie odstawienia/bez paliwa, co ograniczało ryzyko bezpieczeństwa jądrowego w tym konkretnym momencie. [49]

Z perspektywy teorii kaskad jest to przykład, w którym „kaskada" dotyczy warstwy komunikacyjnej: masowe generowanie ruchu i infekcji tworzy dodatnie sprzężenie zwrotne (więcej infekcji → więcej skanowania → więcej przeciążenia), a skutki w systemie krytycznym wynikają z zależności między siecią IT a systemami wspierającymi obserwowalność i operacje. Inżynieryjnie pokazuje to, że nawet nietargetowane zdarzenia cybernetyczne mogą wchodzić w domenę bezpieczeństwa przez kanał dostępności i świadomości sytuacyjnej. [11]

# Energetyka jądrowa: ryzyko, regulacje i projektowanie odporne

## Kaskady awarii jako problem „sprzężeń pomocniczych”

Elektrownia jądrowa jest systemem wielowarstwowym: reaktor i obudowa bezpieczeństwa są rdzeniem, ale bezpieczeństwo zależy od infrastruktury pomocniczej (zasilanie, chłodzenie, automatyka, instrumentacja, organizacja działań awaryjnych). Kaskada typowa dla scenariuszy „station blackout” polega na tym, że utratę zasilania AC (zewnętrznego i/lub wewnętrznego) uruchamia wtórne degradacje: utratę pomp, ograniczenia chłodzenia i instrumentacji, rosnące wymagania dla źródeł rezerwowych, a następnie ryzyko eskalacji stanu reaktora. [50]

W reżimie regulacyjnym U.S. Nuclear Regulatory Commission (NRC) [51] wymóg odporności na blackout stacyjny jest wyrażony w §50.63 („Loss of all alternating current power”): licencjobiorca ma wykazać zdolność radzenia sobie z SBO przez określony czas poprzez „coping analysis” oraz zapewnienie chłodzenia rdzenia i integralności obudowy bezpieczeństwa. [52]

## Standardy projektowe i gotowość na zdarzenia zewnętrzne

W standardach Międzynarodowa Agencja Energii Atomowej (IAEA) [53] dla projektowania elektrowni jądrowych (SSR-2/1 Rev.1) akcentuje się wymagania projektowe zapewniające ochronę ludzi i środowiska, w tym kontekst zdarzeń zewnętrznych i wniosków z poważnych awarii. W praktyce oznacza to wymagania dotyczące barier, redundancji, separacji i odporności systemów bezpieczeństwa na inicjacje zewnętrzne oraz awarie wspólnej przyczyny. [54]

Dla zdarzeń awaryjnych standardy dotyczące gotowości i reagowania (GSR Part 7 i powiązane przewodniki) wzmacniają aspekt „organizacyjnej odporności”: nawet jeśli kaskada techniczna jest trudna do zatrzymania, sprawne zarządzanie awaryjne może ograniczać konsekwencje radiologiczne i społeczne. [55]

## Cyberbezpieczeństwo jako czynnik ryzyka kaskadowego w energetyce jądrowej

Regulacja §73.54 („Protection of digital computer and communication systems and networks”) wymaga „wysokiego poziomu pewności” ochrony systemów cyfrowych przed cyberatakami (do poziomu zagrożenia projektowego, design basis threat) oraz wdrożenia planu cyberbezpieczeństwa. [56]

Z kolei przewodniki regulacyjne (np. RG 5.71) opisują metody uznawane za akceptowalne w budowie programu cyberbezpieczeństwa dla obiektów jądrowych, co praktycznie wspiera podejście „defense-in-depth” w domenie cyfrowej i zarządzania aktywami krytycznymi. [57]

W ujęciu Międzynarodowa Agencja Energii Atomowej (IAEA) [53] bezpieczeństwo komputerowe jest również adresowane w serii Nuclear Security Series (np. publikacje o cyberbezpieczeństwie w obiektach jądrowych i planowaniu reakcji na incydenty), co odzwierciedla fakt, że kaskady cyber–fizyczne mogą omijać klasyczne granice „systemów bezpieczeństwa” przez kanał zależności i błędów wspólnej przyczyny (np. infrastruktura teleinformatyczna, utrata obserwowalności, nieautoryzowane zmiany konfiguracji). [58]

# Wykrywanie, monitorowanie i mitigacja

## Monitorowanie wczesnych sygnałów kaskady

W energetyce podstawowym narzędziem „wczesnego ostrzegania" jest połączenie estymacji stanu, analizy kontyngencji oraz danych synchrofazorowych (PMU). Standardy synchrofazorowe (np. IEEE C37.118.x) definiują ramy pomiaru i transmisji zsynchronizowanych fazorów, częstotliwości i ROCOF, umożliwiając aplikacje WAMS/WAMPAC (wide-area monitoring/protection/control). Źródła przeglądowe wskazują na ewolucję tych standardów i ich rolę w transmisji danych w czasie rzeczywistym. [59]

W praktycznych analizach kaskad w sieciach przesyłowych stosuje się szybkie przybliżenia przepływu (DC power flow), by w krótkim czasie przeliczać tysiące scenariuszy kontyngencji, co jest krytyczne, gdy system zbliża się do granic termicznych i napięciowych. [35]

## Symulacje i testy odporności

W systemach o dużej złożoności i silnej nieliniowości symulacje stochastyczne (Monte Carlo) są standardowym narzędziem analizy zdarzeń rzadkich i niepewności parametrów. Historycznie metoda Monte Carlo była motywowana potrzebą obliczeń procesów transportu i multiplikacji cząstek w złożonych geometriach, a w nowoczesnym ujęciu jest analogicznie stosowana do szacowania ryzyka kaskad (np. rozkład rozmiarów blackoutów, skutki wspólnych przyczyn). [60]

W modelach blackoutów obserwuje się cechy krytyczności i rozkłady o „ciężkich ogonach" dla rozmiarów zdarzeń; prace modelowe dla sieci przesyłowych (CASCADE/OPA) analizują przejścia krytyczne i własności statystyczne blackoutów jako zjawisk systemowych. [61]

## Tabela środków mitigacji

| Środek | Opis | Skuteczność (typowo) | Koszty/ zasoby | Ograniczenia |
|---|---|---|---|---|
| Segmentacja IT/OT i separacja stref | Rozdział stref zaufania, minimalizacja połączeń, kontrolowane bramy | Wysoka dla redukcji propagacji cyber | Średnie–wysokie (architektura, procesy) | Złożoność integracji operacyjnej; ryzyko obejść proceduralnych |
| Program cyberbezpieczeństwa dla obiektów jądrowych | Identyfikacja aktywów krytycznych, kontrola dostępu, zarządzanie zmianą, monitoring | Wysoka (jeśli konsekwentnie wdrożony) | Wysokie (ciągłe) | Trudność pełnej inwentaryzacji i utrzymania zgodności |

| Środek | Opis | Skuteczność (typowo) | Koszty/ zasoby | Ograniczenia |
|---|---|---|---|---|
| Monitoring synchrofazorowy i analiza w czasie rzeczywistym | PMU, WAMS: detekcja oscylacji, spadków częstotliwości, narastania przeciążeń | Wysoka dla kaskad dynamicznych | Wysokie (urządzenia, łączność, analityka) | Wymaga jakości danych i odpornej telekomunikacji |
| Szybka analiza kontyngencji (N-1/N-k) | Automatyczne przeliczenia scenariuszy utraty elementów i ocena marginesów | Wysoka w fazie pre-kaskadowej | Średnie | Ograniczenia modeli (DC vs AC, reaktywna) |
| Redundancja i różnorodność (diversity) | Wielotorowe źródła, alternatywne ścieżki, różne technologie, rozproszenie | Wysoka (ogranicza awarie wspólnej przyczyny) | Wysokie (CAPEX/OPEX) | Złożoność utrzymania; ryzyko wspólnych zależności ukrytych |
| Ćwiczenia i gotowość awaryjna | Procedury, trening, scenariusze, łączność kryzysowa | Średnia–wysoka (redukuje konsekwencje) | Średnie | Nie eliminuje inicjacji; zależne od kultury organizacyjnej |
| Zarządzanie aktywami i łatkami (patch) w OT | Kontrola wersji, okna serwisowe, walidacja dostawcy | Średnia–wysoka | Średnie | Konflikt z wymaganiami dostępności i certyfikacji |
| Walidacja modeli i „stress testing” | Testy odporności symulacyjnej, analiza wrażliwości, Monte Carlo | Średnia–wysoka | Średnie–wysokie | Wyniki zależą od jakości modeli i danych |

```
flowchart LR
  A[Dane: pomiary sieci/procesu] --> B[Walidacja jakości i synchronizacja]
  B --> C[Estymacja stanu i detekcja anomalii]
  C --> D[Ocena ryzyka kaskady: kontyngencje + progi]
  D --> E{Ryzyko wysokie?}
  E -- nie --> F[Normalna praca + archiwizacja]
  E -- tak --> G[Środki łagodzące: ograniczenie obciążeń, rekonfiguracja,
```

```
procedury]
  G --> H[Monitorowanie skutków i weryfikacja stabilności]
  H --> C
```

# Aspekty etyczne, prawne i polityczne oraz rekomendacje

## Etyka i odpowiedzialność w kontekście ryzyka kaskadowego

W systemach krytycznych wiedza o kaskadach ma charakter dual-use: te same modele, które umożliwiają projektowanie odporności, mogą wspierać identyfikację punktów krytycznych. Z tego powodu standardem odpowiedzialnej praktyki jest: ograniczanie dystrybucji szczegółów operacyjnych, koncentracja na mechanizmach obrony i odporności, oraz zarządzanie ujawnianiem podatności (coordinated vulnerability disclosure). Niniejszy tekst utrzymuje ten reżim przez celowe pominięcie instruktażowych detali technicznych. [8]

## Ramy prawne i regulacyjne

Na poziomie UE dyrektywa NIS2 (2022/2555) ustanawia wymagania zarządzania ryzykiem cyberbezpieczeństwa i raportowania incydentów dla podmiotów kluczowych i ważnych, a dyrektywa CER (2022/2557) dotyczy odporności podmiotów krytycznych (w tym aspektów ryzyka i środków odporności). W kontekście ataków kaskadowych znaczenie ma to, że ramy te przesuwają ciężar na systemowe zarządzanie ryzykiem, raportowanie i uczenie się po incydentach (lessons learned) – czyli elementy redukujące prawdopodobieństwo wejścia systemu w reżim kaskadowy. [62]

W Polsce obowiązuje ustawa o krajowym systemie cyberbezpieczeństwa (tekst jednolity ogłoszony w 2024 r.), stanowiąca ramę organizacyjną dla zarządzania incydentami i rolami operatorów usług kluczowych. Dla kaskad krytyczne jest to, że mechanizmy raportowania i koordynacji mają skracać czas wykrycia i reakcji, co w modelach dynamicznych wpływa na obniżenie „reprodukcji" zdarzeń wtórnych. [63]

W energetyce północnoamerykańskiej ramy zgodności cyber dla sektora elektroenergetycznego są rozwijane m.in. przez North American Electric Reliability Corporation (NERC) [64] w postaci standardów CIP (Critical Infrastructure Protection). W warstwie przemysłowej szeroko cytowanym punktem odniesienia jest seria ISA/IEC 62443 dla bezpieczeństwa IACS, wspierająca projektowanie stref/konduktów i zarządzanie cyklem życia zabezpieczeń. [65]

## Kluczowe wnioski

1. Kaskady w infrastrukturze krytycznej są zjawiskami progowymi: ryzyko gwałtownie rośnie po przekroczeniu krytycznych marginesów (obciążenia, obserwowalność, stabilność), nawet jeśli wcześniej system wydaje się stabilny. [66]
2. Najgroźniejsze kaskady często wynikają z współzależności warstw (energia–komunikacja–sterowanie), gdzie awarie w jednej domenie inicjują wtórne awarie w innej. [67]
3. Blackout 2003 pokazuje, że utrata narzędzi sytuacyjnych i opóźniona diagnostyka mogą przekształcić sytuację „do opanowania" w kaskadę. [68]
4. Fukushima pokazuje, że kaskada może być zdominowana przez awarie wspólnej przyczyny i utratę infrastruktury pomocniczej, a nie przez pojedynczą „główną usterkę" reaktora. [69]
5. TRITON ilustruje przesunięcie zagrożeń na warstwę bezpieczeństwa (SIS), gdzie celem kaskady może być degradacja bariery ochronnej, a nie wyłącznie przerwa w działaniu. [12]

### Rekomendacje praktyczne dla operatorów infrastruktury krytycznej

- Utrzymywać **marginesy bezpieczeństwa** (termiczne, napięciowe, stabilnościowe) i traktować „praca blisko granic" jako stan podwyższonego ryzyka kaskady wymagający dodatkowego nadzoru. [70]
- Inwestować w **obserwowalność i synchronizację danych** (PMU/synchrofazory tam, gdzie właściwe) oraz w procedury zapewnienia jakości danych, bo błędna obserwowalność jest katalizatorem kaskad. [71]
- Projektować architekturę cyber–fizyczną zgodnie z zasadą **segregacji stref** (IT/OT/SIS), minimalizacji połączeń i „defense-in-depth" (szczególnie dla systemów bezpieczeństwa). [72]
- Regularnie prowadzić **symulacje i stress-testy** z uwzględnieniem niepewności i zdarzeń rzadkich (Monte Carlo), a wyniki przekładać na procedury operacyjne. [73]
- W energetyce jądrowej wzmacniać strategie **radzenia sobie z blackoutem stacyjnym** zgodnie z wymaganiami regulatora (coping analysis) i standardami projektowymi; w analizach uwzględniać współzależności z siecią zewnętrzną. [74]
- Budować dojrzałość organizacyjną zgodnie z ramami NIS2/CER (UE) i krajowymi (PL): raportowanie, analiza przyczyn źródłowych, uczenie się po incydentach, współpraca sektorowa. [75]

## Referencje

Poniżej ujęto źródła pierwotne i wysokiej wiarygodności (raporty urzędowe/standardy oraz recenzowane prace naukowe) wykorzystane w tekście.


- „A Simple Model of Global Cascades on Random Networks" (2002). [23]
- „Cascade-based attacks on complex networks" (model przeciążeniowy Motter–Lai; preprint arXiv). [76]
- „Catastrophic cascade of failures in interdependent networks" (modele sieci współzależnych; wersja PDF). [21]
- „The spread of epidemic disease on networks" (SIR na sieciach i mapowanie na perkolację; wersja PDF). [77]
- Analizy krytyczności w modelach blackoutów sieci przesyłowych (CASCADE/OPA). [61]
- „Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations" (raport oficjalny). [78]
- Raport NAIIC (Fukushima Nuclear Accident Independent Investigation Commission) – wersja angielska. [43]
- TEPCO: „Fukushima Nuclear Accident Analysis Report" (2012) oraz streszczenie. [79]
- IAEA: SSR-2/1 (Rev.1) „Safety of Nuclear Power Plants: Design". [54]
- IAEA: „Preparedness and response for a nuclear or radiological emergency" (GSR Part 7 – wymagania). [55]
- NRC: 10 CFR §50.63 (Loss of all alternating current power). [80]
- NRC: 10 CFR §73.54 (Protection of digital computer and communication systems and networks). [56]
- NRC: Regulatory Guide 5.71 (Cyber Security Programs for Nuclear Power Reactors – rev.). [57]
- IAEA Nuclear Security Series: „Computer Security at Nuclear Facilities" i materiały powiązane. [81]
- FBI/IC3: „TRITON Malware Remains Threat to Global Critical Infrastructure Industrial Control Systems (ICS)" (2022). [47]
- CERT-EU: „New TRITON attack" (memo, 2019). [82]
- ABB: „Cyber Security Notification – TRITON/TRISIS malware" (2017). [83]
- „Inside the Slammer Worm" (analiza propagacji robaka; 2003). [84]

- INL CyOTE: „SQL Slammer Worm Infection of Davis-Besse Nuclear Power Plant 2003 – Precursor Analysis” (analiza przypadku). [85]
- DC power flow – notatki dydaktyczne (równania i interpretacja). [86]
- Stabilność systemów elektroenergetycznych – podręcznik P. Kundur (PDF) i kompendium KTH (równanie wahadłowe i definicje stabilności). [87]
- Synchrofazory i standardy transmisji danych – przegląd IEEE C37.118.2 oraz materiały o C37.118.1. [88]
- Dyrektywa NIS2 (UE 2022/2555) – wersja polska w Dzienniku Urzędowym UE / zasoby EUR-Lex. [89]
- Dyrektywa CER (UE 2022/2557) – wersja polska. [90]
- ENISA: Technical Implementation Guidance (2025) – praktyczne wskazówki wdrożeniowe NIS2 (wybrane sektory). [91]
- Polska: tekst jednolity ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024 poz. 1077). [92]
- NERC: indeks standardów CIP (Critical Infrastructure Protection). [93]
- ISA: opis serii standardów ISA/IEC 62443 dla IACS. [94]

---


[1] [5] [7] [13] [22] [23] [66] https://www.stat.berkeley.edu/~aldous/260-FMIE/Papers/watts.pdf
https://www.stat.berkeley.edu/~aldous/260-FMIE/Papers/watts.pdf

[2] [65] [93] https://www.nerc.com/standards/reliability-standards/cip
https://www.nerc.com/standards/reliability-standards/cip

[3] [4] [10] [18] [19] [31] [36] [37] [39] [40] [41] [68] [70] [78] https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf
https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

[6] [21] [27] [67] https://pdodds.w3.uvm.edu/files/papers/others/2010/buldyrev2010a.pdf
https://pdodds.w3.uvm.edu/files/papers/others/2010/buldyrev2010a.pdf

[8] [12] [47] [48] https://www.ic3.gov/CSA/2022/220325.pdf
https://www.ic3.gov/CSA/2022/220325.pdf

[9] [14] [20] [24] https://piccardi.faculty.polimi.it/VarieCsr/Papers/Motter2002.pdf
https://piccardi.faculty.polimi.it/VarieCsr/Papers/Motter2002.pdf

[11] [84] https://skerry-tech.com/papers/2003-slammer.pdf
https://skerry-tech.com/papers/2003-slammer.pdf

[15] [16] [25] [26] [77] https://www.cs.unibo.it/babaoglu/courses/cas02-03/papers/Spread-of-Epidemics.pdf
https://www.cs.unibo.it/babaoglu/courses/cas02-03/papers/Spread-of-Epidemics.pdf

[17] [30] [34] https://sgp.fas.org/othergov/doe/lanl/lib-www/la-pubs/00350385.html
https://sgp.fas.org/othergov/doe/lanl/lib-www/la-pubs/00350385.html

[28] [32] [33] [35] [42] [86] https://home.engineering.iastate.edu/~jdm/ee553/dcpowerflowequations.pdf
https://home.engineering.iastate.edu/~jdm/ee553/dcpowerflowequations.pdf

[29] [51] [87] https://web.nit.ac.ir/~shahabi.m/M.Sc%20and%20PhD%20materials/Power%20System%20Dynamics%201%20Course/Books/Power%20System%20Stability%20and%20Control%20by%20P.%20Kundur/Power%20System%20Stability%20and%20Control_kundur_Vol1.pdf
https://web.nit.ac.ir/~shahabi.m/M.Sc%20and%20PhD%20materials/Power%20System%20Dynamics%201%20Course/Books/Power%20System%20Stability%20and%20Control%20by%20P.%20Kundur/Power%20System%20Stability%20and%20Control_kundur_Vol1.pdf

38 58 81 https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf
https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf

43 69 https://www.nirs.org/wp-content/uploads/fukushima/naiic_report.pdf
https://www.nirs.org/wp-content/uploads/fukushima/naiic_report.pdf

44 https://www.tepco.co.jp/en/press/corp-com/release/betu12_e/images/120620e0103.pdf
https://www.tepco.co.jp/en/press/corp-com/release/betu12_e/images/120620e0103.pdf

45 54 https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1715web-46541668.pdf
https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1715web-46541668.pdf

46 56 https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054
https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054

49 85 https://cyote.inl.gov/content/uploads/24/2025/12/CyOTE-Case-Study_Davis-Besse-SQL-Slammer.pdf
https://cyote.inl.gov/content/uploads/24/2025/12/CyOTE-Case-Study_Davis-Besse-SQL-Slammer.pdf

50 52 74 80 https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0063
https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0063

53 90 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022L2557
https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022L2557

55 https://www-pub.iaea.org/MTCD/Publications/PDF/P_1708_web.pdf
https://www-pub.iaea.org/MTCD/Publications/PDF/P_1708_web.pdf

57 https://www.nrc.gov/docs/ML2225/ML22258A204.pdf
https://www.nrc.gov/docs/ML2225/ML22258A204.pdf

59 71 88 https://kezunovic.engr.tamu.edu/wp-content/uploads/sites/282/2023/04/An_Overview_of_the_IEEE_Standard_C37.118.2Synchrophasor_Data_Transfer_for_Power_Systems.pdf
https://kezunovic.engr.tamu.edu/wp-content/uploads/sites/282/2023/04/An_Overview_of_the_IEEE_Standard_C37.118.2Synchrophasor_Data_Transfer_for_Power_Systems.pdf

60 73 https://mcnp.lanl.gov/pdf_files/TechReport_2021_LANL_LA-UR-21-26274_ForsterRisingEtAl.pdf
https://mcnp.lanl.gov/pdf_files/TechReport_2021_LANL_LA-UR-21-26274_ForsterRisingEtAl.pdf

61 https://research.ece.cmu.edu/cascadingfailures/Criticality-nedicPSCC05.pdf
https://research.ece.cmu.edu/cascadingfailures/Criticality-nedicPSCC05.pdf

62 75 89 https://publications.europa.eu/resource/celex/32022L2555.POL
https://publications.europa.eu/resource/celex/32022L2555.POL

63 92 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20240001077
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20240001077

64 91 https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance
https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

72 94 https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

76 https://arxiv.org/abs/cond-mat/0301086
https://arxiv.org/abs/cond-mat/0301086

79 https://www.tepco.co.jp/en/press/corp-com/release/betu12_e/images/120620e0104.pdf
https://www.tepco.co.jp/en/press/corp-com/release/betu12_e/images/120620e0104.pdf

82 https://cert.europa.eu/publications/threat-intelligence/new-triton-attack/pdf
https://cert.europa.eu/publications/threat-intelligence/new-triton-attack/pdf

83 https://library.e.abb.com/public/f4de78ee1ee141d3bdbab669cd3d627a/9AKK107045A7931%20Cyber%20Security%20Notification%20TRITON%20generic.pdf
https://library.e.abb.com/public/f4de78ee1ee141d3bdbab669cd3d627a/9AKK107045A7931%20Cyber%20Security%20Notification%20TRITON%20generic.pdf