2019

STANDARDY I DOBRE PRAKTYKI OCHRONY INFRASTRUKTURY KRYTYCZNEJ

AUTOMATYKA PRZEMYSŁOWA W SEKTORZE ROPY I GAZU

RCB
Rządowe Centrum Bezpieczeństwa

2019

STANDARDY I DOBRE PRAKTYKI OCHRONY INFRASTRUKTURY KRYTYCZNEJ

AUTOMATYKA PRZEMYSŁOWA W SEKTORZE ROPY I GAZU

RCB
Rządowe Centrum Bezpieczeństwa

SPIS TREŚCI

Niniejszy poradnik powstał dzięki zaangażowaniu przedstawicieli następujących podmiotów sektora ropy i gazu:

- **Grupa Lotos SA**
- **Naftoport Sp. z o.o.**
- **OGP Gaz-System SA**
- **OLPP Sp. z o.o.**
- **PERN SA**
- **PGNiG SA**
- **PKN Orlen SA**
- **Polskie LNG SA**

oraz przy współpracy firm doradczych EY Business Advisory i PricewaterhouseCoopers.

1. CZĘŚĆ I – WPROWADZENIE

Bezpieczeństwo teleinformatyczne jest kluczowym elementem szeroko rozumianego bezpieczeństwa środowiska OT (ang. *Operational Technology*) i powinno być uwzględniane przy projektowaniu, modyfikacjach czy utrzymywaniu systemów automatyki przemysłowej i sieci produkcyjnych. Pomijanie (często nieświadome) tego aspektu na różnych etapach cyklu życia rozwiązań automatyki przemysłowej i sieci produkcyjnych może doprowadzić do sytuacji, w której organizacja będzie funkcjonować na nieakceptowalnym poziomie ryzyka, a jej kierownictwo nie będzie tego świadome.

1.1. CEL STANDARDÓW

Celem dokumentu jest pomoc podmiotom odpowiedzialnym za infrastrukturę krytyczną (IK) w budowaniu szeroko rozumianego bezpieczeństwa w obszarze OT. Przedstawione w dokumencie zalecenia pozwolą na uporządkowanie wiedzy na temat bezpieczeństwa teleinformatycznego systemów automatyki przemysłowej w sektorach ropy i gazu.

Dokument przedstawia podejście oraz zbiór zaleceń i rekomendacji, których spełnienie pomoże zapewnić akceptowany poziom bezpieczeństwa infrastruktury przemysłowej. Wybór proponowanych środków bezpieczeństwa jest dobrowolny i powinien zostać przeprowadzony na podstawie wyników szacowania ryzyka i kontekstu działalności podmiotu.

1.2. ZAKRES PORADNIKA I GRUPA DOCELOWA

Poradnik opisuje najlepsze praktyki z obszaru zarządzania i bezpieczeństwa automatyki przemysłowej z uwzględnieniem specyfiki sektora ropy naftowej i gazu. Opisywane zagadnienia zostały przedstawione w podziale na części:

- Ład organizacyjny środowiska OT
- Procesy bezpieczeństwa środowiska OT
- Architektura środowiska OT

Dokument kierowany jest przede wszystkim do kadry zarządzającej, osób odpowiedzialnych za prawidłowe funkcjonowanie automatyki przemysłowej, osób odpowiedzialnych za bezpieczeństwo w obiektach infrastruktury krytycznej, a także dla operatorów systemów i infrastruktury powiązanej, mogących mieć wpływ na bezpieczeństwo elementów infrastruktury krytycznej.

Wszystkie wskazane w tabelach zalecenia dla danego obszaru należy traktować jako uzupełnienie rekomendacji przedstawionych w tekście danego rozdziału.

1.3. ZNACZENIE SYSTEMÓW OT W BRANŻY ROPY I GAZU

Branża ropy i gazu (ang. *Oil&Gas* lub *O&G*) stanowi niezwykle istotny element gospodarki państwa. Dostęp do surowców energetycznych i zaopatrzenie w energię i paliwa są niezbędne do sprawnego funkcjonowania państwa. Wśród podstawowych usług świadczonych przez sektor O&G wymienić można:

1. Wydobycie surowców energetycznych (górnictwo gazu ziemnego, ropy naftowej);
2. Wytwarzanie paliw gazowych;
3. Wytwarzanie i przetwarzanie produktów rafinacji ropy naftowej;
4. Przesyłanie paliw gazowych;
5. Przesyłanie ropy naftowej i produktów jej rafinacji;
6. Dystrybucję paliw gazowych i ciekłych;
7. Magazynowanie oraz przechowywanie paliw gazowych;
8. Magazynowanie oraz przechowywanie ropy i produktów rafinacji ropy naftowej.

1.4. PODSTAWOWE FUNKCJE ORAZ CHARAKTERYSTYKI SYSTEMÓW OT

Systemy automatyki przemysłowej realizują szereg zadań istotnych dla funkcjonowania instalacji przemysłowych w branży O&G, wspierających świadczenie ww. usług. Postępująca automatyzacja oraz integracja oparta na urządzeniach, systemach i sieciach komputerowych w coraz większym stopniu uzależniają ciągłość procesów technologicznych od dostępności tych systemów. Do podstawowych funkcji systemów automatyki przemysłowej należą:

a. regulacja i sterowanie procesem,
b. monitorowanie stanu procesu,
c. akwizycja danych o stanie procesu,
d. wizualizacja procesu,
e. alarmowanie o odchyleniach od stanu normalnego,
f. automatyczne reagowanie na stany niebezpieczne.

Pomimo wielu podobieństw systemów OT i IT, zwłaszcza w zakresie wykorzystywanych technologii (np. TCP/IP), przy formułowaniu zaleceń dotyczących budowy i organizacji systemów OT wykorzystywanych przy eksploatacji infrastruktury krytycznej, należy zwrócić uwagę na istotne różnice między systemami wykorzystywanymi do wspierania procesów technicznych (OT) i wykorzystywanych do wspierania procesów biznesowych (IT).

Większość różnic wynika z odmiennych zadań stawianych tym systemom. Systemy OT mają bezpośredni wpływ na fizyczny świat tzn. konsekwencje skutecznego ataku mogą obejmować:

- utratę zdolności produkcyjnych,
- pogorszenie jakości produktów,
- uszkodzenie urządzeń i instalacji,
- zagrożenie dla życia i zdrowia pracowników,
- zagrożenie dla zdrowia publicznego,
- zagrożenie dla środowiska,
- naruszenie wymogów prawnych i regulacyjnych,
- utratę wizerunku,

Ze względów bezpieczeństwa są one zwykle separowane od innych systemów informatycznych i posiadają połączenia z fizycznie izolowanymi komponentami takimi jak PLC czy przetworniki pomiarowe lub

urządzenia produkcyjne (np. zawory). Poniżej przedstawione zostały podstawowe różnice pomiędzy środowiskami IT i OT, które należy uwzględnić przy budowie i eksploatacji tych systemów.

Kategoria	IT – Information Technology	OT – Operational Technology
Oddziaływanie na otoczenie	Brak bezpośredniego wpływu na otoczenie – brak oddziaływania fizycznego – niesprawność może rodzić skutki finansowe.	Bezpośrednio oddziałuje na otoczenie i wywołuje fizyczne skutki w procesach produkcyjnych mogących mieć wpływ na bezpieczeństwo, życie i zdrowie ludzkie jak również powodować skutki finansowe.
Zapobieganie zagrożeniom	Wykorzystanie typowych, powtarzalnych rozwiązań bezpieczeństwa zaprojektowanych dla IT. Kontrola dostępu jest dopasowana do obowiązującej polityki.	Narzędzia bezpieczeństwa muszą być przetestowane off-line w celu wykluczenia zakłóceń w normalnej pracy OT. Kontrola dostępu powinna być prowadzona bardzo restrykcyjnie (włączając bezpieczeństwo fizyczne) ze względu na potencjalne (negatywne) skutki oddziaływania na otoczenie.
Systemy operacyjne	Są zaprojektowane do wykorzystania typowych systemów operacyjnych. Aktualizacje są relatywnie proste i wspomagane dostępnymi narzędziami deweloperskimi.	Wykorzystywane są zróżnicowane, czasami dedykowane systemy operacyjne bez wbudowanych mechanizmów bezpieczeństwa. Zmiany oprogramowania muszą być wprowadzane bardzo ostrożnie, najczęściej z udziałem dostawcy, ze względu na specyfikę rozwiązania i ewentualną konieczność modyfikacji lub wymiany urządzeń, co może wpłynąć na procesy produkcyjne.
Wpływ bezpieczeństwa na architekturę systemu	Skupienie uwagi na ochronie zasobów IT oraz informacji przechowywanych na nich lub transmitowanych między nimi.	Skupienie uwagi na zapewnieniu ciągłości działania i ochronie elementów brzegowych (np. stacji roboczych, kontrolerów PLC lub urządzeń wykonawczych) ponieważ są one bezpośrednio odpowiedzialne za kontrolowany proces.
Interakcje czasu rzeczywistego (time critical)	Mniej krytyczne wymagania dopuszczają opóźnienia w przekazaniu danych, a nawet utraty pakietów danych. Z reguły istnieje możliwość odtworzenia informacji lub pozyskania ich z innego źródła.	Przepływ informacji musi być zdeterminowany i dopasowany do procesu technologicznego nadzorowanego on-line. Utrata danych z procesu technologicznego jest bezpowrotna i nie możliwa do odtworzenia.
Zarządzanie zmianą	Zmiany oprogramowania są wprowadzane regularnie (codziennie) zgodnie z politykami bezpieczeństwa i procedurami. Procedury są często zautomatyzowane.	Zmiany muszą być zaplanowane i harmonogramowane z dużym wyprzedzeniem (tygodnie, miesiące), starannie przetestowane pod względem wpływu na integralność systemu OT (włączając w to testy wdrażanych poprawek (patch) i aktualizacje oprogramowania. Zmiany oprogramowania muszą być wprowadzane bardzo ostrożnie, najczęściej z udziałem dostawcy, ze względu na specyfikę rozwiązania i ewentualną konieczność modyfikacji lub wymiany urządzeń.

Kategoria	IT – Information Technology	OT – Operational Technology
Zarządzanie personelem	Pożądana znajomość procesów biznesowych użytkownika, relatywnie duża liczba specjalistów na rynku pracy.	Wymagana znajomość procesów technologicznych i urządzeń wykonawczych. Ze względu na specyfikę i kompleksowość rozwiązań wymagany wyższy i szerszy zakres wiedzy zwłaszcza z obszaru technologii przemysłowych i automatyki.
Zarządzanie wsparciem	Dopuszczalne zdywersyfikowane, różnorodne systemy wsparcia technicznego realizowane przez różnych dostawców usług. Najczęściej wymagane jest wsparcie 8 godz./5 dni roboczych lub na warunkach „*next business day*”.	Wsparcie techniczne jest realizowane zazwyczaj przez jednego dostawcę systemu przy udziale służb użytkownika. Wymagane wsparcie 24 godz./365 dni.
Komunikacja	Komunikacja prowadzona przy wykorzystaniu standardowych, powszechnie dostępnych, protokołów, konieczność zapewnienia dostępu do zasobów Internetu. Dwukierunkowa wymiana dużych ilości informacji.	Wykorzystywane specyficzne lub zamknięte protokoły. Komunikacja ze światem zewnętrznym jest ograniczona do określonego zakresu danych i adresowana do określonych systemów. Dąży się do jednokierunkowego udostępniania danych. Ograniczona liczba rozwiązań typu firewall potrafiąca analizować protokoły przemysłowe.
Czas życia systemu	3 – 5 lat	10 – 15 lat
Dostęp do hardware	Komponenty łatwo dostępne lokalnie. Dostępna szeroka gama zamienników od różnych producentów.	Komponenty w izolowanych, różnych geograficznie lokalizacjach, często wykorzystywany dedykowany, nietypowy sprzęt.

1.5. ROZWIĄZANIA Z OBSZARU AUTOMATYKI PRZEMYSŁOWEJ NAJCZĘŚCIEJ WYSTĘPUJĄCE W BRANŻY O&G

1.5.1. PLC

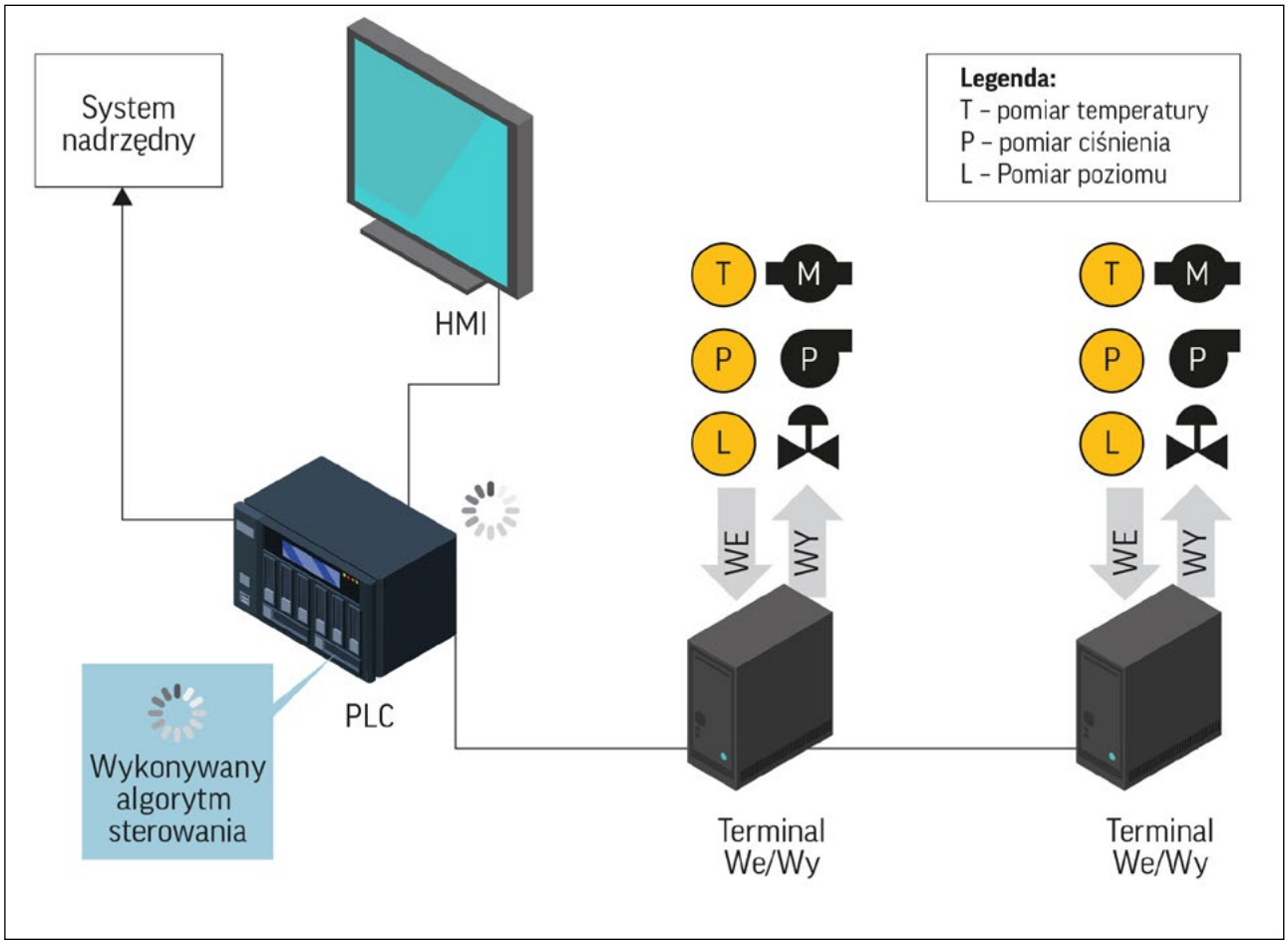
Sterownik PLC (ang. *Programmable Logic Controller*) to urządzenie elektroniczne, zaprojektowane do warunków przemysłowych, wyposażone w pamięć programowalną, wykorzystywaną do realizacji funkcji wg zaprogramowanych algorytmów przy użyciu instrukcji logicznych, arytmetycznych, czasu i zliczania w celu realizacji sterowania procesami technologicznymi poprzez cyfrowe i analogowe sygnały wejściowe i wyjściowe. W połączeniu z systemem SCADA bądź panelem operatorskim (ang. *Human-Machine Interface HMI*) stanowi w pełni funkcjonalny system sterowania.

Sterowniki PLC mają najczęściej modułową budowę, z konfiguracją sprzętową ściśle zależną od konkretnego wdrożenia. Podstawowym elementem jest moduł z procesorem, do którego dołączane są moduły komunikacyjne do wymiany informacji z innymi urządzeniami oraz systemami, a także moduły wejść/wyjść. Do modułów wejść podłączane są przewody czujników i sensorów. Do modułów wyjściowych podłączane są urządzenia wykonawcze, takie jak pompy czy zawory.

Sterowanie elementami wykonawczymi jest realizowane na bazie programowalnego algorytmu. Języki programowania sterowników PLC są zestandaryzowane. Najczęściej stosowane języki to:

a. Język schematów drabinkowych (LD – ang. *Ladder Diagram*) – wywodzący się ze schematów przekaźnikowych i opierający się o podobne symbole.
b. Język schematów bloków funkcyjnych (FBD – ang. *Function Block Diagram*) – opierający się na logicznym łączeniu ze sobą predefiniowanych bloków realizujących wymagane funkcje
c. Język strukturalny (ST – ang. *Structured Text*) – należący do grupy języków tekstowych, często stosowany do opisu złożonych wyrażeń, których realizacja może być trudna w językach graficznych.

Opracowany przez programistę algorytm realizuje operacje na zmiennych reprezentujących sygnały wejściowe, dane z innych systemów, czy też wartości zależne od wcześniejszych operacji.



Rys. 1. Przykładowy schemat systemu sterowania wykorzystującego PLC

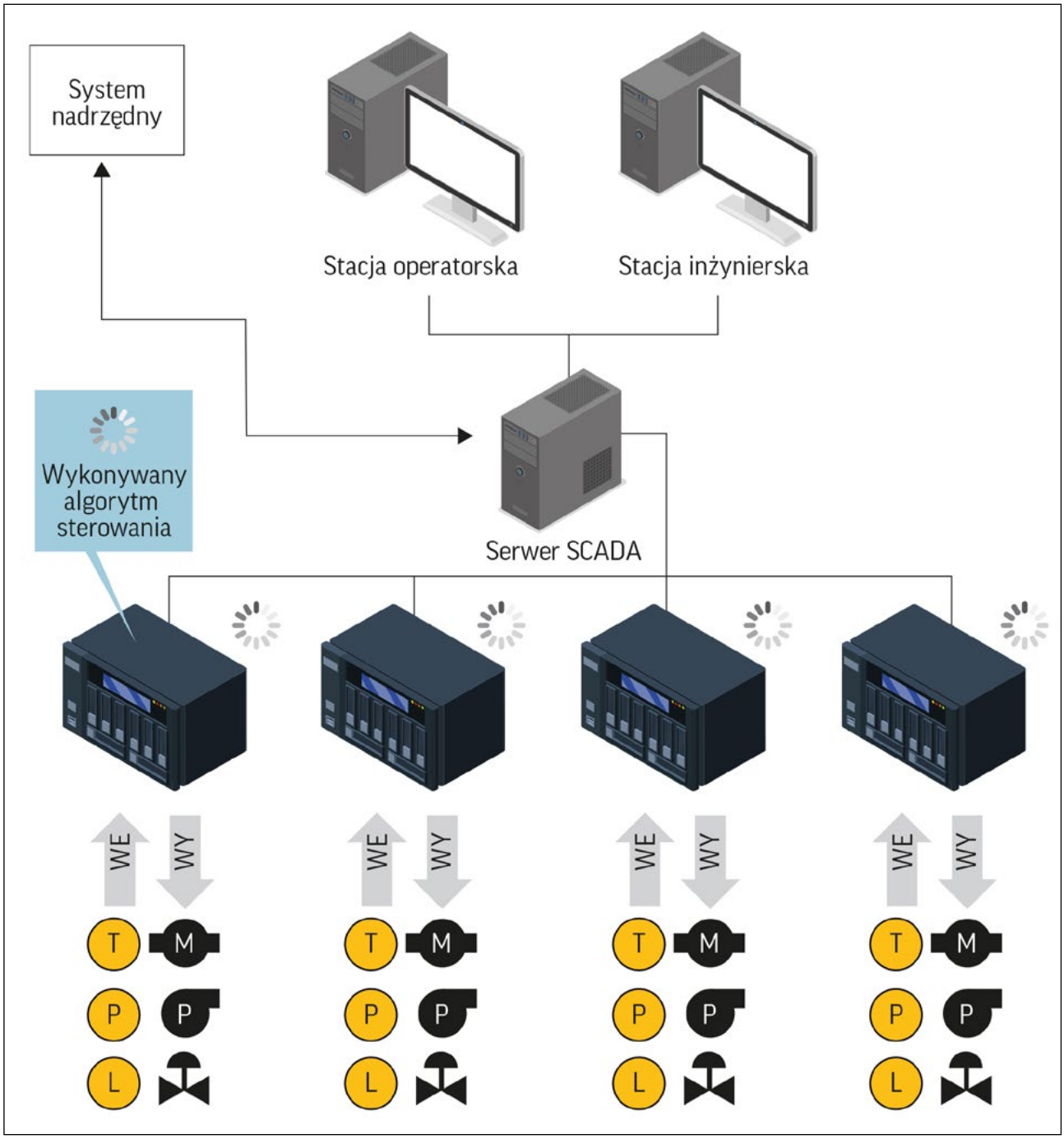
1.5.2. SCADA

W podstawowej konfiguracji służy do monitorowania procesu, archiwizacji danych pomiarowych i przekazywania poleceń operatorów/dyspozytorów. Charakteryzuje się otwartą strukturą, umożliwiającą zastosowanie w obrębie jednego systemu rozwiązań różnych producentów oraz możliwą rozbudową o dodatkowe funkcjonalności. Systemy SCADA są zazwyczaj wdrażane w połączeniu ze sterownikami PLC, lub jako system integrujący wiele systemów sterowania w jeden centralny system.

SCADA w podstawowym zastosowaniu zbiera i przetwarza informacje z poszczególnych urządzeń, a następnie prezentuje je na monitorze (lub wielu monitorach) w formie wizualizacji czytelnej dla operatorów/

dyspozytorów systemu. Do dyspozycji użytkownika na ekranie monitora dostępne są informacje dotyczące mierzonych wartości oraz stanu poszczególnych urządzeń.

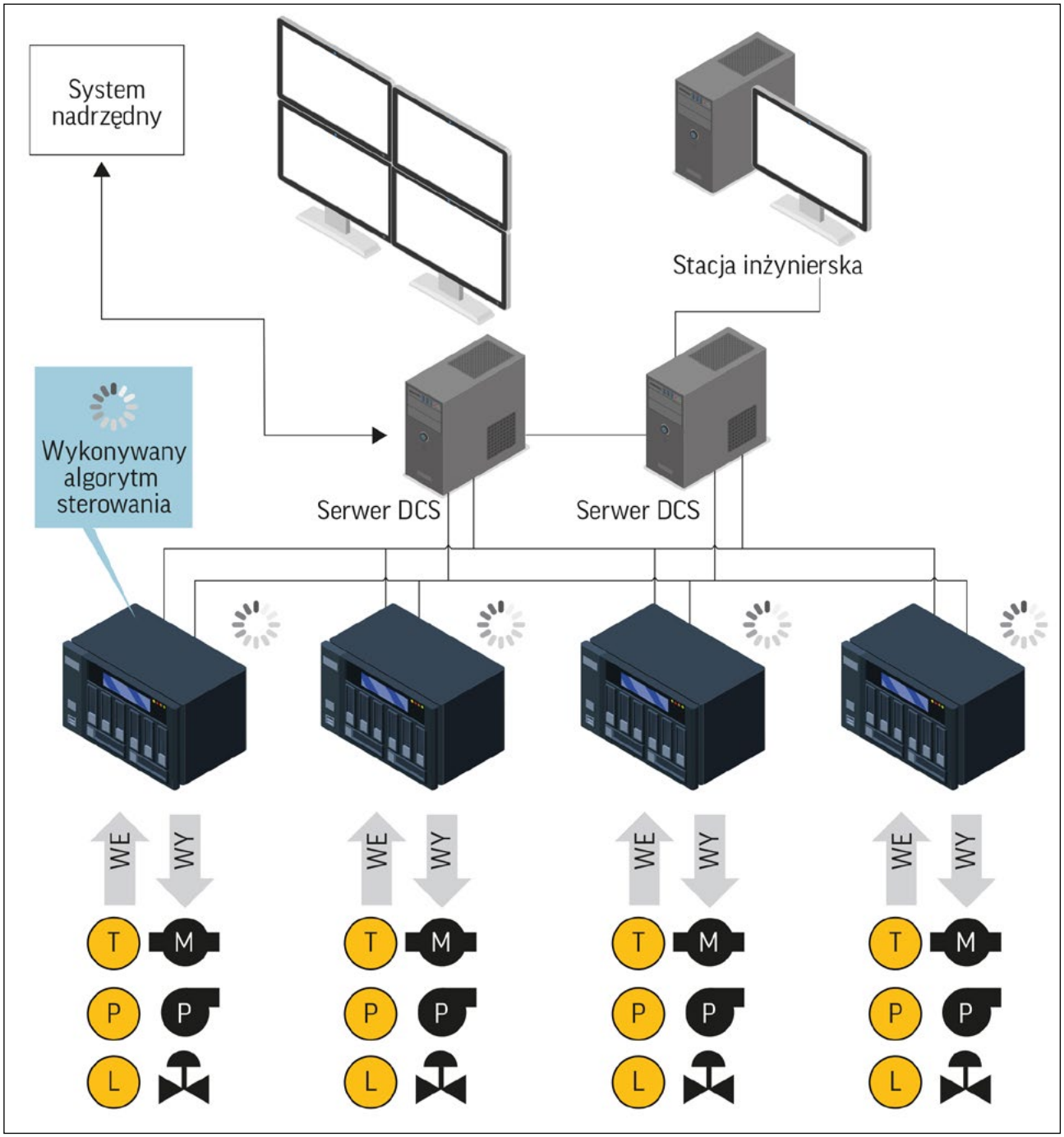
Z punktu widzenia bezpieczeństwa procesowego ważną rolą systemów SCADA jest generowanie informacji o stanach alarmowych i awaryjnych oraz gromadzenie danych archiwalnych na temat sterowanego procesu, w tym zbieranie informacji dotyczących zarówno stanu, jak i parametrów monitorowanych obiektów. Oprogramowanie powinno skutecznie archiwizować pozyskiwane dane, a także cechować się funkcjami pozwalającymi na ich efektywne wyszukiwanie.



Rys. 2. Przykładowy schemat systemu SCADA

1.5.3. DCS

System sterowania, w którym zadania sterowania są rozdzielone pomiędzy rozproszone geograficznie urządzania. Funkcjonalnie posiada on możliwości SCADA, dodatkowo implementuje on również elementy warstwy sterowania. Systemy klasy DCS można opisać, jako połączenie rozporoszonych geograficznie i logicznie jednostek sterujących z systemem sterowania, nadzorującym działanie całego systemu i służącym do zarządzania procesem. DCS nie ma równie otwartej struktury, co system SCADA, zwykle dysponuje on za to bardziej złożonymi algorytmami sterowania i regulacji, a także zapewnia redundancję sterowania i komunikacji. Wykorzystywany jest przede wszystkim do sterowania procesów ciągłych, wymagających dużej dostępności i niezawodności.

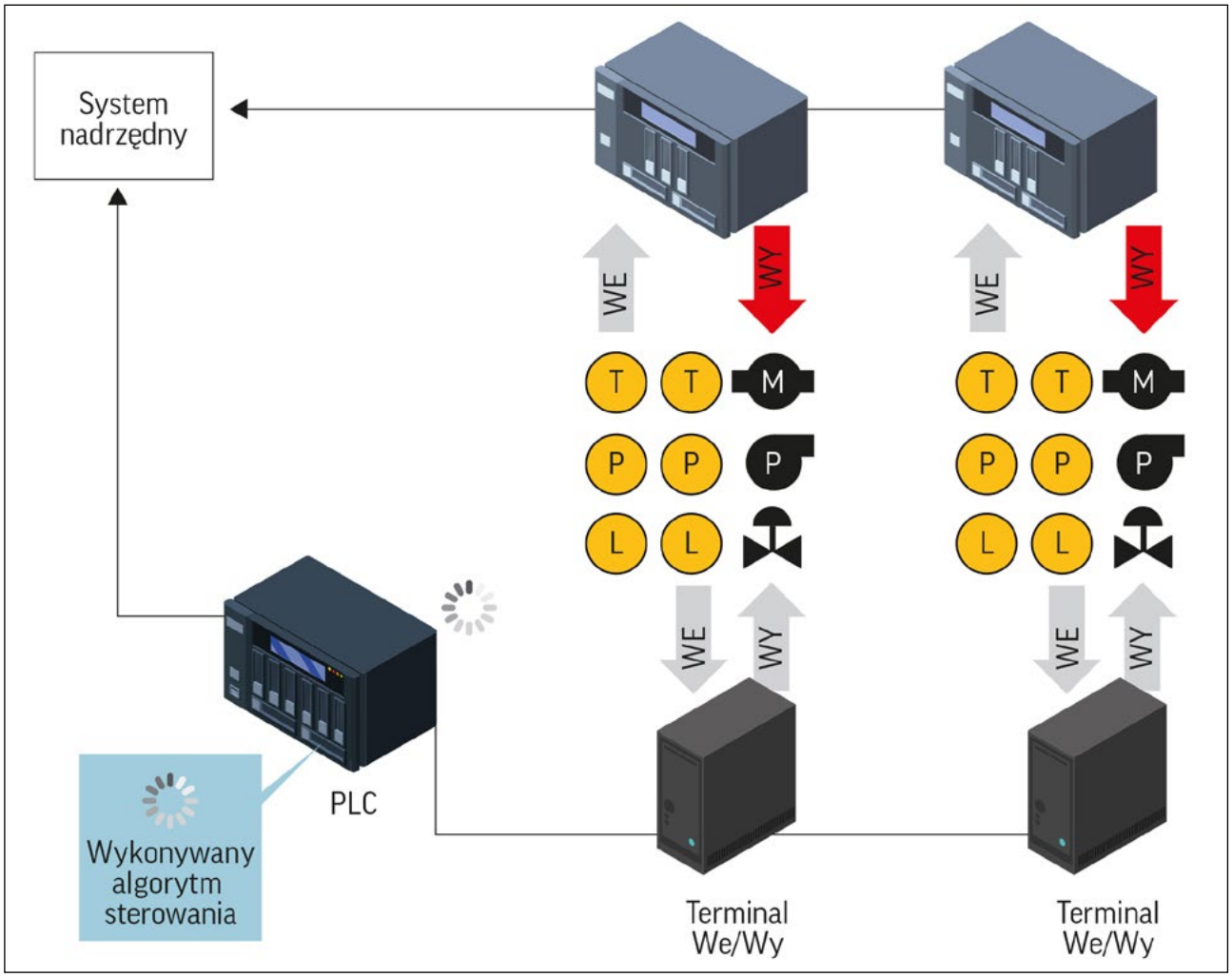


Rys. 3. Przykładowy schemat systemu DCS

1.5.4. SIS/ESD

Niezależne od systemów OT (SCADA/DCS) systemy klasy SIS/ESD realizują funkcje bezpieczeństwa w przypadku odchylenia warunków procesu technologicznego od warunków bezpiecznych. W szczególności do funkcji bezpieczeństwa należy awaryjne, lecz kontrolowane zatrzymanie pracy instalacji technologicznej.

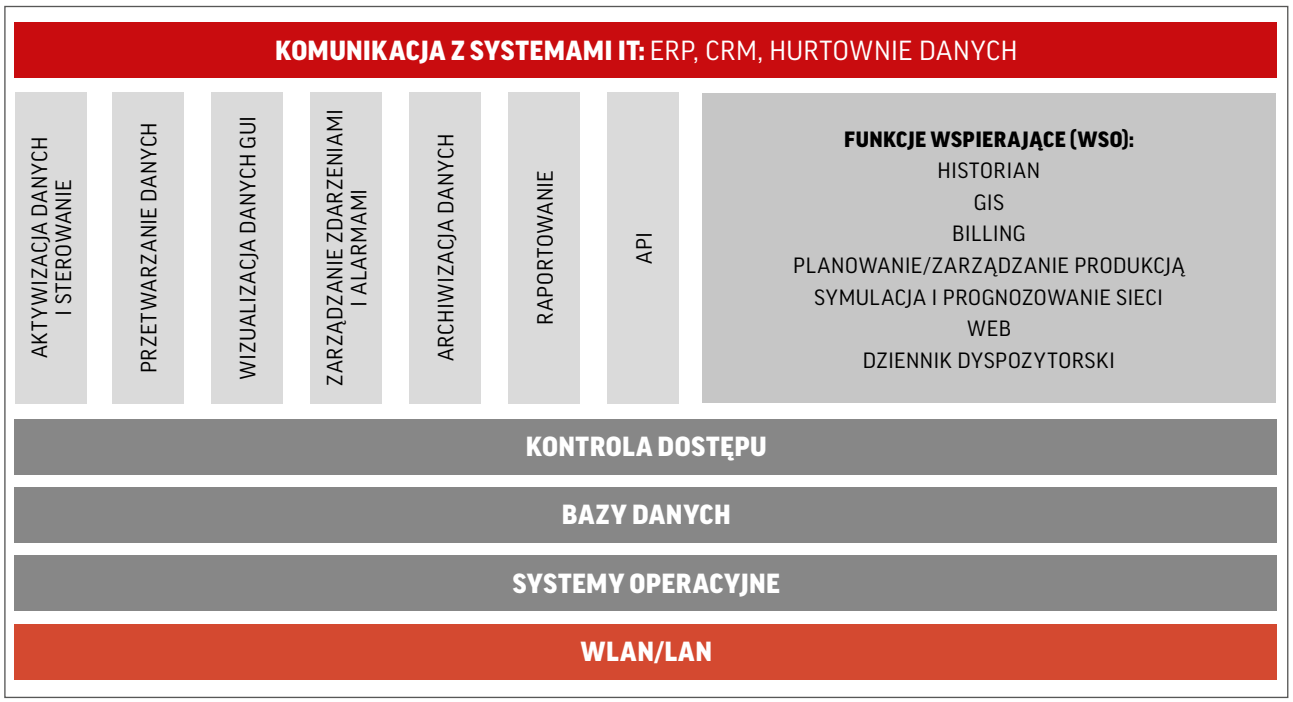
System bezpieczeństwa SIS/ESD tworzą certyfikowane i zaprojektowane do pracy w systemach bezpieczeństwa sterowniki, klasyfikowane w tzw. poziomach nienaruszalności bezpieczeństwa SIL, wraz z niezależnymi czujnikami i dedykowanymi elementami wykonawczymi.



Rys. 4. Przykładowy schemat systemu SIS/ESD

1.6. MODEL FUNKCJONALNY OPISU SYSTEMU OT

Model funkcjonalny systemu OT został przedstawiony na schemacie poniżej.



Rys. 5. Ogólny schemat funkcjonalny systemów OT

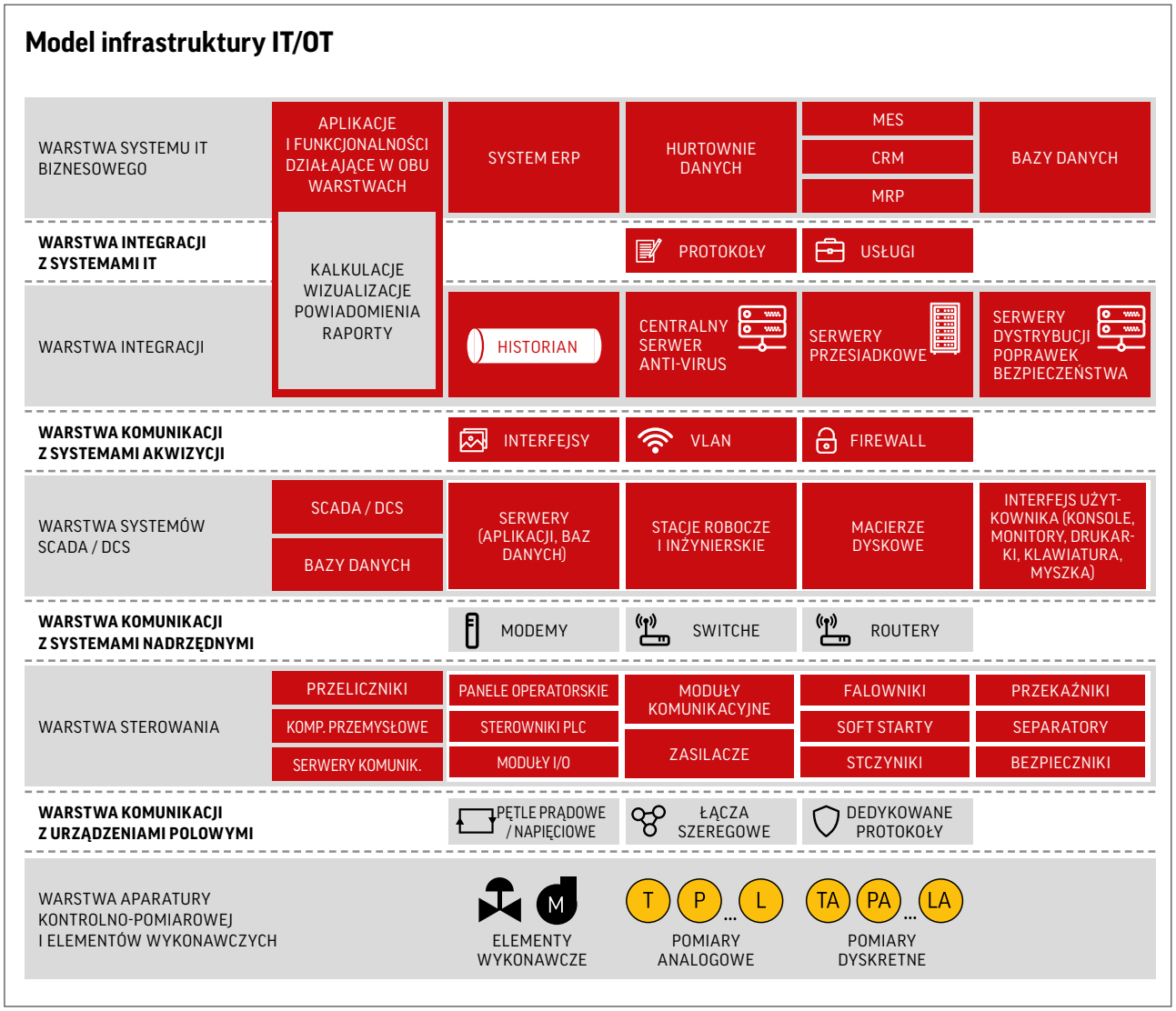
W każdym systemie OT występuje grupa głównych, uniwersalnych funkcjonalności odpowiadających za zbieranie danych, ich przetwarzanie, wizualizację oraz archiwizację i dalsze udostępnianie danych (kolor niebieski ciemny). Funkcjonalności te w zależności od zastosowania i specyfiki działania użytkownika są uzupełniane o dodatkowe funkcje wspierające (Systemy Wspierające System OT – WSO) stosowane ze względu na przeznaczenie systemu. Na schemacie pokazano charakterystyczne dla branży Oil&Gas rodzaje funkcji wspierających.

Od strony procesów biznesowych realizowanych przez firmy z branży Oil&Gas systemy OT są wykorzystywane jako narzędzia wspierające dwa zasadnicze procesy:

- procesy utrzymania instalacji technicznych i sterowania instalacjami technicznymi (maintenance + control) do czego są wykorzystywane przede wszystkim ww. główne funkcjonalności. Przy pomocy tych funkcji obserwowane są parametry i stany pracy urządzeń oraz wykonywane akcje sterujące lub regulacyjne,
- procesy zarządzania operacyjnego związane z realizowaną przez dane przedsiębiorstwo lub instalację usługą. Do tego celu wykorzystywane są przede wszystkim funkcje wspierające, np.: GIS – wsparcie przy lokalizacji uszkodzeń i zarządzanie ekipami serwisowymi, Biling – bilansowanie sieci i wsparcie dla rozliczania usług sprzedaży poprzez odczyty urządzeń pomiarowych, itp.

1.7. MODEL 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 systemu IK, środowisko teleinformatyczne operatora może składać się z jednej lub więcej warstw. Model warstwowy środowiska systemów i sieci teleinformatycznych przedstawia poniższy rysunek:



Rys. 6. Model przykładowej infrastruktury OT

1.7.1. Warstwa systemu IT/biznesowego

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) czy MRP (systemy służące do planowania zapotrzebowania na zasoby materiałowe).

1.7.2. Warstwa integracji i systemów wspierających

Systemy warstwy integracji odpowiadają za gromadzenie danych oraz zaawansowaną analitykę, raportowanie i udostępnianiem informacji a także funkcję wspierające. Przykładem systemów warstwy integracji są: historian, systemy klasy MES (z ang. *Manufacturing Execution System* – systemy służące do zbierania informacji o procesie produkcyjnym), a także niektóre systemy wspierające, np. centralne serwery dystrybucji sygnatur AV, serwery przesiadkowe, serwery wymiany plików, serwery usług katalogowych, itp.

1.7.3. Warstwa systemów SCADA/DCS

Systemy te pełnią rolę interfejsu użytkownika dla operatorów/dyspozytorów i pozwalają na monitorowanie oraz sterowanie (również zdalne) procesem technologicznym. W warstwie tej możemy wyróżnić m.in. następujące komponenty:

a) Serwery aplikacji SCADA/DCS,
b) Stacje operatorskie i inżynierskie,
c) Serwery baz danych,
d) Macierze dyskowe,
e) Serwery komunikacyjne.

1.7.4. Warstwa sterowania

Systemy i urządzenia tej warstwy w sposób bezpośredni oddziałują na proces technologiczny poprzez sterowanie elementami wykonawczymi, takimi jak: zawory, klapy, pompy, elektryczne elementy łączące.

1.7.5. Warstwa aparatury kontrolno-pomiarowej i elementów wykonawczych

Warstwą, która jest najbliżej infrastruktury i procesu przemysłowego jest warstwa aparatury kontrolno-pomiarowej i elementów wykonawczych. Zawiera ona elementy pomiarowe takie jak czujniki temperatury ciśnienia, poziomu, przepływu itp. pozwalające monitorować stan procesu technologicznego oraz elementy wykonawcze takie jak pompy, wentylatory, przenośniki, zawory, zasuwy itp. pozwalające zmieniać stan procesu technologicznego.

1.8. KLASYFIKACJA SYSTEMÓW OT

Nie wszystkie systemy OT pełnią krytyczną funkcję w podstawowym procesie technologicznym. Z punktu widzenia ciągłości działania, niektóre systemy OT mogą być przywrócone do działania po kliku dniach po awarii bez istotnego wpływu na przedsiębiorstwo. Dla innych systemów nawet chwilowa niedostępność skutkuje przerwami w produkcji i poważnymi stratami. Dlatego też zalecane jest utrzymywanie aktualnej inwentaryzacji systemów OT i ich komponentów oraz sklasyfikowanie systemów pod kątem ich krytyczności. Poniżej przedstawiona została tabela, która może posłużyć do klasyfikacji:

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.

2. CZĘŚĆ II – ŁAD ORGANIZACYJNY ŚRODOWISKA AUTOMATYKI PRZEMYSŁOWEJ

Ustanowienie i formalizacja organizacji bezpieczeństwa środowiska OT pozwoli na spójne zarządzanie i bezpieczne funkcjonowanie środowiska OT w organizacji. Bez odpowiedniego ładu organizacyjnego w OT, prowadzenie procesu technologicznego może odbywać się na niewystarczającym poziomie bezpieczeństwa i narażać organizację na dodatkowe ryzyko. Skuteczne ramy zarządzania zapewnione są poprzez jasno zdefiniowane role i obowiązki w środowisku OT, aktualną politykę bezpieczeństwa, procedury zarządzania środowiskiem OT oraz pewność, że polityka i procedury są przestrzegane.

2.1. ROLE I ODPOWIEDZIALNOŚCI

Zaleca się, aby odpowiedzialności związane z bezpieczeństwem środowiska OT były wyraźnie zdefiniowane i określone.

Powinny zostać opisane, co najmniej następujące role oraz ich obowiązki istotne z punktu widzenia odpowiedzialności za bezpieczeństwo systemów automatyki przemysłowej:

a) właściciel biznesowy systemu,
b) administrator techniczny systemu,
c) administrator biznesowy systemu,
d) koordynator bezpieczeństwa systemów OT.

Osoby pełniące powyższe role mogą delegować zadania związane z infrastrukturą automatyki przemysłowej innych osobom. Nie zwalnia ich to jednak z odpowiedzialności za wszystkie delegowane zadania.

2.2. POLITYKA BEZPIECZEŃSTWA SYSTEMÓW OT I PROCEDURY

Polityka bezpieczeństwa OT powinna zostać zatwierdzona przez Zarząd Spółki oraz opublikowana i przekazana pracownikom posiadającym dostęp do środowiska OT, a także odpowiednim podmiotom zewnętrznym, mającym dostęp do środowiska OT. Polityka bezpieczeństwa OT może być zawarta w ramach polityki bezpieczeństwa informacji w organizacji lub jako oddzielna polityka.

Kadra kierownicza odpowiedzialna za bezpieczeństwo OT powinna być identyfikowalna przez: imię, nazwisko, tytuł, numer telefonu służbowego, adres firmy i datę mianowania. Zmiany kierownictwa powinny być udokumentowane w ciągu trzydziestu (30) dni kalendarzowych od daty wejścia w życie i przekazane do wiadomości pracownikom organizacji.

Polityka bezpieczeństwa powinna być poddawana przeglądowi nie rzadziej niż raz w roku, w celu zapewnienia jej stałej przydatności, adekwatności i efektywności.

2.3. WERYFIKACJA ZGODNOŚCI I TESTY BEZPIECZEŃSTWA

Zalecane jest wykonywanie cyklicznych audytów bezpieczeństwa systemów OT (nie rzadziej niż raz na dwa lata) lub czynności kontrolnych, które mają na celu potwierdzenie stanu faktycznego z założonymi wymaganiami. Wykryte w trakcie audytu nieprawidłowości wraz z rekomendacjami powinny zaleźć się w raporcie poaudytowym. W realizację zamieszczonych w raporcie rekomendacji należy zaangażować osoby merytoryczne oraz kadrę zarządzającą.

Rekomenduje się również przeprowadzanie cyklicznych testów bezpieczeństwa, które weryfikowałyby skuteczność zabezpieczeń środowiska OT. Testy powinny ograniczać się do weryfikacji skuteczności zabezpieczeń brzegowych (np. firewall pomiędzy warstwami IT/OT) oraz do weryfikacji architektury środowiska OT, wersji oprogramowania, konfiguracji systemu operacyjnego na systemach OT itp. Ze względu na znaczenie systemów OT dla ciągłości działania procesów biznesowych nie rekomenduje się używania jakichkolwiek aktywnych narzędzi sieciowych w środowisku produkcyjnym np. służących do analizy podatności. Identyfikację podatności przy użyciu aktywnych narzędzi sieciowych należy przeprowadzać w środowisku laboratoryjnym lub w fazie wdrażania systemu OT.

2.4. PROGRAM SZKOLEŃ I ZWIĘKSZANIA ŚWIADOMOŚCI

Pracownicy mający kontakt z systemami automatyki przemysłowej powinni zostać przeszkoleni z zakresu zasad i procesów wpływających w szczególności na:

- cyberbezpieczeństwo OT
- bezpieczeństwo operacyjne OT
- bezpieczeństwo fizyczne OT

oraz ze sposobów zachowania się w przypadku wykrycia nietypowego funkcjonowania infrastruktury automatyki przemysłowej.

2.5. ZALECENIA DLA OBSZARU ŁADU ORGANIZACYJNEGO

Numer Zalecenia	Opis zalecenia	Zalecenie (podstawowe/dodatkowe)
K-2.1. Role i odpowiedzialności		
K-2.1.1.	Organizacja wyznaczyła osobę odpowiedzialną za cyberbezpieczeństwo w środowisku OT	podstawowe
K-2.1.2.	Role i odpowiedzialności w środowisku OT są jasno zdefiniowane i udokumentowane	podstawowe
K-2.1.3.	Kadra zarządzająca wspiera bezpieczeństwo środowiska OT	podstawowe
K-2.1.4.	Organizacja powołała multidyscyplinarne komitety odpowiedzialne za podejmowanie decyzji mających wpływ na bezpieczeństwo OT	dodatkowe
K-2.1.5.	Wybrane funkcje bezpieczeństwa IT oraz OT są integrowane w celu uzyskania efektu synergii	dodatkowe

Numer Zalecenia	Opis zalecenia	Zalecenie (podstawowe/dodatkowe)
K-2.2. Polityka bezpieczeństwa i procedury		
K-2.2.1.	Organizacja przyjęła politykę bezpieczeństwa OT, która wspiera bezpieczeństwo oraz ciągłość działania procesów technologicznych	podstawowe
K-2.2.3.	Przyjęta polityka jest regularnie przeglądana oraz aktualizowana.	podstawowe
K-2.2.4.	Organizacja opracowała standardy i procedury opisujące szczegółowo zarządzanie bezpieczeństwem OT (np. ochronę antywirusową, proces aktualizacji systemów operacyjnych w OT)	podstawowe
K-2.2.5.	Polityka zarządzania bezpieczeństwem OT wraz z obowiązującymi procedurami jest częścią zintegrowanego systemu zarządzania	dodatkowe
K-2.3. Weryfikacja Zgodności i testy bezpieczeństwa		
K-2.3.1.	Organizacja ustanowiła program regularnych przeglądów zgodności z przyjętą polityką bezpieczeństwa OT	podstawowe
K-2.3.2	Opracowano cykliczny plan testów bezpieczeństwa. Na bazie wyników przeprowadzana jest analiza ryzyka wraz z planem naprawczym.	dodatkowe
K-2.3.3.	Organizacja priorytetyzuje zadania związane z bezpieczeństwem OT zgodnie z podejściem opartym na ryzyku	dodatkowe
K-2.3.4.	Organizacja posiada minimalne wymagania bezpieczeństwa stanowiące warunek zakupu nowych rozwiązań OT	dodatkowe
K-2.3.5.	Organizacja posiada proces zarządzania zgodnością dla nowych projektów wdrożenia rozwiązań OT	dodatkowe
K-2.4. Program szkoleń i zwiększania świadomości		
K-2.4.1.	Organizacja opracowała program szkoleń dostosowany do specyfiki organizacji, mający na celu zapoznanie pracowników z zagadnieniami bezpieczeństwa	podstawowe
K-2.4.2.	Organizacja regularnie przegląda oraz usprawnia program szkoleń oraz zwiększania świadomości	dodatkowe
K-2.4.3.	Organizacja regularnie wysyła informacje do wszystkich pracowników w celu podnoszenia świadomości w zakresie bezpieczeństwa OT	dodatkowe

3. CZĘŚĆ III – PROCESY BEZPIECZEŃSTWA ŚRODOWISKA AUTOMATYKI PRZEMYSŁOWEJ

3.1. ZARZĄDZANIE INCYDENTAMI

Celem procesu zarządzania incydentami w środowisku OT jest minimalizacja skutków zaistniałego incydentu bezpieczeństwa. Organizacja powinna rozumieć jakie implikacje może nieść za sobą określony rodzaj incydentu i wypracować reakcję na poszczególne typy incydentów, oraz wiedzieć gdzie, kiedy i jakiego wsparcia może szukać w przypadku wystąpienia incydentu.

3.2. ODTWARZANIE SYSTEMÓW OT

Ustalenie planu odtworzenia po awarii (ang. *disaster recovery plan*, DRP) jest niezbędne dla utrzymania dostępności krytycznych zasobów środowiska OT.

W celu umożliwienia organizacji odtworzenia stanu sprzed wystąpienia zakłócenia (o potencjalnie katastrofalnych skutkach), jako minimum DRP powinien obejmować następujące elementy:

- warunki, w których procedura odtwarzania po awarii zostanie aktywowana;
- listę kontaktową z procedurą eskalacji uwzględniającą wszystkie osoby biorące udział w planie DRP;
- role i obowiązki wszystkich stron, w tym wspierających dostawców;
- kopie zapasowe;
- schematy systemów, informacje o sieci, hasła, karty katalogowe, aplikacje i licencje;
- zarządzanie zmianami w DRP i aktualizacja;
- procedurę okresowego testowania planu odzyskiwania po awarii.

Skuteczne odtworzenie po awarii ma kluczowe znaczenie z punktu widzenia bezpieczeństwa środowiska procesowego. Odpowiedni DRP jest zaprojektowany w oparciu o poprawną ocenę ryzyka oraz środki ograniczające ryzyko do akceptowalnego dopuszczalnego poziomu.

3.3. AKTUALIZACJE I POPRAWKI BEZPIECZEŃSTWA

Producenci oprogramowania i sprzętu regularnie udostępniają aktualizacje produktów w postaci: łat bezpieczeństwa (ang. *patch*), poprawek, pakietów serwisowych. Aktualizacje te mają głównie na celu poprawę wydajności lub funkcjonalności oprogramowania bądź usunięcie lub zniwelowanie luk w zabezpieczeniach, które to luki zostały wykryte dopiero po wprowadzeniu produktu na rynek. Luki te mogą potencjalnie zostać wykorzystane przez osobę lub złośliwe oprogramowanie i w efekcie doprowadzić do niestabilności, zatrzymania bądź przejęcia systemu. Wdrażanie aktualizacji dla produktu tzw. „łatanie" (patchowanie) produktu jest procesem ograniczającym ryzyko występowania takich sytuacji. Z drugiej strony, przy złożoności oprogramowania w środowisku OT, aktualizacje, których wpływ na stabilność systemu OT nie został zweryfikowany mogą zakłócić prawidłową pracę systemu.

Rekomendowane jest ustalenie procedur weryfikacji wszystkich poprawek (w tym aktualizacji systemów antywirusowych) w środowiskach testowych przed ich instalacją w systemach produkcyjnych. Procedury

te muszą określać zakresy odpowiedzialności i sposoby współdziałania administratorów technicznych oraz dostawców/serwisantów systemów OT lub poszczególnych komponentów wchodzących w ich skład.

Zalecane jest by Organizacja utrzymywała Plan Zarządzania Poprawkami i Aktualizacjami w środowisku OT ze szczególnym uwzględnieniem zaleceń producentów systemów OT, który określa szczegółowo:

- zasady i sposób przekazywania przez producenta lub serwisanta poprawek w sposób zapewniający ich integralność,
- procedury wdrażania poprawek i ich weryfikacji pod kątem wpływu na działanie systemów OT,
- częstotliwość wdrażania i poziomy istotności poprawek (podział co najmniej na poprawki zalecane i poprawki wymagane) udostępnianych np. przez producentów systemów operacyjnych i ochrony antywirusowej,
- zasady wdrażania poprawek instalowanych w sytuacjach awaryjnych,
- dodatkowe środki mitygujące ryzyko w przypadku systemów OT, które są wykluczone z procesu aktualizacji.

3.4. ZARZĄDZANIE DOKUMENTACJĄ

Dokumentacja związana z systemami OT taka jak:

- rysunki i dokumenty techniczne,
- adresy IP i listy nazw hostów,
- dane operacyjne i dane historyczne,
- inwentaryzacja zasobów, numery modeli, wersje i specyfikacje,
- rysunki i mapy topologii sieci,
- raporty z przeglądów/audytów bezpieczeństwa,
- konfiguracje urządzeń – pliki programów, pliki konfiguracyjne dla urządzeń automatyki, np. konfiguracja PLC, DCS, SIS, ESD itp.

powinna być odpowiednio zabezpieczona. Informacje te, jeśli są przechowywane w systemach elektronicznych, powinny znajdować się wewnątrz zabezpieczonej sieci.

Przechowywanie nie powinno mieć miejsca na współdzielonym dysku korporacyjnym bez wcześniejszej oceny ryzyka zagrożenia dla bezpieczeństwa teleinformatycznego. Dystrybucja i dostęp do tych informacji powinien być kontrolowany i w pełni rozliczalny. Powinna zostać opracowana procedura umożliwiająca kontrolę nad dostępem i wersjonowaniem dokumentacji w środowisku OT.

3.5. ZARZĄDZANIE DOSTĘPAMI DO SYSTEMÓW OT

Przyznawanie, kontrolowanie i monitorowanie elektronicznego dostępu do systemów OT jest kluczowe z punktu widzenia ich bezpieczeństwa. Poniżej przedstawiono najważniejsze procesy i zasady związane z zarządzaniem dostępem do systemów OT:

Tworzenie konta użytkownika

- osoba (posiadacz konta) musi przejść obowiązkowe szkolenie związane z przyznanym jej poziomem dostępu i uprawnień, zanim dostęp zostanie autoryzowany;
- wniosek o dostęp i poziom uprawnień jest przesyłany do właściciela biznesowego i/lub do administratora systemu w celu zatwierdzenia. Właściciel biznesowy i/lub administrator systemu potwierdza lub zmienia zaproponowany poziom dostępu;

- dane uwierzytelniające przekazywane są w sposób uniemożliwiający podgląd danych osobom nieupoważnionym.

Utrzymanie stałego dostępu

- powinno się monitorować aktywność i logi bezpieczeństwa pod kątem niewłaściwej aktywności i naruszeń bezpieczeństwa;
- powinno się zbierać wszystkie informacje dotyczące poziomów uprawnień i wysyłać do właściciela biznesowego w celu corocznego przeglądu i ponownego zatwierdzenia uprawnień;
- administrator systemu powinien być niezwłocznie informowany o wszelkich zmianach wpływających na przyznany poziom dostępu.

Administrator i dostęp uprzywilejowany

- nazwane konta uprzywilejowane powinny być poddawane corocznemu przeglądowi i zatwierdzane przez właściciela biznesowego.

Zmiana lub odbieranie uprawnień do dostępu

- wniosek o zmianę poziomu uprawnień jest przesyłany do właściciela biznesowego i/lub do administratora systemu w celu zatwierdzenia. Właściciel biznesowy i/lub administrator systemu potwierdza zaproponowany poziom dostępu;
- informacja o konieczności odebrania uprawnień dostępu do systemów OT musi być niezwłocznie przekazana administratorowi systemu przez właściwe komórki kadrowe lub odpowiedzialne za bezpieczeństwo np. w przypadku przeniesienie na inne stanowisko służbowe, wygaśnięcie stosunku pracy, zakończenia prac serwisowych itp. Informowanie powinno zostać włączone do procedur postępowania komórek kadrowych i/lub odpowiedzialnych za bezpieczeństwo.

3.6. ZARZĄDZANIE FIRMAMI TRZECIMI

Bezpieczeństwo systemów OT może być narażone na znaczne ryzyko ze strony innych podmiotów, na przykład: producentów, firm świadczących serwis czy wsparcie techniczne itp. Technologie, takie jak zdalny dostęp, wprowadzają nowe zagrożenia z zewnątrz organizacji. W związku z tym, partnerzy zewnętrzni muszą być zaangażowani i podejmować działania w kierunku ograniczenia tych potencjalnych zagrożeń. Zarządzanie firmami zewnętrznymi można podzielić na trzy obszary:

- identyfikacja ryzyka – proces umożliwiający określenie realnego zagrożenia wynikającego ze współpracy z firma zewnętrzną uwzględniając aspekty fizycznego jak i zdalnego dostępu tych firm do systemów OT;
- migracja oraz mitygacja ryzyka – celem odnoszenia się do bezpieczeństwa w umowach z podmiotami trzecimi jest wdrożenie i utrzymanie odpowiedniego poziomu bezpieczeństwa informacji i realizacji usług. Zakres informacji przekazywany podmiotom zewnętrznym powinien być ograniczony do zakresu realizowanych przez niego usług z uwzględnieniem zachowania ich poufności;
- kontrola/weryfikacja – wykonywanie cyklicznych kontroli opisujących poziom techniczny i organizacyjny jaki powinny posiadać współpracujące firmy – kontrole te powinny być uzależnione od zakresu dostępu do systemów OT.

3.6.1. Zarządzanie firmami trzecimi – aspekt prawny

Dobre praktyki z obszaru prawnego, mające na celu minimalizację ryzyka związanego z działalnością osób fizycznych lub innych podmiotów gospodarczych (państwowych lub prywatnych), których działania mogą prowadzić do zakłócenia w funkcjonowaniu systemów OT zostały opisane w Narodowym Programie

Ochrony Infrastruktury Krytycznej – Załącznik nr 1, w rozdziale *2.9.1. Rekomendacje do umów zawieranych z podmiotami zewnętrznymi.*

http://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

3.7. ZARZĄDZANIE PROJEKTAMI

Wdrożenie środków ochrony w eksploatowanych rozwiązaniach automatyki przemysłowej jest zwykle dużo trudniejsze i kosztowniejsze w stosunku do uwzględnienia bezpieczeństwa na etapie projektowania i konfigurowania rozwiązania.

Celem zapewnienia, że wszystkie projekty i inicjatywy mogące mieć wpływ na środowisko OT identyfikowane były już na początku ich cyklu życia i obejmowały odpowiednie środki bezpieczeństwa w ich architekturze i specyfikacji rekomendowane jest aby:

- organizacja uwzględniała wymogi bezpieczeństwa w architekturze i specyfikacji systemów OT i zapewniała, że polityka bezpieczeństwa systemów OT organizacji i dobre praktyki były przestrzegane;
- testy akceptacyjne (FAT/SAT) pokrywały weryfikację zalecanych wymogów bezpieczeństwa;
- dla krytycznych systemów OT wykonywany był cyklicznie przegląd bezpieczeństwa.

3.8. ZALECENIA DLA OBSZARU PROCESÓW BEZPIECZEŃSTWA

Numer Zalecenia	Opis zalecenia	Zalecenie (podstawowe/dodatkowe)
K-3.1. Zarządzanie Incydentami		
K-3.1.1.	Organizacja opracowała procedury zarządzania incydentami w obszarze OT	podstawowe
K-3.1.2.	Organizacja dokumentuje i opisuje incydenty bezpieczeństwa zaistniałe w środowisku OT	podstawowe
K-3.2. Odtwarzanie systemów OT		
K-3.2.1.	Organizacja opracowała DRP (Disaster Recovery Plan) dla systemów OT	podstawowe
K-3.2.2.	DRP jest regularnie testowany a wyniki testów są udokumentowane	podstawowe
K-3.2.3.	Organizacja opracowała standardy i procedury opisujące szczegółowo tworzenie i odtwarzanie kopii zapasowych systemów OT	podstawowe
K-3.2.4.	Tworzone kopie zapasowe są regularnie testowane pod kątem możliwości odtworzenia	podstawowe

Numer Zalecenia	Opis zalecenia	Zalecenie (podstawowe/dodatkowe)
K-3.2.5.	Nośniki wykorzystywane do przechowywania kopii zapasowych są odpowiednio zabezpieczone (logicznie oraz fizycznie)	podstawowe
K-3.2.6.	Nośniki wykorzystywane do przechowywania kopii zapasowych są przechowywane poza lokalizacją w której znajdują się komponenty systemu OT	dodatkowe
K-3.3. Aktualizacje i poprawki bezpieczeństwa		
K-3.3.1.	Organizacja opracowała standardy i procedury opisujące dystrybucję aktualizacji i poprawek bezpieczeństwa	podstawowe
K-3.3.2.	Wykorzystywane są narzędzia umożliwiające testowanie aktualizacji i poprawek bezpieczeństwa przed ich implementacją	podstawowe
K-3.3.3.	Wykorzystywane są narzędzia umożliwiające weryfikację aktualizacji i poprawek bezpieczeństwa przez dostawcę systemu OT	dodatkowe
K-3.4. Zarządzanie dokumentacją		
K-3.4.1.	Organizacja posiada pełną dokumentację dotyczącą wykorzystywanych systemów OT oraz architektury sieciowej	podstawowe
K-3.4.2.	Dokumentacja jest regularnie weryfikowana i aktualizowana	podstawowe
K-3.4.3.	Dokumentacja jest zabezpieczone przed dostępem osób nieuprawnionych	podstawowe
K-3.5. Zarządzanie dostępami do systemów OT		
K-3.5.1.	Polityka zarządzania dostępem do systemów OT (wraz z adekwatną strukturą oraz podziałem na role i związane z nimi uprawnienia) została zdefiniowana i zatwierdzona	podstawowe
K-3.5.2.	Pracownik przed otrzymaniem dostępu do systemu OT przechodzi szkolenie z otrzymanych uprawnień, uwzględniające aspekty bezpieczeństwa	podstawowe
K-3.5.3.	Baza użytkowników jest przynajmniej raz na rok weryfikowana pod kątem aktualności i przyznanych uprawnień	podstawowe
K-3.6. Zarządzanie firmami trzecimi		
K-3.6.1.	Organizacja zidentyfikowała wszystkie firmy trzecie, z jakimi współpracuje	podstawowe

Numer Zalecenia	Opis zalecenia	Zalecenie (podstawowe/dodatkowe)
K-3.6.2.	Zdefiniowane zostały wymagania bezpieczeństwa, jakie muszą znaleźć się w umowach z firmami trzecimi	podstawowe
K-3.6.3.	Wykonywane są przynajmniej raz na rok przeglądy firm trzecich w zakresie bezpieczeństwa dostarczanych usług	dodatkowe
K-3.6.4.	Organizacja przed podpisaniem umowy weryfikuje firmy trzecie pod kątem wewnętrznych procedur adresujących obszar bezpieczeństwa systemów OT oraz bezpieczeństwo wykorzystywanego sprzętu komputerowego np. ochronę antywirusową, aktualność poprawek bezpieczeństwa Systemu Operacyjnego itp.	dodatkowe
K-3.6.5.	Organizacja przed podpisaniem umowy weryfikuje firmy trzecie pod kątem doświadczenia i posiadania niezbędnej wiedzy (np. poprzez weryfikację referencji, certyfikatów, szkoleń itp.)	dodatkowe
K-3.7. Zarządzanie projektami		
K-3.7.1.	Organizacja weryfikuje projekty pod kątem ich wpływu na systemy OT	podstawowe
K-3.7.2.	W trakcie realizacji projektu jest prowadzona ciągła weryfikacja implementowanych rozwiązań pod kątem bezpieczeństwa	podstawowe
K-3.7.3.	Projekty są finalizowane poprzez odpowiednio zaprojektowane testy SAT/FAT	podstawowe

4. CZĘŚĆ IV – ARCHITEKTURA ŚRODOWISKA AUTOMATYKI PRZEMYSŁOWEJ

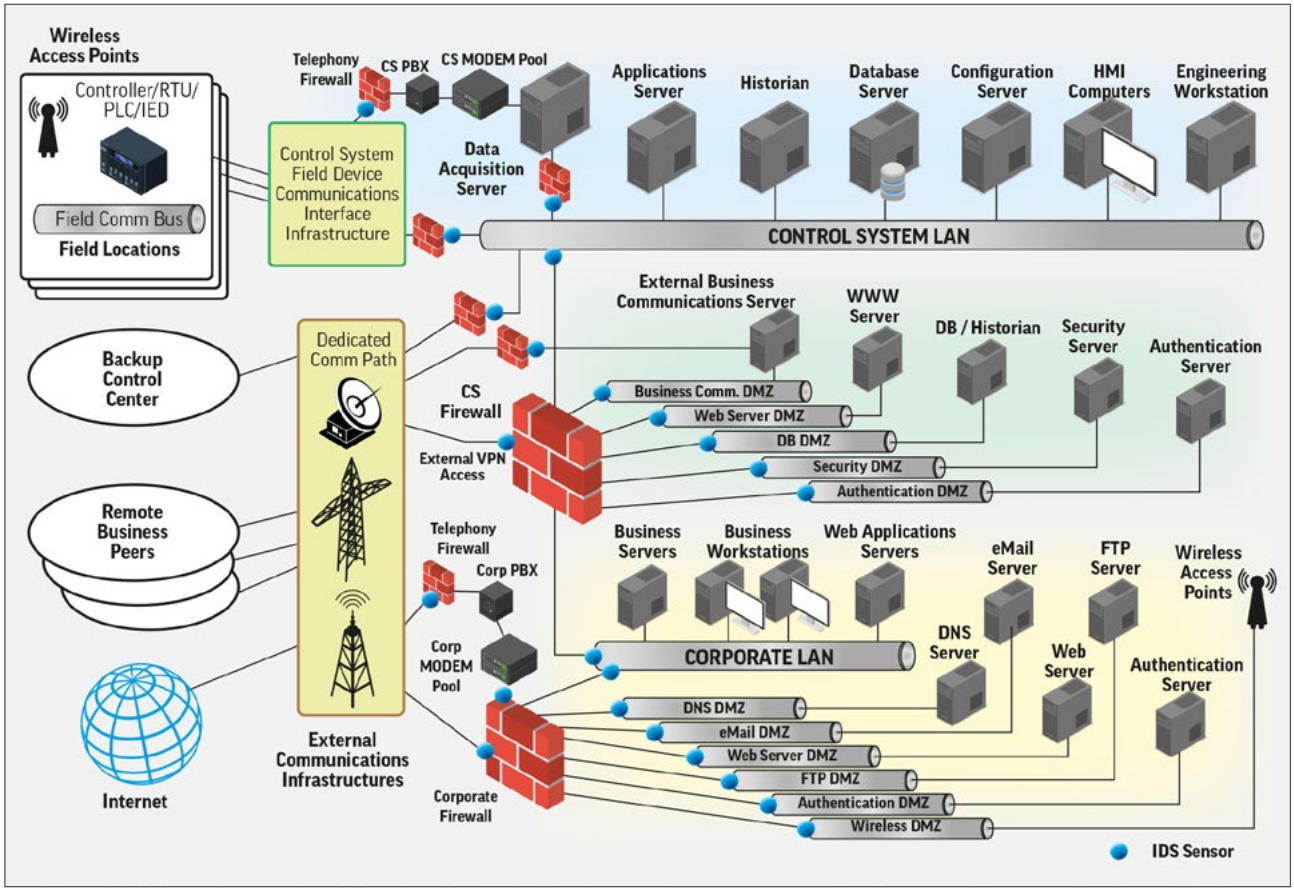
4.1. ARCHITEKTURA SIECI

Jedną z podstawowych zasad w zakresie bezpieczeństwa sieci jest jej budowa w myśl strategii "defense-in-depth", tj. zapewnianie wdrożenia wielu warstw technicznej i administracyjnej kontroli, w celu minimalizacji potencjalnych zagrożeń dla sieci.

W przypadku wdrożenia pojedynczego środka ochrony systemu lub sieci, istnieje ryzyko, że jeżeli zawiedzie, system pozostanie narażony na skuteczną próbę ataku. W modelu "defense-in-depth" celem jest uniknięcie pojedynczych punktów awarii i wprowadzenie wielu warstw środków bezpieczeństwa, aby ograniczyć negatywny wpływ incydentów bezpieczeństwa. Sposobem realizacji modelu „defense-in-depth" jest segmentacja sieci do różnych stref bezpieczeństwa i szczebli sieci w taki sposób, aby możliwe było tworzenie wyraźnych granic.

Efektywna segmentacja ogranicza komunikację pomiędzy sieciami lub strefami bezpieczeństwa, a także zmniejsza ekspozycję na atakującego przechodzącego z jednej sieci do drugiej. Wszystkie systemy i urządzenia w sieci OT są rozmieszczone w wydzielonych sieciach lub odpowiednich strefach bezpieczeństwa, w zależności od stopnia ich krytyczności i klasyfikacji systemu – te strefy bezpieczeństwa są reprezentowane przez LAN biznesowy (strefa niezaufana), DMZ (strefa umiarkowanie zaufana), sieci OT (strefy zaufane). Sieci OT powinny być podłączone do biznesowego LAN za pośrednictwem warstwy DMZ.

Analogicznie jak to opisano dla komunikacji z obszarem IT należy zapewnić narzędzia do kontroli ruchu w warstwie akwizycji danych zwłaszcza w przypadku wykorzystania systemów transmisji danych nie zarządzanych przez właściciela systemu OT.



Rys. 7. Rekomendowana architektura segmentacji sieci według NIST

4.2. BEZPIECZEŃSTWO SIECI BEZPRZEWODOWYCH

Nie rekomenduje się wykorzystywania sieci bezprzewodowych w środowisku OT. W przypadku uzasadnienia biznesowego użycia sieci WLAN, które wymagają przewodowego dostępu do sieci OT, urządzenia klienta powinny mieć zezwolenie jedynie na dostęp do wymaganego hosta lub podsieci w sieci przewodowej, używając jedynie koniecznych protokołów. Jeżeli sieć WLAN ma inny profil bezpieczeństwa, musi być całkowicie oddzielona od sieci OT przy użyciu zapory np. zewnętrzny bezprzewodowy LAN utworzony dla gości musi być fizycznie i logicznie oddzielony od sieci OT.

Jeżeli organizacja wykorzystuje sieci WLAN w środowisku OT rekomenduje się by:

- używać silnych protokołów szyfrowania i uwierzytelniania,
- użycie silnego nie-słownikowego hasła (o długości co najmniej 12 znaków, i jeśli możliwe, składające się z losowych znaków),
- regularne zmienianie lub rotowanie kluczy dla wszystkich klientów,
- stosować niestandardowe nazwy SSID (niewskazujące np. na lokalizację, dział itp.),
- zarządzanie urządzeniami dostępowymi powinno być możliwe wyłącznie z sieci przewodowej.

4.3. ZDALNY DOSTĘP

Zdalny dostęp do systemów OT musi być zatwierdzony przez właściciela biznesowego systemu OT.

Zdalny dostęp spoza sieci biznesowej organizacji musi być realizowany poprzez szyfrowane połączenie i wykorzystywać co najmniej dwu-składnikowe uwierzytelnianie (np. kod pin + token). Zdalny dostęp do systemów OT powinien przebiegać zawsze z wykorzystaniem odpowiednich narzędzi zlokalizowanych w strefie DMZ.

Dedykowane rozwiązanie do zdalnego dostępu powinno być wdrożone w segmencie sieci DMZ, kontrolując dostęp do systemów utrzymywanych w sieci OT. Po uwierzytelnieniu użytkownika w rozwiązaniu zdalnego dostępu, użytkownik albo otrzymuje zestaw aplikacji do uruchomienia albo może uruchomić oddzielną sesję terminala bezpośrednio do systemu w sieciach OT. Wszelki dostęp użytkownika powinien być ściśle kontrolowany i monitorowany na rozwiązaniach zdalnego dostępu.

Zdalny dostęp realizowany dla potrzeb serwisowych, zwłaszcza realizowany przez firmy zewnętrzne powinien być zablokowany lub musi się odbywać w oparciu o ustalone procedury, gwarantujące identyfikację serwisantów oraz ustalające techniczne środki zapewniające bezpieczeństwo realizacji takich usług (zabezpieczenia i identyfikacja sprzętu wykorzystywanego przez serwisanta).

4.4. OCHRONA ANTYWIRUSOWA

Ochrona antywirusowa stanowi środek zmniejszający ryzyko zainfekowania systemów OT złośliwym oprogramowaniem, które może być wprowadzone nie tylko poprzez sieć ale również przez różnego typu przenośne nośniki danych np. pamięci typu Flash, CD, DVD, zewnętrzne dyski twarde. Poniżej przedstawione zostały najważniejsze zasady związane z ochroną antywirusową.

1. Rekomenduje się, aby serwery, komputery stacjonarne, laptopy, zdalnie podłączone systemy komputerowe, tablety oraz inne urządzenia mobilne w środowisku OT lub wymieniające ze środowiskiem OT bezpośrednio informacje były chronione przez oprogramowanie antywirusowe.
2. Posiadaczom kont do systemów OT nie wolno wyłączać lub odinstalowywać oprogramowania antywirusowego.
3. Oprogramowanie antywirusowe powinno być aktualizowane zgodnie z przyjętymi procedurami (patrz 3.3. Aktualizacje i poprawki bezpieczeństwa).
4. Wszyscy pracownicy i współpracownicy muszą zgłaszać przypadki podejrzenia infekcji złośliwym oprogramowaniem.
5. Wszyscy pracownicy i współpracownicy powinny przestrzegać odpowiednich zaleceń lub procedur reagowania na incydenty bezpieczeństwa.
6. Przed zainstalowaniem jakiejkolwiek ochrony antywirusowej należy skonsultować się ze dostawcą systemu OT – każde wybrane rozwiązanie powinno być w pełni wspierane przez dostawcę systemu.
7. Aktualizacje sygnatur wirusów powinny być wykonywane tylko w czasie, gdy służby wsparcia i administratorzy systemów są łatwo dostępni, aby mogli zareagować na wszelkie nieprzewidziane problemy.

4.5. BEZPIECZEŃSTWO SERWERÓW, STACJI ROBOCZYCH I URZĄDZEŃ OT

Rekomenduje się blokowanie nadmiarowych, niewykorzystywanych funkcjonalności, aby zapobiec nieautoryzowanemu dostępowi lub zmianom w systemie OT. Ponadto należy:

- usunąć wszystkie zbędne funkcje, elementy, porty TCP / UDP i usługi w celu zabezpieczenia przed nieuprawnionym użyciem,
- stosować ścisłą kontrolę nad mediami, takimi jak przenośne urządzenia USB lub zablokowanie ich portów w przypadku, gdy są nieużywane,

- wyłączyć automatyczne uruchamianie aplikacji (funkcja auto-run) dla wszystkich nośników przenośnych,
- uruchomić logowanie na wszystkich systemach i urządzeniach sieciowych, takich jak zapory, serwery DNS, przełączniki i routery,
- utrzymywać aktualne oprogramowanie firmware na urządzeniach sieciowych oraz urządzeniach OT,
- wymagać autoryzacji administratora w przypadku zamiany lub aktualizacji firmware,
- weryfikować integralność plików aktualizacji/firmware poprzez porównywanie funkcji skrótu pobranego pliku z funkcją skrótu opublikowaną przez producenta (jeśli dokonano takiej publikacji),
- zmienić domyślne ustawienia fabryczne związane z bezpieczeństwem (np. hasła dostępu) na urządzeniach sieciowych i OT,
- wyłączyć w systemach sterowania dostępy do poczty e-mail i sieci Internet,
- uruchomić automatyczne informowanie administratora o zmianach (podniesieniu) uprawnień użytkowników.

4.6. BEZPIECZEŃSTWO FIZYCZNE

Bezpieczeństwo fizyczne obejmuje całokształt działań operatora infrastruktury krytycznej chroniących przed nieautoryzowanym dostępem do urządzeń, instalacji i osób warunkujących funkcjonowanie systemów OT. Właściciel biznesowy we współpracy z jednostką organizacyjną właściwą w zakresie ochrony i bezpieczeństwa organizuje zasady ochrony systemów OT celem minimalizacji ryzyka zakłócenia ich funkcjonowania.

Przyznawanie, kontrolowanie i monitorowanie fizycznego dostępu do urządzeń, systemów i osób jest niezwykle ważne dla bezpieczeństwa systemów OT. Rekomendowane są następujące zasady związane z bezpieczeństwem fizycznym:

- Identyfikacja (precyzyjna i udokumentowana) urządzeń, instalacji i osób warunkujących funkcjonowanie systemów OT u operatora infrastruktury krytycznej.
- Proces przyznawania fizycznego dostępu do zasobu OT musi zawierać uzasadnioną zgodę właściciela biznesowego w konsultacji z jednostką organizacyjną właściwą w zakresie ochrony i bezpieczeństwa.
- Osoba starająca się o dostęp musi w sposób udokumentowany odbyć niezbędne szkolenia związane między innymi z ochroną fizyczną w dostępie do aktywów OT, zanim dostęp ten zostanie nadany.
- Karty dostępu i / lub klucze dostępowe wydawane muszą być indywidualnie w sposób policzalny i nie mogą być współużytkowane lub wypożyczone innym osobom.
- Karty dostępu i / lub klucze dostępowe, które nie są już potrzebne, nie są wykorzystywane muszą zostać zwrócone do odpowiedniej osoby odpowiedzialnej po stronie właściciela biznesowego. Karty, klucze nie mogą być przekazane innej osobie, z pominięciem procesu zdania i udokumentowania tego faktu.
- Fakt zgubienia bądź kradzieży karty i/lub kluczy dostępu należy natychmiast zgłosić zgodnie z funkcjonującymi u operatora IK zasadami do wskazanej osoby odpowiedzialnej za obsługiwanie tego typu zgłoszeń.
- Logi związane z dostępem fizycznym (w przypadku systemu kontroli dostępu) powinny być pod kątem identyfikacji nieprawidłowości w zakresie dostępu lub zakresu korzystania z nadanych uprawnień. Logi muszą być przechowywane w sposób uniemożliwiający nieuprawnioną ingerencję, w stanie kompletnym przez okres przewidziany w regulacjach wewnętrznych organizacji.

Wszelkie incydenty związane z nadawaniem uprawnień, z dostępem fizycznym oraz z zakresem wykorzystania nadanych uprawnień muszą być zgłaszane w określonym trybie i formie oraz w sposób udokumentowany wyjaśnione przez właściwą merytorycznie jednostkę organizacyjną operatora IK .

4.7. MONITOROWANIE SYSTEMÓW OT

Każda organizacja powinna wdrożyć narzędzia umożliwiające agregację oraz korelację danych i informacji, w szczególności dotyczących aspektów bezpieczeństwa pozyskanych z rozwiązań typu IDS/IPS, zapory, ochrony antywirusowej, systemów kontroli dostępu i aplikacji.

Jako uzupełnienie rozwiązań typu firewall w celu monitorowania ruchu w sieci OT i odpowiedniej reakcji rekomendowane jest wdrożenie rozwiązań typu IDS dedykowanych dla środowiska OT pozwalające na analizę ruchu sieci i detekcję wszelkich anomalii. Informacje przekazywane przez rozwiązania typu IDS do rozwiązań korelujących informacje powinny uwzględniać m.in.:

- datę i stempel czasowy zdarzenia,
- typ zdarzenia lub alert,
- priorytet, waga, wpływ,
- adresy IP (źródłowy oraz docelowy),
- protokoły sieciowe, transportowe, i warstwy aplikacji,
- źródłowe i docelowe porty TCP/ UDP, typy i kody ICMP.

4.8. ZARZĄDZANIE HASŁAMI

Podstawowym sposobem dostępu do systemu informatycznego jest użycie nazwy użytkownika i hasła. Dla systemów informatycznych, w tym systemów OT często są to jedyne klucze do systemu i muszą być odpowiednio chronione. Narzędzia do łamania haseł są zdolne do złamania hasła opartego na cyfrach i literach w przeciągu kilku godzin. W Internecie istnieją również witryny, które publikują domyślne hasła dla sprzedawanych systemów, w tym urządzeń systemu sterowania. Zaleca się:

- zmianę domyślnych haseł, o ile jest to możliwe technicznie,
- zastosowanie odpowiedniej polityki haseł uwzględniając w niej złożoność i cykliczną zmianę,
- ograniczenie wykorzystywania wspólnych kont,
- bezpieczną dystrybucję haseł,
- określenie zasad przechowywania haseł w sposób gwarantujący ich poufność, ale i dostępność w sytuacjach awaryjnych,
- wprowadzenie wieloskładnikowego uwierzytelniania dla administratorów.

4.9. ZALECENIA DLA OBSZARU ARCHITEKTURY

Numer Zalecenia	Opis zalecenia	Zalecenie (podstawowe/dodatkowe)
K-4.1. Architektura sieci		
K-4.1.1.	Połączenie pomiędzy systemami OT a siecią korporacyjną powinny być zabezpieczone co najmniej poprzez firewall oraz strefę (DMZ)	podstawowe
K-4.1.2.	Reguły firewalla powinny podlegać okresowym przeglądom	podstawowe
K-4.1.3.	Wszelkie zmiany konfiguracji i reguł firewalla powinny podlegać ścisłej kontroli i być dokumentowane	podstawowe

Numer Zalecenia	Opis zalecenia	Zalecenie (podstawowe/dodatkowe)
K-4.1.4.	Dostęp do sieci Internet z zasobów w sieci OT powinien być zablokowany	podstawowe
K-4.1.5.	Połączenie pomiędzy systemami OT a siecią korporacyjną realizowane jest z wykorzystaniem rozwiązań zapewniających jednokierunkową komunikacją.	dodatkowe
K-4.2. Bezpieczeństwo sieci bezprzewodowych		
K-4.2.1.	Biurowa sieć bezprzewodowa jest odseparowana od systemów OT	podstawowe
K-4.2.2.	Sieci bezprzewodowe są zabezpieczone przy użyciu odpowiednich mechanizmów bezpieczeństwa (patrz opis)	podstawowe
K-4.2.3.	Dostęp do sieci bezprzewodowych jest zabezpieczony przy użyciu odpowiedniego mechanizmu uwierzytelniania użytkowników	podstawowe
K-4.3. Zdalny dostęp		
K-4.3.1.	Prowadzona jest inwentaryzacja wszystkich połączeń zdalnych do systemów OT	podstawowe
K-4.3.2.	Połączenia zdalne są regularnie weryfikowane pod kątem ich zasadności	podstawowe
K-4.3.3.	Połączenia zdalne są zabezpieczona przy użyciu odpowiedniego mechanizmu uwierzytelniania użytkowników	podstawowe
K-4.3.4.	Stacje robocze lub serwery, do których możliwy jest zdalny dostęp powinny być odpowiednio zabezpieczone (np. oprogramowanie AV)	podstawowe
K-4.4. Ochrona Antywirusowa		
K-4.4.1.	Wszystkie stacje robocze oraz serwery są zabezpieczone oprogramowaniem antywirusowym	podstawowe
K-4.4.2.	Oprogramowanie antywirusowe jest regularnie aktualizowane zgodnie z przyjętymi procedurami	podstawowe
K-4.4.3.	W organizacji funkcjonują zalecenia lub procedura zarządzania incydentami, która uwzględnia postępowania w przypadku wykrycia złośliwego oprogramowania	podstawowe
K-4.5. Bezpieczeństwo serwerów, stacji roboczych i urządzeń OT		
K-4.5.1.	Jest zaimplementowana polityka bezpieczeństwa stacji roboczych, obejmująca korzystanie z zewnętrznych nośników danych	podstawowe

Numer Zalecenia	Opis zalecenia	Zalecenie (podstawowe/dodatkowe)
K-4.5.2.	Urządzenia sieciowe mają zmienione wszystkie fabryczne hasła	podstawowe
K-4.5.3.	Niewykorzystywane porty komunikacyjne/usługi systemowe są zdezaktywowane	podstawowe
K-4.5.4.	Porty USB/napędy optyczne są odpowiednio zabezpieczone przed nieuprawnionym dostępem lub zablokowane.	podstawowe
K-4.5.5.	Dostęp do urządzeń sterowania np. sterowników PLC tam gdzie to możliwe zabezpieczony jest hasłem.	dodatkowe
K-4.6. Bezpieczeństwo fizyczne		
K-4.6.1.	Dostęp do budynków/pomieszczeń jest regulowany przy użyciu odpowiedniego systemu kontroli dostępu.	podstawowe
K-4.6.2.	Dostępy do budynków/pomieszczeń nadane pracownikom lub podmiotom zewnętrznym są regularnie weryfikowane.	podstawowe
K-4.6.3.	Logi z systemu kontroli dostępu korelowane są z innymi zdarzeniami przez rozwiązaniem typu SIEM (ang. *Security Information and Event Management*).	dodatkowe
K-4.7. Monitorowanie systemów OT		
K-4.7.1.	Ruch sieciowy wysyłany do oraz z systemów OT jest monitorowany, wszelkie zdarzenia są logowane	podstawowe
K-4.7.2.	Logi z systemów automatyki są archiwizowane oraz regularnie weryfikowane i analizowane pod kątem potencjalnych nieprawidłowości i/lub naruszeń bezpieczeństwa.	podstawowe
K-4.7.3.	Zostało zaimplementowane odpowiednie narzędzie umożliwiające automatyczną korelację informacji	dodatkowe
K-4.7.4.	Zostały zaimplementowane narzędzia klasy IDS umożliwiające zaawansowaną detekcję incydentów bezpieczeństwa	dodatkowe
K-4.8. Zarządzanie hasłami		
K-4.8.1.	Organizacja wdrożyła politykę haseł dla systemów OT	podstawowe
K-4.8.2.	Wszystkie systemy OT objęte są polityka haseł, a zgodność kont użytkowników systemów OT z polityką jest okresowo weryfikowana	podstawowe
K-4.8.3.	Polityka haseł zaimplementowana jest w kontrolerze Domeny, który weryfikuje zgodność haseł użytkowników z polityką haseł systemów OT organizacji	dodatkowe

5. CZĘŚĆ V – WSPÓŁPRACA SEKTOROWA

Bezpieczeństwo systemów OT nie powinno być traktowane jako aspekt przewagi konkurencyjnej, a jako wartość wspólna, budująca zaufanie do sektora i zapewniająca ciągłość procesów krytycznych. Z tego względu wszelkie przejawy współpracy sektorowej w obszarze bezpieczeństwa powinny być postrzegane jako korzystne i wspierane przez najwyższe kierownictwo operatorów infrastruktury krytycznej. Jako przykłady zasadnej współpracy sektorowej można przytoczyć:

- tworzenie centrów analizy i wymiany informacji (ang. *Information Sharing and Analysis Center* – ISAC) czy sektorowych jednostek CSIRT (szczególnie w zakresie rejestrowania zdarzeń bezpieczeństwa, alarmowanie innych organizacji w sektorze, opracowywanie rekomendacji itp.),
- organizowanie wspólnych warsztatów, szkoleń, konferencji z zakresu bezpieczeństwa,
- wspólna realizacja inicjatyw poprawy bezpieczeństwa, szczególnie w pracach rozwojowych, wymagających zaangażowania zasobów ludzkich i finansowych (opracowywanie koncepcji, realizacja tzw. dowodów poprawności – ang. *proof of concept*).

Współpraca sektorowa powinna być realizowana z zachowaniem ochrony tajemnicy poszczególnych przedsiębiorstw oraz oparta na formalnie zdefiniowanych zadaniach (regulaminach, porozumieniach, itp.).

ZAŁĄCZNIK NR 1 – SKRÓTY I DEFINICJE

Atak
Celowe i zaplanowane działanie, powodujące błędne funkcjonowanie, zakłócenie pracy lub wyłączenie systemu automatyki przemysłowej.

Centrum sterowania
Lokalizacja wyposażona w odpowiednie narzędzia umożliwiające monitorowanie parametrów pracy oraz sterowanie infrastrukturą technologiczną zainstalowaną na obiekcie/obiektach.

DCS (ang. *Distributed Control System*) – Rozproszony System Sterowania
Rozproszony system sterowania rozumiany jako system mogący składać się z wielu jednostek obliczeniowych (kontrolerów) zbierających sygnały z instalacji technologicznej oraz wysyłających sygnały sterowania do urządzeń wykonawczych ze zintegrowanymi funkcjami sterowania, wizualizacji i nadzoru, wykorzystujący jedną wspólną bazę danych pomiarowo-sterujących pracujący w systemie czasu rzeczywistego.

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

Brama sieciowa (ang. *Gateway*)
Mechanizm pośredniczący w komunikacji dwóch odrębnych sieci komputerowych.

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

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:

a. zaopatrzenia w energię, surowce energetyczne i paliwa,
b. łączności,
c. sieci teleinformatycznych,
d. finansowe,
e. zaopatrzenia w żywność,
f. zaopatrzenia w wodę,
g. ochrony zdrowia,
h. transportowe,
i. ratownicze,
j. zapewniające ciągłość działania administracji publicznej,
k. 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 regulować i monitorować dostęp do zasobów systemu, zgodnie z przyjętą polityką bezpieczeństwa.

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

Log
Rejestr zdarzeń w którym automatycznie zapisywane są informacje o zdarzeniach i działaniach dotyczące pracy programu / systemu informatycznego.

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

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

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.

Pomiar
Wskazanie zbierane z urządzenia pomiarowego. Rozróżniamy pomiar rozliczeniowy oraz technologiczny (związany z realizacją procesu technologicznego).

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.

Sieć automatyki zabezpieczeniowej
Sieć komunikacyjna będąca częścią SIS, dedykowana do przyrządowych systemów bezpieczeństwa oraz zapewniająca odpowiednio wysoki poziom niezawodności.

DMZ (Demilitarized Zone)
Logicznie wydzielony segment sieci znajdujący się pomiędzy sieciami o różnym poziomie krytyczności dla danej organizacji. W kontekście najlepszych praktyk bezpieczeństwa automatyki przemysłowej, DMZ jest najczęściej rozumiany, jako pośredniczący segment sieci (ograniczonego zaufania pomiędzy siecią

użytkowników biurowych (niezaufaną), a sieciami produkcyjnymi, w których pracują systemy automatyki przemysłowej (zaufaną – chronioną przez zaporę ogniową).

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 Wspierający System OT (WSO)
System wspierający działanie Systemu OT, to taki system teleinformatyczny, bez którego System OT nie może realizować postawionego przed nim celu zastosowania, lub działanie systemu OT może być narażone na niebezpieczeństwo. Systemy WSO mogą być współdzielone i mogą świadczyć swoje usługi również na potrzeby Systemów ICT.

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).

WLAN (ang. *Wireless Local Area Network*)
Bezprzewodowa lokalna sieć komputerowa wykorzystująca mikrofale/fale podczerwieni jako medium przenoszenia sygnałów. Sieci typu WLAN standaryzuje norma IEEE 802.11.

Zapora sieciowa (ang. *Firewall*)
Dedykowane urządzenie lub oprogramowanie mające na celu ochronę na poziomie sieci teleinformatycznej przed nieuprawnionym dostępem poprzez filtrowanie ruchu i odrzucanie nieautoryzowanych prób połączeń.

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

ZAŁĄCZNIK NR 2 – MIĘDZYNARODOWE INICJATYWY Z OBSZARU BEZPIECZEŃSTWA SYSTEMÓW OT

Bezpieczeństwo środowiska OT od lat jest adresowane przez standardy bezpieczeństwa dedykowane dla systemów przemysłowych, m.in. przez:

1. Seria standardów ISA/IEC-62443 opracowywana przez International Society for Automation (ISA) opisująca metody i rekomendacje zabezpieczeń proceduralnych oraz technicznych w środowisku OT. Standardy podzielone są na grupy odbiorców dla których są dedykowane: właścicieli zasobów (systemów OT), integratorów systemów, specjalistów z obszaru bezpieczeństwa OT oraz producentów rozwiązań OT.

2. Standardy amerykańskiej agencji NIST (National Institute of Standards and Technology) która opublikowała *Special publication 800-53*, *„Security and Privacy Controls for Federal Information Systems and Organizations”*, opisująca zestaw kontroli zwiększających bezpieczeństwo systemów informatycznych. Instytut opublikował również dokument dedykowany bezpieczeństwu OT *Special Publication 800-82*, *„Guide to Industrial Control System (ICS) Security”*, bazujący na dokumencie *800-53 ale rozszerzający kontrole o specyfikę środowiska OT.*

Bezpieczeństwo OT jest również przedmiotem wielu witryn internetowych, wśród nich m. in.:

1. Strona ICS-CERT Departamentu Bezpieczeństwa Stanów Zjednoczonych zbierająca informacje o incydentach i zagrożeniach dla środowiska OT
   https://ics-cert.us-cert.gov/

2. Strona SANS Industrial Control Systems Security Blog poświęcona tematyce bezpieczeństwa systemów OT
   https://ics.sans.org/blog

RCB
Rządowe Centrum
Bezpieczeństwa

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