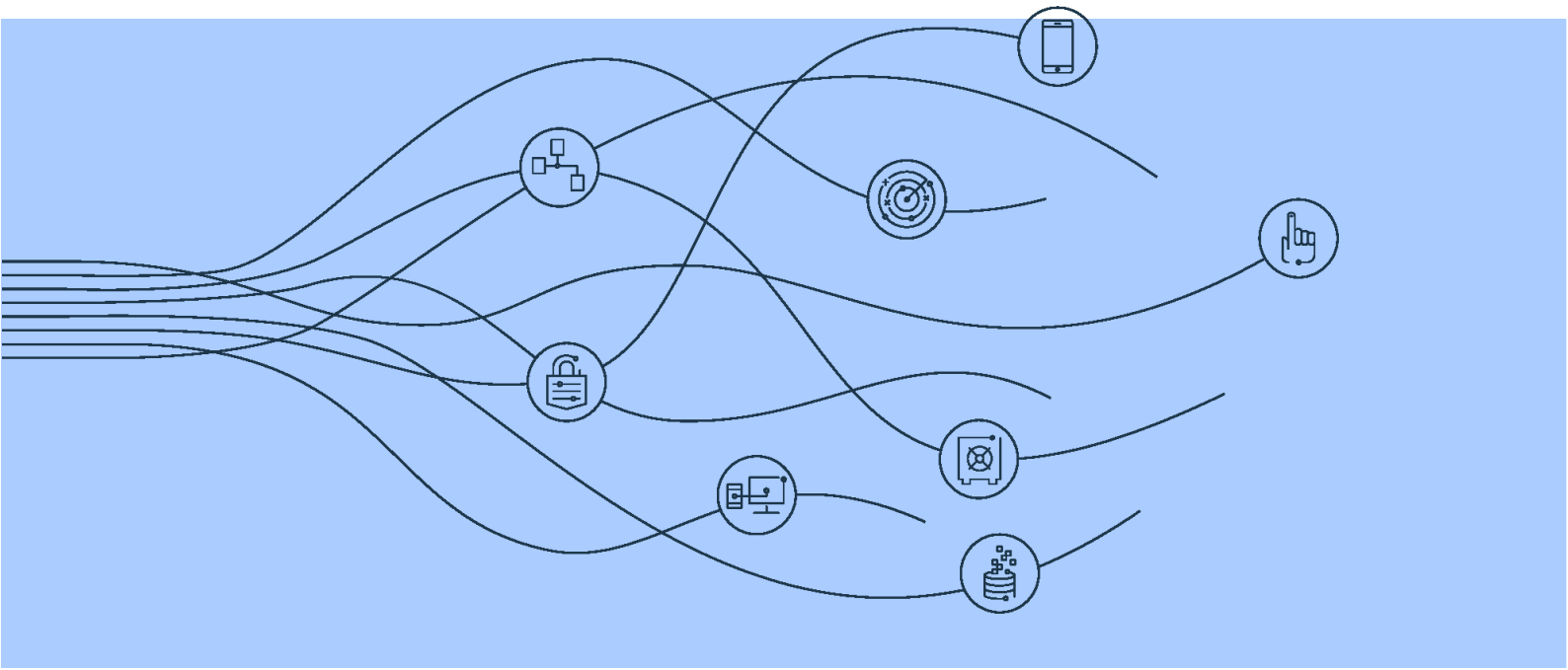
# Wzmacnianie Bezpieczeństwa Technologii Operacyjnych (OT)

## Przewodnik dla Operatorów Infrastruktury Krytycznej

Opracowano na podstawie:

IEC 62443 • NIST SP 800-82 • ENISA ICS • CISA

Styczeń 2026



## Spis treści

## 1. Inwentaryzacja Zasobów

"Nie możesz chronić tego, czego nie znasz" – to fundamentalna zasada bezpieczeństwa systemów OT[1]

Tylko dokładny rejestr zasobów OT umożliwia priorytetyzację podatności, wykrywanie nieautoryzowanych urządzeń i skuteczniejszą reakcję na incydenty.

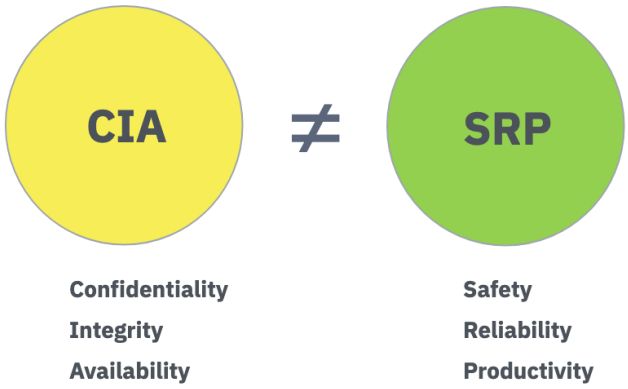
Kluczowe elementy inwentaryzacji:

- **Stacje operatorskie i HMI** – systemy operacyjne, użytkownicy.
- **Sterowniki PLC/RTU** – producent, model, wersja firmware, lokalizacja.
- **Systemy SCADA/DCS** – wersje oprogramowania, połączenia sieciowe.
- **Urządzenia polowe** – czujniki, siłowniki, przetworniki.
- **Infrastruktura sieciowa** – switche przemysłowe, routery, firewalle.

Cybersecurity and Infrastructure Security Agency (CISA) zaleca tworzenie taksonomii OT – systemu kategoryzacji uwzględniającego krytyczność (wpływ na bezpieczeństwo), ekspozycję (narażenie na zagrożenia) oraz dostępność (możliwość konserwacji).

## 2. Zrozumienie Ryzyka i Priorytetów

W środowiskach OT priorytety bezpieczeństwa fundamentalnie różnią się od priorytetów w obszarach IT. W IT kluczowa jest ochrona danych i triada CIA (Confidentiality, Integrity, Availability – Poufność, Integralność, Dostępność). W OT kluczowa jest zasada SRP (Safety-Reliability-Productivity), która definiuje hierarchię celów w środowiskach przemysłowych.




Rysunek 1. Porównanie priorytetów bezpieczeństwa w środowiskach IT (CIA) i OT (SRP)

[1] Rozwinięcia i objaśnienia skrótów stosowanych w publikacji znajdują się w Słowniku terminów OT/ICS

Dlaczego to rozróżnienie jest krytyczne?

W IT naruszenie poufności oznacza wyciek danych – poważny, ale zazwyczaj nie zagrażający życiu. W OT błędna konfiguracja lub atak na system sterowania może doprowadzić do wybuchu, wycieku substancji toksycznych lub wypadku śmiertelnego. Dlatego bezpieczeństwo fizyczne (Safety) zawsze musi być priorytetem nadrzędnym.

Kolejna różnica dotyczy dostępności. W IT krótka przerwa w działaniu systemu jest akceptowalna – użytkownicy poczekają kilka minut. W OT nawet kilkusekundowa przerwa w sterowaniu procesem chemicznym lub energetycznym może wywołać reakcję łańcuchową z katastrofalnymi skutkami. Stąd niezawodność (Reliability) zajmuje drugie miejsce w hierarchii SRP.

Produktywność (Productivity), choć ważna z perspektywy biznesowej, nigdy nie powinna być osiągana kosztem bezpieczeństwa lub niezawodności. Każda decyzja dotycząca zabezpieczeń OT musi być oceniana przez pryzmat tej hierarchii.

## 2.1. Zasada SRP – Fundament Bezpieczeństwa OT

PRIORYTET: Safety (Bezpieczeństwo) > Reliability (Niezawodność) > Productivity (Produktywność)

**Safety (Bezpieczeństwo fizyczne) – najwyższy priorytet:**

- Ochrona życia i zdrowia ludzi (pracowników, społeczności lokalnej).
- Zapobieganie katastrofom środowiskowym (wycieki, emisje).
- Utrzymanie integralności fizycznej instalacji i sprzętu.
- Systemy Safety Instrumented Systems (SIS) muszą pozostać nienaruszone.


Rysunek 2. Hierarchia priorytetów SRP w środowiskach OT

**Reliability (Niezawodność i dostępność) – drugi priorytet:**

- Ciągłość procesów produkcyjnych i operacyjnych.
- Stabilność systemów sterowania i automatyki.
- Minimalizacja przestojów nieplanowanych.
- W OT nawet krótka przerwa może kosztować miliony lub zagrażać życiu.

**Productivity (Produktywność) – trzeci priorytet:**

- Efektywność operacyjna i optymalizacja procesów.
- Jakość produktów i usług.
- Cele biznesowe i rentowność.

Zgodnie z IEC 62443-1-1 i NIST 800-82, każda decyzja dotycząca bezpieczeństwa OT musi być oceniana przez pryzmat SRP. Kontrola bezpieczeństwa, która mogłaby zakłócić działanie systemów bezpieczeństwa (SIS) lub spowodować nieplanowany przestój, musi być dokładnie przeanalizowana.

**Wykorzystuj matrycę „MITRE ATT&CK for ICS" do mapowania potencjalnych ataków i priorytetyzacji działań obronnych w kontekście zasady SRP.**

## 3. Monitoring Sieci, Zdarzeń i Zasobów

ZASADA: Gdy nie możesz natychmiast usunąć podatności w OT – zwiększ zdolności monitorowania i logowania.

### 3.1. Widoczność sieci ICS

**Pasywne monitorowanie ruchu:**

- Nasłuchiwanie ruchu sieciowego bez ingerencji w procesy przemysłowe.
- Analiza protokołów przemysłowych.
- Baseline zachowań – ustalenie wzorca normalnej komunikacji.
- Detekcja anomalii – automatyczne alerty przy odchyleniach od baseline.
- Deep Packet Inspection (DPI) dla protokołów OT.

Aktywne odpytywanie:

Według NIST 800-82 i najlepszych praktyk. aktywne odpytywanie jest kluczowym uzupełnieniem monitoringu pasywnego.

Czym różni się od skanowania IT:

- Wykorzystuje natywne protokoły.
- Odpytuje urządzenia w sposób zgodny z ich specyfikacją – bez ryzyka zakłóceń.
- Zbiera szczegółowe informacje o firmware, konfiguracji i stanie urządzeń.
- Nie generuje nadmiernego ruchu sieciowego ani obciążenia CPU sterowników.

Korzyści z aktywnego odpytywania:

- Pełna inwentaryzacja – wykrycie urządzeń niewidocznych w ruchu pasywnym.
- Identyfikacja wersji firmware i podatności CVE.
- Wykrycie zmian konfiguracji PLC/RTU w czasie rzeczywistym.
- Weryfikacja zgodności z baseline i politykami bezpieczeństwa.
- Detekcja nieautoryzowanych modyfikacji programów sterowników.

### 3.2. Centralizacja i korelacja logów

Wdróż centralizację logów w systemie SIEM z korelacją zdarzeń IT i OT oraz retencją zgodną z wymogami regulacyjnymi (NIS2, IEC 62443). Integruj dane z systemów DCS, Historian, HMI oraz urządzeń sieciowych dla pełnej widoczności.

## 4. Kontrola Dostępu i Segmentacja Sieci

Defensible Architecture opiera się na modelu Purdue – hierarchicznej segmentacji sieci OT, uznanej przez IEC 62443 i NIST 800-82 jako fundament bezpieczeństwa ICS.

### 4.1. Model Purdue – Architektura Referencyjna

| Poziom | Nazwa | Komponenty |
|---|---|---|
| L5 | Enterprise | Sieć korporacyjna, Internet, chmura |
| L4 | Business IT | ERP, email, aplikacje biznesowe |
| DMZ | IT/OT DMZ | Firewall, jump host, proxy, diody danych |
| L3 | Operations | MES, Historian, serwery SCADA |
| L2 | Supervisory | HMI, stacje operatorskie, inżynierskie |
| L1 | Control | PLC, RTU, sterowniki DCS, SIS |
| L0 | Process | Czujniki, siłowniki, procesy fizyczne |

### 4.2. Zasady segmentacji (IEC 62443-3-3)

- Zones and Conduits – definiuj strefy bezpieczeństwa i kontrolowane kanały komunikacji.
- Ruch tylko na zasadzie "need-to-communicate" – domyślnie blokuj, explicite zezwalaj.
- Firewalle ze świadomością protokołów OT.
- Diody danych dla jednokierunkowego przepływu (np. do Historian).
- Mikrosegmentacja krytycznych systemów (SIS, kontrolery safety).

### 4.3. Bezpieczny dostęp zdalny

Według statystyki, 65% środowisk OT nie ma bezpiecznych konfiguracji dostępu zdalnego. ENISA i CISA rekomendują:

- MFA (Multi-Factor Authentication) dla wszystkich połączeń zdalnych.
- Jump hosty / Bastion hosts zamiast bezpośredniego dostępu do OT.
- Nagrywanie i audyt wszystkich sesji zdalnych.

- Zasadę minimalnych uprawnień (least privilege).
- Czasowe ograniczenie sesji i automatyczne wylogowanie.
- Oddzielne konta dla dostępu zdalnego i lokalnego.

### 4.4. Zarządzanie tożsamością w OT

- Eliminacja współdzielonych kont operatorskich.
- Integracja z centralnym IdP, tam gdzie to możliwe (z zachowaniem SRP).
- Przeglądy uprawnień co najmniej kwartalnie.
- Natychmiastowe odbieranie dostępu przy zmianach kadrowych.

## 5. Wielowarstwowa Obrona (Defense-in-Depth)

Założenie: Każda pojedyncza warstwa może zostać przełamana. Siła obrony leży w ich kombinacji i wzajemnym wspieraniu się.

Żadne pojedyncze zabezpieczenie nie jest wystarczające. Zgodnie z IEC 62443 i NIST 800-82, skuteczna ochrona OT wymaga wielowarstwowego podejścia, gdzie każda warstwa niezależnie chroni przed zagrożeniami.

### 5.1. Dlaczego wielowarstwowość jest krytyczna

- Redundancja zabezpieczeń – awaria jednej warstwy nie oznacza kompromitacji całego systemu.
- Zwiększony koszt dla atakującego – musi pokonać wiele barier, co wymaga więcej czasu, zasobów i wiedzy.
- Większa szansa na detekcję – każda warstwa generuje logi i alerty; im więcej warstw, tym większa szansa wykrycia.
- Zgodność z regulacjami – NIS2, IEC 62443-3-3 i NIST wyraźnie wymagają Defense-in-Depth.


Rysunek 3. Model obrony warstwowej w OT

### 5.2. Warstwy ochrony i ich współdziałanie

| Warstwa | Mechanizmy ochrony |
|---|---|
| Fizyczna | Kontrola dostępu, CCTV, zabezpieczenia szaf sterowniczych, alarmy |
| Sieciowa | Firewalle OT, IDS/IPS przemysłowe, diody danych, mikrosegmentacja, VPN |
| Hostowa | Whitelisting aplikacji, hartowanie systemów, EDR, kontrola USB, antywirus |
| Aplikacyjna | Bezpieczna konfiguracja SCADA/HMI, uwierzytelnianie, autoryzacja, audyt |
| Proceduralna | Polityki, szkolenia, zarządzanie zmianą, kontrola dostawców |

### 5.3. Zarządzanie podatnościami

W środowiskach OT natychmiastowe łatanie luk często jest niemożliwe ze względu na wymagania dostępności i certyfikacje. Stosuj zabezpieczenia kompensacyjne:

- Wirtualne łatanie przez IPS z sygnaturami dla znanych CVE.
- Izolacja podatnych systemów w dedykowanych VLAN.
- Wzmocniony monitoring systemów bez możliwości aktualizacji.
- Planowanie okien serwisowych z wyprzedzeniem.
- Priorytetyzacja podatności według kontekstu OT i zasady SRP.

## 6. Procedury i Procesy OT

KLUCZOWE: Nawet najlepsze technologie są bezużyteczne bez odpowiednich procedur i przeszkolonego personelu.

### 6.1. ICS Incident Response Plan

Plan reakcji na incydenty musi uwzględniać unikalne aspekty środowisk OT:

- Role i odpowiedzialności – włącznie z zespołem operacyjnym i inżynierami procesu.
- Procedury izolacji – jak bezpiecznie odseparować systemy bez zakłócania procesów krytycznych.
- Przejście na sterowanie ręczne – procedury backup dla operacji bez automatyki.
- Odtwarzanie systemów – ze zweryfikowanych kopii zapasowych konfiguracji i programów.
- Komunikacja kryzysowa – wewnętrzna i z regulatorami (zgodnie z NIS2).

### 6.2. Zarządzanie zmianą (Change Management)

Według IEC 62443-2-4 i ENISA, każda zmiana w środowisku OT musi przejść formalny proces:

1. Dokumentowanie i uzasadnienie zmiany (kto, co, dlaczego).
2. Ocena wpływu na bezpieczeństwo, operacje i zgodność z SRP.
3. Zatwierdzenie przez upoważnione osoby (CAB – Change Advisory Board).
4. Testowanie w środowisku nieprodukcyjnym, gdy jest to możliwe.
5. Wdrożenie z możliwością natychmiastowego wycofania (rollback).
6. Weryfikacja, dokumentacja końcowa i aktualizacja baseline.

### 6.3. Zgodność ze standardami i regulacjami

Procedury OT muszą być zgodne z obowiązującymi standardami i regulacjami:

- IEC 62443 – kompleksowy standard cyberbezpieczeństwa OT (wymagany przez wielu regulatorów).
- NIST SP 800-82 – praktyczny przewodnik implementacji bezpieczeństwa ICS.
- NIS2/KSC – europejskie/polskie wymagania dla operatorów infrastruktury krytycznej.
- ISO 27001 – system zarządzania bezpieczeństwem informacji.
- Regulacje sektorowe – energetyka (NC ER), wodociągi, transport, przemysł chemiczny.

Regularne audyty wewnętrzne i zewnętrzne powinny weryfikować zgodność procedur z wymaganiami.

## 7. Ćwiczenia TTX i AEV

Tabletop Exercises (TTX) to symulowane ćwiczenia testujące procedury bez wpływu na rzeczywiste systemy.

Regularne testowanie procedur jest kluczowe dla utrzymania gotowości operacyjnej. Ćwiczenia powinny obejmować trzy komplementarne obszary:

### 7.1. Tabletop Exercises (TTX)

Tabletop Exercises stanowią pierwszy poziom walidacji w ramach podejścia **AEV (Adversarial Exposure Validation)**. Są to symulowane ćwiczenia dyskusyjne, które poprzedzają techniczne testy penetracyjne i automatyczne symulacje ataków.

**Cel TTX w modelu AEV:**

- Weryfikacja teoretycznej skuteczności mechanizmów detekcji i reakcji.

- Identyfikacja luk w procedurach przed uruchomieniem kosztownych symulacji technicznych.
- Mapowanie scenariuszy ataków do frameworka MITRE ATT&CK for ICS.
- Przygotowanie zespołów do pełnych ćwiczeń AEV z rzeczywistą emulacją przeciwnika.

Po zakończeniu TTX, zidentyfikowane hipotezy bezpieczeństwa powinny być walidowane technicznie poprzez kontrolowane symulacje AEV w środowisku testowym lub przy użyciu narzędzi do emulacji przeciwnika (np. AEV dostosowane do OT).

### 7.2. Ćwiczenia Incident Response (IR)

Praktyczne testy reagowania na incydenty w kontrolowanych warunkach:

- Symulowana detekcja złośliwego ruchu sieciowego – test SOC i zespołu OT.
- Ćwiczenia izolacji segmentów sieci bez zakłócania produkcji.
- Testy komunikacji kryzysowej między zespołami IT, OT i kierownictwem.
- Weryfikacja procedur eskalacji i powiadamiania regulatorów.
- Praktyczne przejście na sterowanie ręczne (gdy jest bezpieczne).

### 7.3. Ćwiczenia Disaster Recovery (DR)

Testy odtwarzania systemów i ciągłości działania:

- Odtwarzanie konfiguracji PLC/SCADA z kopii zapasowych.
- Przełączanie na systemy redundantne / zapasowe lokalizacje.
- Weryfikacja RTO (Recovery Time Objective) i RPO (Recovery Point Objective).
- Testy integralności kopii zapasowych programów sterowników.
- Symulacja utraty kluczowych systemów i procedury Fallback.

### 7.4. Podejście CTEM – Ciągłe doskonalenie

CTEM (Continuous Threat Exposure Management) – cykl identyfikacji, weryfikacji i eliminacji zagrożeń.

Po każdym ćwiczeniu TTX/IR/DR należy:

1. Udokumentować przebieg ćwiczenia i zidentyfikowane luki.
2. Ocenić reakcję zespołów Security i OT – czas, skuteczność, koordynacja.
3. Opracować plan naprawczy (remediation plan) dla zidentyfikowanych słabości.
4. Zaktualizować procedury i polityki na podstawie wniosków.
5. Przeprowadzić szkolenia uzupełniające dla personelu.

6. Zaplanować kolejne ćwiczenie weryfikujące wprowadzone zmiany.

Rekomendacje: TTX co najmniej raz na kwartał, pełne ćwiczenia IR/DR co najmniej raz na rok. Scenariusze powinny być aktualizowane o nowe zagrożenia identyfikowane przez CISA i MITRE ATT&CK for ICS.

## 8. Słownik Terminów OT/ICS

| Termin | Definicja |
|---|---|
| **AEV** | Adversarial Exposure Validation – walidacja ekspozycji na zagrożenia poprzez kontrolowaną emulację taktyk, technik i procedur (TTP) rzeczywistych przeciwników |
| **CTEM** | Continuous Threat Exposure Management – ciągłe zarządzanie ekspozycją na zagrożenia; cykliczny proces identyfikacji, priorytetyzacji i eliminacji podatności |
| **DCS** | Distributed Control System – rozproszony system sterowania |
| **DMZ** | Demilitarized Zone – strefa zdemilitaryzowana |
| **DR** | Disaster Recovery – odtwarzanie po awarii |
| **ENISA** | European Union Agency for Cybersecurity – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, odpowiedzialna za wytyczne i standardy bezpieczeństwa dla infrastruktury krytycznej |
| **HMI** | Human Machine Interface – interfejs człowiek-maszyna |
| **ICS** | Industrial Control Systems – przemysłowe systemy sterowania |
| **IdP** | Identity Provider – dostawca tożsamości, centralny system uwierzytelniania i zarządzania tożsamością użytkowników (np. Active Directory, Okta, Azure AD) |
| **IEC 62443** | Standard cyberbezpieczeństwa dla automatyki przemysłowej |
| **IR** | Incident Response – reagowanie na incydenty |
| **NIST 800-82** | Przewodnik NIST dot. bezpieczeństwa ICS |
| **OT** | Operational Technology – technologie operacyjne |
| **PLC** | Programmable Logic Controller – programowalny sterownik logiczny |

| Termin | Definicja |
|---|---|
| **RTU** | Remote Terminal Unit – zdalna jednostka terminalowa |
| **SCADA** | Supervisory Control and Data Acquisition – system nadzoru i akwizycji danych; służy do zdalnego monitorowania i sterowania procesami przemysłowymi |
| **SIS** | Safety Instrumented System – system bezpieczeństwa |
| **SRP** | Safety, Reliability, Productivity – bezpieczeństwo, niezawodność, produktywność; hierarchia priorytetów w środowiskach OT |
| **TTX** | Tabletop Exercise – ćwiczenie symulacyjne typu "dyskusja przy stole", testujące procedury reagowania na incydenty bez wpływu na rzeczywiste systemy |

## Źródła i referencje

- IEC 62443 Series – International Electrotechnical Commission
- NIST SP 800-82 Rev. 3 – Guide to Operational Technology Security
- ENISA – Good Practices for ICS and Critical Infrastructure
- CISA – Cross-Sector ICS Guidance & Advisories (cisa.gov)
- SANS ICS 5 Critical Controls & GIAC ICS Resources
- MITRE ATT&CK for ICS Framework

Dokument opracowany na podstawie wytycznych IEC 62443, NIST 800-82, ENISA, CISA oraz SANS Institute.