SEBOR'26

System Elektroenergetyczny: Bezpieczeństwo Operacyjne i Rynkowe

Analiza ryzyka cybernetycznego dla systemów automatyki w elektrowniach: identyfikacja słabych punktów i rekomendacje zabezpieczeń

Łukasz Czapla

ien Instytut Energetyki
Oddział Gdańsk

Kazimierz Dolny, 17–19 marca 2026 r.

Analiza ryzyka dla systemów elektrowni

Zagrożenie	Prawdopodobieństwo wystąpienia	Skutki (dla elektrowni)	Ryzyko	Środki zaradcze

Identyfikacja zagrożeń

Ryzyko = Prawdopodobieństwo * Skutki

Wskazanie Środków zaradczych

Cel: mitygacja ryzyka- zmniejszenie prawdopodobieństwa (likwidacja podatności) lub ograniczenie skutków.

Identyfikacja Zagrożeń

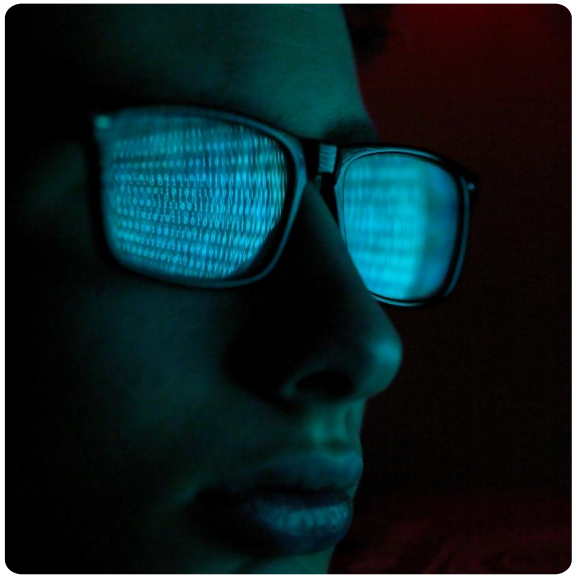
Awarie techniczne sprzętowe i zakłócenia

Starzenie się sprzętu, przepięcia, czynniki fizyczne.

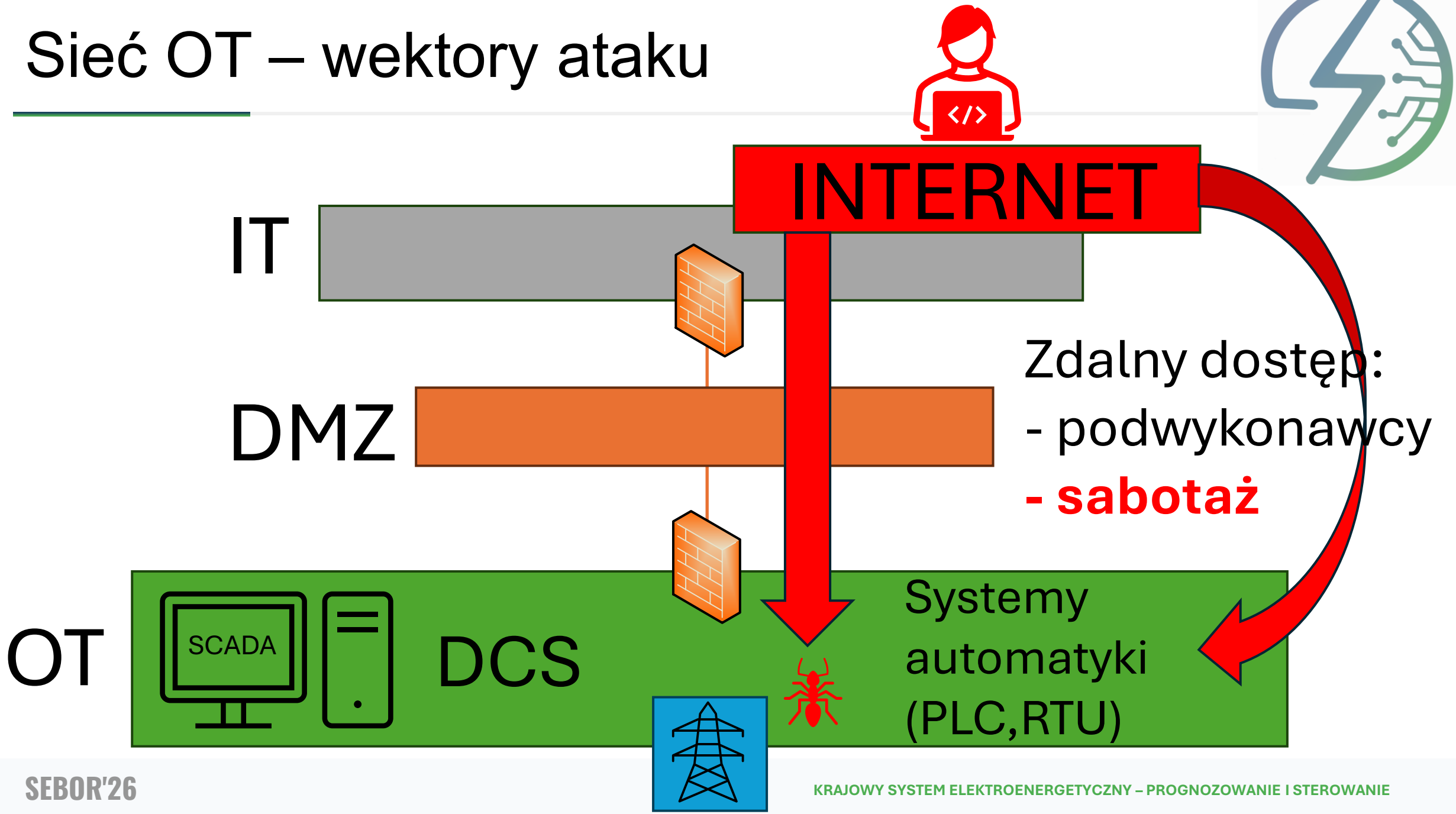
Najczęściej nośniki danych, zasilacze, urządzenia komunikacyjne i kable.

Przejęcie kontroli nad pracą bloków energetycznych (SCADA)

- wykorzystanie błędów w architekturze sieci i kontroli dostępu,
- wykorzystanie dostępu zdalnego,
- wykorzystanie podatności w systemach operacyjnych (brak poprawek),
- instalacja złośliwego oprogramowania (malware),
- eskalacja uprawnień i ataki „brute force”.

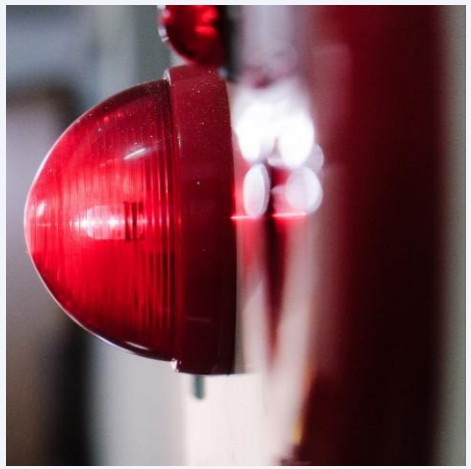


Sieć OT – wektory ataku



Przebieg ataku na sieć OT

- Terytorium zachodniej Ukrainy,
- 23 grudnia 2015 roku.
- Efekt: Połowa mieszkańców regionu, pozbawiona była energii elektrycznej.



- fałszywy **email**, zawierający plik Office **(marzec),**
- uruchomione zostały makra, co skutkowało zainfekowaniem komputera (**malware**),
- atakujący uzyskują **zdalny dostęp do SCADA**,
- **wyłączają ok. 30 wyłączników** w stacjach elektroenergetycznych **(grudzień)**
- następnie paraliżują całkowicie systemy zdalnego sterowania (min**. usuwają firmware** urządzeń komunikacyjnych).

Identyfikacja Zagrożeń cd…

Unieczynnienie systemu

– uszkodzenie lub zaszyfrowanie danych konfiguracyjnych (**ransomware**),
– uszkodzenie/usunięcie firmware urządzeń
– ataki DoS (przeciążenie lub zablokowanie elementów),

Uszkodzenie integralności danych (przesyłanych i przechowywanych)

– atak „**man-in-the-middle**”- wykorzystanie luk w protokołach,
– modyfikacja wartości zadanych/nastaw lub pomiarów.
– modyfikacja plików konfiguracyjnych urządzeń.

„Czynnik ludzki”

– atak socjotechniczne typu „phishing” (z wykorzystaniem algorytmów AI),
– ujawnianie informacji (analiza OSINT),
– atak fizyczny na infrastrukturę.

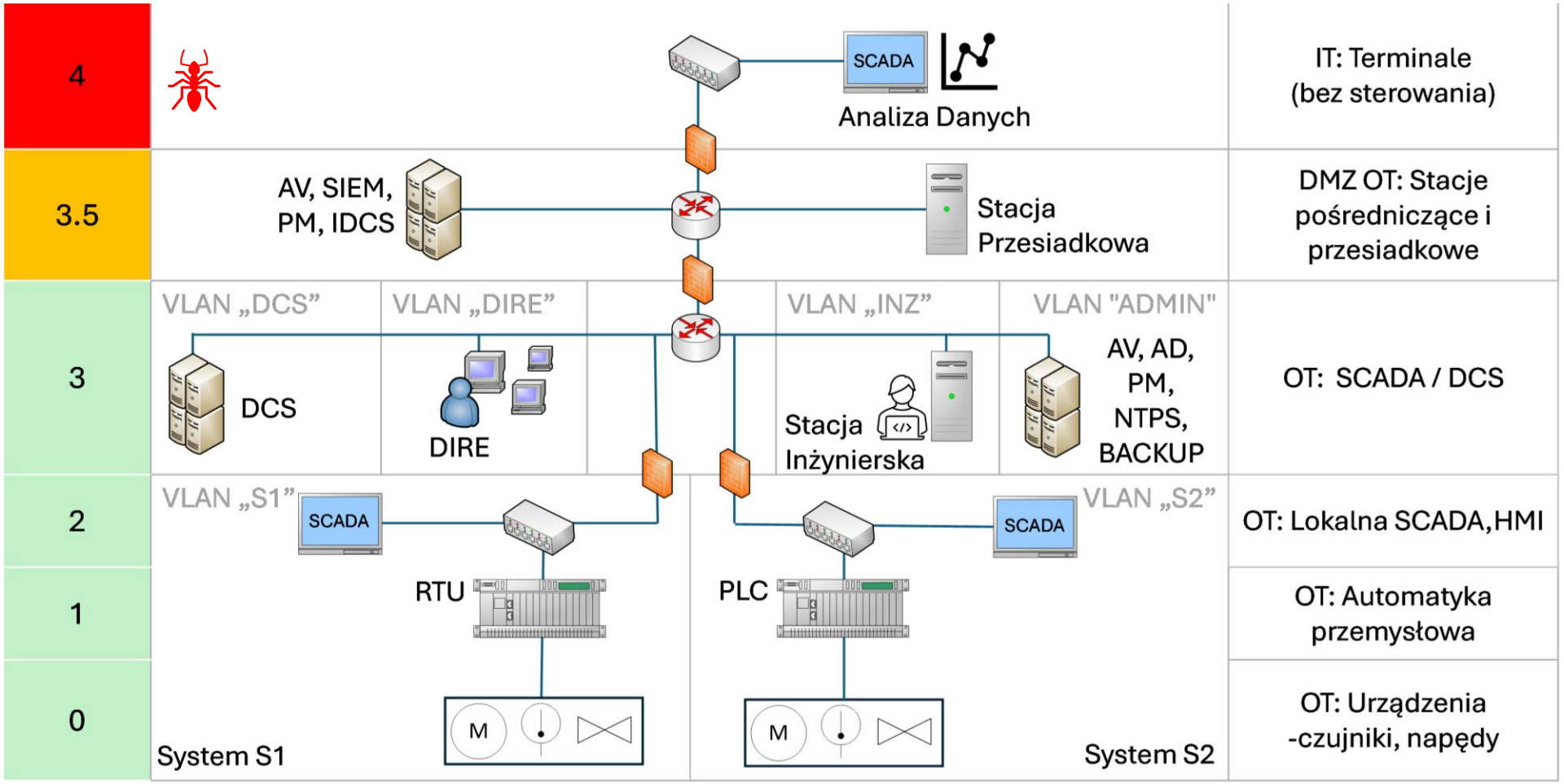
Wskazanie środków zaradczych - Seria norm IEC 62443

Wymagania podstawowe:

1. Kontrola identyfikacji i uwierzytelniania
2. Użycie kontroli
3. Integralność systemu
4. Poufność danych
5. Ograniczony przepływ
6. Terminowa reakcja na zdarzenia
7. Dostępność zasobów

Cztery poziomy bezpieczeństwa SL1-SL4 dla poszczególnych wymagań.

Architektura sieci teleinformatycznej



PERA (ang. **Purdue** Enterprise Reference Architecture) - POZIOMY
IEC 62443 Zones & Conduit – SEGMENTY „VLAN”

Przygotowanie komputerów w sieci OT

Standardowe platformy komputerowe- wymagana ochrona

Serwery usług + agenci na maszynach:

Agent zarządzania poprawkami PM (ang. Patch Management agent)

Selektywne wdrażanie aktualizacji systemu operacyjnego.

Agent antywirusowy AV (ang. Antivirus agent),

Ochrona maszyny przed złośliwym oprogramowaniem (**malware**).

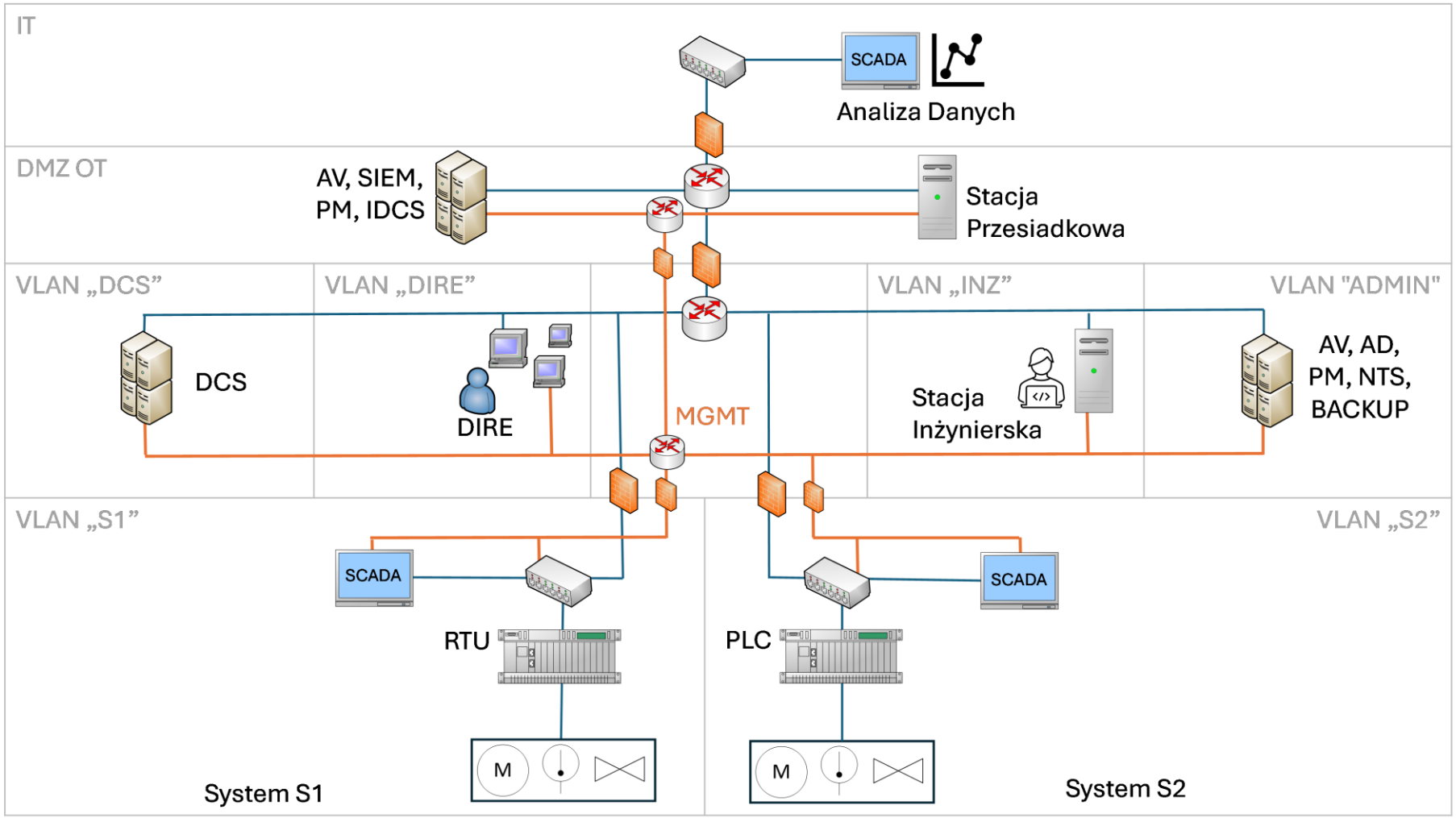
Agent kopii zapasowych (ang. **Backup** agent)

Kopie całego systemu operacyjnego. Testy odtworzeniowe.

Hardening, czyli utwardzanie wszystkich elementów systemów OT:

- dezaktywacja niewykorzystywanych interfejsów,
- usuwanie zbędnych kont użytkowników,
- wyłączenie niepotrzebnych funkcji i protokołów komunikacyjnych.

Sieć Zarządcza: MGMT



Separacja ruchu zarządczego MGMT od ruchu procesowego

MGMT:

AD - Kontrola dostępu OT
AV - Antywirus,
PM – Poprawki OS,
Backup - Kopie Zapasowe,
NTS - Synchronizacja czasu,
SIEM - Repozytorium Logów,
IDCS – Analiza ruchu sieciowego (kontekst komunikacji),

Kontrola dostępu do elementów OT

Identyfikacja (login) - **Uwierzytelnianie** (sprawdzenie hasła) - **Autoryzacja** (przyznanie dostępu).

- Kontroler domeny **AD** (ang. Active Directory) w sieci OT.
- Kok 1: zweryfikować tożsamość. Krok 2: egzekwowanie uprawnień.
- Dostęp do funkcji i usług za pomocą ról (ang. **Role-Based Access Control**).
- Najmniejsze uprawnienia i rozdział obowiązków, **brak „superkont”.**
- **Dzienniki zdarzeń** (niezaprzeczalność działań).
- Dobre praktyki: Silne hasła. Ukrywanie informacji zwrotnej. Konfigurowalna liczba kolejnych nieudanych prób (wyjątek DIRE). Ostrzeżenie o użyciu systemu.

Ochrona fizyczna, monitoring wizyjny.

Serwerownie i szafy zabezpieczone kluczem.

Poufność informacji

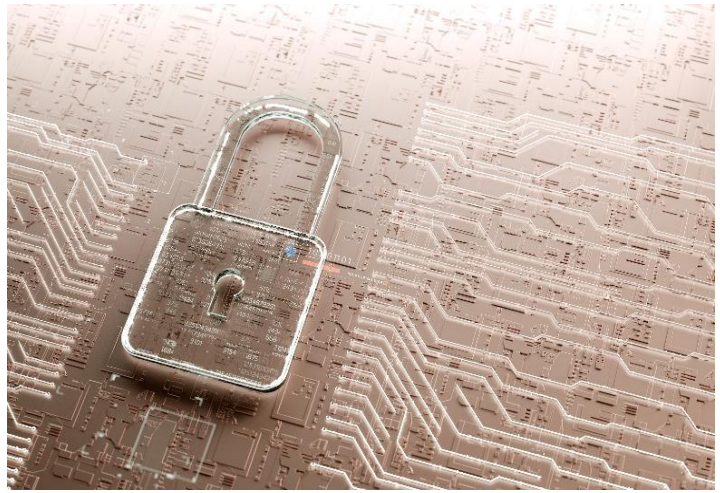
Ochronę poufności informacji **zarówno podczas przesyłania i przechowywania danych**.

- Dane krytyczne powinny być chronione także po odstawieniu systemu i w kopiach zapasowych.
- Nieszyfrowana komunikacja jest podatna na podsłuch i modyfikację danych.
- **Poufność transmisji, integralność danych oraz uwierzytelnienie stron**.

Należy stosować **uznane standardy, algorytmy, protokoły**:

- algorytm szyfrowania symetrycznego **AES** (ang. Advanced Encryption Standard),
- funkcja skrótu **SHA** (ang. Secure Hash Algorithm).
- protokół **TLS** (ang. Transport Layer Security).

W przyszłości do dystrybucji kluczy do szyfrowania będzie wykorzystywana **mechanika kwantowa** z wykorzystaniem technologii QKD (ang. Quantum Key Distribution).

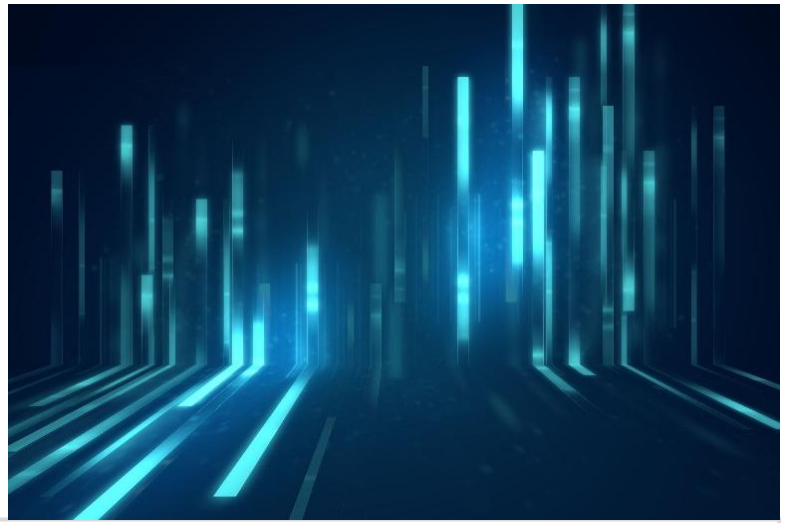


Monitorowanie OT, analiza ruchu, AI/ML

Systemy klasy SIEM

(ang. Security Information and Event Management).

- **Centralne zbieranie i analiza zdarzeń** pochodzących z krytycznych elementów systemów.
- Właściwa **reakcja na zdarzenia** (IEC 62443).
- Analiza zdarzeń po wystąpieniu incydentów (NISP2).



Systemy ciągłej analizy ruchu sieciowego **IDCS** (ang. Industrial Detection and Control Systems)

Nowej Generacji Zapory Sieciowe **NGFW** (ang Next Generation FireWall).

- analizują w czasie rzeczywistym **kontekst komunikacji** pomiędzy elementami danego systemu,
- wykrywanie anomalii, nieautoryzowanych połączeń oraz **odchyleń od normalnych wzorców:**

np. zmiana kierunku komunikacji, nietypowe polecenia z niewłaściwego elementu.

Oporność na awarie. Szkolenia.

ODPORNOŚĆ NA AWARIE TECHNICZNE

- Stosowanie **scenariuszy nadmiarowości**: redundantnych źródeł zasilania i macierzy dyskowych RAID1, zapasowych urządzeń komunikacyjnych oraz redundantnych ścieżek sieciowych.
- **Monitorowanie** stanu zasobów (min. pamięć RAM, procesor CPU) i regularną wymianę podzespołów, co określoną liczbę przepracowanych okresów.
- Rozwiązania scentralizowane dla wysokiej dostępności **HA (ang. High Avability)**. Virtualne maszyny na klastrach, wzajemnie się rezerwujących, (szybkie przywrócenie usług).

SZKOLENIA DLA OBSŁUGI i PROCEDURY

Zasady bezpiecznej obsługi systemu, **zachowania poufności** oraz rozpoznawania **ataków socjotechnicznych**.

Procedury postępowania w sytuacjach awaryjnych, co znacznie poprawia **reakcję na zdarzenia**.

Podsumowanie

Elektrownie są narażone na **szereg zagrożeń** związanych z awariami technicznymi i incydentami naruszenia bezpieczeństwa cybernetycznego.

Ryzyko cybernetyczne elektrowni można minimalizować poprzez zastosowanie wielowarstwowych środków zaradczych („Defence in Depth”):
- właściwą architekturę sieci teleinformatycznej elektrowni,
- **Segmentacja OT + separacji sieci OT/IT**,
- Sieć zarządcza **MGMT**,
- ograniczenia do minimum (i monitorowania) zdalnego dostępu do sieci OT,
- kontroli dostępu i „hardening” dla wszystkich elementów OT (komputery).
- monitorowania sieci OT i odpowiedniej reakcji na zdarzenia (SIEM),
- poufność przesyłanych i przechowywanych danych,

Zmniejszamy prawdopodobieństwo ataku, a gdy do ataku dojdzie, ograniczamy skutki tego ataku dla elektrowni.

Dziękuję za uwagę

mgr inż. Łukasz Czapla
l.czapla@ien.gda.pl