2019

STANDARDY I DOBRE PRAKTYKI OCHRONY INFRASTRUKTURY KRYTYCZNEJ

AUTOMATYKA PRZEMYSŁOWA W SEKTORZE ELEKTROENERGETYCZNYM

RCB
Rządowe Centrum Bezpieczeństwa

2019

STANDARDY I DOBRE PRAKTYKI OCHRONY INFRASTRUKTURY KRYTYCZNEJ

AUTOMATYKA PRZEMYSŁOWA W SEKTORZE ELEKTROENERGETYCZNYM

RCB
Rządowe Centrum Bezpieczeństwa

SPIS TREŚCI

Niniejszy poradnik powstał dzięki zaangażowaniu przedstawicieli następujących operatorów infrastruktury krytycznej sektora elektroenergetycznego:

- **Enea Centrum Sp. z o.o.;**
- **Enea Operator Sp. z o.o.;**
- **Enea SA;**
- **Enea Wytwarzanie SA;**
- **ENERGA Elektrownie Ostrołęka SA;**
- **ENERGA Informatyka i Technologie Sp. z o.o.;**
- **ENERGA Operator SA;**
- **ENERGA SA;**
- **ENERGA Wytwarzanie SA;**
- **Innogy Polska SA;**
- **PGE Dystrybucja SA;**
- **PGE Energia Odnawialna SA;**
- **PGE Górnictwo i Energetyka Konwencjonalna SA;**
- **PGE SA;**
- **PGE Systemy SA;**
- **PKP Energetyka SA;**
- **PSE SA;**
- **Tauron Dystrybucja SA;**
- **Tauron Polska Energia SA;**
- **Tauron Wytwarzanie SA;**

oraz przy współpracy firm doradczych EY Business Advisory i PricewaterhouseCoopers.

1. CZĘŚĆ A – WPROWADZENIE

1.1. CEL DOKUMENTU

Celem dokumentu jest pomoc podmiotom odpowiedzialnym za infrastrukturę krytyczną (IK) w budowaniu szeroko rozumianego bezpieczeństwa w obszarze automatyki przemysłowej, wykorzystywanej w sektorze elektroenergetycznym.

Dokument przedstawia podejście oraz zbiór zaleceń, których spełnienie pomoże zapewnić minimalny poziom bezpieczeństwa infrastruktury przemysłowej. Wybór proponowanych środków bezpieczeństwa powinien zostać przeprowadzony na bazie analizy ryzyka i kontekstu działalności podmiotu.

Mierniki mają na celu wsparcie zarządcze w zakresie wskazania obszarów, które wymagają szczególnej uwagi lub poprawy w organizacji. Mierniki określono w **Załączniku nr 2** do niniejszego dokumentu.

1.2. ZAKRES STOSOWANIA

Poradnik opisuje najlepsze praktyki z obszaru zarządzania i bezpieczeństwa automatyki przemysłowej, z uwzględnieniem specyfiki sektora elektroenergetycznego. Kierowany jest do podmiotów z sektora elektroenergetycznego oraz podmiotów wspierających podstawowe procesy operacyjne dla sektora elektroenergetycznego.

Głównym odbiorcą dokumentu jest kadra zarządzająca oraz osoby zaangażowane w proces budowania, eksploatacji, zarządzania, rozwoju oraz wygaszenia systemów automatyki przemysłowej. Zostały w nim wskazane przykłady rozwiązań, które mają zapewnić przede wszystkim bezpieczeństwo procesów technologicznych.

Charakterystyczne dla systemów automatyki przemysłowej jest nieco odmienne, od powszechnego w świecie IT, podejście do podstawowych cech bezpieczeństwa informacji: poufności, integralności i dostępności. W odniesieniu do danych przetwarzanych w systemach automatyki przemysłowej, w pierwszej kolejności należy skupić się na wsparciu w zapewnieniu dostępności informacji, potem integralność, a dopiero w następnej kolejności poufność danych przetwarzanych.

Dokument koncentruje się na 6 (pokazanych poniżej) obszarach.

Rys. 1

Dla ułatwienia, w dalszej części poradnika, systemy automatyki przemysłowej lub systemy OT (patrz również definicje w załączniku nr 1) będą nazywane skrótowo „system".

1.3. ZGODNOŚĆ Z NORMAMI, STANDARDAMI I WYMAGANIAMI PRAWNYMI

Rekomenduje się, aby w procesie budowania bezpieczeństwa systemów automatyki przemysłowej wykorzystywać dobre praktyki i standardy opracowane w innych krajach lub w ramach innych prac. Znajdują się one między innymi w:

- normach serii ANSI/ISA – 62443;
- normach serii PN-ISO/IEC 27000;
- normach serii PN-ISO/IEC 31000;
- zaleceniach NIST Special Publication serii 1800 i 800;
- instrukcjach Organizacji Bezpiecznej Pracy przy Urządzeniach Elektroenergetycznych, obowiązujących w podmiocie eksploatującym systemy automatyki przemysłowej;
- Instrukcji Ruchu i Eksploatacji Sieci Przesyłowej;
- Instrukcjach Ruchu i Eksploatacji Sieci Dystrybucyjnej;
- Prawie Geologicznym i Górniczym[1].

1. patrz np. §636 rozporządzenia Ministra Gospodarki z dnia 28 czerwca 2002 r. w sprawie bezpieczeństwa i higieny pracy, prowadzenia ruchu oraz specjalistycznego zabezpieczenia przeciwpożarowego w podziemnych zakładach górniczych

2. CZĘŚĆ B – AUTOMATYKA PRZEMYSŁOWA W SEKTORZE ELEKTROENERGETYCZNYM

2.1. ELEMENTY SEKTORA ELEKTROENERGETYCZNEGO W POLSCE

Ciągłość i stabilność dostaw energii elektrycznej jest gwarantowana przez zespół podmiotów tworzących podsystemy w ramach Krajowego Systemu Elektroenergetycznego (dalej KSE). Podmioty te stanowią odrębne jednostki, podlegające oddzielnym instytucjom i regulacjom. Podsystemy tworzące KSE to:

- wytwarzanie – są to wszystkie źródła wytwórcze na terenie kraju;
- przesył – na który składają się linie najwyższych napięć (NN) o napięciu 220 i 400 kV oraz stacje energetyczne najwyższych napięć, a także systemy zarządzania ruchem w sieci NN;
- dystrybucja – zarządzanie dostawami energii elektrycznej do odbiorców końcowych za pomocą linii energetycznych o napięciu 110 kV i niższym oraz stacji energetycznych wysokiego i średniego napięcia, a także systemy zarządzania ruchem w sieciach WN i ŚN;
- obrót – przedsiębiorcy zajmujący się handlem energią kupowaną od wytwórców i sprzedawaną odbiorcom finalnym. Ceny i warunki transakcji są ustalane indywidualnie pomiędzy firmą sprzedającą, a kupującą energię lub wynikają z zasad jej zakupu. Energia sprzedawana jest odbiorcom końcowym po cenach określonych w taryfach zatwierdzonych przez Urząd Regulacji Energetyki.

2.2. PODSTAWOWE PROCESY BIZNESOWE, KTÓRE WSPIERA AUTOMATYKA PRZEMYSŁOWA

Podstawowe procesy biznesowe wspierane przez automatykę przemysłową w sektorze elektroenergetycznym:

- wydobycie;
- dostarczenie paliwa;
- wytwarzanie energii elektrycznej i ciepła:
  - zabezpieczenie procesu produkcji,
  - eksploatacja, prowadzenie i optymalizacja ruchu jednostek wytwórczych i instalacji pomocniczych z zachowaniem norm BHP, ppoż. i innych,
  - pomiary, monitorowanie, analizy, rozliczenia ilościowe, jakościowe produkcji, zużycia paliw i komponentów oraz emisji;
- przesył:
  - prowadzenie ruchu sieci przesyłowej,
  - pozyskiwanie, przetwarzanie oraz udostępnianie danych pomiarowych,
  - świadczenie usług przesyłowych;
- dystrybucja energii elektrycznej i ciepła:
  - prowadzenie ruchu w sieci dystrybucyjnej,
  - pozyskiwanie, przetwarzanie oraz udostępnianie danych pomiarowych,
  - świadczenie usług dystrybucyjnych;
- obrót hurtowy energią elektryczną i produktami powiązanymi:
  - zarządzanie i sprzedaż energii elektrycznej,
  - TPA (ang. *Third Party Access* – zasada dostępu stron trzecich do sieci, umożliwiająca zakup paliwa gazowego lub energii elektrycznej od dowolnego sprzedawcy);

- realizacja inwestycji w obszarze wydobycia i wytwarzania;
- zarządzanie majątkiem w obszarze wydobycia i wytwarzania;
- zarządzanie kryzysowe i zachowanie ciągłością działania przedsiębiorstwa;
- szkolenia dla własnej kadry, oraz dostęp do wiedzy w celu utrzymania i prawidłowej eksploatacji systemów automatyki.

Procesy wydobycia i obrotu jest poza zakresem niniejszego dokumentu.

2.3. GŁÓWNE ELEMENTY I FUNKCJE AUTOMATYKI PRZEMYSŁOWEJ W SEKTORZE ELEKTROENERGETYCZNYM

Obiekty technologiczne podsystemów wytwarzania, przesyłu i dystrybucji są kontrolowane i nadzorowane w warstwach:

1. sterowanie:
   - warstwa realizacji pomiarów i oddziaływań sterujących –> systemy łączone SCADA PLC, HMI PLC, inteligentne urządzenia pomiarowe i wykonawcze wyposażone w jednostki mikroprocesorowe,
   - warstwa sterowania bezpośredniego –> systemy łączone SCADA PLC, HMI PLC, inteligentne urządzenia pomiarowe i wykonawcze wyposażone w jednostki mikroprocesorowe,
   - warstwa sterowania nadrzędnego –> systemy klasy DCS, systemy łączone SCADA PLC,
   - warstwa nadzorowania, koordynacji i optymalizacji procesu –> procesy ciągłe i dyskretne realizowane przez systemy klasy DCS, systemy łączone SCADA PLC;

2. wizualizacja i obsługa:
   - HMI, stacje operatorskie, stacje inżynierskie oraz stacje nadzorcze (informacyjne) w celu wyświetlania przetworzonych i przygotowanych danych, pochodzących z innych warstw podsystemów;

3. zabezpieczenia:
   - systemy klasy DCS,
   - łączone SCADA – PLC – SIS,
   - system klasy SIS;

4. zarządzanie:
   - zarzadzanie produkcją – systemy MES (Manufacturing Execution Systems),
   - zarzadzania przedsiębiorstwem – systemy ERP (Enterprise Resource Planning),
   - nadzór i kontrola obiektów technologicznych – systemy klasy SCADA/DCS/MES.

Systemy OT winny być zaprojektowane tak, aby awaria pojedynczego elementu nie spowodowała przerwania świadczenia jego funkcji. Konstrukcja systemu powinna także zmniejszać prawdopodobieństwo i skutki zdarzeń, które występują ze względu na nadmierne zużycie zasobów, np. CPU, RAM, zasoby dyskowe, nadmierne obciążenie sieci np. poprzez redundancję wybranych (kluczowych) zasobów.

2.4. CYKL ŻYCIA AUTOMATYKI PRZEMYSŁOWEJ

Przykładowe fazy życia systemów OT:

Rys. 2

Poszczególne fazy charakteryzują się różnymi cechami dla producenta, projektanta, dostawcy lub użytkownika oraz są przesunięte w czasie.

Poszczególne fazy charakteryzują się, z punktu widzenia użytkownika końcowego, odmiennymi cechami.

2.4.1. Faza koncepcji i architektury

- pozyskanie kompetencji w zakresie architektonicznym i bezpieczeństwa;
- zebranie wymogów, w tym funkcjonalnych i bezpieczeństwa;
- określenie ograniczeń, w tych technicznych i finansowych;
- badanie rynku pod kątem spełnienia wymogów;
- planowanie, budżetowanie, uzyskiwanie wewnętrznych zgód na realizację.

2.4.2. Faza implementacji

- implementacja założonych funkcjonalności;
- wykorzystanie rozwiązań, o szacowanym długim czasie eksploatacji;
- sukcesywne uruchomianie podsystemów;
- budowanie dodatkowych kompetencji wymaganych przy eksploatacji;
- rozwiązywanie problemów realizowane głównie przez producenta, projektanta lub dostawcę w trakcie implementacji;
- weryfikacja podatności i ocena ryzyka;
- przygotowanie poprawek, dedykowane rozwiązaniu specyficznych problemów;
- przeprowadzanie walidacji / testów systemu.

2.4.3. Faza stabilna

- pełna implementacja założonych funkcjonalności;
- system działający w przetestowanym środowisku;
- uruchomienie zespołu pierwszej linii wsparcia, nadzorującego poprawność pracy systemu;
- uruchomienie zespołów drugiej i trzeciej linii wsparcia rozwiązujących złożone problemy, również przy wsparciu producenta, projektanta lub dostawcy;
- znane podatności systemu usuwane przy użyciu poprawek i aktualizacji, również przy wsparciu producenta, projektanta lub dostawcy;
- okresowe zaplanowane audyty bezpieczeństwa systemu;
- walidacja/testy systemów związana z planowanymi postojami lub modernizacjami.

2.4.4. Faza końcowa

- zespoły nadzorujące poprawność pracy systemu posiadają wysokie kompetencje;
- pojawiają się ograniczenia w dostępności niektórych części zamiennych;
- producent ogłosił datę zakończenia dostaw i/lub wsparcia;

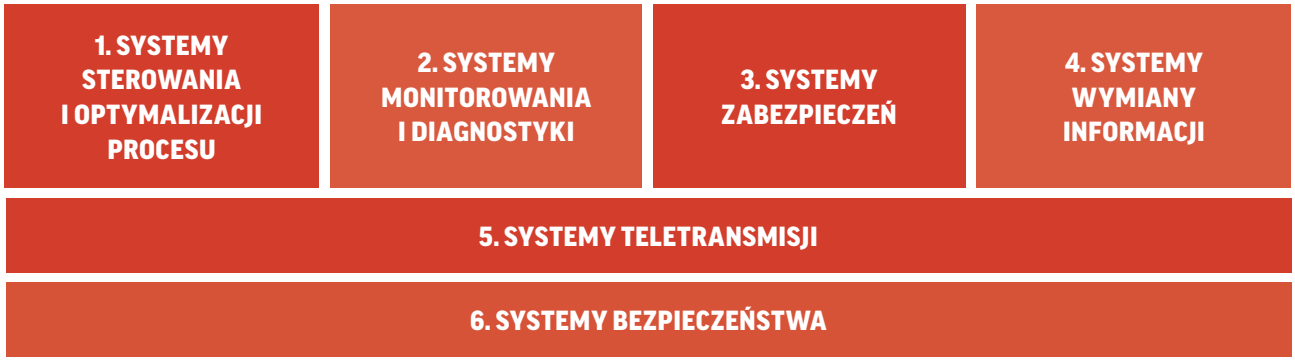
- wzrasta liczba problemów sprzętowych i/lub związanych z bezpieczeństwem systemu zgłaszanych do producenta, projektanta lub dostawcy;
- okresowe audyty/przeglądy systemu wykazują większą liczbę obserwacji wymagających uwagi.

2.4.5. Faza wycofania

- funkcjonalność systemu nie jest rozbudowywana;
- pojawiają się narzędzia dublujące funkcjonalność systemu i realizujące ją w sposób zgodny z aktualnymi uregulowaniami lub środowiskiem;
- zwiększająca się liczba istotnych interwencji serwisowych, które nie mogą być rozwiązane przez zespoły nadzorujące poprawność pracy systemu;
- produkt nie jest wspierany przez producenta;
- producent nie dostarcza części zamiennych;
- potencjalnie drogie naprawy realizowane bez wsparcia producenta;
- wzrost liczby podatności;
- okresowe audyty/przeglądy systemu wykazują niską jakość systemu oraz wysokie ryzyko związane z dalszą eksploatacją systemu;
- przygotowanie założeń do migracji do nowych rozwiązań.

2.5. MODEL FUNKCJONALNY OPISU SYSTEMÓW OT

Strukturę systemów OT można przedstawić za pomocą modelu opisującego podział funkcjonalny wraz z realizowanymi zadaniami przez poszczególne elementy składowe. Systemy zostaną sklasyfikowane zgodnie z ich strukturą funkcjonalną oraz ze względu na realizowany cel.



Rys. 3

1. Systemy sterowania i optymalizacji procesu – system OT mający na celu oddziaływanie na procesy i zdarzenia w Instalacjach Technologicznych.
2. Systemy monitorowania i diagnostyki – system OT umożliwiający przeprowadzenie oceny i analizy stanu instalacji technologicznej.
3. Systemy zabezpieczeń – system OT mający na celu zapewnienie bezpieczeństwa Instalacji Technologicznych w szczególności w zakresie: ochrony życia i zdrowia ludzi, zabezpieczenie przez skutkami nieprawidłowego działania, takimi jak uszkodzenie czy zniszczenie Instalacji Technologicznej.
4. Systemy wymiany informacji (wewnętrznej i zewnętrznej) – system OT mający na celu przekazywanie informacji technologicznych pochodzących z urządzeń Instalacji Technologicznej oraz do innych systemów OT lub systemów biznesowych w ramach organizacji lub poza nią.

5. Systemy teletransmisji – kategoria systemu wspierającego systemy OT. System ten składa się z urządzeń aktywnych i biernych. Urządzenia służą do przesyłania informacji z innych systemów niezależnie od ich topologii, sposobu zestawianych połączeń, rodzaju przenoszonych informacji, mediów i protokołu transmisji.
6. Systemy bezpieczeństwa – system chroniący, nadzorujący i/lub kontrolujący poprawność i ciągłość pracy zarówno systemów OT, jak również ich komponentów np. aplikacji, usług i elementów teletransmisji.

2.6. TABELA KLASYFIKACJI KRYTYCZNOŚCI SYSTEMÓW OT

Stopień krytyczności systemu OT	Wpływ na ciągłość procesów technologicznych	Wpływ na bezpieczeństwo procesów technologicznych
Wysoki (Krytyczny)	Zakłócenie prawidłowego działania systemu bezpośrednio wpłynie na ciągłość działania głównych i najistotniejszych procesów biznesowych organizacji lub w znacznym stopniu je utrudni	Zakłócenie prawidłowego działania systemu może bezpośrednio zagrażać życiu i zdrowiu ludzi lub skażeniu środowiska naturalnego
Średni (Ważny)	Zakłócenie prawidłowego działania systemu może obniżyć wydajność istotnego procesu technologicznego, jednak w krótkim okresie czasu nie spowoduje przerwania najistotniejszych procesów biznesowych organizacji i w znacznym stopniu nie utrudni ich prowadzenia	Zakłócenie prawidłowego działania systemu nie będzie bezpośrednio zagrażać życiu i zdrowiu ludzi lub skażeniu środowiska naturalnego, lecz wymagane będzie zastosowanie dodatkowych środków ochrony
Niski (Pomocniczy)	Zakłócenie prawidłowego działania systemu w żaden sposób nie wpłynie na ciągłość działania procesów biznesowych	Zakłócenie prawidłowego działania systemu w żaden sposób nie wpłynie na bezpieczeństwo ludzkie oraz środowiska naturalnego

3. CZĘŚĆ C – ZARZĄDZANIE BEZPIECZEŃSTWEM AUTOMATYKI PRZEMYSŁOWEJ

3.1. ROLE W PROCESACH ZARZĄDZANIA BEZPIECZEŃSTWEM AUTOMATYKI PRZEMYSŁOWEJ

Poprawne zarządzanie bezpieczeństwem systemów OT w Spółce wymaga zbudowania organizacji z podziałem na role reprezentujące:

- nadzór nad działaniami związanymi z bezpieczeństwem systemów OT;
- potrzeby biznesowe;
- realizację techniczną;
- weryfikujące bezpieczeństwo systemów OT;
- korzystanie z systemów OT.

Role związane z zarządzaniem bezpieczeństwem automatyki przemysłowej zostaną przedstawione niezależnie od struktury organizacyjnej przedsiębiorstwa.

3.1.1. Koordynator ds. bezpieczeństwa systemów OT

Osoba pracująca w przedsiębiorstwie, posiadająca odpowiednią wiedzę i doświadczenie w zakresie systemów OT oraz norm i uwarunkowań prawnych powiązanych z tymi systemami, koordynująca całość działań w ramach przedsiębiorstwa związanych z bezpieczeństwem systemów OT. W zależności od struktury organizacyjnej przedsiębiorstwa rola może być nadawana na różnych poziomach, tj.: koordynator na poziomie przedsiębiorstwa, grupy kapitałowej, spółki, dowolnej innej jednostki organizacyjnej.

3.1.2. Właściciel biznesowy systemu OT

Osoba decyzyjna pracująca w przedsiębiorstwie, która ma zatwierdzoną odpowiedzialność za funkcjonowanie, rozwój, utrzymanie, korzystanie i bezpieczeństwo powierzonego systemu OT.

3.1.3. Architekt systemów OT

Osoba pracująca w przedsiębiorstwie, posiadająca odpowiednią wiedzę i doświadczenie w temacie systemów OT, koordynująca i harmonizująca całość działań związanych z aspektami technicznymi systemów OT w przedsiębiorstwie.

3.1.4. Administrator merytoryczny systemu OT

Osoba odpowiedzialna pod względem merytorycznym za prawidłowość funkcjonowania, korzystania i bezpieczeństwa informacji przetwarzanych przez system OT. Administrator merytoryczny systemu określa uprawnienia użytkowników na poziomie systemu dziedzinowego. Administrator merytoryczny wyznaczany jest przez właściciela biznesowego.

3.1.5. Administrator techniczny systemu OT

Podmiot lub osoba odpowiedzialna za utrzymanie ciągłości działania i prawidłowości funkcjonowania sytemu OT w zakresie określonych funkcjonalności, bez uprawnień do samodzielnego wprowadzania zmian w zakresie urządzeń Instalacji Technologicznej.

3.1.6. Użytkownik systemu OT

Osoba posiadająca dostęp do danych przetwarzanych przez system OT przy użyciu narzędzi udostępnionych przez ten system.

3.1.7. Audytor bezpieczeństwa systemów

Osoba upoważniona do przeprowadzania audytów bezpieczeństwa systemów OT pod kątem zgodności z obowiązującymi normami oraz według ustalonych kryteriów.

3.2. ZARZĄDZANIE RYZYKIEM

Celem zarządzania ryzykiem w obszarze OT jest zapewnienie/zagwarantowanie, że ryzyka są identyfikowane i utrzymywane na przyjętym (zaplanowanym) poziomie. Optymalizacja poziomu ryzyka OT musi uwzględniać profil działalności organizacji, koszty postępowania z ryzykiem oraz ewentualne ograniczenie/utrudnienie działalności operacyjnej. Ocenę ryzyka należy przeprowadzać okresowo (nie rzadziej niż raz na 2 lata) oraz przy znaczących zmianach w uwarunkowaniach wewnętrznych oraz zewnętrznych.

Każda organizacja powinna posiadać sformalizowany proces zarządzania ryzykiem w obszarze OT.

Proces zarządzania ryzykiem powinien uwzględniać następujące etapy:

1. Określenie kontekstu – obejmuje zebranie i uporządkowanie informacji o wewnętrznych (np. organizacyjnych) oraz zewnętrznych (powiązania z innymi podmiotami oraz aspekty prawne) uwarunkowaniach funkcjonowania podmiotu, niezbędnych dla procesu zarządzania ryzykiem. Określenie celu i zakresu procesu zarządzania ryzykiem. Wybór zasobów środowiska OT do analizy. Zdefiniowanie ról i odpowiedzialności jednostek organizacyjnych/pracowników, biorących udział w procesie. Zdefiniowanie apetytu na ryzyko. Zdefiniowanie powiązań pomiędzy procesami: zapewnienia ciągłości działania, zarządzania incydentami, zarządzania ryzykiem IT, zarządzania ryzykiem korporacyjnym.

2. Identyfikacja zagrożeń – zgromadzenie i uporządkowanie informacji o wszystkich zdarzeniach niekorzystnych, adekwatnych do profilu działalności organizacji. Stworzenie listy zdarzeń niekorzystnych, z uwzględnieniem co najmniej następujących obszarów: technologia, cyberbezpieczeństwo, aspekty prawne, BHP, bezpieczeństwo fizyczne, bezpieczeństwo środowiskowe, relacje zewnętrzne. Jeśli jest to możliwe, należy zagregować zdarzenia niekorzystne (np. te posiadające wspólną przyczynę wystąpienia).

3. Analiza i ocena ryzyka – przypisanie prawdopodobieństwa dla każdego zdarzenia niekorzystnego oraz jego wpływu na działalność organizacji (uwzględniając rejestr incydentów w obszarze OT oraz wyniki procesu zarządzania ciągłością działania, w tym powiązań między procesami). Stworzenie mapy ryzyka. Porównanie efektów analizy ryzyka z ustalonym wcześniej apetytem na ryzyko, co pozwoli na opracowanie listy zarządzanych zdarzeń oraz podjęcie decyzji dotyczącej sposobu zarządzania nimi. Przypisanie właścicieli ryzyka oraz zdefiniowane kluczowe wskaźniki ryzyka (ang. *key risk indicators, KRI*) dla ryzyk, które będą podlegały dalszemu zarządzaniu (pozostałe ryzyka zostaną zaakceptowane i monitorowane).

4. Postępowanie z ryzykiem – wybór sposobu postępowania z ryzykiem: przeniesienie skutków ryzyka na inny podmiot, np. poprzez wykupienie polis ubezpieczeniowych, podjęcie działań, które mają na celu ograniczenie prawdopodobieństwa lub skutku materializacji ryzyka oraz rezygnacja z działań, które mogą spowodować materializację ryzyka. Opracowanie planów awaryjnych dla ryzyk, które po realizacji planu postępowania nadal będą powyżej ustalonego apetytu na ryzyko.

5. Monitorowanie i kontrola (proces ciągły) – monitorowanie statusu wdrożenia postępowania z ryzykiem. Monitorowanie zmian uwarunkowań wewnętrznych i zewnętrznych, które mogą wpłynąć na konieczność ponownego przeprowadzenia analizy ryzyka. Ciągłe doskonalenie procesu oraz wzrost jakości i efektywności wykonywanych zadań.

6. Komunikacja i konsultacja (proces ciągły) – zapewnienie, że wszyscy uczestnicy procesu jednakowo rozumieją zagrożenia występujące w działalności organizacji. Zapewnienie odpowiedniego poziomu świadomości uczestników procesu zarządzania ryzykiem.

3.3. NADZÓR I AUDYT

Ze względu na możliwe konsekwencje, zalecane jest prowadzenie regularnych czynności nadzorczych i audytowych. Rekomenduje się przeprowadzenie czynności audytowych w obszarach:

- weryfikacja połączeń z siecią – połączenia sieciowe systemów OT;
- weryfikacja połączeń z siecią – dostęp dla dostawców;
- weryfikacja połączeń z siecią – połączenia sieci OT i IT;
- bezpieczeństwo platformy OT – weryfikacja bezpieczeństwa platformy OT;
- bezpieczeństwo fizyczne;
- procesy i narzędzia bezpieczeństwa – narzędzia bezpieczeństwa;
- komunikacja z dostawcami;
- procesy bezpieczeństwa;
- organizacja bezpieczeństwa;
- regulacje wewnętrzne.

3.4. MONITOROWANIE STANU BEZPIECZEŃSTWA INFRASTRUKTURY AUTOMATYKI PRZEMYSŁOWEJ ORAZ REAGOWANIE NA ZDARZENIA

Dla zapewnienia skutecznego monitorowania bezpieczeństwa infrastruktury OT oraz reagowania na zidentyfikowane incydenty bezpieczeństwa i zagrożenia wskazane jest utworzenie w organizacji komórki Security Operations Center (SOC).

Nadrzędnym celem utworzenia SOC jest centralizacja monitorowania bezpieczeństwa w celu wykrywania zdarzeń niepożądanych, a następnie właściwego reagowania na wykryte zdarzenia. SOC odpowiedzialny jest także za koordynowanie zadań związanych z obsługą niepożądanych zdarzeń w organizacji oraz ich raportowanie.

Zapewnienie jednolitego i ciągłego procesu monitorowania bezpieczeństwa pozwoli na skuteczne zapobieganie i reagowanie na incydenty bezpieczeństwa, a w przypadku ich wystąpienia zapewni szybką i skoordynowaną reakcje organizacji.

3.4.1. Funkcjonowanie SOC

Funkcjonowanie komórki SOC oparte jest na trzech podstawowych filarach:

- personel (operatorzy, analitycy, role w komórce, zakres odpowiedzialności);
- technologia (monitorowanie zdarzeń, zbieranie i korelacja zdarzeń);
- procesy (procedury, obsługa incydentów, reakcja na zdarzenia).

3.4.2. Obsługa incydentów

Obsługa incydentów bezpieczeństwa przez SOC musi być realizowana w oparciu o przyjęty w organizacji proces obsługi incydentów, a działania związane z prowadzonymi czynnościami muszą być dokumentowane. Umiejscowienie komórki SOC w strukturach organizacyjnych powinno zapewniać niezależność i swobodę działania pozwalające na efektywne realizowanie zadań operacyjnych.

Skuteczne reagowanie i obsługa incydentów wymaga wyposażenia zespołu SOC w narzędzia techniczne pozwalające na monitorowanie bezpieczeństwa infrastruktury i zbieranie danych w sposób ciągły z następujących źródeł:

- ruch sieciowy;
- przepływy sieciowe;
- logi systemowe;
- logi z urządzeń bezpieczeństwa (IDP, IPS, zapory sieciowe, system antywirusowy);
- logi z końcówek (stacje dyspozytorskie, inżynierskie);
- informacje z zewnętrznych zaufanych źródeł (CSIRT.GOV.PL, RCB, inne CSIRTy i organizacje bezpieczeństwa);
- wymiana informacji z innymi komórkami SOC (zwłaszcza sektorowymi);
- informacje pozyskiwane z zewnętrznych platform Threat Intelligence;
- systemy wczesnego ostrzegania;
- systemy zarządzania aktywami;
- logi z urządzeń automatyki przemysłowej;
- logi systemów bezpieczeństwa fizycznego (system kontroli dostęp).

3.4.3. Infrastruktura SOC

Infrastruktura techniczna komórki SOC musi być zbudowana z systemów informatycznych umożliwiających monitorowanie stanu bezpieczeństwa, alarmowanie w momencie wykrycia zagrożenia lub naruszenia bezpieczeństwa. Wykorzystanie rozwiązań klasy SIEM (z ang. *Security Information and Event Management*) dostarcza funkcjonalności pozwalające na:

- wykrywanie incydentów bezpieczeństwa i przeszukiwanie zdarzeń;
- archiwizacja/przechowywanie logów i danych audytowych dotyczących zdarzeń i incydentów bezpieczeństwa;
- korelację zdarzeń w czasie zbliżonym do rzeczywistego;
- proste podłączanie różnych systemów źródłowych.

3.4.4. Organizacja SOC

Zespół SOC, aby efektywnie realizować swoje zadania, musi pracować w trybie ciągłym 24/7/365 w oparciu o wykwalifikowany personel świadczący pracę w trybie zmianowym. W celu produktywnego wykorzystania zasobów ludzkich zespołu SOC rekomendowane jest dokonanie podziału na linie operacyjne. Pierwsza linia operacyjna odpowiedzialna jest za monitorowanie bieżących zdarzeń i obsługę standardowych incydentów bezpieczeństwa, druga za obsługę zdarzeń niestandardowych, które nie zostały obsłużone przez pierwszą linię wsparcia oraz trzecia linia obsadzona ekspertami specjalizującymi się w konkretnych obszarach analizy incydentów bezpieczeństwa, posiadającymi kompetencje pozwalające rozwiązywać skomplikowane zagadnienia.

Podczas projektowania komórki SOC w organizacji należy mieć na uwadze także aspekty bezpieczeństwa, wynikające z otoczenia prawnego. W obszarze infrastruktury krytycznej szczególnie istotne jest uwzględnienie wymagań Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego, wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii oraz Rozporządzenia Parlamentu Europejskiego i Rady (EU) nr 1227/2011 z dnia 25 października 2011 r. w sprawie integralności i przejrzystości hurtowego rynku energii (Rozporządzenie REMIT).

3.5. KOMUNIKACJA

Infrastruktura systemów OT (sieciowa i aplikacyjna) ma zapewnić wymianę informacji między wszystkimi elementami tego systemu, a także zapewnić, jeśli jest to wymagane, wymianę informacji z systemami IT i innymi systemami zewnętrznymi w celu realizacji zadań biznesowych.

Sieć automatyki przemysłowej winna być traktowana jako „zaufana". Każda inna sieć w tym: biznesowa, publiczna (Internet), WAN – powinna być traktowana jako obca.

Rekomenduje się wprowadzenie elementów ograniczających i kontrolujących przepływ informacji na każdej granicy między warstwami systemów, zgodnie z Rys. 3 (Model warstwowy opisu środowiska OT). W przypadku potrzeby wymiany danych (niezbędne ze względu na potrzeby biznesowe), punkt wymiany winien być dozorowany i chroniony. Punkty wymiany danych winny być ograniczone do niezbędnego minimum poprzez zastosowanie „bezpiecznych bram" wymiany danych lub z wykorzystaniem rozwiązań zapewniających jednokierunkową komunikacją.

Rekomenduje się segmentację sieci na poziomie fizycznym lub logicznym w zależności od wymaganego poziomu separacji między poszczególnymi jej segmentami. Rekomenduje się również głębszą segmentację sieci w oparciu o takie podziały jak: funkcjonalny, przeznaczenie, przestrzenny/geograficzny, poziomu ochrony fizycznej itp.

W modelu warstwowym komunikacji wskazane jest wyodrębnienie funkcji bezpieczeństwa realizowanej przez infrastrukturę sieciową i aplikacyjną. W zakresie infrastruktury sieciowej wskazane jest stosowanie elementów bezpieczeństwa na wszystkich warstwach, zarówno w zakresie opisanej segmentacji jak i monitorowania, kontroli, uwierzytelnienia i autoryzacji. Natomiast na poziomie aplikacyjnym wskazane jest budowanie aplikacji w taki sposób, by strony uprawnione do komunikacji podlegały wzajemnemu uwierzytelnieniu, zarówno na poziomie uwierzytelnienia, jak i autoryzacji. Rekomenduje się łączne wykorzystanie funkcji bezpieczeństwa opisanych powyżej warstw infrastruktury sieciowej i aplikacyjnej w celu dywersyfikacji funkcji bezpieczeństwa. Elementy ochrony poszczególnych warstw należy dobierać adekwatnie do realizowanych funkcji biznesowych, uwzględniając ograniczenia technologiczne i wagę poszczególnych elementów zabezpieczeń.

W zależności od przeznaczenia, infrastruktura komunikacyjna może mieć charakter lokalny lub rozproszony. W każdym z tych przypadków należy stosować, jeśli jest to możliwe i zasadne, wszystkie elementy ochrony fizycznej, logicznej i systemowej, przed niepowołanym dostępem do sieci oraz wykrywaniem zdarzeń bezpieczeństwa.

W przypadku systemów rozproszonych, gdzie do komunikacji wykorzystuje się infrastrukturę publiczną lub infrastrukturę stron trzecich (np. dostawca łączy lub APNów), należy traktować je jako niezaufane. Rekomenduje się wprowadzenie na granicy z takimi sieciami elementy szyfrujące transmisję. Szyfrowanie ma za zadanie zapewnić poufność i integralność transmitowanych danych. Zaleca się, aby przy wyborze standardów kryptograficznych stosowanych w systemach OT uwzględniano prawo do używania tych standardów na terenie Unii Europejskiej, a w szczególności Polski. Wybór standardu kryptograficznego ma się opierać na aktualnym stanie wiedzy naukowej i technicznej – w szczególności wybór ma uwzględniać metody kryptograficzne, które aktualnie i w zakładanej przyszłości zapewnią ochronę zasobów. Nie rekomenduje się stosowania rozwiązań autorskich, wykorzystywanych w małej skali, w niewielkiej liczbie rozwiązań lub jednocześnie przypisanych tylko do jednego podmiotu.

3.6. BEZPIECZEŃSTWO ZASOBÓW LUDZKICH

Pozycja zajmowana w strukturze operatora IK (stanowisko i przypisane do niego zakres zadań) determinuje poziom dostępu fizycznego do kolejnych stref bezpieczeństwa, komponentów systemu oraz dostęp do informacji w nim przetwarzanych. Nieodpowiednie nadanie uprawnień dla personelu (dotyczy to także usługodawców, dostawców i gości) mogą służyć zakłóceniu funkcjonowania systemów sterowania przemysłowego.

Bezpieczeństwo zasobów ludzkich (zapewnienie bezpieczeństwa osobowego) to zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka związanego z osobami, które przez dostęp do obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, mogą wpływać na ich funkcjonowanie.

Zapewnienie bezpieczeństwa osobowego jest związane z bezpieczeństwem fizycznym, organizacyjnym i teleinformatycznym systemów automatyki przemysłowej. Zagrożenia wewnętrzne i zewnętrznymi w obszarze zarządzania personelem to np.: rozczarowany pracownik, prowokacje, konkurencja, obce rządy oraz przestępczość zorganizowana.

Personel zarządzający, utrzymujący, projektujący, a także obsługujący systemy sterowania przemysłowego posiada istotną (unikalną) wiedzę na temat funkcjonowania głównych procesów technologicznych organizacji. Jest on szczególnie cenny, ponieważ zaangażowany jest w utrzymanie ciągłości kluczowych procesów operacyjnych dla organizacji. W celu ochrony informacji, mających istotne znaczenie dla organizacji, rekomenduje się, aby z personelem wewnętrznym były zawierane odrębne umowy o zakazie konkurencji w czasie trwania i po ustaniu stosunku pracy oraz umowy o poufności. Organizacja powinna zapewnić możliwość sukcesywnego podnoszenia kompetencji oraz wsparcie podmiotów zewnętrznych w realizacji powierzonych zadań. Ochrona kluczowego personelu oznacza także bardziej restrykcyjne wymogi kontrolne w stosunku do tych osób. Należy także podjąć kroki w celu zapewnienia zastępstwa personelu (podobne kwalifikacje oraz uprawnienia).

Wytyczne, dotyczące zapewnienia bezpieczeństwa osobowego infrastruktury krytycznej zawarte są w załączniku nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej[2] i mogą stanowić punkt odniesienia do wyboru konkretnych rozwiązań organizacyjnych lub technicznych.

3.7. REKOMENDACJE W ZAKRESIE DOKUMENTACJI PROCESÓW BEZPIECZEŃSTWA OT

Rekomenduje się, aby w dokumentacji zwrócić uwagę na interakcje i zależności elementów systemu, które wpływają na zachowanie ciągłości jego działania.

Rekomenduje się, aby dokumentacja zapewniała opis wymagań istotnych dla bezpiecznego działania systemu np. scenariusze dotyczące podstawowych zachowań użytkowników w zależności od pełnionej roli (np. użytkownik, administrator, czy dyspozytor), elementy techniczne, w tym środowisko sieciowe oraz wymagania dotyczące interakcji i komunikacji z innymi systemami.

Dokumentacja powinna jasno i czytelnie opisywać mechanizmy komunikacji działające w systemie OT. Rekomenduje się, aby w dokumentacji były określone w szczególności: wykorzystane aktywne i pasywne elementy sieciowe, budowa i konfiguracja sieci, wszystkie połączenia sieciowe (fizyczne i logiczne), wykorzystane protokoły sieciowe.

2. https://rcb.gov.pl/wp-content/uploads/Standardy-s%C5%82u%C5%BC%C4%85ce-zapewnieniu-sprawnego-funkcjonowania-IK-%E2%80%93-dobre-praktyki-i-rekomendacje.pdf

Rekomenduje się, aby dokumentacja systemu zawierała również pakiet instrukcji dotyczących administrowania systemem, miedzy innymi: wykonywania kopii zapasowych, odtwarzania z kopii bezpieczeństwa, zasady i sposób wprowadzania oraz testowania aktualizacji systemu oraz instrukcje zarządzania jego bezpieczeństwem.

Rekomenduje się, aby istotne dane dotyczące systemów OT takie jak np. hasła, parametry konfiguracji systemów bezpieczeństwa, dane określone regulacjami prawnymi oraz dane istotne dla Spółek były przechowywane i przekazywane w formie zaszyfrowanej (np. poprzez zastosowanie odpowiednich protokołów lub zabezpieczenie na warstwie sieciowej transmisji lub systemu operacyjnego, gdy system na to nie pozwala).

3.7.1. Procedura zarządzania zmianą

Procedura ma na celu zapewnienie badania wpływu zmiany na bezpieczeństwo środowiska OT, z uwzględnieniem ich znaczenia dla zachowania ciągłości działania procesów technologicznych. Zmiana jest to czynność mająca na celu wprowadzenia modyfikacji w działaniu systemu OT. Procedura zawiera również informacje o ścieżce akceptacji, rekomenduje się wykorzystanie Macierzy RACI.

3.7.2. Zarządzanie dostępem stron trzecich

Procedura definiuje sposób realizacji współpracy ze stronami trzecimi. W szczególności opisuje sposób realizacji świadczenia wsparcia, w tym:

- zakresu uprawnień,
- realizacji połączeń w przypadku świadczenia serwisu zdalnego (np. dostęp do systemu lub jego elementów poprzez precyzyjnie zdefiniowany kanał),
- minimalnych wymagań monitorowania.

Rekomenduje się wykorzystanie, jednego punktu dostępu dla stron trzecich, poprzez rozwiązania klasy Privileged Account Management.

W przypadku potrzeby wykorzystania podmiotów zewnętrznych do serwisu lub wsparcia, każdorazowo w umowach należy umieścić zapis o pojedynczym punkcie kontaktu (np. pojedynczy numer telefonu, email, fax) oraz o sposobie komunikacji.

Zaleca się, aby w umowach z podmiotami zewnętrznymi, w stosunku do Spółki, znalazły się zapisy chroniące aktywa systemów OT. Komórka nadzoru nad bezpieczeństwem systemów OT jest odpowiedzialna za weryfikację zapisów umowy z podmiotami zewnętrznymi w stosunku do Spółki pod kątem ich wpływu na bezpieczeństwo tych systemów. W ramach komunikacji serwisu z systemem, należy określić metodę i sposób komunikacji serwisowej w kontekście oceny ryzyka i zachowania rozliczalności podejmowanych przez serwis działań.

Rekomenduje się, aby w całym zaplanowanym i określonym czasie funkcjonowania, Wykonawca zapewnił poprawki bezpieczeństwa dla wszystkich elementów systemu OT – także tych wytworzonych przez swoich podwykonawców, takie jak np. oprogramowanie układowe, systemy operacyjne, aplikacje bazodanowe, pakiety oprogramowania sterowania lub wizualizacji. Wykonawca powinien modernizować system, żeby zapewnić odporność na aktualne zagrożenia np. w przypadku uniemożliwiającym pozyskanie poprawek ze strony swoich podwykonawców.

3.7.3. Procedura zarządzania incydentami bezpieczeństwa

Procedura opisująca postępowanie w przypadku wystąpienia zdarzeń związanych z bezpieczeństwem systemów OT. Rekomenduje się utworzenie kategorii incydentów, w celu spójnej oceny stanu bezpieczeństwa poszczególnych systemów automatyki przemysłowej oraz określeniu ścieżek eskalacji.

Procedury zarządzania incydentami stanowią również element funkcjonowania SOC (patrz rozdz. 3.4).

3.7.4. Procedura zgłoszenia incydentów do Rządowego Zespołu Reagowania na Incydenty Komputerowe – CSIRT.GOV.PL

Przedmiotem procedury jest zdefiniowanie rodzaju (katalogu), formy i kanału przesyłania informacji o incydentach do Rządowego Zespołu Reagowania na Incydenty Komputerowe CSIRT.GOV.PL

3.7.5. Opis techniczny i biznesowy systemów OT

Procedura opisuje, jakie elementy winna zawierać dokumentacja systemu OT oraz jak przechowywać, przetwarzać i udostępniać w/w informacje. Zawiera ona w szczególności zbiór rekomendacji w zakresie niezbędnym do wypracowania właściwego, wspólnego i ujednoliconego szablonu opisu systemów OT.

3.7.6. Procedura nadawania i odbierania uprawnień do systemów OT

Dokument definiuje sposób nadawania i odbierania uprawnień do systemów OT. Określa poziomy uprawnień i sposób zakładania kont. Ponadto, procedura definiuje sposób dostępu i jego miejsce.

Rekomenduje się, aby dostęp do systemu był możliwy na podstawie imiennych kont dostępu. Nadanie i odebranie imiennego dostępu dla użytkownika systemu powinno być możliwe na podstawie wniosku bezpośredniego przełożonego oraz odnotowywane w dedykowanym rejestrze. W porozumieniu z producentem systemu, gdy jest to możliwe, aplikacje i usługi nie powinny być uruchamiane i wykorzystywane z poziomu uprawnień administratora systemu operacyjnego. W ramach aplikacji powinna być gradacja uprawnień użytkowników, zezwalająca lub zabraniająca na wykonanie sterowania na urządzeniach instalacji technologicznej.

Użytkownik otrzymuje uprawnienia do systemu zgodnie z zakresem jego czynności służbowych oraz zasadą „minimum koniecznego", oznaczającą udostępnianie najmniejszych, niezbędnych przywilejów i praw dostępu, które pozwalają na wykonywanie przypisanych do nich obowiązków. Uzyskanie dostępu dla użytkownika reprezentującego podmiot zewnętrzny wymaga dodatkowo zaakceptowania wymagań i postanowień z zakresu bezpieczeństwa obowiązujących w organizacji.

Mechanizmy uwierzytelniania powinny zostać zdefiniowane już na etapie projektowania i obejmować także istniejące elementy aktywne infrastruktury (np. router, switch, PLC, RTU). Uwierzytelnienie może być zrealizowane przy użyciu metod organizacyjnych, technicznych lub stanowić ich połączenie. Przykładowy mechanizm organizacyjny to wykorzystanie procedury przekazywania zmian służb ruchowych. Przykładowymi metodami technicznymi mogą być np. karty chipowe, czujniki biometryczne, monitoring miejsca wykonywania czynności ruchowych, umożliwiający identyfikację osoby i wykonywanych prac (w tym kombinacji użytkownik/hasło).

Rekomenduje się, aby system zarządzania uwierzytelnieniem (np. AD, Radius, PKI) był zlokalizowany geograficznie w tej samej lokalizacji, w której użytkuje się system OT i był używany we wszystkich systemach OT w danej lokalizacji geograficznej lub była zapewniona redundancja dostępu do w/w systemu. Wybór winien być określony na podstawie analizy ryzyka i w uzgodnieniu z głównymi interesariuszami (np. Dyrektor Majątku, Dyrektor IT, Główny Dyspozytor).

3.7.7. Procedura zarządzania podatnościami i aktualizacją systemów OT

Procedura definiuje sposób weryfikacji i pozyskiwania informacji o podatnościach, w tym „threat intelligence". Kolejno procedura określa sposób i częstotliwość dokonywania aktualizacji systemów OT w tym ścieżkę komunikacji w zakresie dokonywanej zmiany.

3.7.8. Procedura zarządzania Architekturą systemów OT

Dokument definiuje proces zarządzania architekturą systemów OT, uwzględniając warstwy:

- biznesową;
- aplikacyjną;
- danych;
- techniczną.

3.7.9. Procedura zarządzania odstępstwami

Celem dokumentu jest ustanowienie zasad postępowania w sytuacjach wymagających zastosowania odstępstw i wyjątków od obowiązujących w zakresie bezpieczeństwa systemów OT. Ponadto procedura definiuje zasady nadzoru nad odstępstwami w obszarze systemów OT.

3.7.10. Procedura – plany ciągłości działania

W celu opracowania Planów Ciągłości Działania dla zidentyfikowanych systemów należy określić dopuszczalne przerwy czasowe, które nie powodują nieodwracalnych lub trudnych do usunięcia strat. Stopień krytyczności mierzony jest czasem odzyskania częściowej kontroli nad instalacją technologiczną, pozwalającą na bezpieczne wyłączenie tej instalacji poprzez system OT lub przywrócenie działania systemu wspierającego systemy OT. Plany winny zawierać:

- informacje o aktywach objętych planem;
- kategorię systemu OT;
- zadania realizowane w procesie technologicznym;
- dokumentację systemu OT;
- informację o osobach odpowiedzialnych za funkcjonowanie systemu oraz elementów powiązanych;
- określenie akceptowalnego poziomu utraty informacji i czasu niedostępności systemu OT;
- działania do podjęcia w przypadku przewidywanego przekroczenia dopuszczalnego czasu odtworzenia;
- działania do podjęcia po przywróceniu systemu OT.

3.7.11. Procedura działań doskonalących

Procedura określa ścieżki przeprowadzenia cyklicznego przeglądu zarządzania w zakresie bezpieczeństwa systemów OT. Proces doskonalenia identyfikuje potrzeby w zakresie:

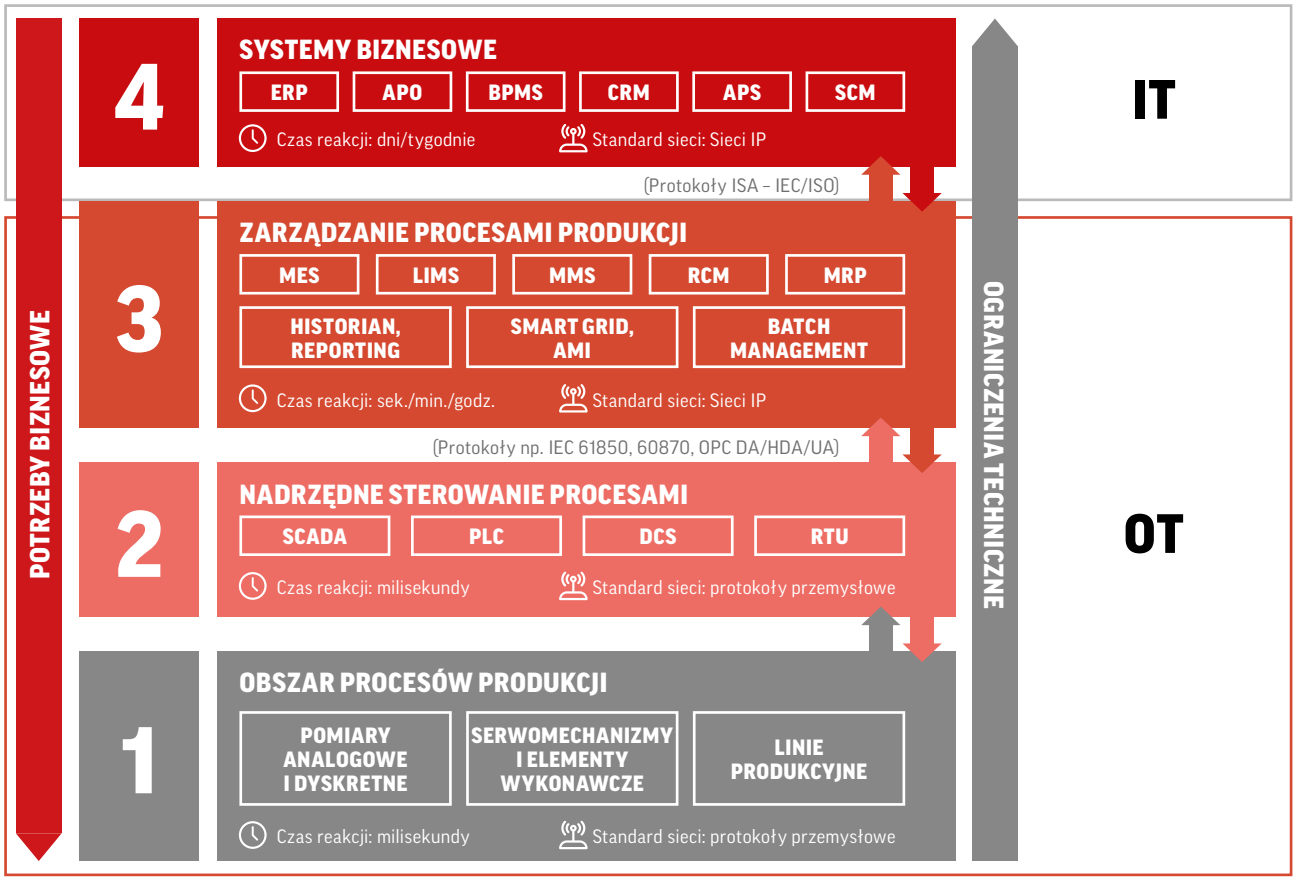
- organizacyjnym;
- technicznym;
- fizycznym.

4. CZĘŚĆ D – ARCHITEKTURA BEZPIECZEŃSTWA AUTOMATYKI PRZEMYSŁOWEJ

4.1. MODEL OPISU INFRASTRUKTURY IT/OT

Środowisko teleinformatyczne operatorów IK można przedstawić w postaci modelu warstwowego, którego najwyższą warstwę stanowią klasyczne systemy IT, a najniższą aparatura kontrolno-pomiarowa oraz elementy wykonawcze oddziałujące na procesy technologiczne. W zależności od wykorzystanego systemu IK i jego skali, środowisko teleinformatyczne operatora może składać się z jednej lub więcej warstw przedstawionych na poniższym modelu.

Model warstwowy środowiska OT/IT



Rys. 4

4.1.1. Warstwa 4 – Systemy biznesowe

Warstwa ta zawiera systemy IT wspierające funkcjonowanie procesów biznesowych przedsiębiorstw, np. poczta elektroniczna, systemy klasy ERP (systemy służące do zarządzania zasobami przedsiębiorstwa), systemy CRM (systemy służące do zarządzania kontaktami z klientami).

4.1.2. Warstwa 3 – Zarządzanie procesami produkcji

Systemy warstwy integracji odpowiadają za gromadzenie danych, zaawansowaną analitykę, raportowanie i udostępnianie informacji do systemów IT. Przykładem systemów warstwy integracji są: historia, systemy klasy MES (systemy służące do zbierania informacji o procesie produkcyjnym), czy MRP (systemy służące do planowania zapotrzebowania na zasoby materiałowe).

4.1.3. Warstwa 2 – Nadrzędne sterowanie procesami

Systemy te pełnią rolę interfejsu użytkownika dla operatorów/dyspozytorów i pozwalają na monitorowanie oraz sterowanie (również zdalne) procesem technologicznym. Systemy i urządzenia tej warstwy w sposób bezpośredni oddziałują na proces technologiczny. W warstwie tej wyróżniamy następujące systemy:

- serwery aplikacji SCADA/DCS;
- stacje operatorskie i inżynierskie;
- serwery baz danych;
- macierze dyskowe;
- interfejsy użytkownika;
- inne (np. serwery systemu prognozowania).

4.1.4. Warstwa 1 – Obszar procesów produkcji

Warstwą, która jest najbliżej infrastruktury i procesu przemysłowego jest warstwa aparatury kontrolno-pomiarowej i elementów wykonawczych. Zawiera ona elementy pomiarowe, pozwalające monitorować stan procesu technologicznego oraz elementy wykonawcze, pozwalające zmieniać stan procesu technologicznego.

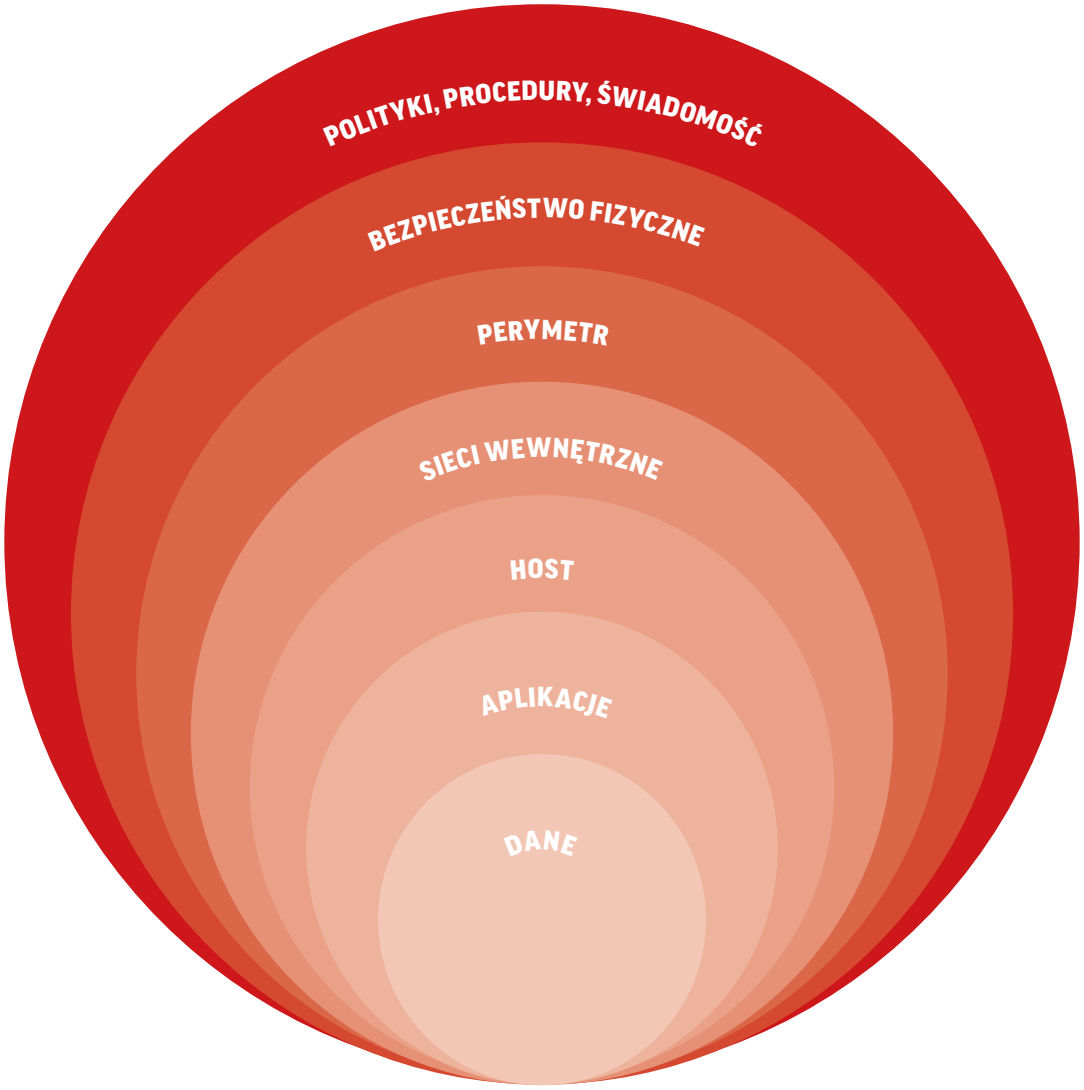
4.2. KONCEPCJA OCHRONY WARSTWOWEJ I JEJ ELEMENTY

Jednym z podstawowych sposobów na ochronę jest podział na strefy ochrony (stref ograniczonego dostępu) i zaprojektowanie ich zgodnie z zasadą ochrony w głąb (ang. *Defense-In-Depth*). Polega ona na wprowadzeniu wielu, niezależnych warstw zabezpieczeń. Każda z warstw musi być zaprojektowana w celu maksymalnego spowolnienia (uniemożliwienia) działań potencjalnego napastnika, a natężenie sił i środków ochrony powinno rosnąć w miarę „zbliżania się" potencjalnych napastników do strefy chroniącej kluczowe elementy infrastruktury OT organizacji. Ochrona warstwowa ma minimalizować ryzyko uzyskania dostępu do chronionego zasobu, jednocześnie podnosząc prawdopodobieństwo wykrycia takiej próby.

Zintegrowany system bezpieczeństwa ma zastosowanie w obszarze bezpieczeństwa fizycznego, organizacyjnego i teleinformatycznego.

Zaleca się, aby środowisko automatyki przemysłowej było wyposażone w podstawowe komponenty zintegrowanego systemu bezpieczeństwa:

- monitorowanie komunikacji sieciowej na styku z siecią biznesową;
- system kontroli plików na zawartość złośliwego kodu;
- monitorowanie zdarzeń bezpieczeństwa;
- system zarządzania podatnościami i aktualizacjami bezpieczeństwa;
- system ochrony przed złośliwym oprogramowaniem opartego na technologii „whitelistingu";
- system detekcji ataków sieciowych na styku z siecią biznesową.



Rys. 5

Poniżej wskazano elementy składowe zintegrowanego systemu bezpieczeństwa w podziale na ich przeznaczenie:

- przeciwdziałanie (ang. *prevention*);
- zniechęcanie (ang. *deter*);
- wykrywanie (ang. *detect*);
- opóźnianie (ang. *delay*);
- ocenianie (ang. *assess*).

4.3. BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

Bezpieczeństwo fizyczne i środowiskowe ma zapewnić efektywną ochronę przed:

- negatywnym wpływem środowiska na systemy OT (zasilanie, temperatura, wilgotność, itp.);
- nieautoryzowanym dostępem fizycznym;
- fizyczną manipulacją, modyfikacją, kradzieżą, zniszczeniem systemów, infrastruktury, mediów komunikacyjnych, ludzi i obiektów budowlanych;
- nieautoryzowaną możliwością obserwacji i utrwalenia wrażliwych informacji;
- nieautoryzowaną instalacją nowej infrastruktury;

- instalacją urządzeń umożliwiających zdalny nadzór, podsłuch lub inny negatywny wpływ na środowisko OT.

Zapewnienie bezpieczeństwa fizycznego to zespół działań proceduralnych, organizacyjnych i technicznych, mających na celu minimalizację ryzyka zakłócenia funkcjonowania wykorzystywanych systemów sterowania przemysłowego w następstwie działań osób, które w sposób nieuprawniony podjęły próbę dostania się lub znalazły się na terenie IK. Składają się na nie m.in. bezpośrednia ochrona fizyczna oraz zabezpieczenia techniczne (elektroniczne i budowlano-mechaniczne).

System bezpieczeństwa fizycznego powinien zapewnić:

- prewencję;
- wykrycie;
- przekazanie informacji o wykryciu intruza (alarmowanie);
- opóźnienie intruza w dotarcia do stref chronionych;
- reakcje/interwencję za zdarzenie.

Oprócz wymienionych funkcji system bezpieczeństwa fizycznego spełniać może funkcje odstraszania napastnika np. na etapie prewencji (np. tablice informujące), alarmowania (sygnalizatory zewnętrzne) oraz interwencji (wezwanie do zachowania zgodnego z prawem). Częściowo realizowana jest także funkcja dowodowa w przypadku systemów dozoru wizyjnego.

Zaznaczyć należy, że żadne działania zmierzające do zapewnienia bezpieczeństwa fizycznego nie zapewnią całkowitego bezpieczeństwa. Środki ochronne zwiększają jedynie prawdopodobieństwo skutecznego przeciwdziałania.

Implementacja systemu bezpieczeństwa fizycznego powinna przebiegać w następujących krokach:

- ustalenie chronionych elementów;
- przyjęcie podstawowych założeń projektowych dla systemu (ustalenie kto może być potencjalnym atakującym i jego charakterystyki);
- ocena koniecznych czasów opóźnień dla przewidywanych scenariuszy ataku;
- ustalenie chronionych stref i zasad dostępu do nich;
- ustalenie technicznych środków wspomagających (zabezpieczenia technicznego);
- opracowanie procedur pracy systemu (w tym ludzi);
- zainstalowanie i konfiguracja elementów systemu;
- test systemu;
- przegląd procedur;
- test całego systemu bezpieczeństwa;
- systematyczne przeglądy systemu.

Przyjęcie założeń dotyczących wiedzy, umiejętności, wyposażenia oraz determinacji potencjalnych intruzów jest kluczowym elementem projektowania systemu bezpieczeństwa fizycznego.

Dokumentem stanowiącym odniesienie do wyboru konkretnych rozwiązań organizacyjnych, osobowych lub technicznych są wytyczne dotyczące zapewnienia bezpieczeństwa fizycznego infrastruktury krytycznej, zawarte w załączniku nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej[3]. Wybór określonych rozwiązań jest uzależniony od oceny ryzyka zakłócenia funkcjonowania IK, możliwości technicznych oraz finansowych operatora.

3. https://rcb.gov.pl/wp-content/uploads/Standardy-s%C5%82u%C5%BC%C4%85ce-zapewnieniu-sprawnego-funkcjonowania-IK-%E2%80%93-dobre-praktyki-i-rekomendacje.pdf

4.4. BEZPIECZEŃSTWO TELEINFORMATYCZNE

4.4.1. Izolacja ruchu pomiędzy systemami sterowanymi

Z punktu widzenia kierunków komunikacji, transmisja pomiędzy systemem sterującym a systemami sterowanymi powinna odbywać się na zasadzie punkt-punkt, z realizacją naczelnej zasady „najmniejszych, niezbędnych uprawnień". Coraz powszechniej wykorzystywany protokół IP **w sieciach zbudowanych w oparciu o protokół Ethernet** daje możliwość zestawiania połączeń pomiędzy różnymi obiektami w sieci – z punktu widzenia bezpieczeństwa transmisje takie powinny zostać ograniczone do minimum niezbędnego do wykonywania pracy. W przeciwnym przypadku napastnik, który uzyskał dostęp do sieci obsługującej urządzenia sterowane może wykorzystać to do ataku na kolejne elementy systemu (stacje dyspozytorskie, inne urządzenia sterujące).

Realizacja:

- na poziomie poszczególnych instalacji wykorzystanie podziału sieci w warstwie logicznej, dla protokołu Ethernet może to być podział na podsieci za pomocą tzw. VLAN-ów (802.1q) tak, aby minimalizować możliwość wzajemnego komunikowania się urządzeń, które nie potrzebują tego do poprawnej pracy;
- w warstwie IP poprzez odpowiednie polityki routingu, uniemożliwiające komunikowanie się systemom do tego nieprzewidzianym – dotyczy to komunikacji pomiędzy sieciami logicznymi w ramach obiektu jak i pomiędzy obiektami;
- stosowanie firewalli z odpowiednimi listami kontroli dostępu;
- stosowanie szyfrowanych kanałów transmisji pomiędzy systemem sterującym, a sterowanym.

4.4.2. Zapewnienie poufności i wiarygodności komunikatów sterujących

Należy upewnić się, że transmisja nie jest podatna na podsłuchanie lub zafałszowanie (również: podszycie się). W przypadku transmisji na duże dystanse, przy wykorzystaniu sieci dzierżawionych od innych podmiotów (np. APN dla transmisji GSM/LTE), nie można mieć całkowitej pewności bezpieczeństwa takiej transmisji. Może ona zostać zakłócona nie tylko na skutek świadomego działania napastnika, ale też na skutek awarii lub błędów ludzkich.

Realizacja:

- uwierzytelnianie komend sterujących oferowane przez wersje protokołu DNP3 jako zabezpieczenie w warstwie protokołu aplikacyjnego wg. modelu OSI;
- wykorzystanie protokołu TLS lub jego następców jako zabezpieczenie w warstwie prezentacji modelu OSI;
- wykorzystanie bezpiecznych połączeń VPN tzn. zbudowanych za pomocą technologii zakładających szyfrowanie danych przesyłanych tunelem i uwierzytelnianie klienta/serwera zestawiających między sobą tunel.

Jeśli bezpieczna transmisja realizowana jest za pośrednictwem dodatkowego urządzenia (co często ma miejsce w przypadku połączeń VPN) należy pamiętać o zabezpieczeniu połączenia z chronionym urządzeniem (np. sterownikiem stacyjnym) poprzez odpowiednie zaprojektowanie sieci i wykorzystanie mechanizmów – zarówno fizycznych, utrudniających np. odłączenie kabla ethernetowego jak i konfiguracyjnych, np. wykorzystanie funkcji „port-based MAC security – utrudniających podszycie się pod chronione urządzenie.

Zaszyfrowanie transmisji nie zwalnia z obowiązku zapewnienia izolacji i kontroli ruchu – napastnik może przejąć kontrolę nad wyniesionym urządzeniem sterującym bądź zastąpić takie urządzenie własnym.

4.4.3. Zachowanie kontroli nad siecią

Podczas projektowania, eksploatacji i rozwijania sieci należy dbać o posiadanie aktualnej wiedzy na temat budowy sieci, szczególnie miejsc wymiany ruchu pomiędzy poszczególnymi sieciami oraz o zachowanie kontroli nad zdarzeniami w niej zachodzącymi. W sieci powinny znajdować się punkty, które umożliwiają dostęp do nieszyfrowanej transmisji, pozwalające na jej analizę w zakresie poprawności i integralności. Bez wiedzy na temat miejsc, w których może zachodzić transmisja pomiędzy wydzielonymi podsieciami, nie mamy możliwości świadomego kształtowania i kontrolowania transmisji w sieci. Nie wiemy też, które miejsca powinny podlegać naszej obserwacji. Bez obserwacji zdarzeń zachodzących w sieci nie będziemy świadomi niepożądanych zachowań, takich jak np.:

- próba zestawienia transmisji pomiędzy urządzeniami, które nie powinny tego robić (w zależności od możliwości naszej infrastruktury zostaniemy poinformowani o braku możliwości przekazania takiego ruchu czy to z warstwy odpowiadającej za routing czy to z poziomu access-listy firewalla);
- nieautoryzowane zamiany urządzeń (próbę podpięcia się w miejsce np. sterownika);
- pojawienie się w sieci nieautoryzowanych urządzeń (co może wskazywać zarówno na próbę ataku jak również sygnalizować zaniedbania obowiązków – takich jak obowiązek wyłączenia zbędnych portów dostępowych ze strony pracowników lub podwykonawców).

Realizacja:

- planowe, kontrolowane rozwijanie sieci;
- ewidencja sieci (paszportyzacja);
- wdrożenie systemu monitorowania sieci, w szczególności wdrożenie rozwiązań dedykowanych dla środowiska OT;
- agregacja i korelacja w systemach klasy SIEM.

ZAŁĄCZNIK NR 1 – SKRÓTY I DEFINICJE

Atak
Celowe i zaplanowane działanie, mające na celu zakłócenie lub zatrzymanie pracy systemów automatyki przemysłowej (systemów OT).

Administrator biznesowy systemu OT
Określony podmiot odpowiedzialny pod względem biznesowym i merytorycznym za poprawność i bezpieczeństwo informacji przetwarzanych przez system OT.

Administrator techniczny systemu OT
Określony podmiot odpowiedzialny za utrzymanie ciągłości działania i prawidłowości funkcjonowania danego systemu OT w zakresie określonych funkcjonalności bez uprawnień do samodzielnego wprowadzania zmian w zakresie urządzeń Instalacji Technologicznej.

AMI
Zaawansowana infrastruktura pomiarowa (ang. *Advanced Metering Infrastructure*).

BIA – (ang. *Business Impact Analysis*)
Analiza wpływu na działalność (Business Impact Analysis) to proces analizy funkcji biznesowych pozwalający określić, jaki wpływ na działalność organizacji miałoby ich ewentualne poważne zakłócenie lub przerwanie procesu.

Centrum sterowania/Dyspozycja/Dyspozytura
Lokalizacja służąca do zarządzania określoną grupą zasobów. Zarządzanie jest najczęściej realizowane w oparciu o tablice synoptyczne prezentowane na ekranach nadrzędnych systemów monitorowania i sterowania (SCADA lub DCS). W starszych instalacjach tablice synoptyczne mogą być realizowane w oparciu o elementy elektryczne (lampki, przełączniki) oraz elektroniczne (np. wyświetlacze cyfrowe).

CRM
Zarządzanie relacjami z klientami (ang. *Customer Relationship Management*).

DoS (ang. *Denial of Service*) – Blokada usługi
Zakłócenie lub uniemożliwienie autoryzowanego dostępu do systemu, dostępu do zasobów systemu lub też opóźnienie lub zakłócenie pracy samego systemu.

DMS (ang. *Distributed Management System*) – Rozproszony System Sterowania
Rozproszony system sterowania zakładów i obiektów technologicznych ze zintegrowanymi funkcjami sterowania, wizualizacji i nadzoru, wykorzystujący jedną wspólną bazę danych pomiarowo-sterujących, pracujący w systemie czasu rzeczywistego.

DMZ (ang. *Demilitarized Zone*)
Logicznie wydzielony segment sieci, znajdujący się pomiędzy siecią wewnętrzną i siecią zewnętrzną. W kontekście najlepszych praktyk bezpieczeństwa automatyki przemysłowej, DMZ jest najczęściej rozumiany jako pośredniczący segment sieci pomiędzy siecią użytkowników biurowych a sieciami systemów wspierających procesy przemysłowe.

ERP
Planowanie zasobów przedsiębiorstwa (ang. *Enterprise Resource Planning*).

Brama sieciowa (ang. *Gateway*)
Mechanizm pośredniczący w komunikacji dwóch odrębnych sieci komputerowych lub serwer pośredniczący w komunikacji pomiędzy dwoma odrębnymi systemami OT lub IT (systemami różniącymi się celem zastosowania).

HMI (ang. *Human Machine Interface*) – Interfejs człowiek-maszyna
Element/zespół elementów, najczęściej z własnym wyświetlaczem, służący do interakcji użytkownika z maszyną lub do oddziaływania na proces technologiczny np. panel operatorski, panel komputerowy.

Incydent bezpieczeństwa OT/Incydent
Pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z odmiennym zachowaniem systemu, które stwarzają znaczne prawdopodobieństwo zakłócenia procesów technologicznych oraz działań biznesowych.

Infrastruktura krytyczna
Zgodnie z ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym przez Infrastrukturę Krytyczną należy rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy:

- zaopatrzenia w energię, surowce energetyczne i paliwa;
- łączności;
- sieci teleinformatycznych;
- finansowe;
- zaopatrzenia w żywność;
- zaopatrzenia w wodę;
- ochrony zdrowia;
- transportowe;
- ratownicze;
- zapewniające ciągłość działania administracji publicznej;
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Klient
Urządzenie lub aplikacja, które komunikują się z serwerem.

Kontrola dostępu
Ochrona systemu przed nieautoryzowanym dostępem logicznym lub fizycznym, obejmująca proces pozwalający monitorować i regulować dostęp do zasobów systemu, zgodnie z przyjętymi zasadami bezpieczeństwa.

Kryptografia
Zestaw środków i metod, mających na celu zabezpieczenie przesyłanych informacji przed nieupoważnionym dostępem, przykładowo poprzez szyfrowanie.

LAN – Sieć lokalna (ang. *Local Area Network*)
Lokalna sieć komputerowa, łącząca zasoby sieciowe znajdujące w ograniczonej odległości.

MES –System Realizacji Produkcji (ang. *Manufacturing Execution Systems*)
System umożliwiający efektywne zbieranie informacji w czasie rzeczywistym ze stanowisk produkcyjnych oraz transfer tych informacji na obszar biznesowy.

Model referencyjny
Struktura pozwalającą w spójny sposób opisać elementy oraz interfejsy systemu.

MRP
Planowanie zapotrzebowania materiałowego (ang. Material Requirements Planning).

OPC (ang. *OLE for process control*)
Jeden ze standardów komunikacji przeznaczony do łączenia aplikacji bazujących na systemach operacyjnych ogólnego stosowania (np. Windows) ze sprzętem i oprogramowaniem aplikacyjnym automatyki przemysłowej.

PLC (ang. *Programmable Logic Controller*)
Programowalne urządzenie mikroprocesorowe, które realizuje akwizycję sygnałów pomiarowych i generuje na ich podstawie sygnały sterujące, zgodnie z zaimplementowanym algorytmem.

Sterownik PLC to urządzenie elektroniczne, zaprojektowane do warunków przemysłowych, wyposażone w pamięć programowalną, wykorzystywaną do realizacji funkcji za pomocą instrukcji logicznych, arytmetycznych, czasu i zliczania w celu realizacji sterowania procesami technologicznymi poprzez cyfrowe i analogowe sygnały wejściowe i wyjściowe.

Podatność
Cecha charakterystyczna systemu np. luka w implementacji, działaniu bądź zarządzaniu systemu, która pozwala na zakłócenie jego pracy lub złamanie przyjętej polityki bezpieczeństwa.

Polityka bezpieczeństwa
Zestaw reguł, instrukcji, standardów i procedur, określający, w jaki sposób organizacja chroni swoje zasoby.

RTU (ang. *Remote Terminal Unit*) – zdalny terminal
Uniwersalne urządzenie służące do zdalnego monitorowania i sterowania różnymi urządzeniami i systemami automatyki. Jest on zwykle wdrażany w środowisku przemysłowym i służy w podobny sposób programowalnym obwodom logicznym (PLC), ale w wyższym stopniu. RTU jest uważany za samodzielny komputer, ponieważ ma wszystkie podstawowe części, które razem definiują komputer: procesor, pamięć i pamięć masową. Z tego powodu może być używany jako inteligentny kontroler lub kontroler nadrzędny dla innych urządzeń, które razem automatyzują proces.

SIS (ang. *Safety Instrumented System*) – Przyrządowy System Bezpieczeństwa także System Automatyki Zabezpieczeniowej

Specjalnie zaprojektowane rozwiązania umożliwiające odstawienie do bezpiecznego punktu pracy instalacji w przypadku wykrycia zdarzeń z obszaru ryzyka nietolerowanego przez daną organizację np.

- systemy awaryjnego zatrzymania ESD,
- systemy bezpiecznego zatrzymania SSD.

SIL (ang. *Safety Integrity Level*) – Poziom Nienaruszalności Bezpieczeństwa
Wartość (od 1 do 4), określająca wymagany poziom tolerancji zagrożenia wyrażony poprzez oczekiwany poziom niezawodności funkcji bezpieczeństwa zaimplementowanych w SIS. Poziomy nienaruszalności zostały określone przez normy EN61508, EN62061.

SCADA (ang. *Supervisory Control And Data Acquisition*)
Aplikacja służąca do monitorowania stanu procesu technologicznego i przekazywania poleceń operatów do systemów sterowania. Do innych, podstawowych funkcji SCADA należą: akwizycja danych pomiarowych, prezentacja przebiegów czasowych, alarmowanie. Aplikacja SCADA stanowi najczęściej główny element systemów sterowania, monitoringu i akwizycji danych pomiarowych, pracujących w strukturze rozproszonej geograficznie i wykorzystujących różne grupy urządzeń pomiarowo-sterujących.

System
Zbiór powiązanych ze sobą elementów sprzętowych i oprogramowania, realizujących wspólnie co najmniej jedną funkcję.

System OT (ang. *Operational Technology*)
Systemy teleinformatyczne, które realizują funkcje nadzoru, zarządzania, sterowania, regulacji, pomiaru, monitoringu, bezpieczeństwa (lub kilku tych funkcji łącznie) dla procesów technologicznych i przemysłowych. Systemy te, w literaturze oraz istniejących standardach, są alternatywnie nazywane: ICS (ang. Industrial Control Systems).

System bezpieczeństwa
System nadzorujący lub kontrolujący poprawność i ciągłość pracy zarówno całych systemów OT, jak również ich aplikacji, usług i elementów, w tym telekomunikacyjnych i teletransmisyjnych wykorzystywanych w systemach OT.

Urządzenia sterujące
Zbiór wszelkich systemów i urządzeń, biorących udział w sterowaniu procesem technologicznym. Grupa ta obejmuje m.in. sensory, przetworniki pomiarowe, elementy wykonawcze, urządzenia realizujące algorytmy sterujące (PLC, kontrolery DCS), nadrzędne systemy sterowania (SCADA, HMI).

Uwierzytelnianie
Środki bezpieczeństwa, mające na celu potwierdzenie wiarygodności połączenia, wiadomości lub też potwierdzenie dostępu danego użytkownika do zastrzeżonych zasobów.

VLAN (ang. *Virtual Local Area Network)*
Wirtualna, lokalna sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej.

WAN (ang. *Wide Area Network, rozległa sieć komputerowa*)
Sieć komputerowa znajdująca się na obszarze wykraczającym poza miasto, kraj, kontynent, łącząc ze sobą urządzenia rozmieszczone na dużych obszarach.

Zasób
Fizyczny bądź logiczny obiekt, posiadany przez bądź powierzony organizacji, mający dla niej faktyczną bądź umowną wartość.

Zdarzenie
Usterka lub potencjalna przyczyna incydentu mogącego wywołać szkodę w systemie OT.

ZAŁĄCZNIK NR 2 – PRZYKŁADOWE MIERNIKI BEZPIECZEŃSTWA SYSTEMÓW AUTOMATYKI PRZEMYSŁOWEJ W ELEKTROENERGETYCE

Cel	Miernik	Źródło danych	Sposób pomiaru	Wartość oczekiwana	Częstotliwość oceny
Ustanowienie ram zarządzania w celu zainicjowania, zarządzania wdrożeniem i eksploatacji bezpieczeństwa OT wewnątrz organizacji	z – liczba zdefiniowanych ról związanych z bezpieczeństwem OT y – liczba zdefiniowanych ról związanych z bezpieczeństwem OT, do których są przypisane osoby	Przypisane role w ramach wewnętrznych regulacji	X= (y/z)*100%	X=100%	rocznie
Zapewnienie bezpieczeństwa dostępu zdalnego	z – liczba incydentów związanych z dostępem z sieci publicznej do sieci OT bez dodatkowego mechanizmu uwierzytelniającego	Rejestr incydentów bezpieczeństwa	X=z	X=0	rocznie
Zapewnienie, że pracownicy i kontrahenci są świadomi oraz wypełniają swoje obowiązki związane z bezpieczeństwem OT	z – liczba osób (pracowników, wykonawców, użytkowników reprezentujących stronę trzecią), która powinna zostać przeszkolona z zakresu bezpieczeństwa OT y – liczba osób, która została przeszkolona z zakresu bezpieczeństwa OT	Rejestr szkoleń bezpieczeństwa informacji	X= (y/z)*100%	X=100%	rocznie
Identyfikacja aktywów OT organizacji oraz określenie odpowiedzialności za ich ochronę	z – liczba wykrytych przypadków aktywów OT bez przypisanego właściciela	Rejestr incydentów bezpieczeństw, wyniki audytów, przeglądów oraz innych działań monitorujących	X=z	X=0	rocznie
Zapewnienie, że informacje dotyczące systemów OT uzyskują ochronę na odpowiednim poziomie, zgodnym z ich znaczeniem dla organizacji	z – liczba wykrytych przypadków źle sklasyfikowanej informacji o systemach OT (np. dokumentacja techniczna, dane pomiarowe itp.)	Rejestr incydentów bezpieczeństw, wyniki audytów, przeglądów oraz innych działań monitorujących	X=z	X=0	rocznie

Cel	Miernik	Źródło danych	Sposób pomiaru	Wartość oczekiwana	Częstotliwość oceny
Zapobieganie nieautoryzowanemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu informacji dotyczących systemów OT	z – liczba incydentów związanych z naruszeniem zasad postępowania z informacjami dotyczących systemów OT	Rejestr incydentów bezpieczeństw, wyniki audytów, przeglądów oraz innych działań monitorujących	X=z	X=0	rocznie
Ograniczenie dostępu do systemów OT i systemów wspierających	z – liczba wykrytych nieautoryzowanych dostępów do sieci i do usług sieciowych w obszarze systemów OT	Rejestr incydentów bezpieczeństw, wyniki audytów, przeglądów oraz innych działań monitorujących	X=z	X=0	rocznie
Zapewnienie dostępu autoryzowanym użytkownikom i zapobieganie nieuprawnionemu dostępowi do systemów OT i do systemów wspierających	z – wybrana próbka użytkowników (dla wybranych systemów) y – liczba użytkowników, którym poprawnie przydzielono prawa dostępu na podstawie procedury (odpowiednie wnioski i akceptacje)	Wyniki audytów, przeglądów oraz innych działań monitorujących	X= (y/z)*100%	X=100%	rocznie
Uczynienie użytkowników odpowiedzialnymi za zabezpieczenie ich danych uwierzytelniających	z – liczba incydentów związanych z naruszeniem zasad bezpieczeństwa systemów OT przez użytkowników	Rejestr incydentów bezpieczeństw	X=z	X=0	rocznie
Ochrona przed nieautoryzowanym dostępem do systemów OT	z – liczba wykrytych przypadków niewłaściwie zdefiniowanych/ograniczonych praw	Wyniki audytów, przeglądów oraz innych działań monitorujących	X=z	X=0	rocznie
Zapewnienie właściwego i efektywnego użycia kryptografii do ochrony integralności danych systemów OT	z – liczba wykrytych przypadków niestosowania zabezpieczeń kryptograficznych, tam gdzie jest to wymagane i możliwe	Wyniki audytów, przeglądów oraz innych działań monitorujących	X=z	X=0	rocznie

Cel	Miernik	Źródło danych	Sposób pomiaru	Wartość oczekiwana	Częstotliwość oceny
Zapewnienie ochrony przed nieautoryzowanym dostępem fizycznym, uszkodzeniami lub zakłóceniami w odniesieniu do systemów OT i ich komponentów należących do organizacji	z – liczba wszystkich wejść (per lokalizacja) y – liczba nieautoryzowanych wejść do stref	Rejestr incydentów bezpieczeństw	X= (y/z)*100%	X=100%	rocznie
Zapobieganie utracie, uszkodzeniu, kradzieży lub naruszeniu infrastruktury systemów OT oraz przerwaniu działalności organizacji	z – liczba wykrytych przypadków związanych z nieautoryzowanym dostępem do sprzętu wchodzącego w skład systemów OT	Rejestr incydentów bezpieczeństw	X=z	X=0	rocznie
Zapewnienie prawidłowej i bezpiecznej eksploatacji systemów OT	z – liczba wykrytych przypadków braku procedur eksploatacyjnych tam, gdzie są one wymagane	Wyniki audytów, przeglądów oraz innych działań monitorujących	X=z	X=0	rocznie
Zapewnienie ochrony Systemów OT przed szkodliwym oprogramowaniem	z – liczba wszystkich zarejestrowanych ataków przy użyciu szkodliwego oprogramowania y – liczba ataków zakończonych niepowodzeniem	Wyniki audytów, przeglądów oraz innych działań monitorujących	X= (y/z)*100%	X=100%	rocznie
Ochrona przed utratą konfiguracji oraz istotnych danych systemów OT	z – liczba systemów, dla których wymagany jest backup y – liczba systemów rzeczywiście objętych backupem	Wyniki audytów, przeglądów oraz innych działań monitorujących	X= (y/z)*100%	X=100%	rocznie
Rejestracja zdarzeń i monitorowania	z – liczba systemów, w których zdarzenia powinny być logowane zgodnie z określonymi wymaganiami y – liczba systemów, w których zdarzenia są logowane zgodnie z określonymi wymaganiami (np. centralny log)	Wyniki audytów, przeglądów oraz innych działań monitorujących	X= (y/z)*100%	X=100%	rocznie

Cel	Miernik	Źródło danych	Sposób pomiaru	Wartość oczekiwana	Częstotliwość oceny
Zapewnienie integralności środowiska pracy systemów OT (systemów operacyjnych)	z – liczba incydentów związana z niekontrolowaną instalacją oprogramowania na eksploatowanych systemach OT	Rejestr incydentów bezpieczeństw	X=z	X=0	rocznie
Ochrona przed wykorzystaniem podatności technicznych infrastruktury systemów OT	z – liczba awarii systemów, spowodowanych podatnościami technicznymi	Rejestr incydentów bezpieczeństw	X=z	X=0	rocznie
Minimalizacja oddziaływania czynności audytowych na systemy OT	z – liczba audytów, wobec których jednostki odpowiedzialne za systemy OT zgłosiły zakłócenie funkcjonowania procesów operacyjnych	Wyniki audytów, przeglądów oraz innych działań monitorujących	X=z	X=0	rocznie
Zapewnienie ochrony w sieciach wykorzystywanych w systemach OT	z – liczba wszystkich zarejestrowanych ataków sieciowych y – liczba ataków sieciowych zakończonych niepowodzeniem	Wyniki audytów, przeglądów oraz innych działań monitorujących	X= (y/z)*100%	X=100%	rocznie
Utrzymanie bezpieczeństwa systemów OT i ich infrastruktury wewnątrz organizacji oraz z każdym podmiotem zewnętrznym	z – liczba incydentów związanych z naruszeniem zasad wymiany informacji (ujawnienia, utraty, itp.)	Rejestr incydentów bezpieczeństw	X=z	X=0	rocznie
Zapewnienie, że bezpieczeństwo OT jest integralną częścią systemów OT w całym okresie życia	z – liczba nowych systemów niezaopiniowanych przez właściwą jednostkę organizacyjną odpowiedzialną za bezpieczeństwo systemów OT	Wyniki audytów, przeglądów oraz innych działań monitorujących	X=z	X=0	rocznie
Zapewnienie, że bezpieczeństwo systemów OT jest zaprojektowane i wdrożone w ramach cyklu rozwoju systemów	z – liczba zmian wdrożonych niezgodnie z obowiązującymi procedurami (dotyczy również testowania)	Wyniki audytów, przeglądów oraz innych działań monitorujących	X=z	X=0	rocznie

Cel	Miernik	Źródło danych	Sposób pomiaru	Wartość oczekiwana	Częstotliwość oceny
Zapewnienie ochrony danych testowych wykorzystywanych do testowania pracy systemów OT	z – liczba przypadków niekontrolowanego wykorzystywania danych testowych	Wyniki audytów, przeglądów oraz innych działań monitorujących	X=z	X=0	rocznie
Zapewnienie ochrony systemów OT, które są dostępne dla dostawców	z – liczba umów ze stronami trzecimi z ujawnionymi brakami w zakresie wymagań bezpieczeństwa	Wyniki audytów, przeglądów oraz innych działań monitorujących	X=z	X=0	rocznie
Utrzymanie odpowiedniego poziomu bezpieczeństwa systemów OT i dostarczanie usług zgodnie z umowami serwisowymi zawartymi z dostawcami	z – liczba zaplanowanych przeglądów usług strony trzeciej y – liczba przeprowadzonych przeglądów usług strony trzeciej	Umowy SLA, OLA	X= (y/z)*100%	X=100%	rocznie
Zapewnienie, że stosowane jest spójne i skuteczne podejście do zarządzania incydentami związanymi z bezpieczeństwem informacji z uwzględnieniem komunikacji zdarzeń związanych z bezpieczeństwem oraz słabości systemów OT	z – liczba incydentów związanych z bezpieczeństwem systemów OT y – liczba incydentów związanych z bezpieczeństwem systemów OT, których czas przyjęty na rozwiązanie/ zamknięcie incydentu został przekroczony	Rejestr incydentów bezpieczeństw	X= (y/z)*100%	X=100%	rocznie
Ciągłość bezpieczeństwa systemów OT powinna być osadzona w systemach zarządzania ciągłością działania organizacji	z – liczba incydentów bezpieczeństwa związanych z naruszeniem ciągłości działania	Wyniki audytów, przeglądów oraz innych działań monitorujących	X=z	X=0	rocznie
Unikanie naruszenia przepisów prawa, regulacji wewnętrznych, wytycznych organów nadzoru, wymagań wynikających z umów oraz jakichkolwiek wymagań bezpieczeństwa w obszarze systemów OT	z – liczba zastrzeżeń lub kar związanych z niewłaściwą współpracą z organami władzy	Dokumenty	X=z	X=0	rocznie

Cel	Miernik	Źródło danych	Sposób pomiaru	Wartość oczekiwana	Częstotliwość oceny
Zapewnienie, że bezpieczeństwo systemów OT zostało zaimplementowane i jest zarządzane w zgodzie z politykami i procedurami organizacji	z – ilość zaplanowanych przeglądów bezpieczeństwa systemów OT y – ilość wykonanych przeglądów systemów OT	Wyniki audytów, przeglądów oraz innych działań monitorujących	X= (y/z)*100%	X=100%	rocznie

RCB
Rządowe Centrum
Bezpieczeństwa

ul. Rakowiecka 2A
00-993 Warszawa
e-mail: poczta@rcb.gov.pl