**­­**

**Załącznik nr B7 – Cyberbezpieczeństwo OT**

**Program Funkcjonalno - Użytkowy**

Spis treści

[1 Definicje i skróty 4](#_Toc185321370)

[2 Ogólne założenia w zakresie cyberbezpieczeństwa systemów OT 4](#_Toc185321371)

[Pomieszczenia OT. Miejsca instalacji infrastruktury sprzętowej 6](#_Toc185321372)

[4 Serwerownie – pomieszczenia dedykowane 6](#_Toc185321374)

[5 Obiekt - Wydzielenie szaf infrastruktury OT 6](#_Toc185321375)

[Obiekt - Wydzielenie szaf z osprzętem ICT 8](#_Toc185321376)

[6 Oprogramowanie antywirusowe 8](#_Toc185321377)

[4.1 Licencje 8](#_Toc185321378)

[4.2 Aktualizacje w okresie gwarancyjnym 9](#_Toc185321379)

[7 Architektura i topologia sieci 9](#_Toc185321380)

[Segmentacja sieci 9](#_Toc185321381)

[Wydzielenie sieci fizycznych 10](#_Toc185321382)

[Separacja stref poprzez firewall 10](#_Toc185321383)

[Standard urządzeń Firewall na styku IDMZ <-> OT 10](#_Toc185321384)

[Urządzeń Firewall w warstwie 1na styku warstwy operatorskiej (system SCADA) a warstwy sterowniczej (systemy PLC) 11](#_Toc185321385)

[8 Łączność OT 11](#_Toc185321386)

[9 Infrastruktura sprzętowa (serwery, macierze, stacje robocze) OT 11](#_Toc185321387)

[10 Badanie cyberbezpieczeństwa systemów OT metodą HAZOP 12](#_Toc185321388)

[11 System kopi bezpieczeństwa 12](#_Toc185321389)

[11.3 Systemy DCS, SCADA i pozostałe systemy wspierające 12](#_Toc185321390)

[11.4 Instrukcje, szkolenia 13](#_Toc185321391)

[Kopie bezpieczeństwa 14](#_Toc185321392)

[12 Monitorowanie infrastruktury OT 14](#_Toc185321393)

[Wymagania w zakresie systemu IDS 14](#_Toc185321394)

[Monitoring ruchu sieciowego 14](#_Toc185321395)

[Monitorowane infrastruktury sprzętowej 14](#_Toc185321396)

[Syslog, SIEM 14](#_Toc185321397)

[13 Hardening - utwardzanie 14](#_Toc185321398)

[Przełącznik, router 14](#_Toc185321399)

[System operacyjny, komputer 15](#_Toc185321400)

[14 Wymiana danych 15](#_Toc185321401)

[15 Architektura systemów uwierzytelniania i autoryzacji 15](#_Toc185321403)

[16 Strefa zdemilitaryzowana Industrial DMZ (iDMZ) 15](#_Toc185321404)

[17 System AntyAPT 15](#_Toc185321405)

[18 Serwer czasu 16](#_Toc185321406)

# Definicje i skróty

1. CVE – Common Vulnerabilities and Exposures , czyli słownik identyfikatorów nadanych podatnościom i zagrożeniom. Projekt tworzenia i utrzymywania słownika jest współfinansowany przez biuro Cybersecurity and Communications Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych. W skrócie jest to po prostu baza podatności.
2. ICS - Przemysłowe systemy sterowania (Industrial Control Systems)
3. WAN - Wide Area Network - oznacza sieć komputerową, która swoim zasięgiem wykracza poza miasto, kraj, lub nawet kontynent.
4. Malware - skrót, który pochodzi od słów malicious software. Oznacza złośliwe oprogramowanie, które zostało stworzone z myślą o uszkodzeniu sprzętu lub kradzieży danych.
5. Atak APT - atak złożony, zaplanowany i należący do grupy zaawansowanych. Atak APT bardziej przypomina szpiegostwo niż tradycyjne hakowanie. Grupy APT działają na podstawie ciągłego podsłuchiwania i zbierania informacji na temat organizacji w celu identyfikacji słabych punktów i potencjalnego miejsca ataku.
6. Ataki typu DoS - Denial of Service - są ukierunkowane na serwery przez naruszanie usług sieci w dążeniu do wyczerpania zasobów aplikacji. Osoby przygotowujące te ataki zalewają witrynę mylącym ruchem, co powoduje nieprawidłowe działanie serwera lub całkowite przeniesienie jej do trybu offline.
7. System operacyjny - oprogramowanie, które zarządza całym systemem IT/OT. Dzięki niemu możliwe jest uruchamianie programów oraz sprawowanie kontroli nad resztą zadań na infrastrukturze sprzętowej.

# Ogólne założenia w zakresie cyberbezpieczeństwa systemów OT

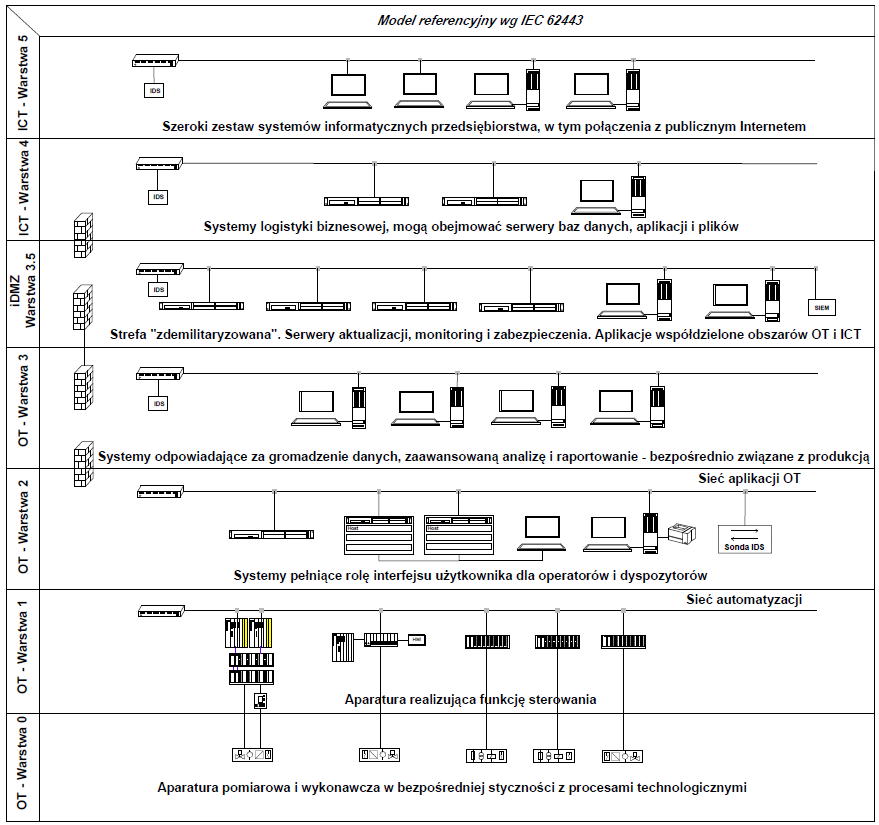
W celu zapewnienia odpowiedniego poziomu cyberbezpieczeństwa obszaru OT (OT – ang. Operational Technology) projekt techniczny i realizacja zadania docelowo musi zapewnić min. :

1. całkowitą separację obszaru OT od ICT poprzez strefę DMZ (strefa zdemilitaryzowana) zgodnie z modelem w normie IEC62443 – brak bezpośredniego dostępu do WAN z poziomu systemów OT oraz dostępu do obszaru OT z pominięciem DMZ
2. automatyczne wykonywanie kopii zapasowych
3. ochronę antywirusową
4. ochronę przed malware i atakami APT
5. tzw. hardering serwerów i stacji inżynierskich oraz operatorskich
6. segmentację sieci OT zgodnie z modelem w normie IEC 62443
7. ochronę poszczególnych warstw sterowania (zgodnych z modelem opisanym w normie IEC 62443) poprzez firewall oraz system IDS
8. monitoring infrastruktury OT w tym pasywny monitoring sieci OT
9. logowanie zdarzeń obszaru OT do centralnego systemu SIEM.

Wymaga się aby wszystkie urządzenia w obszarze infrastruktury OT typu firewall, switch, router posiadały co najmniej certyfikat Common Criteria EAL3+ lub PP Compliant. Wszelkie odstępstwa od tego wymagania musza zostać zatwierdzone przez Zamawiającego (Departament Cyberbezpieczeństwa i ICT PGE EC) na etapie zatwierdzania dokumentacji wykonawczej.

Wymaga się zastosowania wdrożenia co najmniej poziomu bezpieczeństwa (ang. Security level) SL2, który jest podstawowym wymaganiem dla systemów przemysłowych zgodnie z normą 62443 ( Definicja według normy IEC 62443 - miara pewności, że system IACS jest wolny od luk w zabezpieczeniach i działa w zamierzony sposób). Norma IEC 62443-3-3 specyfikuje 23 wymagania, które muszą być spełnione.

Wymagane jest aby nowo wdrożone środowisko teleinformatyczne przedstawione było w postaci modelu warstwowego zgodnie z normą IEC 62443, którego najwyższą warstwę stanowią klasyczne systemy IT, a najniższą aparatura kontrolno-pomiarowa oraz elementy wykonawcze oddziałujące na procesy technologiczne. Środowisko teleinformatyczne powinno składać się z warstw przedstawionych na poniższym przykładowym modelu.



W obszarze OT wyróżnić należy:

Warstwa 3 – Zarządzanie procesami produkcji. W tej warstwie powinny się znaleźć systemy  
 integracji odpowiadające za gromadzenie danych, zaawansowaną analitykę, raportowanie.

Warstwa 2 – Nadrzędne sterowanie procesami. W tej warstwie powinny się znaleźć systemy pełniące rolę interfejsu użytkownika dla operatorów/dyspozytorów które pozwalają na monitorowanie oraz sterowanie procesem technologicznym. Systemy, które powinny być tutaj usytuowane to m.in:

a) serwery aplikacji SCADA/DCS;

b) stacje operatorskie i inżynierskie;

c) serwery baz danych;

d) macierze dyskowe;

e) interfejsy użytkownika;

Warstwa 1 – warstwa automatyki sterowniczej. Warstwa powinna zawierać elementy aparatury sterowniczej sterowniki PLC, kontrolery, urządzenia typy black box

Warstwa 0 – warstwa procesu technologicznego. Warstwa zawiera maszyny, roboty, sensory, czujniki, serwomechanizmy, elementy pomiarowe, pozwalające monitorować stan procesu technologicznego oraz elementy wykonawcze, pozwalające zmieniać stan procesu technologicznego.

# Pomieszczenia OT. Miejsca instalacji infrastruktury sprzętowej

Wymagania w powyższym zakresie zostały ujęte w załączniku 1PD Cyberbezpieczeństwo – wymagania serwerowni/pomieszczeń technicznych.

# Serwerownie – pomieszczenia dedykowane

W przypadku budowy systemów OT i ICT wymaga się zabudowy lub adaptacji istniejących pomieszczeń (np. zabudowa ścian działowych z gk oddzielonych drzwiami z Kontrolą Dostępu zgodnie z normą PN-EN 1627 )celem uzyskania dwóch niezależnych serwerowni (lub pomieszczeń technicznych) systemów OT i ICT. W uzasadnionych przypadkach, za zgodą Zamawiającego dopuszcza się dostosowanie jednego pomieszczenia, jednak szafy obu systemów muszą być fizycznie odseparowane oraz wyposażone w czytniki kontroli dostępu do szaf.

Wejście do serwerowni musi być również objęte monitoringiem wizyjnym, Systemem Kontroli Dostępu oraz systemem ppoż.

# Obiekt - Wydzielenie szaf infrastruktury OT

Podstawową normą dotyczącą wykonywania instalacji okablowania infrastrukturalnego jest norma PN-EN 50174 (Instalacja okablowania): PN-EN 50174-1 – Część 1, Specyfikacja i zapewnienie jakości. PN-EN 50174-2 – Część 2, Planowanie i wykonawstwo instalacji wewnątrz. PN-EN 50174-3 – Część 3, Planowanie i wykonawstwo instalacji na zewnątrz.

Istotą zastosowania okablowania strukturalnego jest możliwość współdzielenia zasobów w ramach jednej instalacji przez wiele systemów teleinformatycznych i teletechnicznych.

**Główny punkt dystrybucyjny (GPD)**, to centralne miejsce gdzie zbiega się okablowanie strukturalne, bardzo często fizycznie oraz CPD (centrum przetwarzania danych). Jest to miejsce w którym kończy(-ą) się kabel(-le) redundantnego ringu światłowodowego.

**Budynkowy (lokalny) punkt dystrybucyjny (BPD)** – miejsce koncentracji, zbioru komponentów aktywnych oraz pasywnych w odrębnych szafach teleinformatycznych zlokalizowanych w danym budynku składająca się budynkowego (lokalnego) punktu infrastruktury aktywnej oraz budynkowego (lokalnego) punktu infrastruktury pasywnej.

**Budynkowy (lokalny) punkt infrastruktury aktywnej** – cześć BPD składająca się z szafy teleinformatycznej (teletechnicznej) oraz przełączników, routerów, lokalnego FW, komputera przemysłowego wraz konsolą KVM.;

**Budynkowy (lokalny) punkt infrastruktury pasywnej** – cześć BPD składająca się z szafy teleinformatycznej (teletechnicznej) oraz zespołu komponentów służących do łączenia kabli (panele krosowe 2U, kable krosowe, kaseta światłowodowa, adaptery światłowodowe, złącza światłowodowe, Panel typu panel HD, zasilacze UPS ).

**Okablowanie systemu strukturalnego** budowane jest w oparciu o połączenia fizyczne z wykorzystaniem topologii ringu redundantnego. W skład podsystemów okablowania strukturalnego, podsystemów urządzeń infrastruktury aktywnej, podsystemów infrastruktury centrów danych wchodzą następujące elementy funkcjonalne:

1. Punkt styku iDMZ;
2. Kable szkieletowe redundantnego ringu światłowodowego;
3. GPD (główny punkt dystrybucyjny) z podziałem na część z elementami pasywnymi (osobna szafa teleinformatyczna (teletechniczna) zawierająca zespół komponentów służących do łączenia kabli (panele krosowe 2U, kable krosowe, kaseta światłowodowa, adaptery światłowodowe, złącza światłowodowe, Panel typu panel HD, zasilacze UPS) oraz z elementami aktywnym (osobna szafa teleinformatyczna zawierająca klaster przełączników corowych, klaster FW, przełączniki dostępowe) oraz CPD ( główne centrum przetwarzania danych);
4. Budynkowy (lokalny) punkt dystrybucyjny (BPD) składający się z budynkowego (lokalnego) punktu dystrybucyjnego infrastruktury pasywnej ,który składa się on najczęściej z szafy teleinformatycznej (teletechnicznej) oraz zespołu komponentów służących do łączenia kabli (panele krosowe 2U, kable krosowe, kaseta światłowodowa, adaptery światłowodowe, złącza światłowodowe, panel typu panel HD ).oraz budynkowy (lokalny) punkt infrastruktury aktywnej składający się z szafy teleinformatycznej (teletechnicznej), przełączników, routerów, lokalnego FW, komputera przemysłowego wraz konsolą KVM. Dopuszcza się łączenie punktu dystrybucyjnego infrastruktury pasywnej oraz lokalnego punkt infrastruktury aktywnej wydzielonych w budynkach posiadających ograniczoną liczbę punktów elektryczno-logicznych oraz urządzeń końcowych do 20 (wymagających nie więcej niż dwóch urządzeń infrastruktury aktywnej)
5. Budynkowe (lokalne) okablowanie (okablowanie pionowe);
6. kable telekomunikacyjne pomiędzy punktami dystrybucyjnymi a punktami elektryczno-logicznymi (okablowanie poziome);

## Obiekt - Wydzielenie szaf z osprzętem ICT

Nie dopuszcza się montażu we wspólnej szafie infrastruktury ICT oraz OT. Sprzętową infrastrukturę ICT należy zabudować w niezależnych szafach. Wymaga się wydzielenie odrębnych szaf dla Systemów Ochrony Technicznej.

Jako Systemy Ochrony Technicznej (SOT) rozumie się:

a) SKD Systemy kontroli dostępu

b) CCTV Systemy monitoringu wizyjnego – monitoring dozorowy

c) PPoż Systemy przeciwpożarowe nieautonomiczne

d) SSWIN Systemy antywłamaniowe

e) HVAC Systemy klimatyzacji i wentylacji

# Oprogramowanie antywirusowe

## Licencje

Wszystkie komputery, serwery fizyczne oraz maszyny wirtualne (systemy operacyjne) poziomu operatorskiego dostarczane w ramach zadania m.in.:

a) serwery operatorskie

b) serwery inżynierskie

c) serwery archiwizacyjno-raportowe

d) stacje operatorskie

e) stacje robocze/procesowe

powinny posiadać zainstalowane licencjonowane oprogramowanie antywirusowe i na bieżąco aktualizowane o nowe sygnatury poprzez serwer aktualizacyjny znajdujący się w iDMZ. System ten powinien zawierać następujące funkcje bezpieczeństwa:

1. Ransomware Shield - dodatkowa warstwa chroniąca użytkowników przed złośliwym oprogramowaniem ransomware. Ta technologia pozwala monitorować i weryfikować wszystkie uruchamiane aplikacje w oparciu o ich zachowanie i reputację. Jest przeznaczona do wykrywania i blokowania procesów przypominających swoim zachowaniem działanie oprogramowania ransomware.
2. System HIPS - monitoruje aktywność wszystkich procesów systemu Windows i wykorzystuje predefiniowane reguły do rozpoznawania podejrzanego działania systemu. W razie wykrycia takiej aktywności HIPS automatycznie unieszkodliwia działanie złośliwego procesu.
3. Ochrona przed atakami sieciowymi – identyfikuje luki w protokołach sieciowych i blokuje ich wykorzystanie, dzięki czemu uniemożliwia rozprzestrzenianie się zagrożeń (m.in. ransomware) wewnątrz sieci OT.
4. Zaawansowany skaner pamięci – zaawansowany skaner pamięci monitoruje zachowanie procesów skanując je w bezpiecznym, odizolowanym środowisku. Skaner ten pozwala wykrywać nowe zagrożenia bezplikowe w przypadku, kiedy konwencjonalne skanery antywirusowe pozostają bezradne.
5. Sandboxing – symuluje działanie zagrożenia w wirtualnym, izolowanym od systemu operacyjnego środowisku.
6. Exploit Blocker – monitoruje aplikacje narażone na ataki exploitów (m.in. przeglądarki, czytniki dokumentów, programy pocztowe, Flash, Java i inne) i zamiast skupiać się tylko na identyfikatorach luk CVE, koncentruje się na rozpoznawaniu technik wykorzystywanych przez exploity. W momencie wykrycia próby wykorzystania exploitu, zagrożenie jest natychmiast blokowane.
7. Ochrona przed botnetami – funkcjonalność, która wykrywa złośliwą komunikację wykorzystywaną przez sieci komputerów zombie, czyli tzw. botnety. Każda zidentyfikowana podejrzana próba komunikacji jest blokowana i zgłaszana użytkownikowi.
8. Dwukierunkowy firewall – zapobiega nieautoryzowanemu dostępowi do sieci firmowej. Zapewnia ochronę przed hakerami oraz naruszeniom danych. Umożliwia definiowanie zaufanych sieci, sprawiając, że wszystkie inne połączenia, na przykład publiczne sieci Wi-Fi, domyślnie mają ograniczony dostęp.

Dostarczone systemy SCADA muszą posiadać instrukcje aktualizacji oprogramowania antywirusowego. Ze względu na standaryzacje rozwiązań dopuszcza się instalację i konfiguracje oprogramowania antywirusowego trzech producentów:

a) ESET

b) Trellix (McAfee)

c) Rozwiązanie klasy EDR TXONE NETWORKS | STELLAR

## Aktualizacje w okresie gwarancyjnym

Dla systemów SCADA wymaga się wskazanie miejsca i sposobu pozyskiwania aktualnych i zwalidowanych baz danych (baza sygnatur wirusów i komponentów programu antywirusowego). Aktualizowanie online bazy sygnatur wirusów oraz komponentów programu antywirusowego możliwe będzie tylko poprzez strefę DMZ.

Wymaga się zapewnienia licencji i aktualizacji sygnatur bazy wirusów na okres co najmniej 5 lat lub na okres gwarancyjny systemów OT o ile jest dłuższy niż 5 lat.

Wymaga się instalacji i konfiguracji centralnej konsoli zarządzającej dla obszaru OT na infrastrukturze serwerowej (VMWare) zamawiającego zlokalizowanej w strefie iDMZ. Wszelkie aktualizacje (oprogramowania i bazy sygnatur wirusów) muszą być odzwierciedlone w logach systemu. Nie dopuszcza się ręcznej aktualizacji oprogramowania antywirusowego i baz wirusów na poszczególnych stacjach systemu OT poprzez nośniki typu pendrive, zewnętrzne dyski USB itp.

W przypadku braku możliwości spełnienia powyższego warunku wymaga się uzgodnień

i akceptacji Zamawiającego na etapie projektu.

# Architektura i topologia sieci

## Segmentacja sieci

Wymaga się podziału obszaru OT na strefy oraz definicję kanałów komunikacyjnych pomiędzy strefami opisanąa w IEC 62443.

Wymaga się podziału infrastruktury sieciowej OT na VLAN-y. Poddział na poszczególne VLAN-y musi być zaakceptowany na etapie zatwierdzania projektu technicznego. Zakłada się iż każda samodzielna jednostka produkcyjna powinna pracować w wydzielonym VLAN-ie.

## Wydzielenie sieci fizycznych

Wymaga się aby w obszarze infrastruktury sieci OT wydzielić oddzielne dedykowane fizycznie sieci LAN dla:

a) obszaru danych technologicznych,

b) obszaru kopii bezpieczeństwa,

c) obszaru zarządzania infrastrukturą sprzętową (typu serwer, macierz, router, switch i firewall),

d) obszaru SOT, BMS,

e) obszaru monitoring ruchu sieciowego,

f) wszystkich pozostałych sieci OT.

## Separacja stref poprzez firewall

Wymaga się separacji sieci stref iDMZ oraz OT poprzez niezależnie pracujące firewalle różnych producentów w układzie klastra HA. Dostawa i konfiguracja firewalli w obszarze iDMZ realizowana jest przez Zamawiającego poza niniejszym projektem.

### Standard urządzeń Firewall na styku IDMZ <-> OT

System zabezpieczeń Firewall powinien składać się z w pełni redundantnego klastra HA . W razie awarii aktywnego węzła, funkcje natychmiast przejmuje drugi węzeł, pracujący przez cały czas w trybie stand-by. Dopuszczalna jest konfiguracja typu active – active.

Urządzenie musi spełniać wymagania wymienione poniżej:

1. Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 1000 znaczników VLAN.
2. System Firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje cały ruch poza dozwolonym przez politykę bezpieczeństwa.
3. System musi posiadać możliwość uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron HTTP.
4. System musi posiadać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
5. System musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP
6. System transparentnie ustala tożsamość użytkowników sieci (integracja z Active Directory, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu precyzyjnie definiuje prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. Ponadto system musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
7. System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.
8. System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
9. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
10. Urządzenie zabezpieczeń musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 100 GB. Muszą zostać dostarczone narzędzia monitorowania, analizy logów i raportowania – jeśli w tym celu wymagany jest zakup zewnętrznych urządzeń, oprogramowania i/lub licencji, to muszą być dostarczone w ramach niniejszego zamówienia.
11. System zarządzania bezpieczeństwem musi umożliwiać usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
12. System zarządzania bezpieczeństwem (w tym również narzędzia monitorowania, analizy logów i raportowania) musi działać w konfiguracji na poziomie Oddziału. Zastosowane rozwiązanie musi zapewniać w przyszłości możliwość zcentralizowania systemu zarządzania bezpieczeństwem.
13. System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.

### Urządzeń Firewall w warstwie 1na styku warstwy operatorskiej (system SCADA) a warstwy sterowniczej (systemy PLC)

Wymaga się instalacji przemysłowych urządzeń firewall pomiędzy strefami warstwy 2 orazw warstwie 1 zgodnie z opisem pkt. 1 niniejszego załącznika. Urządzenia muszą spełniać m.in. poniższe wymagania:

a) redundantne zasilanie

b) wsparcie protokołów komunikacyjnych (Deep Packet Inspection) przy pomocy których komunikować się będą urządzenia dostarczone w ramach Projektu. Przykładowe protokoły to: Modbus RTU, Modbus TCP/IP, UMAS, S7 Communication200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP,PROFINET, IEC 60870-5-104, IEC 61850-3 & IT, Plant Bus, Profibus, CAN, LonWorks.

c) temperatura pracy: -25..+60 °C

d) Stopień ochrony zapewnianej przez urządzenie: IP30

# Łączność OT

Wymagania w powyższym zakresie zostały ujęte w załączniku B7A Cyberbezpieczeństwo – łączność OT .

# Infrastruktura sprzętowa (serwery, macierze, stacje robocze) OT

Wymagania w powyższym zakresie zostały ujęte w załączniku B7C Cyberbezpieczeństwo – Infrastruktura sprzętowa OT.

# Badanie cyberbezpieczeństwa systemów OT metodą HAZOP

Wymagania w powyższym zakresie zostały ujęte w załączniku B7E Cyberbezpieczeństwo – Badanie CS Hazop.

# System kopi bezpieczeństwa

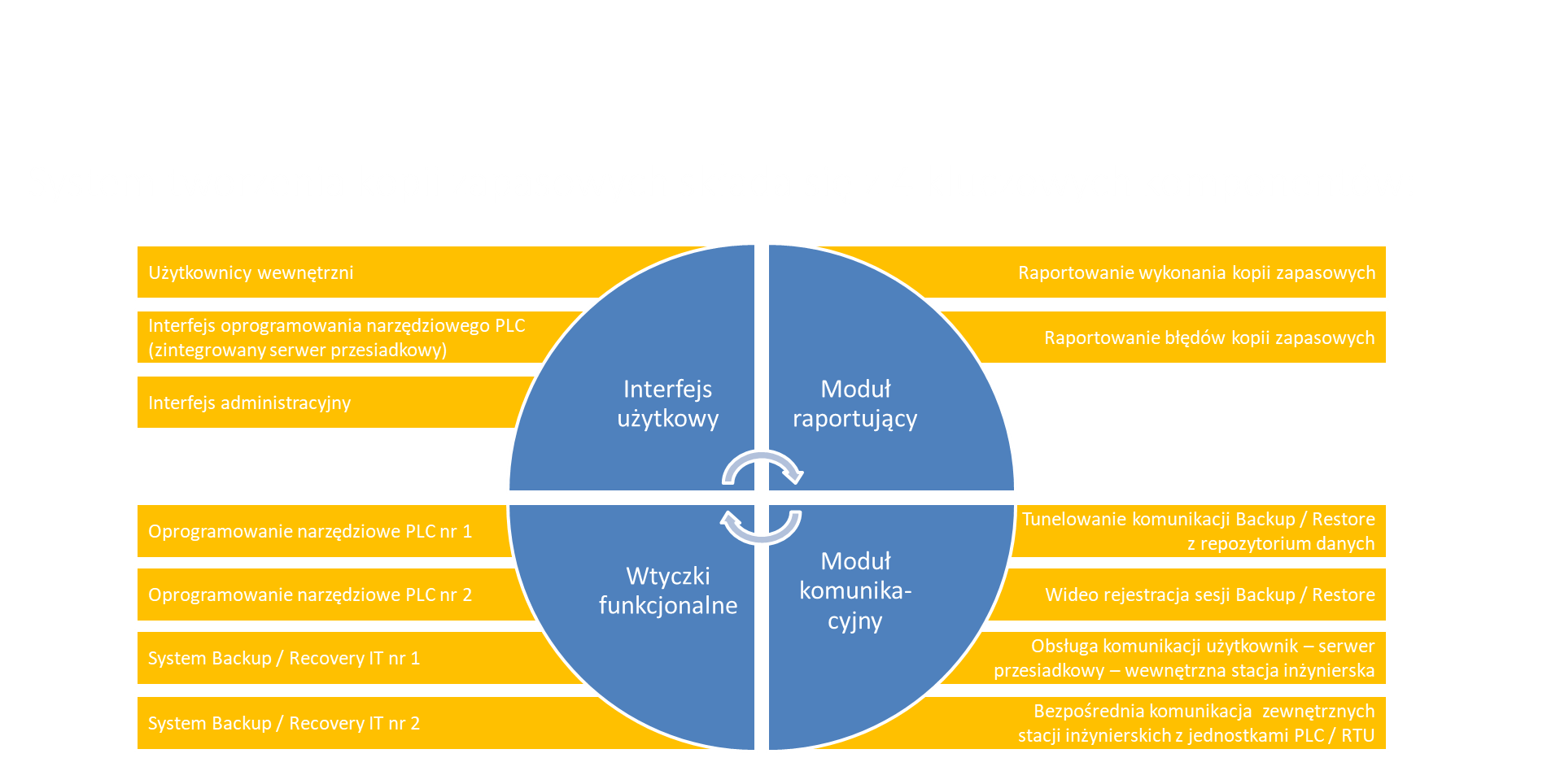
Zabezpieczenie kopii danych należy realizować zgodnie z zasada 3-2-1. Wymaga się przechowania przynajmniej trzech kopii danych (3 x backup), dwóch kopii backupu na różnych urządzeniach  
(2 x backup), z których jedna (1 x backup) znajduje się w innej lokalizacji.

Dodatkowo wymaga się, aby jedna z kopii była typu offline – urządzenia taśmowe, płyty DVD lub równoważne rozwiązania. Wymagania w powyższym zakresie zostały ujęte w załączniku B7C Cyberbezpieczeństwo – Infrastruktura sprzętowa OT.

## Systemy DCS, SCADA i pozostałe systemy wspierające

System tworzenia kopii zapasowych dla środowiska OT powinien uwzględniać w równym stopniu systemy SCADA (*ang. Supervisory Control And Data Acquisition*) jak i sterowniki programowalne PLC *(ang. Programmable Logic Controller)*, jednostki RTU (*ang. Remote Terminal Unit*), IDE (*ang. Integrated Development Environment*) i inne inteligentne urządzenia polowe. Z uwagi specyfikę ww. urządzeń wymaga się tworzenia kopii zapasowej konfiguracji. Pełna kopia zapasowa systemu SCADA powinna składać się z obrazu serwera/serwerów, stacji operatorskich , stacji inżynierskich wraz z kopią zapasową ich konfiguracji. Konfiguracja urządzeń PLC i urządzeń polowych będzie zapisana na stacji inżynierskiej z której pobierana będzie kopia zapasowa.

System tworzenia kopii zapasowych powinien składać się z 4 kluczowych komponentów:



Dla zastosowanych systemów w obszarze OT (DCS, SCADA i innych) wymaga się automatycznego systemu tworzenia kopii bezpieczeństwa, umożliwiającego pełne odtworzenie konfiguracji i aplikacji systemów OT po awarii.

.

W szczególności system powinien:

1. mieć możliwość utworzenia kopii pełnej, przyrostowej i różnicowej
2. tworzenia kopii typu Bare Metal Recovery
3. umożliwiać składowania kopii bezpieczeństwa na dwóch niezależnych urządzeniach wskazanych przez Zamawiającego
4. umożliwiać transfer kopii do centralnego repozytorium Grupy PGE EC
5. umożliwiać tworzenie tzw. kopii off-line – np. taśma (zabezpieczenie przed atakami ransomware)
6. umożliwiać przeprowadzenie testów odtworzeniowych – weryfikacja poprawności kopii zapasowej
7. zapewnić przestrzeń dyskową która pomieści jednocześnie co najmniej:
   * + 6 kopii pełnych
     + 8 kopii różnicowych
     + 14 kopii przyrostowych
8. należy założyć wykonywanie kopii zgodnie z poniższym schematem

|  |  |  |
| --- | --- | --- |
| **typ** | **czasookres wykonywania** | **okres przechowywania kopii** |
| pełna kopia | miesięczny | 6 miesięcy |
| kopia różnicowa | tygodniowy | 8 tygodni |
| kopia przyrostowa | codzienny | 14 dni |

System tworzenia kopii zapasowych będzie zapewniał następujące funkcjonalności:

1. Możliwość centralnego tworzenia kopii zapasowych konfiguracji jednostek PLC/RTU z poziomu stacji inżynierskiej.
2. Bezpieczny transfer i weryfikacja obrazów serwerów w obszarze OT do/z repozytorium centralnego i zapasowego.

W odniesieniu do jednostek PLC/RTU system powinien zapewnić bezpieczne, ręczne tworzenie kopii zapasowej pełnej konfiguracji wraz z wszelkimi algorytmami sterowania przez użytkownika Zamawiającego.

## Instrukcje, szkolenia

Wymaga się:

1. W ramach dostaw sprzętu i licencji zapewnienia oprogramowania narzędziowego oraz osprzętu umożliwiającego realizację powyższych zadań (pkt 11.1) przez specjalistów Zamawiającego oraz przeprowadzenia szkolenia w tym zakresie
2. dostarczenia instrukcji wykonywania i rotacji kopii zapasowych wraz  
   z wytycznymi w zakresie harmonogramu wykonywania kopii oraz tworzenia wersji off-line.

## Kopie bezpieczeństwa

Wymaga się utworzenia kopii bezpieczeństwa wszystkich systemów obszaru OT po pozytywnie zakończonym ruchu próbnym oraz w ostatnim tygodniu gwarancji.

# Monitorowanie infrastruktury OT

## Wymagania w zakresie systemu IDS

Wymaga się dostawy i konfiguracji systemu klasy IDS, który będzie monitorował urządzenia infrastruktury OT. Wymagania w powyższym zakresie zostały ujęte w załączniku B7B Cyberbezpieczeństwo – monitorowanie infrastruktury OT.

## Monitoring ruchu sieciowego

Wszystkie przełączniki sieciowe (w tym przełączniki systemu SCADA) muszą mieć możliwość mirroringu portu, a producent systemu DCS/SCADA musi gwarantować poprawność pracy systemu OT w takiej konfiguracji. Dobór wydajności przełącznika powinien zapewnić prace z aktywnym przekierowaniem ruchu na port monitorujący z wszystkich portów przełącznika bez utraty pakietów.

## Monitorowane infrastruktury sprzętowej

Wymaga się monitorowania urządzeń infrastruktury OT (poprzez oprogramowanie monitorujące ZABBIX lub CHECK\_MK)) wraz z automatycznym powiadamianiem administratorów o zaistniałych problemach (powiadomienie poprzez email, SMS).

## Syslog, SIEM

Wszystkie urządzenia aktywne powinny mieć możliwość zbierania logów. Należy zaimplementować przekazywanie danych do zewnętrznego centralnego systemu klasy SIEM (Zamawiający posiada obecnie IBM QRadar) w standardzie Syslog. Dostawca do systemów DCS i SCADA dostarczy reguły korelacyjne SIEM.

# Hardening - utwardzanie

## Przełącznik, router

Wymaga się, aby wszystkie urządzenia sieciowe w obszarze OT były zarządzalne. W urządzeniach należy wyłączyć wszystkie nieużywane porty oraz niewykorzystywane funkcjonalności.

W szczególności wymaga się:

1. Kontroli dostępu – automatyczne wylogowanie i blokada dostępu do urządzenia,
2. Integralności danych – kontrola integralności plików konfiguracji, aktualizacji oprogramowania,
3. Stosowania takich mechanizmów jak listy kontroli dostępu w przełącznikach sieciowych (tzw. ACL) - kontrola dostępu przez definiowane listy IP,
4. Poufności danych – wykorzystywanie „bezpiecznych połączeń” (SSL/SSH),
5. Szybkiej reakcji na zdarzenia – budowanie logów zdarzeń w oparciu o śledzenie działań dokonywanych przez konkretnych użytkowników,
6. Szyfrowania konfiguracji,
7. Urządzeń obsługujących protokoły sieci OT,
8. Montażu w szafie 19” typu RACK lub na szynie DIN,

## System operacyjny, komputer

Wymaga się aby wszystkie systemy operacyjne miały uruchomiony wewnętrzy programowy firewall. Wykonawca dostarczy instrukcję tzw. „hardeningu” systemu operacyjnego serwerów, stacji operatorskich i inżynierskich oraz wykona tzw. utwardzenia zgodnie z dostarczoną instrukcją. We wszystkich urządzeniach wymaga się blokady programowej lub sprzętowej portów USB z możliwością użycia autoryzowanych przez administratora urządzeń. Wymaga się instalacji i konfiguracji narzędzia LAPS ( Microsoft Local Administrator Password) zapewniającego automatyczne zarządzanie kontem administratora lokalnego na każdym komputerze przynależącym do usługi Active Directory.

# Wymiana danych

Wymiana danych z systemami poza wewnętrznym obszarem OT musi spełniać wymogi  
i standardy cyberbezpieczeństwa Zamawiającego i odbywać się poprzez strefę iDMZ. W zakresie komunikacji OPC wymaga się użycia standardu OPC UA lub tunelowania OPC.

# Architektura systemów uwierzytelniania i autoryzacji

Wymaga się wdrożenie niezależnej domeny AD w strefie OT oraz jednoznacznej identyfikacji operatorów i administratorów systemu SCADA. Nie dopuszcza się pozostawienia domyślnych kont i haseł w dostarczonych systemach i aplikacjach.

# Strefa zdemilitaryzowana Industrial DMZ (iDMZ)

Strefę zdemilitaryzowaną IDMZ Zamawiający organizuje we własnym zakresie.

# System AntyAPT

System ochrony stacji końcowych, wykorzystywanych w sieci OT powinien składać się z dwóch głównych komponentów:

1. Kontroler, wykorzystywany do komunikacji z agentami.
2. Oprogramowanie agenta instalowane na chronionych hostach w sieci OT.

Poprawne funkcjonowanie całego środowiska wymaga ciągłej komunikacji pomiędzy zainstalowanymi agentami a kontrolerem. Dostarczony system otrzyma aktualizacje sygnatur poprzez iDMZ.

Zadaniem wdrażanego systemu jest detekcja oraz ochrona przed zagrożeniami na stacjach objętych ochroną. Dostarczony system powinien działać w typowej architekturze klient-serwer. Kontroler stanowi centralny element i pełni rolę serwera, z którym komunikują się agenci zainstalowani na stacjach roboczych. Zadaniem agenta jest wykrywanie zagrożeń i ataków na chronionych hostach.

# Serwer czasu

W zależności od zastosowanej technologii i zabezpieczenia jej w niezawodny wzorzec czasu będzie stosowany układ klastrowy lub pojedynczy. Wymagania w tym zakresie określi Zamawiający na etapie przygotowania PFU.

Należy zaimplementować klaster 2 serwerów czasu standby synchronizujący czas Serwer czasu w infrastrukturze OT będzie zgodny z poniższymi wymaganiami:

1. Sposób obsługi dla „Global Navigation Satellite System”:

i. Dwa redundantne wejścia GNSS (ANT1/ANT2)

ii. Wsparcie dla systemów satelitarnych GPS, GLONASS, Galileo, Beidou z możliwością wyłączenia systemów Glonass i Beidou

1. Obsługiwane porty wejściowe

i. 2 porty wejściowe sygnału 1PPS (obsługa sekundy przestępnej)

ii. 2 Porty ToD (Time of Day) ze złączem RJ45

iii. 1 port IRIG-B AM - modulowany 1kHz – złącze BNC 600 Ohm

1. Obsługiwane porty wyjściowe:

i. 2 ×100/10Mbps RJ45 HW/stamps supporting PTP, NTP, and SyncE

ii. 2× 1GbE SFP

iii. 2 ×10GbE SFP

iv. 1×ToD (rs232)

v. 1x rs485

1. Obsługiwane protokoły:

i. IEEE1588-2008(PTP Precision Time Protocol))

ii. NTPv4, NTPv3

iii. IPv4/ IPv6

iv. DHCP

v. SFTP,

vi. VLAN(1x PTP-slave, 9x PTP-master, 10x NTP)

vii. TELNET

viii. SYSLOG

ix. RADIUS

x. SSH

xi. SNMP v 1,2 oraz 3 oraz bazy MIB2.

1. Dokładność pomiaru częstotliwości

i. Tracking toGPS:PRS/PRC/PRTC compliant.

ii. Rubidium (G.812 type ii) < 1×10–11/day

iii. OCXO (G.812typeI) < 1×10–10/day

1. Dokładność pomiaru czasu:
2. Śledzenie GPS (1PPS): <20 ns
3. Dokładność znacznika czasu < 5 ns
4. Wbudowane moduły sprzętowe

i. OCXO

ii. Rubidium

1. Urządzenie musi posiadać mechanizm uwierzytelnienia dla protokołu NTP przy użyciu kluczy MD5 i SHA.
2. Urządzenie musi posiadać obsługę protokołów NTP/SNTP dla co najmniej 1 mln. klientów usługi jednocześnie, z wydajnością obsługi co najmniej 9 tys. zapytań NTP na sekundę.
3. Certyfikaty:

i. NATO NCAGE (9ATKH)

ii. NATO system registered product NSN 6645-17-1256311

iii. CE

iv. ISO 9001

v. EMC

vi. Safety Directive

1. Urządzenie musi posiadać mechanizm uwierzytelnienia dla protokołu NTP przy użyciu kluczy MD5 i SHA.
2. Urządzenie musi posiadać interfejs administracyjny obsługiwany za pomocą protokołu HTTPS (Graphical User Interface) i/lub SSH (Command Line Interface) z uwierzytelnieniem użytkownika za pomocą protokołu Radius.
3. Urządzenie musi być zasilane z sytemu napięcia gwarantowanego.
4. Urządzenie będzie zasilone dwutorowo poprzez dwa odrębne zasilacze.

Dodatkowo wymaga się synchronizacji czasu serwera czasu z wykorzystaniem poniższych wzorców:

1. Serwera czasu NTP – tempus1.gum.gov.pl; tempus2.gum.gov.pl
2. Radiowego sygnału DCF77
3. Polski radiowego sygnału 225kHz – projekt eCzasPL