Ocena skuteczności systemów ochrony cyberfizycznej z uwzględnieniem degradacji elektronicznych systemów zabezpieczeń

Jan Kapusta, Waldemar Bauer, Jerzy Baranowski
AGH Akademia Górniczo-Hutnicza, Katedra Automatyki i Robotyki, Al. Mickiewicza 30, 30-059 Kraków

Streszczenie: W artykule zaproponowano stochastyczny model degradacji Elektronicznych Systemów Bezpieczeństwa w ramach Cyberfizycznych Systemów Ochrony. Model ma na celu zilustrowanie, jak na efektywność CPPS wpływają trzy główne grupy czynników: procesy starzenia się komponentów, kumulacja wiedzy i umiejętności adwersarzy oraz postęp technologiczny narzędzi atakujących, a także losowe zdarzenia związane z pojawianiem się nowych podatności i okresowe działania konserwacyjne. Każdy z tych elementów opisany został za pomocą odpowiedniego rozkładu – normalnego, logarytmicznego lub Bernoulliego – stanowiąc uproszczony, lecz reprezentatywny zestaw procesów degradacyjnych i regeneracyjnych. System efektywności SEi w miesiącu i definiowany jest jako max(100 – X_i, 0), gdzie X_i to skumulowane spadki i podniesienia efektywności. Dzięki symulacjom Monte Carlo (na zbiorze hipotetycznych danych i uproszczonych założeniach) pokazano ogólny kształt krzywej degradacji: system utrzymuje wysoką sprawność w pierwszych latach, po czym następuje przyspieszone obniżenie efektywności, z okresowymi, niewielkimi odbiciami związanymi z konserwacją. Modelowy przykład ilustruje, że klasyczne podejście EASI, nieuwzgledniające degradacji, znacząco przecenia odporność CPPS w długim horyzoncie czasowym. W rezultacie proponujemy uwzględnianie wskaźnika SEi w ocenie ryzyka oraz adaptacyjne harmonogramy utrzymania, które lepiej odpowiadają rzeczywistym procesom zużycia i zmian zagrożeń. Model ten, choć oparty na hipotetycznych założeniach, stanowi punkt wyjścia do dalszej kalibracji na rzeczywistych danych oraz do opracowania dynamicznych polityk modernizacji i konserwacji.

Słowa kluczowe: Elektroniczne Systemy Bezpieczeństwa, Cyberfizyczne Systemy Ochrony, model stochastyczny, degradacja systemów, efektywność operacyjna, symulacje Monte Carlo, adaptacyjna konserwacja, model EASI

1. Wprowadzenie

Ochrona infrastruktury krytycznej to jeden z istotnych elementów bezpieczeństwa narodowego. Cyberfizyczne Systemy Ochrony CPPS (ang. *Cyber-Physical Protection Systems*) obejmują zestaw środków technicznych i informatycznych, architektonicznych, organizacyjnych i prawnych oraz usług ochrony osobowej, mających na celu zabezpieczenie zasobów organizacji przed zamierzonymi i przypadkowymi działaniami o negatywnym wpływie na stabilność organizacji, a w określonych okolicznościach na bezpieczeństwo państwa. W pracy skoncentrowano się na technicznych komponentach CPPS, zwanych Elektronicznymi Systemami Bezpieczeństwa ESS (ang. *Electronic Security Systems*). Budżety przeznaczone na zabezpieczenia stanowią istotne pozycje kosztowe, dlatego stosuje się metodyki i narzędzia oceny skuteczności PPS (ang. *Physical Protection Systems*), które w optymalnym przypadku dostarczają informacji o realnej efektywności systemów. W przeciwnym wypadku zarządzanie jest nieefektywne i może prowadzić do niegospodarności, a nawet do sytuacji, w której PPS może nie zrealizować celów przed nimi stawianymi. Natomiast brak realizacji zadań PPS może prowadzić do poważnych konsekwencji.

Od wprowadzenia metodologii EASI (ang. *Estimated Adversary Sequence Interruption*) autorstwa Bennetta [1], model ten stał się punktem wyjścia dla licznych modyfikacji i rozszerzeń. Clem i Atkins [2] przeanalizowali scenariusze ataków fizyczno-cyfrowych, wskazując na potrzebę integracji ocen ryzyka cybernetycznego z metodami ochrony fizycznej. Porter [3] zbadał

Autor korespondujący:
Waldemar Bauer, bauer@agh.edu.pl

Artykuł recenzowany
nadesłany 05.06.2025 r., przyjęty do druku 16.09.2025 r.

rolę komponentu cyberbezpieczeństwa w ramach PPS, pokazując, jak zabezpieczenia sieciowe wpływają na odporność systemu. Depoy i wsp. [4] opracowali kompleksowe podejście do oceny ryzyka ataków łączących elementy fizyczne i cybernetyczne, uzupełniając klasyczne podejście EASI. Snell i Rivers [5] skupili się na atakach mieszanych (ang. *blended attacks*), demonstrując, jak uwzględnić ich specyfikę w ocenie skuteczności zabezpieczeń nuklearnych. Guo i wsp. [6] wykorzystali technikę cyfrowego bliźniaka do analizy ryzyka cybernetycznego w PPS elektrowni jądrowych, tworząc dedykowaną platformę testową. Bowen i wsp. [7] zaproponowali zintegrowaną platformę do analizy i projektowania PPS, umożliwiając kompleksową ocenę efektywności systemu w warunkach operacyjnych. Równolegle Ji i wsp. [8] rozszerzyli metodę EASI o analizę wielościeżkową z uwzględnieniem zmienności parametrów przy użyciu symulacji Monte Carlo. Kapusta i wsp. [9] ocenili cyberodporność PPS, wprowadzając heurystyczne algorytmy poprawy odporności systemów. O ile m.in. z tego powodu byliśmy w stanie sformalizować termin Cyberfizycznych Systemów bezpieczeństwa, który wydawał się niezbędny do opracowania podstaw modelu degradacji ww. systemów, o tyle, mimo tych zróżnicowanych propozycji, w literaturze nadal brakuje modelu uwzgledniającego rzeczywistą degradację PPS/CPPS w czasie ich eksploatacji.

Degradację PPS/CPPS definiujemy jako negatywne zmiany w skuteczności elementów, wynikające z eksploatacji (np. obniżanie parametrów wraz z wiekiem) oraz zmian środowiskowych (np. pojawienie się nowych narzędzi ataku). Jako ilustrację problemu można przytoczyć przykład ochrony banków, gdzie ryzyko napadu znacząco spadło, a wzrosło ryzyko ataków na bankomaty (ATM), gdzie historycznie dominowały ataki fizyczne (kradzież kluczy, wiercenie, kradzież kaset z pieniędzmi). Natomiast współcześnie, z uwagi na wyższy poziom wiedzy i świadomości ryzyka u przeciwnika, w obszarze fizycznym dominują ataki z użyciem środków wybuchowych (przeważnie gaz ziemny) oraz ataki cyberfizyczne, co znacząco zwiększyło ryzyko i koszty zabezpieczeń, które należy dostosować do zmiany trendu w materializacji ryzyk.

Przegląd badań z zakresu inżynierii elektronicznej wskazał dwie główne grupy prac:

Analiza starzenia się elementów elektronicznych była tematem wielu prac:

- dogłębna analiza struktury i mechanizmów degradacji kondensatorów elektrolitycznych, z wykorzystaniem charakterystyk materiałowych [10],
- badania symulacyjnie wpływu gorących nośników (ang. *hot carrier*) na wydajność konwerterów DC–DC, identyfikujące główne czynniki prowadzące do degradacji, [11]
- opracowany model niezawodności i wydajności konwertera Boost, określający, w jaki sposób zużycie komponentów wpływa na spadek parametrów [12],
- zaproponowany model degradacji pasywnych elementów w długoterminowej analizie emisji elektromagnetycznej, ze szczególnym uwzględnieniem wpływu starzenia się materiałów [13],
- przedstawiona metoda monitorowania punktu przegięcia charakterystyki VCE w IGBT, umożliwiająca wczesne wykrywanie degradacji przewodów [14],
- opisany szybki model strat dla tranzystorów GaN-FET oraz metoda kontroli wrażliwa na degradację transformatorów półprzewodnikowych [15].

Modele prognozowania degradacji:

- zaproponowana metoda estymacji pozostałego czasu życia systemów o dużych fluktuacjach degradacji [16],
- zastosowana statystyczna funkcja kopula (ang. *copula*) do analizy niezawodności systemów ze współzależnymi awariami [17],
- przegląd podstaw uczenia przez wzmacnianie oraz ich zastosowań w optymalizacji decyzji dla systemów degradacyjnych [18],
- omówione podejście wykorzystujące uczenie przez wzmacnianie do optymalizacji wydajności systemów ze sprzężeniem zwrotnym [19],
- zastosowana metoda cyfrowego bliźniaka do estymacji wskaźników zdrowia konwerterów DC–DC [20],
- połączenie cyfrowego bliźniaka z optymalizacją Bayesowską do identyfikacji parametrów degradacji przetwornic [21],
- diagnostyka usterek z użyciem głębokich zespołów sieciowych i wykrywania danych poza rozkładem [22],
- opracowany system monitorowania degradacji przetwornic mocy w czasie rzeczywistym za pomocą sieci neuronowej [23],
- zaproponowane ramy diagnostyczne oparte na nadzorowanym uczeniu dla systemów SMPS-AEC [24].

Żaden z tych modeli nie odnosi się bezpośrednio do degradacji ESS w kontekście CPPS. Opinie ekspertów dotyczące żywotności ESS wahają się od 5 do ponad 10 lat, a decyzje o wymianie zależą od dostępnego budżetu w zestawieniu z wartością księgową systemu. Brak dynamicznego, opartego na danych podejścia utrudnia efektywne zarządzanie cyklem życia CPPS.

W reakcji na tę lukę proponujemy probabilistyczny model degradacji CPPS, uwzgledniający zarówno zużycie komponentów, jak i ewolucję zagrożeń i technologii. Niniejsza praca wprowadza następujące nowe elementy w zakresie modelowania i oceny efektywności omawianych w niej systemów:

- **Dynamiczna metryka efektywności** SE_i, która pozwala na kwantyfikację stanu systemu ochronnego w każdym miesiącu eksploatacji, uwzględniając skumulowany wpływ pięciu zmiennych zdefiniowanych zmiennych probabilistycznych. Obejmują one kolejno: starzenie się komponentów, wzrost poziomu wiedzy przeciwnika, postęp technologiczny narzędzi atakujących, pojawianie się nowych podatności oraz kwartalne usprawnienia systemów — wszystkie parametryzowane na podstawie literatury i eksperckich rekomendacji.
- **Integracja z klasyczną metodyką EASI**, umożliwiającą rozszerzenie oszacowań prawdopodobieństwa przerwania ataku o degradację systemu w czasie, co prowadzi do bardziej zachowawczych i realistycznych decyzji o konserwacji i wymianie sprzętu.
- **Realizacja symulacji Monte Carlo** z $N = 10\ 000$ przebiegów, gwarantujących stabilność estymat średniej efektywności i odchyleń standardowych oraz pozwalających na analizę wrażliwości na poszczególne czynniki.
- **Studium przypadku** demonstrujące praktyczne zastosowanie modelu: przypisanie różnych „wieków" do warstw/elementów ochrony oraz porównanie klasycznej i zmodyfikowanej oceny EASI, a następnie wykazanie różnic w wynikach oceny w różnym wieku eksploatacji.
- **Propozycja podstawy do opracowania lub modyfikacji polityk modernizacji**, opartych nie tylko na amortyzacji finansowej, lecz także na analizie operacyjnej skuteczności.
- **Propozycja adaptacyjnych harmonogramów konserwacji i modernizacji**, opartych na zebranych wynikach, które umożliwiają precyzyjniejsze planowanie interwencji serwisowych i optymalizację budżetu.
- **Propozycja otwartej implementacji**, która pozwoli na dalszą kalibrację modelu na bazie rzeczywistych danych operacyjnych oraz rozwój nowych scenariuszy badawczych.

W dalszej części artykułu kolejno omówiono:

- w Sekcji 2. założenia i metodykę modelu, środowisko obliczeniowe oraz parametry probabilistyczne,

— w Sekcji 3. implementację wraz ze studium przypadku,
— w Sekcji 4. prezentujemy wyniki i dyskusję,
— w Sekcji 5. wskazujemy kierunki dalszych badań i formułujemy wnioski.

2. Metodologia

A. Kluczowe komponenty i dobór parametrów

W wyniku analizy współczesnego środowiska bezpieczeństwa, obejmującego dynamicznie zmieniające się zagrożenia technologiczne, wzrost kompetencji adwersarzy oraz praktyki utrzymania działania systemów, zidentyfikowano następujące kluczowe czynniki wpływające na efektywność Cyberfizycznych Systemów Ochrony (CPPS), które jednocześnie wykazują istotną zmienność w czasie i generują niepewność w ocenie stanu systemu:
— starzenie się komponentów,
— wzrost poziomu wiedzy i umiejętności przeciwnika,
— tempo postępu technologicznego w narzędziach atakujących,
— pojawianie się nowych krytycznych podatności w systemach komputerowych,
— regularne działania konserwacyjne i usprawnienia.

Wartości parametrów zostały dobrane arbitralnie w oparciu o ramy czasowe sugerowane przez ekspertów (5–10 lat cyklu życia ESS). Należy podkreślić, że przyjęte wartości stanowią punkt wyjścia do symulacji i mogą zostać zmodyfikowane na podstawie przyszłych badań oraz danych operacyjnych dotyczących poszczególnych elementów modelu. Jednocześnie przy doborze parametrów posiłkowano się również wynikami:
— eksperymentach przyspieszonego starzenia elektroniki [10],
— analizie tempa przyrostu wiedzy i narzędzi atakujących [4, 8],
— raportach branżowych nt. wdrażania usprawnień w przemyśle obronnym [6].

B. Ogólna formuła modelu

Efektywność systemu w miesiącu i definiujemy jako:

$$SE_i = \max(100 - X_i, 0),$$
$$X_i = \sum_{j=1}^{i} (AG_j + KG_j + TI_j + VI_j - IE_j). \quad (1)$$

gdzie:
SE_i efektywność CPPS w miesiącu i, wyrażona w procentach;
X_i skumulowany spadek efektywności do miesiąca i (punkty procentowe);
AG_j wpływ starzenia się komponentów w miesiącu j;
KG_j wpływ wzrostu poziomu wiedzy i umiejętności przeciwnika w miesiącu j;
TI_j wpływ postępu technologicznego narzędzi atakujących w miesiącu j;
VI_j wpływ pojawienia się nowych krytycznych podatności w miesiącu j;
IE_j efekt kwartalnych usprawnień (konserwacji) w miesiącu j, redukujący X_i.

Zastosowanie funkcji

$$\max()$$

w opracowanym modelu

$$SE_i = \max(100 - X_i, 0)$$

zapewnia, że efektywność systemu nigdy nie przyjmuje wartości ujemnych. Formalnie interpretujemy $SE_i = 0$ jako całkowitą utratę zdolności ochronnych CPPS, co odpowiada sytuacji, w której dalsza degradacja nie ma praktycznego znaczenia (system już jest nieskuteczny).

W przyjętym modelu zastosowaliśmy następujące rodzaje rozkładów do modelowania wpływu zdefiniowanych wcześniej zmiennych:
— **Rozkład normalny** dla AG_j i KG_j: Starzenie się komponentów oraz wzrost poziomu wiedzy adwersarzy są wynikiem sumy wielu niewielkich, niezależnych zdarzeń (mikrouszkodzeń lub zdobycia małych porcji informacji). Zgodnie z centralnym twierdzeniem granicznym naturalny jest wybór rozkładu normalnego, którego parametry (μ,σ) odzwierciedlają średni trend i zmienność tych procesów.
— **Model logarytmiczny** dla TI_j: Postęp technologiczny często przyspiesza na początku rozwoju narzędzi, a w miarę dojrzewania technologii kolejne usprawnienia dają coraz mniejsze przyrosty efektywności. Funkcja logarytmiczna odwzorowuje tę cechę „malejących przychodów" przy stałym wzroście nakładów na badania i rozwój.
— **Proces Bernoulliego** dla VI_j: Nowe, krytyczne podatności pojawiają się rzadko i losowo, ale ich konsekwencje są skokowe. Model Bernoulliego z parametrem p oddaje prawdopodobieństwo wystąpienia takiego zdarzenia w danym miesiącu, a jednorazowy „skok" spadku efektywności odpowiada jego wpływowi.
— **Rozkład normalny** dla IE_j: Kwartalne prace konserwacyjne składają się z wielu drobnych zadań (testy, wymiana części). Ich łączny efekt ma charakter sumaryczny, z naturalną zmiennością wynikającą z zakresu i jakości wykonanych prac, gdzie ponownie centralne twierdzenie graniczne wskazuje na rozkład normalny.

Pamiętając o estymowanym przez ekspertów na około 10–12 lat cyklu życia systemu, wspomaganym przez wyniki badań, przyjęto następujące wartości parametrów rozkładów:
— **Starzenie się komponentów** (AG_j): modelowane rozkładem normalnym ($\mu = 0{,}5$, $\sigma = 0{,}15$), co odzwierciedla średni spadek sprawności o około 50 % w dekadzie (rozrzut ±15 %) [10, 11].
— **Wzrost poziomu wiedzy przeciwnika** (KG_j): rozkład normalny ($\mu = 0{,}1$, $\sigma = 0{,}03$) – odpowiada około 10 % rocznemu przyrostowi skuteczności ataków dzięki lepszemu planowaniu i dostępowi do wiedzy [4].
— **Postęp technologiczny** (TI_j): model logarytmiczny ($\mu = 0{,}7$, $\sigma = 0{,}21$) – odzwierciedla przyspieszone tempo innowacji w narzędziach przeciwnika, gdzie kolejne usprawnienia przynoszą coraz mniejszy przyrost wydajności [6].
— **Wpływ podatności** (VI_j): proces Bernoulliego ($p = 0{,}2$ – prawdopodobieństwo sukcesu zdefiniowany jako jednorazowy spadek = 10 %) — reprezentuje pojawienie się nowych, krytycznych luk z historyczną częstością około 1 na 5 miesięcy [8].
— **Efekty kwartalnych usprawnień** (IE_j): rozkład normalny ($\mu = 0{,}5$, $\sigma = 0{,}15$) – modeluje prewencyjne działania konserwacyjne (testy, wymiana części) co 3 miesiące, redukujące skumulowany spadek efektywności o średnio 50 % z odchyleniem ±15 %.

Uzasadnienie wyboru rozkładów

Dobór rozkładów probabilistycznych dla poszczególnych zmiennych został oparty na charakterystyce procesów, które reprezentują, oraz na przesłankach literaturowych:
— **AG (starzenie komponentów)** — *rozkład normalny.* Starzenie jest efektem sumy wielu drobnych, w dużej mierze niezależnych mikro zjawisk (zużycie materiałów, dryf

parametrów), co uzasadnia wybór rozkładu normalnego. Por. wskazania literaturowe dotyczące degradacji elementów elektronicznych [10, 11].

- **KG (wzrost poziomu wiedzy przeciwnika)** – *rozkład normalny.* Akumulacja wiedzy i umiejętności następuje przyrostowo, z naturalną zmiennością w tempie i jakości pozyskiwanych danych, co uzasadnia wybór modelowania normalnego.
- **TI (postęp technologiczny narzędzi ataku)** – *model logarytmiczny.* W początkowych fazach rozwoju narzędzi obserwuje się szybkie przyrosty efektywności, które następnie maleją (ang. *diminishing returns*). Funkcja logarytmiczna dobrze oddaje tę dynamikę. Por. dyskusję i przykłady trendów technologicznych w kontekście PPS/CPPS [6].
- **VI (pojawianie się nowych krytycznych podatności)** – *proces Bernoulliego.* Zdarzenia rzadkie, skokowe, o trudnej do przewidzenia częstości w krótkich horyzontach (np. zero-day). W modelu ujmowane jako wystąpienie/brak zdarzenia w danym miesiącu. Por. podejścia do zmienności scenariuszy i ryzyka [4, 8].
- **IE (efekt kwartalnych usprawnień/konserwacji)** – *rozkład normalny.* Łączny efekt wielu czynności serwisowych (testy, wymiany, strojenie), z naturalną zmiennością zakresu i jakości prac — uzasadnia to modelowanie sumarycznego efektu rozkładem normalnym.

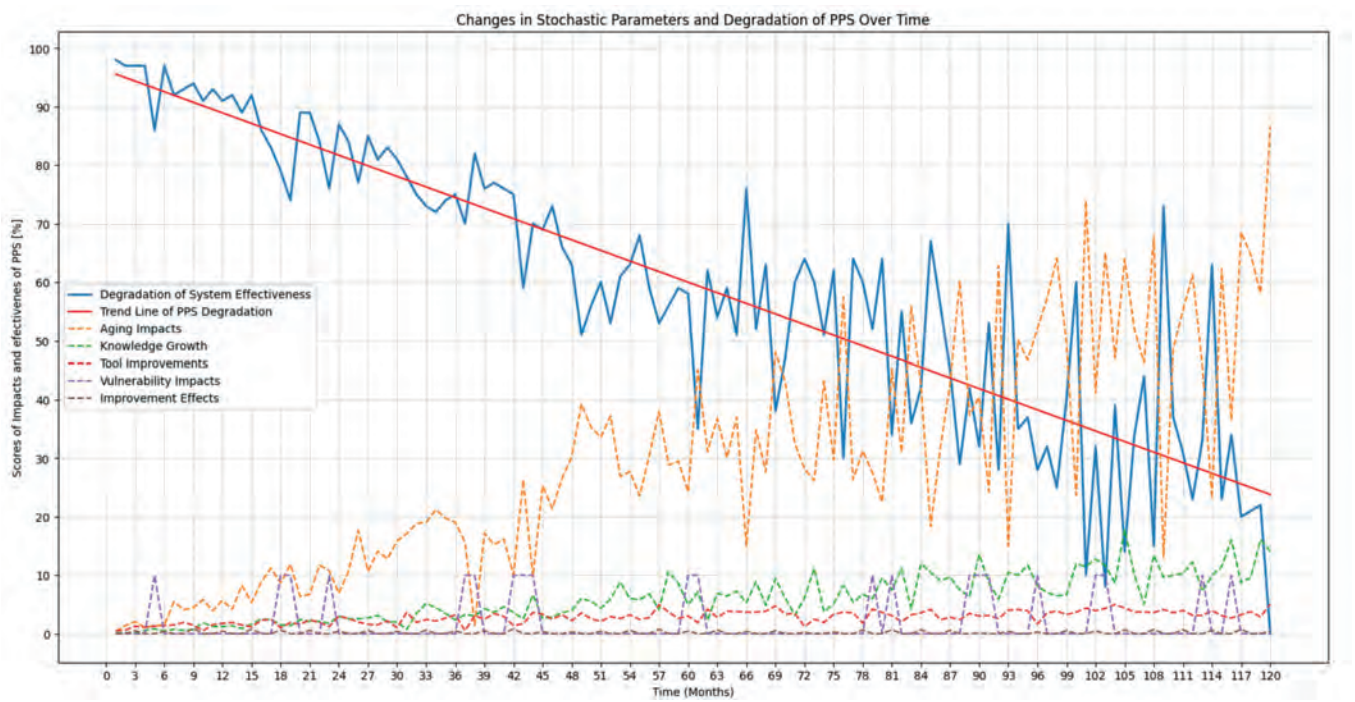
Powyższe wybory wpisują się w ogólny paradygmat, gdzie rozkłady sumy drobnych oddziaływań (AG, KG, IE) opisujemy przy użyciu rozkładu normalnego, proces który można opisać jako rzadko występujące lub nie(VI) — rozkładem Bernoulliego, a TI odwzorowujemy rozkładem logarytmicznym.

C. Środowisko obliczeniowe

Model został zaimplementowany w języku Python, co umożliwiło wykorzystanie nowoczesnych bibliotek do obliczeń numerycznych i wizualizacji wyników. W szczególności:

- numpy – podstawowa biblioteka do przechowywania i realizowania wektoryzowanych obliczeń na wielowymiarowych tablicach danych, zapewniająca wydajność zbliżoną do kodu C/C++.
- scipy.stats – moduł do statystycznego modelowania rozkładów prawdopodobieństwa; stosowany do generowania próbek z rozkładów normalnego, Bernoulliego oraz obliczania funkcji gęstości i dystrybuant.
- matplotlib – biblioteka do tworzenia wizualizacji: wykresów liniowych przebiegów degradacji, histogramów rozkładów parametrów oraz linii trendu; umożliwia eksport do formatów PDF, PNG i SVG.
- Liczba powtórzeń Monte Carlo (N) – w realizowanych symulacjach przyjęto $N = 10\,000$ niezależnych przebiegów. Taka liczba gwarantuje, że oszacowania średniej efektywności i odchyleń standardowych są stabilne, przy akceptowalnym czasie obliczeń. Zgodnie z prawem wielkich liczb błąd standardowy estymowanej średniej maleje w tempie $1/\sqrt{N}$, co dla $N = 10\,000$ skutkuje rzędem wielkości około 1 %, dając wiarygodne wyniki.

Na początku każdej symulacji zostało ustawione ziarno losowości (ang. *seed*), dzięki czemu sekwencja liczb pseudolosowych jest powtarzalna, co jest niezbędne do rzetelnej walidacji modelu oraz porównywania różnych scenariuszy testowych.



Rys. 1. Miesięczna ewolucja efektywności CPPS (niebieska linia) w ciągu dziesięciu lat (120 miesięcy) z linią trendu (czerwona), wskazującą spadek z 96 % do 25 %. Kolorowe linie przerywane przedstawiają składowe probabilistyczne: wpływ starzenia (pomarańczowa), wzrost poziomu wiedzy adwersarzy (zielona), postęp narzędzi atakujących (różowa), skokowe podatności (fioletowa) oraz kwartalne usprawnienia (brązowa). Starzenie i kumulacja wiedzy dominują długoterminową degradację, podatności generują nagłe spadki, a działania konserwacyjne dają jedynie krótkotrwałe odbicia

Fig. 1. Monthly evolution of CPPS effectiveness (blue) over a ten-year (120-month) horizon, with a linear trend line (red) illustrating the overall decline from about 96 % to 25 %. The colored dashed lines show the individual stochastic contributions: aging impacts (orange), adversary knowledge growth (green), tool improvements (pink), vulnerability impacts (purple) and quarterly improvement effects (brown). Note how aging and knowledge growth drive the long-term downward trend, vulnerability spikes cause sudden drops, and maintenance interventions yield only minor temporary recoveries

Przy tak zdefiniowanych parametrach symulacji graficznej jej reprezentację można zobaczyć na wykresie, który pokazuje, jak kolejne czynniki degradacji wpływają na osłabienie skuteczności działania systemu, reprezentowaną przez liniowo opadającą czerwoną linię trendu (Rys. 1.)

3. Przykład użycia

Aby zilustrować zastosowanie opracowanego modelu degradacji CPPS, rozważono typową ścieżkę ataku na obiekt chroniony, którego charakterystyka składa się z czterech kolejnych warstw ochronnych:

- Ochrona obwodowa – sensometryczny przewód światłowodowy monitorujący linię ogrodzenia,
- Nadzór wizyjny – kamery CCTV nadzorujące obszar chroniony,
- Kontrola dostępu – czytniki transponderów RFID oraz czujniki otwarcia (kontaktrony),
- System Sygnalizacji Włamania – pasywne czujki podczerwieni (PIR) wykrywające ruch wewnątrz obiektu.
- Każdemu z tych elementów przypisano przykładowy „wiek":
- przewód sensometryczny – 2 lata,
- kamery CCTV – 7 lat,
- czujniki otwarcia drzwi – 5 lat,
- czujki PIR – 10 lat.

W oparciu o zaproponowany model obliczono dla każdego elementu wartość efektywności SE_i odpowiadającą aktualnemu wiekowi urządzenia. Następnie wykonano dwie oceny efektywności systemu CPPS atak wybraną wcześniej ścieżką.

A. Ocena klasyczna (EASI bez degradacji)

W klasycznym podejściu EASI założono nominalne prawdopodobieństwa detekcji (PD_i) i transmisji alarmu (PC_i) bez uwzględniania upływu czasu ani degradacji. Kumulatywne prawdopodobieństwo przerwania ataku $P_{(I)}$ wyliczane jest według równania:

$$P_{(I)} = (P_{DT_i}) * (P_{C_i}) * (P_{(R|A_1)}) + \sum_{i=2}^{n} \left[(P_{(R|A_i)}) * (P_{C_i}) * (P_{DT_i}) * \prod_{j=1}^{i-1} \left(1 - (P_{DT_j})\right) \right] \quad (2)$$

gdzie: P_{DT_i} – prawdopodobieństwo detekcji podczas i akcji przeciwnika między warstwami zabezpieczenia; P_{C_i} – prawdopodobieństwo skutecznej komunikacji z siłami reagowania; $P_{(R|A_i)}$ – warunkowe prawdopodobieństwo skutecznej odpowiedzi sił reagowania zanim adwersarz osiągnie swój cel i jest równe $P(X > 0)$, gdzie X oznacza pozostały czas do ukończenia ataku (TR) pomniejszonego o pozostały czas do skutecznej reakcji sił reagowania (RTF) (Rys. 2).

B. Ocena z uwzględnieniem degradacji

W zmodyfikowanej ocenie każdy nominalny współczynnik detekcji PD_i został przemnożony przez SE_i, czyli efektywność danej warstwy, wynikającą z jej wieku i stopnia degradacji. Dzięki temu prawdopodobieństwo przerwania ataku maleje wraz ze starzeniem się elementów ochronnych (Rys. 3).

Na podstawie porównania obu ocen widać, że uwzględnienie degradacji obniża szacunki skuteczności CPPS o dodatkowe 15–25 punktów procentowych już po pięciu latach eksploatacji. Jest to istotna wskazówka dla praktyków, sugerująca potrzebę częstszej wymiany lub modernizacji kluczowych komponentów ochronnych.

4. Wyniki i dyskusja

Wykresy na Rys. 1 wskazują, że efektywność systemu (niebieska linia) obniża się z około 98 % na początku symulacji do około 25 % po 120 miesiącach. Czerwona linia trendu pokazuje niemal liniowy spadek z 98 % do 25 % w ciągu dziesięciu lat.

Response Relaybility	Mean time of response (sec.)	Force Time standard dev. (sec.)
0,95	250	90

Task #:	Adversary task description	Pd (probability of detection)	Detection Location (B/M/E)	mean delay	sdev	Normal values	cum Pi
1	cut fence	90%	B	90	3	0,950385092	0,8125793
2	run	90%	B	12	3,6	0,784149763	0,0670448
3	open a door	90%	B	90	27	0,749086947	0,0064047
4	run	90%	B	10	3	0,421259148	0,0003602
5	open a door	90%	B	100	27	0,382797242	3,273E-05
6	sabotage of the asset	90%	B	120	36	0,089938638	7,69E-07
7		0%	0	0	0	0,002736602	0
8		0%	0	0	0	0,002736602	0
9		0%	0	0	0	0,002736602	0
10		0%	0	0	0	0,002736602	0
11		0%	0	0	0	0,002736602	0
12		0%	0	0	0	0,002736602	0
						Probability of interuption (Physical attack)	0,8864

Rys. 2. Zrzut ekranu arkusza EASI w Excelu przedstawiającego ocenę skuteczności CPPS na hipotetycznej ścieżce przeciwnika bez uwzględnienia czynnika degradacji skuteczności. Prawdopodobieństwo przerwania ścieżki ataku przez siły reagowania wynosi ≈ 88,64 %

Fig. 2. A screenshot of the EASI Excel tool showing the evaluation of CPPS effectiveness on a hypothetical adversary path, without incorporating the degradation-based effectiveness factor. The result indicates ≈ 88.64 % probability of interrupting the adversary sequence

Response Relaybility	Mean time of response (sec.)	Force Time standard dev. (sec.)
0,95	250	90

Task #:	Adversary task description	Detection Element/s	Age of system	Mean of estimated efectivenes from degradation model	Probability of detection on the installation day	Pd (probability of detection on the day of evaluation)	Detection Location (B/M/E)	mean delay	sdev	Normal values	cum Pi
1	cut fence	Fiber-optic sensor	3	70%	90%	63%	B	90	3	0,950385092	0,5688055
2	run	CCTV camera	7	30%	90%	27%	B	12	3,6	0,784149763	0,0744197
3	open a door	Door contact	5	50%	90%	45%	B	90	27	0,749086947	0,0864954
4	run	PIR Detector	8	20%	90%	18%	B	10	3	0,421259148	0,0107012
5	open a door	Door contact	5	50%	90%	45%	B	100	27	0,382797242	0,0199345
6	sabotage of the asset	CCTV camera	7	30%	90%	27%	B	120	36	0,089938638	0,0015456
7						0%	0	0	0	0,002736602	0
8						0%	0	0	0	0,002736602	0
9						0%	0	0	0	0,002736602	0
10						0%	0	0	0	0,002736602	0
11						0%	0	0	0	0,002736602	0
12						0%	0	0	0	0,002736602	0
										Probability of interuption (Physical attack)	0,7619

Rys. 3. Zrzut ekranu arkusza EASI w Excelu przedstawiającego ocenę skuteczności CPPS na hipotetycznej ścieżce przeciwnika z uwzględnieniem czynnika degradacji skuteczności. W tym scenariuszu wynik wskazuje na spadek skuteczności systemu o 12,45 % z około 88,64 % do około 76,19 % prawdopodobieństwa przerwania ataku adwersarza

Fig. 3. A screenshot of the EASI Excel tool showing the evaluation of CPPS effectiveness on a hypothetical adversary path, incorporating the degradation-based effectiveness factor. In this scenario, the result indicates a 12.45 % decrease in system effectiveness, from approximately 88.64 % to about 76.19 % probability of interrupting the adversary sequence

A. Moment przekroczenia 50 %

Chociaż pojedyncze realizacje modelu (niebieska linia) czasem schodzą poniżej 50 % już po 60 miesiącach, średnia tendencja (linia trendu) wskazuje, że poziom 50 % zostaje przekroczony dopiero około 75–80 miesiąca (6,5–6,7 roku). Oznacza to, że w rozważanym scenariuszu typowy cykl wymiany CPPS krótszy niż 7 lat byłby uzasadniony, jeżeli chcemy utrzymać skuteczność powyżej połowy wartości nominalnej.

B. Dominujące czynniki degradacji

Analiza poszczególnych składników X_i (pomarańczowa, zielona, fioletowa, magenta i brązowa linia) pokazuje wyraźne, nierówne udziały:

- Starzenie się (AG_j, pomarańczowa) rośnie liniowo od 0 do około 60–80 % w dekadzie i stanowi największy udział w skumulowanym spadku.
- Wzrost poziomu wiedzy przeciwnika (KG_j, zielona) narasta stopniowo od 0 do około 10–15 % w ciągu dziesięciu lat.
- Udoskonalanie narzędzi (TI_j, fioletowa) przyspiesza w drugiej połowie okresu i zbliża się do około 8–10 %.
- Podatności (VI_j, magenta) dają sporadyczne skoki spadku do 5–10 %, ale są rzadkie (średnio jeden na pięć miesięcy).
- Efekty konserwacji (IE_j, brązowa) pojawiają się kwartalnie i mają niewielką wartość – rzędu 1–2 % regeneracji na cykl, co jest niewystarczające, by skompensować skumulowane straty.

C. Porównanie klasycznej i zmodyfikowanej EASI

Dane na rysunkach 2 i 3 dowodzą, że uwzględnienie SE_i w metodzie EASI obniża estymowane prawdopodobieństwo przerwania ataku o dodatkowe 15–25 % już w piątym roku użytkowania. W klasycznym podejściu (bez degradacji) CPPS wygląda na relatywnie znacznie bardziej odporne, co może prowadzić do błędnych decyzji, w tym o zbyt rzadkiej wymianie sprzętu.

D. Implikacje praktyczne

W świetle otrzymanych wyników słuszne wydaje się rozważenie uwzględnienia działań zaradczych:

- wprowadzenie ciągłego monitorowania efektywności i predykcji degradacji,
- adaptacyjne harmonogramy konserwacji, które uwzględniają rzeczywiste tempo zużycia i zmienność zagrożeń.

E. Ograniczenia i dalsze prace

Prezentowany model wymaga kalibracji na danych z rzeczywistych instalacji CPPS, zwłaszcza w odniesieniu do kwartalnych efektów konserwacji i częstotliwości występowania krytycznych podatności. Dopiero wówczas będzie możliwe opracowanie precyzyjnych, ekonomicznie zoptymalizowanych harmonogramów konserwacji i wymiany komponentów.

5. Podsumowanie i perspektywy dalszych badań

W pracy zaproponowano kompleksowy, probabilistyczny model degradacji Cyberfizycznych Systemów Ochrony, który łączy w sobie pięć kluczowych czynników — starzenie się komponentów, wzrost poziomu wiedzy przeciwnika, postęp technologiczny narzędzi atakujących, pojawianie się nowych podatności oraz prewencyjne działania konserwacyjne. Przeprowadzone symulacje wykazały, że w analizowanym hipotetycznym scenariuszu efektywność CPPS spada poniżej 50 % w horyzoncie 6,5–7 lat, co sugeruje konieczność rewizji standardowych, dziesięcioletnich cykli wymiany sprzętu i wdrożenia bardziej elastycznych harmonogramów odnowy systemów. Analiza wrażliwości pokazała, że to właśnie starzenie się komponentów oraz sporadyczne, ale gwałtowne skoki związane z wykrywaniem nowych podatności generują największe ryzyko długoterminowej nieskuteczności ochrony, podczas gdy kwartalne przeglądy zapewniają jedynie krótkotrwałe i niewystarczające ożywienie efektywności.

Obecny model bazuje na założeniu o niezależności zmiennych degradacyjnych (AG, KG, TI, VI, IE), co jest świadomym uproszczeniem, wprowadzonym ze względu na brak danych i badań z zakresu zależności między parametrami oraz ich naturą. W rzeczywistości zależności te mogą być istotne — przykładowo, szybki postęp technologiczny narzędzi ataku (TI) może przyspieszać wzrost wiedzy przeciwnika (KG), a równoczesna intensyfikacja TI i KG może zwiększać prawdopodobieństwo ujawnienia nowych podatności (VI). W przyszłych badaniach planowane jest rozszerzenie modelu o odwzorowanie takich relacji z wykorzystaniem statystycznej funkcji kopula (ang. *statistical copula*), która umożliwia definiowanie rozkładów brzegowych poszczególnych zmiennych niezależnie od struktury ich współzależności, umożliwiając uchwycenie nieliniowych oraz asymetrycznych zależności, a także efektów skrajnych (ang. *tail dependence*). Rozważane są m.in. kopule typu Gumbela (nacisk na zależności w górnych ogonach rozkładów), Claytona (w dolnych ogonach) oraz Franka (symetryczne zależności), co pozwoli lepiej odwzorować zachowanie systemu w warunkach dynamicznych [25, 26].

Integracja wskaźnika efektywności SE_i z klasycznym modelem EASI umożliwiła uzyskanie bardziej realistycznych i konserwatywnych estymat prawdopodobieństwa przerwania ataku, obniżając je o dodatkowe 15–25 % już po pięciu latach eksploatacji. Taka modyfikacja wydaje się być istotna z punktu widzenia planowania budżetowego i zabezpieczenia ciągłości działań ochronnych.

W obecnej wersji modelu działania konserwacyjne (IE_j) zostały ujęte jako przegląd kwartalny schematycznych przeglądów technicznych o stałej skuteczności. W rzeczywistości intensywność, zakres i moment przeprowadzenia konserwacji mogą być silnie zróżnicowane w zależności od kontekstu operacyjnego, charakterystyki obiektu oraz dostępnych zasobów. W kolejnych etapach planowane jest wprowadzenie elastycznego modelu konserwacji, w którym harmonogram i skuteczność interwencji będą modelowane jako zmienne losowe o rozkładach dopasowanych empirycznie na podstawie danych eksploatacyjnych. Rozwiązanie to pozwoli odwzorować scenariusze od reaktywnej konserwacji awaryjnej po prewencyjne działania predykcyjne, a także umożliwi analizę koszt–efektywność dla różnych strategii utrzymaniowych.

Jako naturalną kontynuację tych badań proponujemy cztery główne obszary rozwoju. Po pierwsze, w zakresie innowacji technologicznych warto zbadać wykorzystanie algorytmów sztucznej inteligencji i uczenia maszynowego do predykcji krytycznych momentów degradacji, a także eksperymenty z technologią blockchain dla zapewnienia niezmienności i audytowalności danych pomiarowych. Integracja czujników IoT nowej generacji, takich jak urządzenia akustyczne czy termowizyjne, pozwoli natomiast na wczesne wykrywanie oznak zużycia.

Po drugie, rekomendujemy opracowanie dynamicznych polityk i regulacji, które na bieżąco aktualizują wymagania techniczne CPPS w oparciu o wskaźniki degradacji i ryzyka. Zasadnym wydaje się również rozważenie współpracy międzynarodowej nad ujednoliceniem progów efektywności i cykli zżycia systemów ochrony oraz analizę wpływu lokalnych norm. Tego rodzaju podejście mogłoby wzmocnić spójność praktyk utrzymania i modernizacji.

Po trzecie, zasadne jest pogłębienie badań nad strategiami organizacyjnymi. Wdrożenie kultury proaktywnej konserwacji wymaga zarówno szkoleń technicznych dla personelu, jak i wsparcia ze strony kadry zarządzającej, a także analiz międzysektorowych, które wskażą najlepsze praktyki w branżach takich jak finanse, energetyka czy transport.

Wreszcie, kluczowe znaczenie wydają się mieć badania longitudinalne. Wieloletnie gromadzenie rzeczywistych danych eksploatacyjnych z instalacji CPPS, w tym pomiarów efektywności po każdej interwencji serwisowej, oraz połączenie ich z analizą ekonomiczną kosztów konserwacji, modernizacji i ryzyka awarii. Taka baza danych umożliwi precyzyjną kalibrację modelu w różnych warunkach środowiskowych (temperatura, wilgotność, natężenie ruchu) i pozwoli na regionalizację zaleceń dotyczących utrzymania.

Podsumowując, zaproponowany model stanowi solidną podstawę do przejścia od statycznych harmonogramów wymiany narzędzi ochronnych do dynamicznych, opartych na danych i analizie ryzyka procesów utrzymaniowych. Kolejnym krokiem będzie implementacja prototypu w rzeczywistych systemach CPPS, walidacja jego predykcji wobec danych operacyjnych oraz rozszerzenie o aspekty cyberbezpieczeństwa i zaawansowanej sensoryki IoT, co znacząco wzmocni odporność infrastruktury krytycznej na coraz bardziej złożone i zmienne zagrożenia.

Bibliografia

1. Bennett H.A., *EASI approach to physical security evaluation*, United States, Tech. Rep. SAND–76-0500, 1977.
2. Clem J., Atkins W.D., Urias V., *Investigation of cyber--enabled physical attack scenarios*, Sandia National Lab. (SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2015.
3. Porter S., *Physical protection systems and the cyber security component*, no. llnl-conf-674448, Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States), Tech. Rep., 2015.
4. Depoy J., Phelan J., Sholander P., Smith B., Varnado G., Wyss G., *Risk assessment for physical and cyber attacks on critical infrastructures*, [In:] MILCOM 2005 – 2005 IEEE Military Communications Conference, IEEE, 2005, DOI: 10.1109/MILCOM.2005.1605959.
5. Snell M.K., Rivers J., *The treatment of blended attacks in nuclear security effectiveness assessments*, Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2015.
6. Guo Y., Yan A., Wang J., *Cyber security risk analysis of physical protection systems of nuclear power plants and research on the cyber security test platform using digital twin technology*, [In:] 2021 International Conference on Power System Technology (POWERCON), IEEE, 2021, DOI: 10.1109/POWERCON53785.2021.9697764.
7. Bowen Z., Ming Y., Hidekazu Y., Hongxing L., *Evaluation of physical protection systems using an integrated platform for analysis and design*, "IEEE Transactions on Systems, Man, and Cybernetics: Systems", Vol. 47, No. 11, 2017, 2945–2955, DOI: 10.1109/TSMC.2016.2531995.
8. Andiwijayakusuma D., Setiadipura T., Purqon A., Su'ud Z., *The development of EASi-based multi-path analysis code for nuclear security system with variability extension*, "Nuclear Engineering and Technology", Vol. 54, No. 10, 2022, 3604–3613, DOI: 10.1016/j.net.2022.05.023.
9. Kapusta J., Bauer W., Baranowski J., *Evaluation of the effectiveness of physical protection systems with consideration of its cyber-resilience*, [In:] 2023 27th International Conference on Methods and Models in Automation and Robotics (MMAR), 2023, 457–461, DOI: 10.1109/MMAR58394.2023.10242420.
10. Narale S.B., Verma A., Anand S., *Structure and degradation of aluminum electrolytic capacitors*, [In:] 2019 National Power Electronics Conference, NPEC 2019, DOI: 10.1109/NPEC47332.2019.9034726.
11. Yu C., Jiang L., Yuan J., *Study of performance degradations in DC–DC converter due to hot carrier stress by simulation*, Microelectronics Reliability, Vol. 46, No. 9–11, 2006, 1840–1843, DOI: 10.1016/j.microrel.2006.07.079.
12. Alam M.K., Khan F.H., *Reliability analysis and performance degradation of a boost converter*, [In:] 2013 IEEE

Energy Conversion Congress and Exposition, ECCE 2013, 5592–5597, DOI: 10.1109/ECCE.2013.6647461.
13. Huang H., Boyer A., Dhia S.B., *Analysis and modeling of passive device degradation for a long-term electromagnetic emission study of a DC-DC converter*, "Microelectronics Reliability", Vol. 55, No. 9–10, 2015, 2061–2066, DOI: 10.1016/j.microrel.2015.06.058.
14. Singh A., Anurag A., Anand S., *Evaluation of Vce at inflection point for monitoring bond wire degradation in discrete packaged IGBTs*, "IEEE Transactions on Power Electronics", Vol. 32, No. 4, 2017, 2481–2484, DOI: 10.1109/TPEL.2016.2621757.
15. Haque M.S., Moniruzzaman M., Choi S., Kwak S., Okilly A.H., Baek J., *A fast loss model for cascode GaN-FETs and real-time degradation-sensitive control of solid-state transformers*, "Sensors", Vol. 23, No. 9, 2023, DOI: 10.3390/s23094395.
16. Du D.-B., Zhang J.-X., Zhou Z.-J., Si X.-S., Hu C.-H., *Estimating remaining useful life for degrading systems with large fluctuations*, "Journal of Control Science and Engineering", 2018, DOI: 10.1155/2018/9182783.
17. Fang G., Pan R., Hong Y., *Copula-based reliability analysis of degrading systems with dependent failures*, "Reliability Engineering & System Safety", Vol. 193, 2020, DOI: 10.1016/j.ress.2019.106618.
18. Dong H., Ding Z., Zhang S., *Deep reinforcement learning: Fundamentals, research and applications*, Springer, 2020, DOI: 10.1007/978-981-15-4095-0.
19. Hua C., *Reinforcement Learning Aided Performance Optimization of Feedback Control Systems*, Springer, 2021, DOI: 10.1007/978-3-658-33034-7.
20. Peng Y., Zhao S., Wang H., *A digital twin based estimation method for health indicators of DC–DC converters*, "IEEE Transactions on Power Electronics", Vol. 36, No. 2, 2021, 2105–2118, DOI: 10.1109/TPEL.2020.3009600.
21. Chen S., Wang S., Wen P., Zhao S., *Digital twin for degradation parameters identification of DC–DC converters based on Bayesian optimization*, [In:] 2021 IEEE International Conference on Prognostics and Health Management, ICPHM 2021, 2021, DOI: 10.1109/ICPHM51084.2021.9486446.
22. Han T., Li Y.-F., *Out-of-distribution detection-assisted trustworthy machinery fault diagnosis approach with uncertainty-aware deep ensembles*, "Reliability Engineering and System Safety", Vol. 226, 2022, DOI: 10.1016/j.ress.2022.108648.
23. Fan J., Lee J., Jung I., Lee Y., *Online monitoring of power converter degradation using deep neural network*, "Applied Sciences", Vol. 11, No. 24, 2021, DOI: 10.3390/app112411796.
24. Kareem A.B., Hur J.-W., *Towards data-driven fault diagnostics framework for SMPS-AEC using supervised learning algorithms*, "Electronics", Vol. 11, No. 16, 2022, DOI: 10.3390/electronics11162492.
25. Nelsen R.B., *An Introduction to Copulas*, Springer, 2006, DOI: 10.1007/0-387-28678-0.
26. Fang G., Pan R., Hong Y., *Copula-based reliability analysis of degrading systems with dependent failures,* "Reliability Engineering & System Safety", Vol. 193, 2020, DOI: 10.1016/j.ress.2019.106618.

Evaluation of the Effectiveness of Cyber-Physical Protection Systems Considering the Degradation of Electronic Security Systems

Abstract: This paper introduces a stochastic degradation model for Electronic Security Systems (ESS) within Cyber-Physical Protection Systems (CPPS). The model demonstrates how CPPS effectiveness is influenced by three major groups of factors: component aging processes, accumulation of adversary knowledge and skills, and technological advancements in attack tools, along with random vulnerability events and periodic maintenance actions. Each factor is represented by an appropriate distribution such as normal, logarithmic, or Bernoulli, providing a simplified yet representative set of degradation and recovery processes. System effectiveness SEi in month i is defined as $\max(100 - X_i, 0)$, where X_i aggregates the cumulative declines and improvements. Monte Carlo simulations (using hypothetical data and assumptions) reveal a characteristic degradation curve: high initial performance followed by accelerated decline, punctuated by minor recoveries due to maintenance. A case study indicates that the traditional EASI approach, which neglects degradation, substantially overestimates CPPS resilience over long time horizons. Consequently, we advocate incorporating the SEi metric into risk assessments and adopting adaptive maintenance schedules better aligned with real-world wear and evolving threats. Although based on hypothetical parameters, this model provides a foundation for calibration with operational data and for developing dynamic modernization and upkeep policies.

Keywords: Electronic Security Systems, Cyber-Physical Protection Systems, stochastic degradation model, system effectiveness, Monte Carlo simulation, adaptive maintenance, EASI extension, operational resilience

mgr inż. Jan Kapusta

jkapusta@agh.edu.pl

ORCID: 0000-0003-4523-1227

Ma ponad 20-letnie doświadczenie zawodowe w obszarze bezpieczeństwa w sektorze prywatnym. Obecnie pełni funkcję Menedżera ds. Ryzyka i Bezpieczeństwa Operacyjnego dla regionu Europy Północnej, Centralnej i Wschodniej, w tym krajów Wspólnoty Niepodległych Państw (WNP) w globalnej korporacji IT. Był współzałożycielem i przewodniczącym Forum Bezpieczeństwa Fizycznego działającego przy Radzie ds. Bezpieczeństwa Związku Banków Polskich, a także reprezentował polski sektor bankowy w grupie roboczej ds. bezpieczeństwa w Europejskiej Federacji Bankowej. Ukończył studia z zakresu Bezpieczeństwa Systemów Komputerowych i Zarządzania Kryzysowego, a także posiada dyplom poziomu 6 IQ jako Certyfikowany Specjalista ds. Zarządzania Bezpieczeństwem, nadany przez International Security Management Institute. Jest wykładowcą przedmiotu Bezpieczeństwo Systemów Cyberfizycznych na Akademii Górniczo-Hutniczej oraz członkiem rady programowej i instruktorem w Centrum Szkoleniowym Polskiej Izby Systemów Alarmowych. Obecnie kończy studia doktoranckie.

dr inż. Waldemar Bauer

bauer@agh.edu.pl

ORCID: 0000-0002-8543-0995

Ukończył studia magisterskie na kierunku informatyka oraz uzyskał stopień doktora nauk technicznych w dziedzinie automatyki i robotyki na Akademii Górniczo-Hutniczej w Krakowie, odpowiednio w 2012 r. i 2020 r. Obecnie pracuje jako adiunkt w Katedrze Automatyki i Robotyki AGH w Krakowie. Jego zainteresowania badawcze obejmują analizę danych, uczenie maszynowe, optymalizację, cyfryzację procesów biznesowych, teorię sterowania, metody numeryczne oraz diagnostykę procesów.

prof. dr hab. inż. Jerzy Baranowski

jb@agh.edu.pl

ORCID: 0000-0003-3313-581X

Ukończył studia magisterskie, doktoranckie oraz habilitacyjne w dziedzinie automatyki i robotyki na Akademii Górniczo-Hutniczej w Krakowie w latach 2006, 2010 i 2017. W 2024 r. otrzymał tytuł profesora nadany przez Prezydenta RP. Obecnie pracuje jako profesor zwyczajny w Katedrze Automatyki i Robotyki AGH w Krakowie. Kieruje Laboratorium Informatyki w Zakładzie Sterowania i Zarządzania. Jest autorem ponad 200 publikacji, w tym książki, artykuły naukowe i referaty konferencyjne. Otrzymał stypendium dla najlepszych młodych naukowców oraz Medal Komisji Edukacji Narodowej przyznane przez Ministerstwo Nauki i Szkolnictwa Wyższego. Jego zainteresowania naukowe obejmują diagnostykę procesów, predykcyjne utrzymanie ruchu, systemy wspomagania decyzji, wnioskowanie statystyczne, teorię sterowania oraz efektywne metody obliczeniowe.