BRANŻA POMIAROWA I AUTOMATYKI

Język zamówień publicznych dla zapewnienia bezpieczeństwa cybernetycznego systemów sterowania

Numer dokumentacji: Załącznik do PBT.I01
Standard Urządzeń Technicznych SUT C –
Branża Pomiarów i Automatyki

Stan na dzień: Lipiec 2019

PCC Rokita SA
ul. Sienkiewicza 4
56-120 Brzeg Dolny
kontakt@pcc.rokita.pl
www.pcc.rokita.pl

Spis treści

WYKAZ SKRÓTÓW

ACL list – mechanizm filtrowania pakietów sieciowych wykorzystywany podczas konfiguracji routera

AKP – Aparatura Kontrolno-Pomiarowa

AKPiA – Aparatura Kontrolno-Pomiarowa i Automatyka

AMS – (ang. Alarm Menagement System) –System zarządzania alarmami

APL – (ang. Advanced Process Library) - Zaawansowana biblioteka procesowa

BIOS – (Basic Input/Output System or Basic Integrated Operating System) -

BMS – (ang. Building Management System) – System zarzadzania budynkiem

CPU – (ang. Central Processing Unit) - Jednostka centralna; procesor

DG – Dyrektor Generalny

DCS – (ang. Distributed Control System) - Rozproszony System Sterowania

DMZ – (ang. Demilitarized zone) – Strefa zdemilitaryzowana

DNS – (ang. Domain Name System) – system, którego zadaniem jest tłumaczenie nazw domenowych na adresy IP

EMC – (ang. Electromagnetic Compatibility) – Kompatybilność Elektromagnetyczna

ERP - (ang. Enterprise Resource Planning) - Zarządzanie zasobami przedsiębiorstwa.

ESD – (ang. Emergency Shutdown System) – Układ blokad w sterowaniu przemysłowym

EX – (ang. Explosionproof) – Przeciwwybuchowy

FAT – (ang. Factory Acceptance Tests) – Fabryczne testy akceptacyjne

HART – (ang. Highway Addressable Remote Transducer) – Protokół komunikacyjny sieci przemysłowych

HIDS – (ang. Host Intrusion Detection System) - System wykrywania intruzów hosta

HMI – (ang. Human-Machine Interface) – Interfejs człowiek-maszyna

IED – (ang. Intelligent Electronic Devices) - Inteligentne Urządzenie elektroniczne.

IK – Infrastruktura Krytyczna

MPI – (ang. Multi-Point Interface) – Interfejs wielopunktowy

MR – Matryca Ryzyka

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

NIPS – (ang.Network-based Intrusion Prevention System) – System monitorowania sieci oraz ochrony poufności, integralności i dostępności sieci.

NIDS – (ang. Network Intrusion Detection System) – System wykrywania włamań do sieci.

NPOIK – Narodowy Program Ochrony Infrastruktury Krytycznej

NTP – (ang. Network Time Protocol) - Protokół synchronizacji czasu

OPC – (ang. OLE for process control)

OT – (ang. Operational Technology) – Sterowanie przemysłowe (technologie operacyjne)

P&ID – (ang. Piping and Instrumentation Diagram) - Schemat technologiczno-pomiarowy

PLC – (ang. Programmable Logic Controller) - Programowalny Sterownik Logiczny

RFC – (ang. Request for Comments) – zbiór dokumentów związanych z Internetem oraz sieciami komputerowymi

RTU – (ang. Remote Terminal Unit) – zdalny terminal

SAT – (ang. Site Acceptance Tests) - obiektowe testy akceptacyjne

SCADA – (ang. Supervisory Control And Data Acquisition) - System nadzorujący i akwizycji danych

SIL – (ang. Safety Integrity Level) - Poziom nienaruszalności bezpieczeństwa

SIS – (ang. Safety Instrumented System) – System automatyki zabezpieczeniowej

SSiN – System sterowania i nadzoru (elektroenergetyka)

SDT – Standard Dokumentacji Technicznej

SUT – Standard Urządzeń Technicznych

TCS (SSRK) – (ang. Train Control System) – System sterowania ruchem kolejowym

USB – (ang. Universal Serial Bus) - uniwersalna magistrala szeregowa

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

VPN – (ang. Virtual Private Network) - Wirtualna Sieć Prywatna

WAN – (ang. Wide Area Network) - Rozległa sieć komputerowa

WLAN – (ang. Wireless Local Area Network) – Bezprzewodowa lokalna sieć komputerowa

ZSZ – Zintegrowany System Zarządzania

1. WPROWADZENIE

Kluczowym elementem ochrony infrastruktury krytycznej kraju i kluczowych zasobów w ramach Narodowego programu ochrony infrastruktury krytycznej (NPOIK) jest bezpieczeństwo teleinformatyczne systemów kontroli środowiska OT (Operational Technology) i powinno być ono uwzględniane zarówno przy projektowaniu, modyfikacjach jak i utrzymywaniu systemów automatyki przemysłowej i sieci produkcyjnych tak by zapewnić akceptowalny poziom ryzyka dla funkcjonowania w tym zakresie organizacji.

Ponieważ systemy kontroli funkcjonalnej działają w celu ciągłego i bezpiecznego działania infrastruktury krytycznej kraju, niezbędne jest rozpoznanie i zrozumienie ważnych ról tych systemów. Ponadto powinno wzrosnąć zainteresowanie rozpoznaniem potencjalnych słabości, konsekwencji i wyzwań związanych z zabezpieczeniem tych systemów przed cyberatakami. Obszar produkcji ze względu na zamknięty charakter systemów sterowania, wykorzystujących przestarzałe technologie informatyczne jest szczególnie podatny na ataki zwłaszcza przy łączeniu ich z systemami ERP lub systemami informacji zarządczej. Straty z tym związane (przestoje, wyciek poufnych informacji a w ich wyniku spadek wizerunkowy firmy, spadek zaufania do marki, spadek konkurencyjności firmy) bardzo łatwo można przełożyć na wymiar finansowy.

Czynniki przyczyniające się do eskalacji ryzyka w systemach OT:

1. Systemy sterowania przyjmują znormalizowane technologie o znanych podatnościach.
2. Systemy sterowania są podłączone do innych sieci, które nie są bezpieczne.
3. Niepewne połączenia zaostrzają luki w zabezpieczeniach.
4. Podręczniki dotyczące korzystania z systemów OT są publicznie dostępne zarówno dla terrorystów, jak i dla prawowitych użytkowników.

2. CEL DOKUMENTU

Niniejszy dokument ma na celu zapewnienie organizacji odpowiedniej niezawodności pracy i właściwej ochrony systemów sterowania OT (DCS/SCADA/MES) w zakresie cyberbezpieczeństwa. Dokument ten przedstawia obowiązujące w grupie PCC Rokita wytyczne i rekomendacje projektowe i/lub wykonawcze dla systemów sterowania OT z uwzględnieniem wymogów bezpieczeństwa w architekturze i specyfikacji systemów OT oraz niezbędnych testów akceptacyjnych (FAT/SAT) pokrywających weryfikacje zaleceń bezpieczeństwa tak by było zapewnione przestrzeganie polityki bezpieczeństwa systemów firmy i dobre praktyki, w zakresie zapewnienia dla nich akceptowalnego poziomu bezpieczeństwa cybernetycznego. Korzystanie z tych wytycznych dotyczących zamówień pomoże doprowadzić do zapewnienia bezpieczeństwa w systemach kontroli. Niniejszy dokument zawiera informacje i konkretne przykłady tekstu w języku zamówień, aby pomóc społeczności systemów kontroli, zarówno właścicielom, jak i integratorom, w ustanawianiu wystarczających kontroli

bezpieczeństwa systemów kontroli w ramach umów kontraktowych w celu zapewnienia akceptowalnego poziomu ryzyka.

3. DEFINICJE

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

Backdoor - (pol. tylne drzwi, furtka) – luka w zabezpieczeniach systemu utworzona umyślnie w celu późniejszego wykorzystania.

BIOS – (ang. Basic Input/Output System or Basic Integrated Operating System) - BIOS odnosi się do kodu oprogramowania uruchamianego przez komputer przy pierwszym uruchomieniu. Podstawową funkcją systemu BIOS jest przygotowanie urządzenia, aby inne programy przechowywane na różnych nośnikach (takie jak dyski twarde, dyskietki i dyski CD) mogły ładować, wykonywać i przejąć kontrolę nad komputerem. Ten proces nazywany jest ładowaniem.

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

Czujnik (Sensor) - urządzenie, układ fizyczny, który swoją reakcję na bodziec fizyczny przekształca w mierzalny sygnał innej wielkości fizycznej w celu dostarczenia informacji o wielkości fizycznej.

Canary(ies) – Kanarowe przetwarzanie danych, kanarek lub kanarki to fałszywe urządzenia lub nieużywane porty Ethernet używane w połączeniu z oprogramowaniem wykrywającym w celu ostrzeżenia przed nieautoryzowanym sondowaniem sieci lub inwigilacją. Nazwa jest odniesieniem do używania kanarków jako urządzeń ostrzegawczych w kopalniach węgla.

CPU - (ang. Central Processing Unit) - Jednostka centralna; procesor - urządzenie cyfrowe sekwencyjne, wykonujące rozkazy na podstawie zinterpretowanych danych pobieranych z pamięci.

DCS - (ang. Distributed Control System) - Rozproszony System Sterowania - system sterowania i wizualizacji procesu przemysłowego, który posiada wspólną bazę danych dla sterowania i wizualizacji w odróżnieniu od systemów SCADA bądź PLC.

Deny All – Najbardziej istotna Reguła ochrony lokalnych sieci w zaporach sieciowych określająca, że: "Wszystkie działania, które nie są jawnie dozwolone, są zabronione!" Dzięki tej strategii tylko te dostępy istnieją, które zostały wyraźnie otwarte osobiście przez administratora.

DMZ – (ang. Demilitarized zone) – Strefa zdemilitaryzowana to specjalna konfiguracja sieci lokalnej, mająca na celu poprawę bezpieczeństwa poprzez segregowanie komputerów po każdej stronie zapory sieciowej (firewall). Jest to logicznie wydzielony segment sieci (ograniczonego zaufania) pośredniczący pomiędzy sieciami o różnym poziomie krytyczności dla organizacji pomiędzy siecią użytkowników biurową (strefa niezaufana) a sieciami produkcyjnymi z systemami automatyki przemysłowej (strefą zaufaną – chronioną przez zaporę ogniową).

DoS - (ang. Denial of Service) – Blokada usług – Zakłócenie lub uniemożliwienie autoryzowanego dostępu do system bądź do zasobów systemu lub opóźnienie bądź zakłócenie pracy systemu.

Emergency Shutdown System (ESD) – System blokadowy zapewniający w sterowaniu przemysłowym bezpieczne zatrzymanie procesu na wypadek awarii.

ERP - (ang. Enterprise Resource Planning) to oprogramowanie dla firm (system aplikacji), którego celem jest zintegrowanie wszystkich procesów zachodzących w organizacji.

FAT – **(ang. Factory Acceptance Tests)** – działanie mające na celu potwierdzenie, że dany system działa poprawnie. Przeprowadzany jest u wytwórcy przed transportem do przedsiębiorstwa docelowego

FUZZING – Metoda testowania oprogramowania lub znajdowania w nim luk, przydatnych przy atakach hakerskich.

Heartbeat Signals — Znany również jako zegar watchdoga, utrzymujący przy życiu, stan zdrowia. Sygnały informują o kondycji komunikacji systemu.

HART – (ang. Highway Addressable Remote Transducer) – Protokół komunikacyjny sieci przemysłowych umożliwiający zmianę zakresu oraz diagnostykę urządzeń AKPiA. Jeden ze standardowych protokołów komunikacji urządzeń AKP w przemyśle.

HAZOP – (ang. Hazard and Operability Study) – Metoda analizy zagrożeń.

HIDS – (ang. Host-based Intrusion Detection System) - System wykrywania intruzów hosta. Aplikacja wykrywająca możliwą złośliwą aktywność na hoście z takich cech, jak zmiana plików (sprawdzanie integralności systemu plików), profile połączeń systemu operacyjnego itp.

HMI – (ang. Human-Machine Interface) – Interfejs człowiek-maszyna – Panel sterowniczy (operatorski) - urządzenie elektryczne umożliwiające kontrolę innych urządzeń, realizujących pewne procesy, np. technologiczne lub produkcyjne.

IED – (ang. Intelligent Electronic Devices) - to termin używany w przemyśle elektroenergetycznym do opisywania mikroprocesorowych sterowników urządzeń systemu elektroenergetycznego, takich jak wyłączniki, transformatory i baterie kondensatorów.

IK – Infrastruktura Krytyczna - zasoby (fizyczne i cybernetyczne systemy) mające podstawowe znaczenie (niezbędne) dla funkcjonowania społeczeństwa i gospodarki.

Incydent bezpieczeństwa OT (Incydent) - to zdarzenie lub seria niepożądanych bądź niespodziewanych zdarzeń, które bezpośrednio zagrażają bezpieczeństwu informacji (zagrażają ich poufności, dostępności lub integralności) bądź stwarzają znaczne prawdopodobieństwo zakłócenia procesów technologicznych lub działań biznesowych.

Klient – Urządzenie lub aplikacja komunikujące się z serwerem.

Kontrola dostępu – Ochrona systemu przed nieautoryzowanym dostępem logicznym bądź fizycznym obejmująca proces pozwalający regulować i monitorować dostęp do zasobów systemu z godnie z przyjętą polityką bezpieczeństwa.

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

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

Log – Rejestr zdarzeń z informacjami o zdarzeniach i działaniach dotyczących pracy programu bądź systemu informatycznego.

Malware (ang. Malicious Software) – złośliwe/szkodliwe oprogramowanie niebezpieczne dla systemu operacyjnego i zgromadzonych w komputerze danych.

MES - (ang. Manufacturing Execution System) – System Realizacji Produkcji służący do zbierania informacji o procesie produkcyjnym wprost ze stanowisk produkcyjnych i ich przesyłanie do obszaru biznesowego a także niektóre systemy wspierające np. centralne serwery dystrybucji sygnatur AV, serwery przesiadkowe, serwery wymiany plików, serwery usług katalogowych, itp.

Mikroswitch – Elektryczny przełącznik wyzwalany przez niewielki ruch jego dźwigni.

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

MPI - (ang. Multi-Point Interface) – Interfejs wielopunktowy - sieć przemysłowa do komunikacji pomiędzy sterownikami PLC, stacją programującą, panelami operatorskimi i innymi urządzeniami z rodziny SIMATIC firmy SIEMENS.

MRP - (ang. Material Requirements Planning) - Planowanie zapotrzebowania materiałowego - jest to zbiór procesów, który umożliwia planowanie potrzeb materiałowych na podstawie danych o strukturze wyrobu, informacji o stanach magazynowych, stanu zamówień w toku i planu produkcji.

NIDS – (ang. Network Intrusion Detection System) – System wykrywania włamań do sieci służy do identyfikacji nieautoryzowanego lub nieprawidłowego ruchu sieciowego.

NTP – (ang. Network Time Protocol) - Protokół komunikacyjny, który umożliwia precyzyjną synchronizację czasu pomiędzy urządzeniami teleinformatycznymi.

OPC - (ang. OLE for process control) – Otwarty standard komunikacji stosowany w automatyce przemysłowej i informatycvznych systemach wyższych warstw (biznesowych), służący do łączenia aplikacji bazujących na systemach operacyjnych ze sprzętem i oprogramowaniem aplikacyjnym automatyki przemysłowej.

OT - (ang. Operational Technology) – Technologie operacyjne – kategoria *sprzętu i oprogramowania* monitorujących i kontrolujących działanie fizycznych urządzeń - sprzęt i oprogramowanie przeznaczone do wykrywania lub powodowania zmian w procesach fizycznych poprzez bezpośrednie monitorowanie i/ lub sterowanie fizycznymi urządzeniami, takimi jak zawory, pompy itp.

PLC - (ang. Programmable Logic Controller) - Programowalny Sterownik Logiczny jest to urządzenie mikroprocesorowe wykonujący cyklicznie algorytm sterowania, na podstawie którego

przetwarza stany wejść na odpowiednie stany wyjść.

Podatność – Cecha charakterystyczna systemu taka jak luka w implementacji, działaniu bądź zarządzaniu systemu, która umożliwia zakłócenie jego pracy lub złamanie przyjętej polityki bezpieczeństwa.

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

PROFIBUS DP - Protokół komunikacyjny sieci przemysłowych stworzony dla standardu rozproszonej sieci przemysłowej determistycznej czasu rzeczywistego PROFIBUS. Jeden ze standardowych protokołów komunikacji urządzeń AKPiA w przemyśle.

PROFInet – Oparty na sieci Industrial Ethernet, nowoczesny standard przemysłowy do budowy zintegrowanych i zwartych systemów automatyki oraz rozproszonych systemów automatyki opartych na modelu komponentów.

Przetwornik - Urządzenie przekształcające daną wielkość na inną według określonej zależności oraz z określoną dokładnością.

Przetworniki inteligentne - (ang. Smart transducers) – Przetworniki zapewniające pomiar, obróbkę sygnału i komunikację z zewnętrznym układem pomiarowym lub układem sterowania za pomocą sygnału cyfrowego w oparciu o standardowy protokół komunikacji.

Protokół komunikacyjny – Zespół reguł i kroków wykonywanych przez urządzenia komunikacyjne dla potrzeb przesyłania i wymiany danych.

RTU - (ang. Remote Terminal Unit) – zdalny terminal – Uniwersalne urządzenie służące do zdalnego monitorowania i sterowania różnymi urządzeniami i systemami automatyki, wdrażany zwykle w środowisku przemysłowym.

SAT – **(ang. Site Acceptance Testing)** – działanie, którego zadaniem jest potwierdzenie, że dostarczony do klienta system jest kompletny i nie posiada uszkodzeń mogących powstać w czasie transportu bądź wdrażania.

SCADA – (ang. Supervisory Control And Data Acquisition) - System nadzorujący i akwizycji danych procesu technologicznego lub produkcyjnego, który pełni następujące funkcje: zbieranie aktualnych danych z procesu (w tym pomiarów), wizualizację zebranych danych, sterowanie procesem na podstawie zebranych danych oraz odpowiedniego algorytmu sterowania, alarmowanie oraz archiwizację danych pomiarowych.

SDT – Standard Dokumentacji Technicznej - opracowane przez PCC Rokita SA własne standardy dotyczące dokumentacji technicznej oraz systemu identyfikacji procesowej.

SIL – (ang. Safety Integrity Level) - Poziom nienaruszalności bezpieczeństwa – Jest to poziom wymagań jaki jest spełniony aby układ zapewniający bezpieczeństwo zadziałał.

SIS – (ang. Safety Instrumented System) – System automatyki zabezpieczeniowej – System, który działa automatycznie by utrzymać instalację w stanie bezpiecznym lub doprowadzić do takiego stanu

w przypadku pojawienia się stanów odbiegających od warunków normalnych.

Sterowanie – Oddziaływanie na dany obiekt w celu osiągnięcia określonego celu związane z pewną informacją w postaci sygnału.

Sterowanie automatyczne – sterowanie realizowane za pomocą specjalnie skonstruowanego urządzenia (sterownika, regulatora)

Sterowanie ręczne – sterowanie realizowane przez człowieka.

Sterownik - Układ zajmujący się nadzorowaniem pracy urządzenia elektrycznego. Może być komputerowy, elektryczny, elektroniczny bądź elektromechaniczny.

System – Zbiór powiązanych ze sobą elementów sprzętowych i programowych realizujących wspólnie co najmniej jedna funkcję.

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

Sygnał - Model dowolnej mierzalnej wielkości zmieniającej się w czasie, generowanej przez zjawiska fizyczne lub systemy.

Sygnał analogowy - Sygnał, który może przyjmować dowolną wartość z ciągłego przedziału a jego wartości mogą zostać określone w każdej chwili czasu poprzez określoną dany sygnał funkcję matematyczną.

Sygnał cyfrowy - Sygnał elektryczny, bądź optyczny, który poprzez odpowiednie kodowanie (modulację cyfrową) przenosi dane cyfrowe.

Sygnał pomiarowy – sygnał o zadanych, znanych metrologowi parametrach, służący do pobudzenia mierzonego układu lub sprawdzanego przyrządu.

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

VPN - (ang. Virtual Private Network) – tunel komunikacyjny służący zapewnieniu lepszej efektywności lub większego poziomu bezpieczeństwa przesyłanych danych, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci Internet w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów.

Urządzenia końcowe – (ang. End devices) - komponenty w systemie sterowania, które zbierają informacje lub kontrolują proces. Mogą to być czujniki, kontrolery, zawory, procesory itp. Urządzenia końcowe są dostarczane wraz ze zwykłym oprogramowaniem komputerowym (np. Web, FTP, TELNET) w celu ułatwienia konserwacji i konfiguracji.

Inteligentne urządzenia końcowe, odległe zespoły terminali i programowalne sterowniki logiczne (PLC) zawierają mikroprocesory i są uważane za "inteligentne" urządzenia końcowe. Czujniki, siłowniki i mierniki tradycyjnie zawierają ograniczone możliwości przetwarzania i są znane jako "głupie"(ang. „dumb") urządzenia końcowe. Komunikacja (szeregowa lub Ethernet) do /

z "inteligentnych" lub "niemych" urządzeń końcowych do systemu sterowania może zostać przechwycona i zmodyfikowana wpływając negatywnie na kontrolowany proces.

Urządzenia/elementy wykonawcze (Aktuatory) - urządzenia mechaniczne stosowane w układach regulacji i sterowania, wypracowujące sygnał wejściowy do obiektu regulacji/sterowania na podstawie sygnału sterującego.

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

Watchdog - układ czasowy wykrywający błędne działanie systemu, próbujący je naprawić i zapobiec poważniejszej awarii.

WLAN - (ang. Wireless Local Area Network) – Bezprzewodowa lokalna sieć komputerowa wykorzystująca mikrofale/ fale podczerwieni jako medium przenoszenia sygnałów ustandaryzowana norma IEEE 802.11.

Zapora sieciowa - (ang. Firewall) – Urządzenie dedykowane lub oprogramowanie , które chroni na poziomie sieci teleinformatycznej przed nieuprawnionym dostępem poprzez filtrowanie ruchu i odrzucanie nieautoryzowanych prób połączeń.

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

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

4. MATERIAŁY BAZOWE

1. Department of Homeland Security: Cyber Security Procurement Language for Control Systems - september 2009r.
2. Standardy i dobre praktyki ochrony infrastruktury krytycznej – Automatyka przemysłowa w sektorze ropy i gazu – Poradnik RCB z 2017r.
3. Standardy i dobre praktyki ochrony infrastruktury krytycznej – Automatyka przemysłowa w sektorze elektroenergetycznym– Poradnik RCB z 2017r.
4. Operational Guidelines for industrial Security- Poradnik firmy Siemens AG z 2013r.

Dokumenty powiązane:

1. Matryce ryzyka (MR)
2. Procedura ZSZ **PW.02.PR01 Realizacja zakupów technicznych i usług**
3. Procedura ZSZ **PW.C.09.PR.03 Nadzorowanie wyposażenia do monitorowania i pomiarów**
4. **Instrukcja ZSZ PBT.I02 Polityka haseł w systemach sterowania**
5. Standard Urządzeń Technicznych SUT E-1 Wytyczne dla urządzeń technicznych BRANŻA ELEKTRYCZNA

6. Standard Urządzeń Technicznych SUT M-1 Wytyczne dla urządzeń technicznych BRANŻA MECHANICZNA

5. WYTYCZNE OGÓLNE

5.1 Zakres

W opracowaniu zawarto ogólne wymagania dla projektowania i doboru urządzeń automatyki obiektowej oraz układów sterowania i wizualizacji a także Warunki odbiorów urządzeń i systemów automatyzacji w zakresie cyberbezpieczeństwa OT. Przed przystąpieniem do wykonywania projektu technicznego lub doboru urządzenia należy uzgodnić wszystkie wymagania techniczne, normy przedmiotowe, oraz wytyczne zamieszczone w niniejszym opracowaniu.

Uwaga: Wszystkie odstępstwa od wytycznych technicznych zawartych w tym dokumencie powinny być uzgodnione i pisemnie zaakceptowane przez Inwestora.

5.2 Wyłączenia

Z projektu branży AKPiA wyłącza się następujące systemy:

1. Systemy sterowania i wizualizacji dedykowane dla automatyki budynkowej (Systemy zarządzania budynkiem BMS).
2. Systemy sterowania i wizualizacji dedykowane dla ruchu kolejowego (np. System sterowania ruchem kolejowym **SSRK**).
3. Systemy sterowania i wizualizacji dedykowane dla elektroenergetyki (System sterowania i Nadzoru **SSiN**).
4. Systemy dyspozytorskie.

5.3 Normy i przepisy obowiązujące w PCC Rokita

5.3.1 Wymagania prawne

1. PBT.I02 Polityka haseł w systemach sterowania
2. ZARZĄDZENIE NR 64/2011 DYREKTORA GENERALNEGO PCC Rokita SA z dnia 16 grudnia 2011r. w sprawie systemu technicznej ochrony mienia.

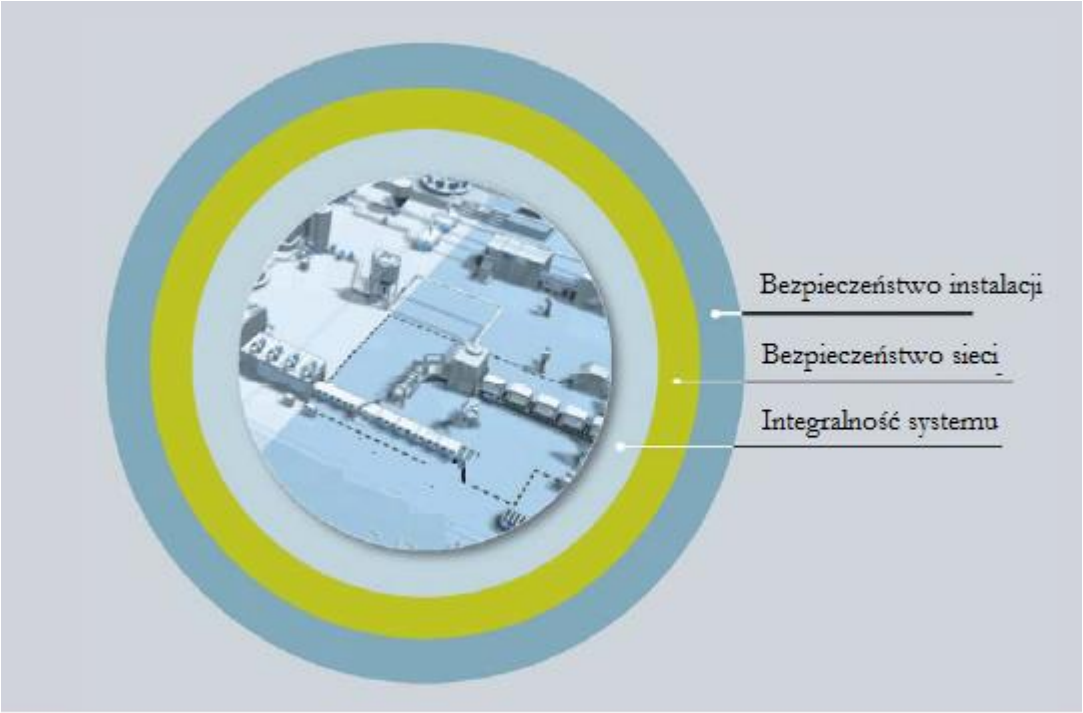
5.3.2 Normy i specyfikacje techniczne

5.4 Ogólne wymagania projektowe i odbiorowe obowiązujące w PCC Rokita

5.4.1 Warunki odbiorów urządzeń i systemów automatyzacji

1. Wyłączenie lub usunięcie w urządzeniu sieciowym jakichkolwiek usług lub programów, które nie są wymagane do normalnej pracy systemu, usuwając w ten sposób potencjalne luki w zabezpieczeniach.
2. Skanowanie portów jest normalną metodą zapewnienia istnienia wymaganych usług i braku niepotrzebnych usług. Skanowanie portów należy przeprowadzić przed FAT z reprezentatywną, w pełni funkcjonalną konfiguracją systemu. Wszystkie porty wejścia / wyjścia (I / O) muszą zostać przeskanowane pod kątem UDP i TCP. Skanowanie należy przeprowadzić przed FAT i ponownie przed SAT. Skanowanie portów rzadko może być używane w systemach produkcyjnych. W większości przypadków skanery zakłócają ich działanie.
3. Skonfigurowanie hostów z najmniejszym dostępem do pliku i dostępem do konta oraz dostarczenie dokumentacji konfiguracji.
4. Skonfigurowanie niezbędnych usług systemowych do wykonania z najniższym poziomem uprawnień użytkownika dla tych usług i dostarczyć dokumentację konfiguracji.
5. Wyłączenie, za pomocą oprogramowania lub fizycznego odłączenia, wszystkie niepotrzebne portów komunikacyjnych i dysków nośników wymiennych lub zapewnienie zaprojektowania barier i dostarczenie wynikowej dokumentacji.
6. Ochrona BIOS przed nieautoryzowanymi zmianami, chyba że nie jest to technicznie wykonalne, w takim przypadku Dostawca udokumentuje to i zapewni środki łagodzące.
7. Lista wszystkich wyłączonych lub usuniętych portów USB, napędów CD / DVD i innych wymiennych urządzeń multimedialnych.
8. Skonfigurowanie urządzeń sieciowych w celu ograniczenia dostępu do / z określonych lokalizacji, w stosownych przypadkach, oraz dostarczenie dokumentacji konfiguracji.

6. Rozwiązania zapewnienia wymaganego poziomu cyberbezpieczeństwa w różnych warstwach ochrony.



Rysunek 1 Warstwy ochrony cyberbezpieczeństwa w systemach OT

6.1 Bezpieczeństwo instalacji

1. Należy stosować się do przepisów obowiązujących w PCC Rokita a w szczególności obowiązuje ZARZĄDZENIE NR 64/2011 DYREKTORA GENERALNEGO PCC Rokita SA z dnia 16 grudnia 2011r. w sprawie systemu technicznej ochrony mienia.

6.1.1 Fizyczny dostęp do elementów cybernetycznych

1. Dostawca/Wykonawca powinien dostarczyć szczegółowy plan odpowiednich mechanizmów bezpieczeństwa fizycznego.
2. Dostawca/Wykonawca powinien zapewnić zamykane lub blokujące obudowy dla komponentów systemu sterowania (np. Serwerów, terminali i sprzętu sieciowego).
3. Dostawca/Wykonawca powinien zapewnić urządzenia blokujące z co najmniej dwoma kluczami w przypadku gdy konieczne jest zabezpieczenie zamkiem z kluczem w zależności od wymagań Zamawiającego
4. Pomieszczenia, w których znajdują się główne komponenty systemu sterowania (np. Serwery, komputery terminali, sprzęt sieciowy, stacje automatyzacji) powinny być zamykane na klucz.

5. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację potwierdzającą, że nie są zainstalowane/zamontowane nieautoryzowane urządzenia rejestrujące (np. key loggers, kamery i mikrofony).
6. Dostawca/Wykonawca w ramach FAT i SAT powinien sprawdzić i dostarczyć dokumentację potwierdzającą, że komponenty bezpieczeństwa fizycznego (np. urządzenia zabezpieczające, zamki) zostały przetestowane.
7. Dostawca/Wykonawca powinien w ramach FAT i SAT odłączyć (unieaktywnić) zarówno sprzętowo jak i programowo wszystkie nieużywane porty i urządzenia wejścia / wyjścia (patrz rozdział **6.3.1**).
8. Dostawca/Wykonawca powinien zapewnić, w ramach procedur SAT, sprawdzenie i udokumentowanie potwierdzające, że wszystkie środki zabezpieczające pomieszczeń zawierających główne komponenty systemu sterowania (np. Serwery, komputery terminali, sprzęt sieciowy, stacje automatyzacji) działają poprawnie.

6.1.2 Fizyczny dostęp do stref (ochrona obwodowa)

1. Zabezpieczenia obwodowe obejmują, m.in. ogrodzenia, ściany, całkowicie zamknięte budynki, bramy lub drzwi wejściowe, bariery samochodowe, oświetlenie, odpowiednie ukształtowanie terenu, systemy nadzoru, systemy alarmowe i osłony. Zabezpieczenie fizyczne może również obejmować rejestrowanie wejścia i wyjścia, a także rejestrowanie pokoju lub obszaru, najczęściej za pośrednictwem systemu dostępu poprzez karty dostępu.
2. Brak określenia stref z ochroną obwodową może ułatwić fizyczne włamania. Zdolność wykrywania naruszeń stref jest kluczem do zapobiegania atakom fizycznym.
3. Jedynie personel, który potrzebuje dostępu do danej lokalizacji, otrzymuje pozwolenie na dostęp. Zabezpieczone obszary o krytycznym wyposażeniu nie mogą posiadać sprzętu ani funkcji, które wymagają dostępu wielu osób włączając w Wykonawców.
4. Fizyczne monitorowanie bezpieczeństwa (np. Kamery, dostęp do karty) powinno przesyłać alarmy do zakładowego centrum kontroli (Ochrony zakładowej). Ze względów bezpieczeństwa cybernetycznego alarmy te nie mogą znajdować się w tej samej sieci, co urządzenia sterowania i wizualizacji procesów technologicznych.
5. Dostawca/Wykonawca powinien zapewnić ocenę bezpieczeństwa lokalnego, zwracając szczególną uwagę na parametry lub zdarzenia, które mogą wpływać na fizyczne wtargnięcia intruzów. Rezultatem tej oceny powinien być udokumentowany fizyczny plan ochrony obiektu, który należy przekazać Zamawiającemu..
6. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację, potwierdzającą, że osłony takie jak ściany, budynki lub ogrodzenia odpowiednio zabezpieczają strefę przed wtargnięciem pieszych, pojazdów i pocisków.

7. Dostawca/Wykonawca powinien zezwolić na dostęp w obrębie strefy chronionej tylko tym pracownikom, kontrahentom lub gościom, którzy zostaną zweryfikowani zarówno przez Dostawcę/Wykonawcę, jak i przez Zamawiającego.
8. Dostawca/Wykonawca powinien zapewnić klucze uniemożliwiające kopiowanie lub karty kodowe do wszystkich zamków.
9. Dostawca/Wykonawca w ramach testów FAT powinien przetestować i dostarczyć dokumentację potwierdzającą, że wszystkie systemy alarmowe wychwytują wszystkie przypadki wtargnięcia do strefy przy zminimalizowaniu fałszywych alarmów.
10. W ramach testów SAT Dostawca/Wykonawca zapewni mechanizmy kontroli dostępu przez Zamawiającego.
11. Dostawca/Wykonawca w ramach testów SAT powinien zapewnić Zamawiającemu oczekiwaną funkcjonalność zabezpieczenia fizycznego.
12. Dostawca/Wykonawca powinien zapewnić odpowiednie szkolenia na miejscu u operatorów i strażników (służby ochrony) przed przekazaniem do eksploatacji.
13. Dostawca/Wykonawca w ramach testów SAT przed uruchomieniem powinien zweryfikować i dostarczyć dokumentację dotyczącą wszystkich funkcji zdalnego alarmu, nadzoru i blokowania.
14. Dostawca/Wykonawca powinien zapewnić utrzymanie mechanizmów kontroli dostępu w bezpiecznej konfiguracji.
15. Dostawca/Wykonawca powinien dokonać walidacji wyników w zakresie ochrony obwodowej zgodnie z warunkami określonymi w umowie/zamówieniu.
16. Dostawca/Wykonawca powinien wymieniać wszystkie zamki, kody blokujące, karty dostępu i itp. zgodnie z warunkami określonymi w umowie/zamówieniu.
17. Dostawca/Wykonawca powinien koordynować zmiany kontroli dostępu z Zamawiającym w celu aktualizacji fizycznej ochrony.

6.1.3 Fizyczny dostęp do sterowania ręcznego

1. Fizyczny dostęp do sterowania ręcznego powinien być ściśle ograniczony wyłącznie dla upoważnionego personelu.
2. Nieautoryzowany dostęp do sterowania ręcznego stanowi ryzyko uszkodzenia lub wtargnięcia do systemu, dlatego musi być zabezpieczony.
3. Dostawca/Wykonawca powinien zapewnić środki do fizycznego zabezpieczenia mechanizmu ręcznego sterowania, poprzez zamykaną obudowę lub funkcję blokowania wbudowaną w sam ręczny mechanizm sterujący.
4. Przed uruchomieniem Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację dotyczącą wszystkich funkcji zdalnego alarmu, nadzoru i blokowania.

5. Dostawca/Wykonawca powinien utrzymywać mechanizmy ręcznego sterownia w bezpiecznej konfiguracji przez okres określony w umowie/zamówieniu.
6. Dostawca/Wykonawca powinien dokonać walidacji wyników w zakresie ochrony mechanizmów ręcznego sterowania.
7. Dostawca/Wykonawca powinien wymienić wszystkie zamki, kody blokujące, karty dostępu itp. na zasadach określonych w umowie/zamówieniu.

6.2 Bezpieczeństwo sieci

6.2.1 Ochrona obwodowa

6.2.1.1 Zapory sieciowe (Firewalle)

1. Dostawca/Wykonawca zapewni zapory sieciowe i zestawy reguł zapory między strefami sieciowymi lub udostępni zestawy reguł zapory, jeśli firewall nie zostanie dostarczony przez Dostawce/Wykonawce.
2. Po udzieleniu zamówienia Dostawca/Wykonawca udziela szczegółowych informacji na temat całej komunikacji, w tym protokołów wymaganych przez zaporę sieciową i identyfikuje każde urządzenie sieciowe inicjujące komunikację zgodnie z odpowiednimi zestawami reguł.
3. Dostawca/Wykonawca sprawdza, czy procedury SAT obejmują walidację i dokumentację wymagań. Wszelkie domyślne nazwy użytkowników, hasła lub inne kody bezpieczeństwa skonfigurowane przez Dostawcę/Wykonawcę lub producenta muszą zostać zmienione w tym momencie
4. Należy na bieżąco sprawdzać czy nie pojawiają się aktualizację firmware (łatki) dla zapór sieciowych.

6.2.1.2 System wykrywania włamań do sieci (NIDS - ang. Network Intrusion Detection System)

1. Dostawca/Wykonawca zapewnia profile ruchu z oczekiwanymi ścieżkami komunikacyjnymi, ruchem sieciowym i przewidywanymi granicami wykorzystania, w przypadku NIDS opartych na anomaliach.
2. Dostawca/Wykonawca dostarczy odpowiednie podpisy dla NIDSs opartych na sygnaturach.
3. Po udzieleniu zamówienia, Dostawca/Wykonawca dostarczy skonfigurowane NIDS i / lub dostarczy informacje do skonfigurowania NIDS.
4. Dostawca/Wykonawca będzie sprawdzał NIDS podczas całego procesu FAT i okresowo wprowadzał odpowiednie złośliwe oprogramowanie. Dostawca/Wykonawca zbada pliki logów i sprawdzi oczekiwane wyniki.

5. Dostawca/Wykonawca będzie używał NIDS podczas całego procesu SAT i okresowo wprowadzał odpowiednie złośliwe oprogramowanie. Dostawca/Wykonawca zbada pliki logów i sprawdzi oczekiwane wyniki.
6. Dostawca/Wykonawca dostraja sygnatury i dostosowuje progi, aby zmniejszyć liczbę fałszywych alarmów i zminimalizować fałszywe wyników.
7. Dostawca/Wykonawca będzie aktualizował konfigurację NIDS i / lub dokumentację w razie potrzeby po wprowadzeniu zmian.

6.2.1.3 System wykrywania próby połączenia (Canaries)

1. Dostawca/Wykonawca dla zapewnienia pasywnego monitorowania sieci zapewnia „Honey pots" analizujące nieautoryzowane połączenia i / lub „Kanarki" (Canary), które sygnalizują, że miała miejsce próba połączenia.
2. Dostawca/Wykonawca skonfiguruje lub przekaże informacje do skonfigurowania „Kanarka" z oprogramowaniem ostrzegającym, aby wskazywać na nieautoryzowane próby połączenia.
3. Dostawca/Wykonawca sprawdzi, czy procedury SAT zawierają pisemną walidację i dokumentację wymagań. Wszelkie domyślne nazwy użytkowników, hasła lub inne kody bezpieczeństwa skonfigurowane przez Dostawcę/Wykonawcę lub producenta muszą zostać zmienione w tym momencie.
4. Dostawca/Wykonawca dokona rekonfiguracji „kanarka (ów)" w miarę potrzeby, gdy zmianie ulegną topologie adresów sieciowych.

6.2.2 Adresowanie sieciowe i rozpoznawanie nazw

1. Aby chronić się przed atakami DNS, serwery DNS dla sieci systemu kontroli wewnętrznej powinny znajdować się wewnątrz zapory i powinny być oddzielone od serwerów DNS w sieci korporacyjnej. Serwery DNS dla sieci systemu sterowania powinny być autorytatywne tylko dla przestrzeni adresowej sieci systemu sterowania. Oznacza to, że serwery DNS powinny zawierać pełne informacje o strefie (odwzorowania nazw na adresy IP) tylko dla hostów w sieci systemu sterowania. Idealnie, sieć systemu sterowania jest odizolowana i hosty nie będą musiały rozwiązywać nazw zewnętrznych. Jeśli jednak hosty muszą rozpoznawać nazwy hostów spoza sieci zaufanych systemów sterowania, zapytania powinny być kierowane do serwera DNS systemu sterowania, który przesyła zapytania przez zaporę do serwera DNS w sieci korporacyjnej.
2. Zalecenia dotyczące bezpiecznej konfiguracji DNS:
   - Korzystanie z dedykowanych serwerów dla DNS i powiązanych usług oraz wyłączanie wszystkich niepotrzebnych usług.

- Używanie najnowszych wersji oprogramowania z aktualnymi poprawkami.
- Okresowe tworzenie kopii zapasowych i przeglądanie plików konfiguracyjnych DNS oraz przeprowadzanie sprawdzeń integralności w celu sprawdzenia integralności plików konfiguracyjnych, danych strefy i innych plików DNS.
- Uruchomienie serwerów DNS jako użytkownik inny niż root. Włączanie kontroli dostępu, aby umożliwić tylko określonym osobom tworzenie, usuwanie lub modyfikowanie danych DNS.
- Włączanie zapobiegania zanieczyszczaniu pamięci podręcznej.
- Ograniczanie adresów, które mogą kierować zapytania do serwerów DNS systemu sterowania, aby kontrolować hosty systemu.
- Ograniczanie transferów stref tylko do zaufanych hostów i uwierzytelnianie transferów stref.
- Używanie statycznego schematu adresowania. Jeśli używane jest adresowanie dynamiczne, zezwól na dynamiczne aktualizacje tylko od zaufanych hostów.
- Konfigurowanie zapory w celu umożliwienia komunikacji między systemem sterowania i korporacyjnymi serwerami DNS tylko w portach UDP i TCP 53.
- Zezwalanie na specjalne uwagi dla hostów z wieloma adresami IP dla nadmiarowości.

3. W przypadku udzielenia zamówienia przed zawarciem Umowy, Dostawca**/**Wykonawca dostarczy zalecaną metodologię adresowania sieciowego i rozpoznawania nazw.
4. Dostawca**/**Wykonawca zapewni środki do weryfikacji integralności plików konfiguracyjnych, danych strefy i innych plików DNS (np. Takie sprawdzanie integralności można wykonać za pomocą urządzenia HIDS).
5. Po przyznaniu kontraktu Dostawca**/**Wykonawca powinien dostarczyć skonfigurowane serwery DNS lub informacje do skonfigurowania serwera (serwerów) DNS, który spełnia wstępnie wynegocjowany standard zabezpieczeń.
6. Dostawca/Wykonawca powinien traktować informacje adresowe jako wrażliwe na biznes i je chronić.
7. Dostawca/Wykonawca będzie instalował i uruchamiał serwery DNS dostarczane przez niego w sposób ciągły podczas całego procesu FAT.
8. Dostawca**/**Wykonawca weryfikuje wszystkie serwery domen, a hosty w domenie biorącej udział w testowaniu mogą być rozwiązywane przez wszystkie systemy klienckie i serwerowe podłączone do sieci.
9. Dostawca/Wykonawca powinien udokumentować zarówno rozwiązanie przekazywania do przodu (nazwa hosta na adres IP), jak i odwrotne (adres IP na nazwę hosta).
10. Dostawca/Wykonawca będzie uruchamiał serwer DNS podczas całego procesu SAT.

11. Dostawca/Wykonawca sprawdzi, czy wszystkie serwery domen i hosty w domenie biorącej udział w testowaniu są rozpoznawalne przez wszystkie systemy klienckie i serwerowe podłączone do sieci.
12. Dostawca/Wykonawca powinien udokumentować zarówno rozwiązanie przekazywania do przodu (nazwa hosta na adres IP), jak i odwrotne (adres IP na nazwę hosta).
13. Dostawca/Wykonawca zapewnia ciągły proces zarządzania poprawkami dla systemu DNS i powiązanych usług, takich jak DHCP.

6.2.3 Zdalny dostęp

6.2.3.1 TCP/IP

1. Dostawca/Wykonawca zapewnia fizyczne i cyberbezpieczne funkcje, w tym między innymi uwierzytelnianie, szyfrowanie, kontrolę dostępu, rejestrację zdarzeń i komunikacji, monitorowanie i alarmowanie w celu ochrony urządzenia i komputera konfiguracyjnego przed nieautoryzowanym modyfikowaniem lub użyciem.
2. Dostawca/Wykonawca powinien wyraźnie zidentyfikować fizyczne i cyberbezpieczne funkcje bezpieczeństwa i dostarczyć metodologię utrzymania funkcji, w tym metody zmiany ustawień od skonfigurowanych przez dostawcę lub domyślnych warunków producenta.
3. Dostawca/Wykonawca sprawdza, czy dodanie funkcji bezpieczeństwa nie ma negatywnego wpływu na łączność, opóźnienie, przepustowość i czas odpowiedzi, w tym podczas SAT po podłączeniu do istniejącego sprzętu.
4. Dostawca/Wykonawca usuwa lub wyłącza wszystkie składniki oprogramowania, które nie są wymagane do działania i konserwacji urządzenia przed FAT. Dostawca/Wykonawca dostarczy dokumentację dotyczącą tego, co zostało usunięte i / lub wyłączone.
5. Dostawca/Wykonawca zapewni, przed upływem okresu negocjacji, odpowiednie aktualizacje stosu protokołów i / lub obejścia, aby złagodzić wszystkie luki związane z produktem i utrzymać ustalony poziom bezpieczeństwa systemu.
6. Dostawca/Wykonawca weryfikuje i dostarcza dokumentację potwierdzającą, że system bezpieczeństwa (SIS) jest certyfikowany po włączeniu urządzeń zabezpieczających.
7. Dostawca/Wykonawca użyje implementacji protokołu TCP / IP, która będzie w pełni zgodna z bieżącymi dokumentami RFC protokołu TCP / IP.
8. Dostawca/Wykonawca dostarczy produkt zgodny z IPv6.
9. Dostawca/Wykonawca zapewni możliwość monitorowania ruchu w systemie szyfrowania.
10. Po udzieleniu zamówienia, Dostawca/Wykonawca zapewni niezależną, zewnętrzną weryfikację zabezpieczeń implementacji IPv6 (np. Za pomocą technik fuzzingu). Dostwca/Wykonawca dostarczy dokumentację wyników niezależnej weryfikacji bezpieczeństwa strony trzeciej implementacji IPv6.

11. Dostawca/Wykonawca powinien zmniejszyć wszystkie luki wykryte podczas testowania implementacji IPv6 i dostarczyć dokumentację wyników.
12. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację fizycznych i cyberbezpiecznych funkcji, w tym między innymi uwierzytelniania, szyfrowania, kontroli dostępu, rejestrowania zdarzeń i komunikacji, monitorowania i alarmowania w celu ochrony systemu przed nieautoryzowanymi modyfikacjami lub użyciem.
13. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację, że wszystkie zatwierdzone aktualizacje i poprawki bezpieczeństwa są instalowane i testowane na początku FAT.
14. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację, że wszystkie nieużywane oprogramowanie i usługi zostały usunięte lub wyłączone.
15. Po FAT, Dostawca/Wykonawca utworzy linię bazową komunikacji i konfiguracji systemu, w tym między innymi funkcje bezpieczeństwa cybernetycznego, oprogramowanie, protokoły, porty i usługi oraz dostarczy dokumentację opisującą każdy przedmiot i zmiany.
16. Dostawca/Wykonawca dokonuje weryfikacji za pomocą skanów bezpieczeństwa cybernetycznego systemu i dostarcza dokumentacji, że dodanie funkcji bezpieczeństwa nie wpływa negatywnie na odpowiednią łączność, opóźnienie, przepustowość i czas odpowiedzi.
17. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację oraz zmiany funkcji zabezpieczeń fizycznych i cyberbezpieczeństwa, w tym między innymi uwierzytelnianie, szyfrowanie, kontrolę dostępu, rejestrowanie zdarzeń i komunikacji, monitorowanie i alarmowanie w celu ochrony komputera systemowego przed nieautoryzowanym modyfikowaniem lub użyciem.
18. Po zakończeniu SAT, Dostawca/Wykonawca utworzy linię bazową komunikacji i konfiguracji systemu, w tym między innymi funkcje bezpieczeństwa cybernetycznego, oprogramowanie, protokoły, porty i usługi oraz udostępni dokumentację opisującą wszelkie zmiany.
19. Dostawca/Wykonawca sprawdzi i dostarczy dokumentację, że wszelkie domyślne konta skonfigurowane przez producenta, nazwy użytkowników, hasła, ustawienia zabezpieczeń, kody bezpieczeństwa i inne metody dostępu są zmienione, wyłączone lub usunięte.
20. Dostawca/Wykonawca zapewnia konserwację dostarczonych funkcji bezpieczeństwa systemu.
21. Dostawca/Wykonawca dokumentuje wszystkie uzupełnienia i zmiany w urządzeniu zdalnego dostępu w okresie gwarancyjnym.
22. Dostawca/Wykonawca powinien zweryfikować uprawnienia i ustawienia zabezpieczeń w systemie bazowym przed dostarczeniem uaktualnień lub wymian w celu utrzymania ustalonego poziomu bezpieczeństwa systemu.

6.2.3.2 VPN

1. Miejsce docelowe serwera VPN i jego własność powinny zostać uzgodnione dla każdego wdrażanego VPN. Dobrym rozwiązaniem jest umieszczenie serwera VPN w strefie DMZ oddzielnie od sieci sterowania i zezwolenie użytkownikowi na połączenie się z siecią kontrolną przy użyciu procesu uwierzytelniania wymaganego dla użytkownika, który uzyskuje dostęp lokalnie do sieci. VPN są silnie uzależnione od reguł zapory sieciowej i jako takie powinny być brane pod uwagę przy żądaniu rozwiązań firewall.
2. Dostawca/Wykonawca zapewnia fizyczne i cyberbezpieczne funkcje, w tym między innymi uwierzytelnianie wieloskładnikowe (np. Token zabezpieczający, znany klucz i / lub certyfikat), szyfrowanie, kontrola dostępu, rejestrowanie zdarzeń i komunikacji, monitorowanie i alarmowanie w celu ochrony komputer systemowy i konfiguracyjny przed nieautoryzowanym modyfikowaniem lub użyciem.
3. Dostawca/Wykonawca powinien wyraźnie zidentyfikować fizyczne i cyberbezpieczne funkcje bezpieczeństwa i dostarczyć metodologię utrzymania funkcji, w tym metody zmiany ustawień od skonfigurowanych przez dostawcę lub domyślnych warunków producenta.
4. Dostawca/Wykonawca sprawdza, czy dodanie funkcji bezpieczeństwa nie ma negatywnego wpływu na łączność, opóźnienie, przepustowość i czas odpowiedzi, w tym podczas SAT po podłączeniu do istniejącego sprzętu. Dostawca/Wykonawca dokumentuje powyższe weryfikacje.
5. Dostawca/Wykonawca usuwa lub wyłącza wszystkie składniki oprogramowania, które nie są wymagane do działania i konserwacji urządzenia przed FAT. Dostawca/Wykonawca dostarczy dokumentację dotyczącą tego, co zostało usunięte i / lub wyłączone.
6. Dostawca/Wykonawca zapewni, przed upływem okresu negocjacji, odpowiednie aktualizacje stosu protokołów i / lub obejścia, aby złagodzić wszystkie luki związane z produktem i utrzymać ustalony poziom bezpieczeństwa systemu.
7. Dostawca/Wykonawca weryfikuje i dostarcza dokumentację potwierdzającą, że system bezpieczeństwa (SIS) jest certyfikowany po włączeniu urządzeń zabezpieczających.
8. Dostawca/Wykonawca zapewni strefę DMZ poza siecią kontrolną, aby serwer VPN mógł rezydować.
9. Dostawca/Wykonawca będzie stosował różne metody uwierzytelniania w celu ustanowienia dostępu do sieci kontrolnej i połączenia VPN.
10. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację fizycznych i cyberbezpiecznych funkcji, w tym między innymi uwierzytelniania wieloskładnikowego (np. Token zabezpieczający, znany klucz i/lub certyfikat) szyfrowania, kontroli dostępu, rejestrowania zdarzeń i komunikacji, monitorowania i alarmowania w celu ochrony systemu przed nieautoryzowanymi modyfikacjami lub użyciem.

11. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację, że wszystkie zatwierdzone aktualizacje i poprawki bezpieczeństwa są instalowane i testowane na początku FAT.
12. Dostawca/Wykonawca utworzy linię bazową komunikacji i konfiguracji systemu, w tym między innymi funkcje bezpieczeństwa cybernetycznego, oprogramowanie, protokoły, porty i usługi oraz dostarczy dokumentację opisującą funkcjonalność każdego elementu i zmiany.
13. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację, że wszystkie nieużywane oprogramowanie i usługi zostały usunięte lub wyłączone.
14. Dostawca/Wykonawca sprawdzi i dostarczy dokumentację, że wszelkie domyślne konta skonfigurowane przez producenta, nazwy użytkowników, hasła, ustawienia zabezpieczeń, kody bezpieczeństwa i inne metody dostępu są zmienione, wyłączone lub usunięte.
15. Dostawca/Wykonawca zapewni, przed upływem okresu negocjacji, odpowiednie aktualizacje i poprawki, w miarę zidentyfikowania problemów związanych z bezpieczeństwem w celu utrzymania ustalonego poziomu bezpieczeństwa systemu.
16. Dostawca/Wykonawca powinien zweryfikować uprawnienia i ustawienia zabezpieczeń w systemie bazowym przed dostarczeniem uaktualnień lub wymian w celu utrzymania ustalonego poziomu bezpieczeństwa systemu.
17. Dostawca/Wykonawca zapewnia konserwację dostarczonych funkcji bezpieczeństwa systemu.
18. Dostawca/Wykonawca dokumentuje wszystkie uzupełnienia i zmiany w urządzeniu zdalnego dostępu w okresie gwarancyjnym.

6.2.4 Partycjonowanie sieci

6.2.4.1 Urządzenia sieciowe

1. Dostawca/Wykonawca zapewni i zweryfikuje metodę zarządzania urządzeniami sieciowymi i zmieniającymi się schematami adresowania.
2. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację, że interfejs zarządzania konfiguracją sieci jest zabezpieczony.
3. Dostawca/Wykonawca zapewni oraz zweryfikuje listy ACL, listy adresów bezpieczeństwa portów i ulepszone zabezpieczenia dla dublowania portów.
4. Dostawca/Wykonawca powinien usunąć lub dezaktywować nieużywane funkcje konfiguracji i zarządzania siecią na urządzeniach sieciowych.
5. Dostawca/Wykonawca zapewni zasady zapory sieciowej dla ruchu przychodzącego i wychodzącego w oparciu o zestawy reguł odmowy dla wszystkich.
6. Dostawca/Wykonawca zapewnia zasady NIDS i narzędzia do przeglądania dzienników, które sprawdzają działanie zapory i wykrywają nietypowy ruch.

7. Dostawca/Wykonawca zapewni architekturę NIPS, która będzie działać z metodą komunikacji.
8. Dostawca/Wykonawca zapewni koncentratory VPN skonfigurowane z filtrami i zabezpieczeniami portów oraz dostarczy dokumentację na temat urządzeń sieciowych zainstalowanych z ustawieniami bezpieczeństwa.
9. Dostawca/Wykonawca powinien zeskanować porty sieciowe, zasygnalizować powstawanie i funkcjonalność ruchu dla każdego portu.
10. Dostawca/Wykonawca zapewnia aktualizacje i poprawki w celu utrzymania ustalonego poziomu bezpieczeństwa systemu.
11. Dostawca/Wykonawca powinien zweryfikować uprawnienia i ustawienia zabezpieczeń w systemie podstawowym przed dostarczeniem jakichkolwiek uaktualnień lub wymian.

6.2.4.2 Architektura sieci

1. Uproszczenie sieci powinno być priorytetem podczas projektowania początkowej architektury lub reguł zapory sieciowej. Różnorodność protokołów otwartych dla danych powinna być ograniczona do minimum. Dane modyfikowane wielokrotnie i retransmitowane, takie jak baza danych, Internet i FTP, należy najpierw przenieść do strefy DMZ, zmodyfikować w strefie DMZ i przesłać z DMZ do innych sieci.Wykonawca zapewni i zweryfikuje metodę zarządzania urządzeniami sieciowymi i zmieniającymi się schematami adresowania.
2. Dostawca/Wykonawca powinien zapewnić i udokumentować bezpieczną architekturę sieci, w której wyższe strefy bezpieczeństwa nawiązują łączność z mniej bezpiecznymi strefami.
3. Dostawca/Wykonawca powinien zapewnić i udokumentować projekt dla wszystkich ścieżek komunikacyjnych między sieciami różnych stref bezpieczeństwa za pośrednictwem DMZ.
4. Dostawca/Wykonawca powinien zweryfikować i udokumentować, że punkty rozłączenia są ustanowione między partycjami sieciowymi i zapewnić metody izolowania podsieci w celu kontynuowania ograniczonych operacji.
5. Dostawca/Wykonawca powinien zapewnić i udokumentować dostosowane reguły filtrowania i monitorowania dla wszystkich stref bezpieczeństwa i alarm dla nieoczekiwanego ruchu.
6. Dostawca/Wykonawca powinien dostarczyć i udokumentować strefę DMZ, która jest ograniczona do komunikacji, w której cały ruch jest monitorowany, alarmowany i filtrowany.
7. Dostawca/Wykonawca powinien zapewnić i udokumentować filtrowanie wychodzące i alarmy dotyczące nieoczekiwanego ruchu w strefach bezpieczeństwa.
8. Dostawca/Wykonawca powinien określić i udokumentować wszystkie źródła i miejsca przeznaczenia z wymuszonym rozpoczęciem komunikacji, nawet podczas restartu między strefami bezpieczeństwa.
9. Dostawca/Wykonawca powinien dostarczyć i udokumentować dwie architektury DMZ przy użyciu różnych produktów wykonujących tę samą funkcjonalność równolegle.

10. Dostawca/Wykonawca powinien dostarczyć i udokumentować mechanizm łatania pojedynczej architektury DMZ działającej w konfiguracji równoległej bez zakłócania działania drugiego DMZ działającego równolegle.
11. Dostawca/Wykonawca powinien ocenić potrzebę oraz zapewnić aktualizacje i łaty w miarę rozpoznawania luk w celu utrzymania ustalonego poziomu bezpieczeństwa systemu. Dostawca/Wykonawca sprawdzi i udokumentuje, że profil bezpieczeństwa architektury sieci jest zachowany.

6.3 Integralność systemu

6.3.1 „Utwardzanie" systemu

6.3.1.1 Usunięcie niepotrzebnych usług i programów

1. Zalecaną czynnością utwardzania jest wyłączenie lub usunięcie w urządzeniu sieciowym jakichkolwiek usług lub programów, które nie są wymagane do normalnej pracy systemu, usuwając w ten sposób potencjalne luki w zabezpieczeniach.
2. Skanowanie portów jest normalną metodą zapewnienia istnienia wymaganych usług i braku niepotrzebnych usług. Skanowanie portów należy przeprowadzić przed FAT z reprezentatywną, w pełni funkcjonalną konfiguracją systemu. Wszystkie porty wejścia / wyjścia (I / O) muszą zostać przeskanowane pod kątem UDP i TCP. Skanowanie należy przeprowadzić przed FAT i ponownie przed SAT. Skanowanie portów rzadko może być używane w systemach produkcyjnych. W większości przypadków skanery zakłócają ich działanie.
3. Po udzieleniu zamówienia, Dostawca/Wykonawca dostarczy dokumentację szczegółowo opisującą wszystkie aplikacje, narzędzia, usługi systemowe, skrypty, pliki konfiguracyjne, bazy danych i wszelkie inne wymagane oprogramowanie oraz odpowiednie konfiguracje, w tym wersje i / lub poziomy poprawek dla każdego z systemów komputerowych powiązanych z system kontroli.
4. Dostawca/Wykonawca dostarczy wykaz usług wymaganych dla dowolnego systemu komputerowego z uruchomionymi aplikacjami systemu sterowania lub wymaganego do połączenia aplikacji systemu sterowania. Wykaz obejmuje wszystkie porty i usługi wymagane do normalnego działania, a także wszelkie inne porty i usługi wymagane dla działania w trybie awaryjnym. Wykaz powinien zawierać również wyjaśnienie lub odsyłacz, aby uzasadnić, dlaczego każda usługa jest niezbędna do działania.
5. Dostawca/Wykonawca sprawdzi i dostarczy dokumentację, że wszystkie usługi są załatane do bieżącego statusu. Dostawca/Wykonawca zapewnia, w ramach wcześniejszego okresu negocjacji, odpowiednie aktualizacje oprogramowania i usług i / lub obejścia, aby złagodzić

wszystkie luki w zabezpieczeniach związane z produktem i utrzymać ustalony poziom bezpieczeństwa systemu.

Dostawca/Wykonawca usuwa i / lub wyłącza wszystkie składniki oprogramowania, które nie są wymagane do działania i konserwacji systemu kontroli przed FAT. Dostawca/Wykonawca dostarczy dokumentację dotyczącą tego, co zostało usunięte i / lub wyłączone. Oprogramowanie do usunięcia i / lub wyłączenia obejmuje, ale nie ogranicza się do:

1. Gry.
2. Sterowniki urządzeń dla urządzeń sieciowych, które nie zostały dostarczone.
3. Usługi przesyłania wiadomości (np. MSN, AOL IM).
4. Serwery lub klienci nieużywanych usług internetowych.
5. Kompilatory oprogramowania na wszystkich stacjach roboczych użytkowników i serwerach, z wyjątkiem programistycznych stacji roboczych i serwerów.
6. Kompilatory oprogramowania dla języków, które nie są używane w systemie sterowania.
7. Nieużywane protokoły sieciowe i komunikacyjne.
8. Niewykorzystane narzędzia administracyjne, diagnostyka, zarządzanie siecią i funkcje zarządzania systemem.
9. Kopie zapasowe plików, baz danych i programów używanych tylko podczas tworzenia systemu.
10. Wszystkie nieużywane dane i pliki konfiguracyjne.
11. Przykładowe programy i skrypty.
12. Nieużywane narzędzia do przetwarzania dokumentów (Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice itp.).

6. Dostawca/Wykonawca sprawdzi, czy Zamawiający wymaga wyników skanowania cybernetycznego (jako minimum luki w zabezpieczeniach i aktywnego skanowania portu, z najbardziej aktualnymi plikami sygnatur) uruchamianych w systemie sterowania jako podstawowa działalność FAT. Ta ocena jest następnie porównywana z wykazem wymaganych usług, stanem poprawek i dokumentacją, aby potwierdzić ten wymóg. Inne przewidziane środki obejmują:
   1. Dostawca/Wykonawca zapewnia dla każdego urządzenia sieciowego lub klasy urządzeń (np. Serwera, stacji roboczej i przełącznika) następujące dokumenty dotyczące konfiguracji:
      - Usługi sieciowe wymagane do działania tego urządzenia. Wskaż nazwę usługi, protokół (np. TCP i UDP) i zakres portów.
      - Zależności od podstawowych usług systemu operacyjnego.
      - Zależności w usługach sieciowych rezydujących na innych urządzeniach sieciowych.

- Wszystkie parametry konfiguracyjne oprogramowania wymagane do prawidłowego działania systemu.
- Certyfikowany system operacyjny, sterownik i inne wersje oprogramowania zainstalowane w urządzeniu.
- Results found by the vulnerability scans with mitigations affected. (Wyniki wykryte przez skany narażone na atak ze szkodliwym wpływem).

2. Dostawca/Wykonawca powinien zainstalować aktualizacje oprogramowania wewnętrznego dostępnego dla komputera lub urządzenia sieciowego certyfikowanego przez producenta systemu w momencie instalacji i dostarczać dokumentację.
3. Dostawca/Wykonawca dostarczy tabelę zbiorczą wskazującą każdą ścieżkę komunikacyjną wymaganą przez system z uwzględnieniem następujących informacji:
a. Nazwa urządzenia źródłowego i kontrola dostępu do nośnika (MAC) i / lub adres IP.
b. Nazwa urządzenia docelowego i MAC i / lub adres IP.
c. Protokół (na przykład TCP i UDP) i port lub zakres portów.
4. Dostawca/Wykonawca przeprowadza sieciowe etapy walidacji i dokumentacji na każdym urządzeniu:
Pełne skanowanie portów TCP i UDP w portach 1-65535. Skanowanie to należy wykonać podczas symulowanej "normalnej pracy systemu".

7. Dostawca/Wykonawca będzie porównywał wyniki skanowania bezpieczeństwa cybernetycznego uruchomionego w systemie, jako podstawową działalność SAT, z wykazem wymaganych usług, stanem poprawek i wymaganą dokumentacją. Po zakończeniu SAT i przed zmianą lub uruchomieniem, powyższe skanowanie bezpieczeństwa cybernetycznego (z najnowszymi plikami sygnatur) musi zostać uruchomione ponownie.

6.3.1.2 HIDS

1. Dostawca/Wykonawca zapewnia skonfigurowane urządzenia HIDS i / lub dostarczy informacje do skonfigurowania urządzeń HIDS zawierające, statyczne nazwy plików, dynamiczne wzorce nazw plików, kont systemowych i kont użytkowników, wykonywania nieautoryzowanego kodu, wykorzystania hosta i procesu uprawnienia wystarczające do skonfigurowania HIDS.
2. Dostawca/Wykonawca powinien skonfigurować urządzenia HIDS w taki sposób, aby rejestrowane były wszystkie połączenia kont systemowych i kont użytkowników. Ten rejestr powinien być skonfigurowany w taki sposób, aby alarm mógł być wyświetlany operatorowi lub pracownikowi ochrony w przypadku wystąpienia nietypowej sytuacji.
3. Dostawca/Wykonawca powinien przedstawić zalecaną konfigurację HIDS w sposób, który nie ma negatywnego wpływu na funkcje systemu operacyjnego ani na cele biznesowe.

4. Dostawca/Wykonawca powinien podać zalecane narzędzia do przeglądania logów i powiadomień.
5. Dostawca/Wykonawca powinien skonfigurować urządzenia jako "append only", aby zapobiec zmianie zapisów na lokalnych urządzeniach pamięci.
6. Dostawca/Wykonawca będzie zarządzał HIDS podczas całego procesu FAT i okresowo wprowadzał odpowiednie złośliwe oprogramowanie. Dostawca/Wykonawca zbada pliki logów i sprawdzi oczekiwane wyniki. Procedury FAT powinny objąć walidację i dokumentację tego wymogu.
7. Dostawca/Wykonawca będzie zarządzał HIDS podczas całego procesu SAT i okresowo wprowadzał odpowiednie złośliwe oprogramowanie. Dostawca/Wykonawca zbada pliki logów i sprawdzi oczekiwane wyniki. Procedury SAT powinny objąć walidację i dokumentację tego wymogu
8. Dostawca/Wykonawca powinien wygenerować obraz systemu na zakończenie SAT, który będzie później użyty jako kontrolna linia bazowa.

6.3.1.3 Zmiany w systemie plików i uprawnieniach systemu operacyjnego

1. Dostawca/Wykonawca powinien skonfigurować hosty z najmniejszym dostępem do pliku i dostępem do konta oraz dostarczyć dokumentację konfiguracji.
2. Dostawca/Wykonawca powinien skonfigurować niezbędne usługi systemowe do wykonania z najniższym poziomem uprawnień użytkownika dla tej usługi i dostarczyć dokumentację konfiguracji.
3. Dostawca/Wykonawca udokumentuje, że zmiana lub wyłączenie dostępu do takich plików i dokumentację przyznanych uprawnień.
4. Dostawca/Wykonawca powinien zapewnić, w ramach procedur SAT, zatwierdzenie i dokumentację przypisanych uprawnień.

6.3.1.4 Konfiguracja sprzętu

1. Dostawca/Wykonawca powinien wyłączyć, za pomocą oprogramowania lub fizycznego odłączenia, wszystkie niepotrzebne porty komunikacyjne i dyski nośników wymiennych lub zapewnić zaprojektowane bariery i dostarczyć wynikową dokumentację.
2. Dostawca/Wykonawca powinien zapewnić ochronę BIOS przed nieautoryzowanymi zmianami, chyba że nie jest to technicznie wykonalne, w takim przypadku Dostawca udokumentuje to i zapewni środki łagodzące.
3. Dostawca/Wykonawca powinien dostarczyć pisemną listę wszystkich wyłączonych lub usuniętych portów USB, napędów CD / DVD i innych wymiennych urządzeń multimedialnych.

4. Dostawca/Wykonawca powinien skonfigurować urządzenia sieciowe w celu ograniczenia dostępu do / z określonych lokalizacji, w stosownych przypadkach, oraz dostarczyć dokumentację konfiguracji.
5. Dostawca/Wykonawca powinien skonfigurować system, aby umożliwić administratorom systemu możliwość ponownego włączenia urządzeń, jeżeli urządzenia są wyłączone przez oprogramowanie i dostarczyć dokumentację konfiguracji.
6. Dostawca/Wykonawca powinien zapewnić, w ramach procedur FAT, zatwierdzanie i dokumentowanie wyłączonego lub zablokowanego dostępu fizycznego i usuniętych sterowników.
7. Dostawca/Wykonawca powinien zapewnić, w ramach procedur SAT, zatwierdzanie i dokumentowanie wyłączonego lub zablokowanego dostępu fizycznego i usuniętych sterowników.

6.3.1.5 Sygnały „Heartbeat”

1. Dostawca/Wykonawca powinien zidentyfikować sygnały lub protokoły „Heartbeat” i zalecić włączenie monitora do sieci.
2. Po udzieleniu zamówienia Dostawca/Wykonawca dostarczy pakiety definicji sygnałów „Heartbeat” i przykładów ruchu „Heartbeat”, jeśli sygnały są uwzględnione w monitorowaniu sieci.
3. W ramach procedur FAT Dostawca/Wykonawca zapewni dokumentację wymagań.
   Dostawca/Wykonawca utworzy linię bazową ruchu komunikacyjnego „Heartbeat”, aby uwzględnić częstotliwość, rozmiary pakietów i oczekiwane konfiguracje pakietów.
4. Dostawca/Wykonawca zapewni, w ramach procedur SAT, dokumentację wymagań.
   Dostawca/Wykonawca utworzy linię bazową ruchu komunikacyjnego „Heartbeat” i sprawdzi wyniki w odniesieniu do dokumentacji FAT.

6.3.1.6 Instalowanie systemów operacyjnych, aplikacji i aktualizacji oprogramowania innych firm

1. Dostawca/Wykonawca będzie prowadził proces zarządzania i aktualizacji łatek.
   Przed zawarciem umowy Dostawca przekazuje szczegółowe informacje dotyczące zarządzania łatkami i procesem aktualizacji. Należy określić odpowiedzialność za instalację i aktualizację poprawek.
2. Dostawca/Wykonawca powinien powiadamiać o znanych lukach mających wpływ na dostarczony lub wymagany przez Dostawcę system operacyjny, aplikacje i oprogramowanie stron trzecich w okresie wcześniejszego wynegocjowania po publicznym ujawnieniu.

3. Dostawca/Wykonawca powinien przekazywać powiadomienia o poprawkach mających wpływ na bezpieczeństwo w przedterminowym negocjowanym okresie, określonym w procesie zarządzania poprawkami. Przed dystrybucją Dostawca stosuje, testuje i zatwierdza odpowiednie aktualizacje i / lub obejścia na bazowym systemie odniesienia. Łagodzenie tych słabych punktów nastąpi w okresie negocjacji wstępnych.

6.3.2 Zarzadzanie sesją

1. Dostawca/Wykonawca nie powinien zezwalać na przekazywanie danych uwierzytelniających użytkownika w postaci zwykłego tekstu.
2. Dostawca/Wykonawca zapewni najsilniejszą metodę szyfrowania współmierną do platformy technologicznej i ograniczeń czasu reakcji.
3. Dostawca/Wykonawca nie może zezwolić na:
   - wielokrotne równoczesne logowanie, aby zachować informacje logowania między sesjami,
   - zapewnienie funkcji automatycznego uzupełniania podczas logowania,
   - anonimowe logowanie.
4. Dostawca/Wykonawca ustawi sposób wylogowania i limit czasu na koncie użytkownika.
5. Dostawca/Wykonawca sprawdza, czy procedury SAT obejmują walidację i dokumentację wymagań.

6.3.3 Zarzadzanie i polityka haseł/autoryzacji

1. Należy stosować się do instrukcji **Instrukcja ZSZ PBT.I02 Polityka haseł w systemach sterowania**
2. Dostawca/Wykonawca zapewnia konfigurowalny system zarządzania hasłami do konta, który umożliwia wybór długości hasła, częstotliwości zmiany, ustawienie wymaganej złożoności hasła, liczbę prób logowania, nieaktywne wylogowanie sesji, blokadę ekranu według aplikacji i odmowę ponownego użycia tego samego hasła.
3. Dostawca/Wykonawca nie powinien przechowywać haseł w postaci elektronicznej ani w dokumentacji dostarczonej przez Dostawcę w formie czytelnej, chyba że nośnik jest fizycznie chroniony.
4. Dostawca/Wykonawca powinien kontrolować dostęp do interfejsu konfiguracyjnego systemu zarządzania kontem.
5. Dostawca/Wykonawca sprawdza, czy procedury SAT obejmują sprawdzanie poprawności i dokumentację hasła i zasad uwierzytelniania oraz zarządzania.

6.3.4 Praktyki kodowania

1. Dostawca/Wykonawca dostarczy dokumentację przeglądów kodu i innych etapów procesu tworzenia oprogramowania wykorzystywanych do oceny bezpieczeństwa oprogramowania. Oprogramowanie podlegające tym przeglądom obejmuje zarówno aplikacje opracowane przez Dostawców/Wykonawców, jak i każdy inny kod źródłowy, nad którym Dostawca/Wykonawca sprawuje kontrolę, stanowiącą niezbędną część systemu sterowania. Oprogramowanie innych producentów zintegrowane z produktami dostawców/wykonawców powinno być oceniane pod kątem luk w zabezpieczeniach. Doświadczenie pokazuje, że integracja systemu często przyczynia się do ogólnej podatności systemu na atak.
2. Dostawca/Wykonawca powinien przy tworzeniu kodu kierować się następującymi zasadami:

a. Dane wejściowe należy sprawdzać pod kątem sensownych wartości.
b. Pliki z danymi powinny być szyfrowane.
c. Należy uwzględnić wpływ systemów operacyjnych i innych bibliotek stron trzecich na bezpieczeństwo.
d. Należy upewnić się, że systemy operacyjne i inne biblioteki firm trzecich mają zasady aktualizacji.
e. Nie można umożliwiać przepełnienia bufora.
f. Należy sprawdź, czy pliki dzienników są niezmienne.
g. Należy stosować kompleksowe sprawdzanie autentyczności i integralności w procesie komunikacji danych między procesami.
h. Należy stosować projekt i przegląd kodu.
i. Należy sprawdzić, czy w kodzie nie są wpisane hasła ani klucze szyfrowania.
j. Należy tworzyć kod w taki sposób by blokady i regulacje nie następowały z urządzeń spoza sieci wewnętrznej systemu sterowania.

3. Dostawca/Wykonawca powinien dostarczyć kody źródłowe stworzonego oprogramowania
4. Dostawca/Wykonawca dostarczy dokumentację praktyk rozwojowych i standardów stosowanych do oprogramowania systemu sterowania napisanego przez producenta, w tym firmweru, używanego w celu zapewnienia wysokiego poziomu ochrony przed nieautoryzowanym dostępem
5. Dostawca/Wykonawca powinien przeprowadzić FAT obejmujący walidację i dokumentację procesu tworzenia oprogramowania i / lub przeglądu kodu.
6. Dostawca/Wykonawca powinien przeprowadzić SAT obejmujący walidację i dokumentację procesu tworzenia oprogramowania i / lub przeglądu kodu.
7. Dostawca/Wykonawca sprawdza, czy aktualizacje oprogramowania i „łatki”(poprawki) są sprawdzane zgodnie z tym samym procesem opracowywania oprogramowania lub planu przeglądu.

6.3.5 Korekta defektów

1. Korekta defektów odnosi się do czynności, które należy wykonać, gdy zostaną wykryte błędy w oprogramowaniu systemu sterowania, sprzęcie i architekturach systemów utworzonych przez lub pod kontrolą dostawcy/Wykonawcy. Potrzebne są wskazówki dotyczące działań korygujących, napraw lub monitorowania w celu złagodzenia wszystkich luk w zabezpieczeniach związanych z podatnością. Podatności i usterki zwykle są ściśle utrzymywane, dopóki nie zostaną udostępnione środki zaradcze. Jednak niektóre luki w zabezpieczeniach są upubliczniane, zanim poprawka zostanie opracowana, a następnie konieczne jest złagodzenie tych podatności.
2. Wymagana jest historia błędów i kroków naprawczych/"łat" aby móc wycofać określone poprawki.
3. Dostawca/Wykonawca powinien dostarczyć udokumentowany proces naprawczy defektów.
4. Dostawca/Wykonawca zapewni odpowiednie aktualizacje oprogramowania i / lub sposoby postępowania w celu złagodzenia wszystkich luk w zabezpieczeniach związanych z podatnością przez ustalony w umowie/zamówieniu okresie.
5. Dostawca/Wykonawca powinien dostarczy dokumentację FAT dotyczącą walidacji defektów i środków zaradczych.
6. Dostawca/Wykonawca powinien dostarczy dokumentację SAT dotyczącą walidacji i naprawy defektów.
7. Dostawca/Wykonawca będzie utrzymywał przez okres określony w umowie/zamówieniu listę główną wszystkich defektów i działań korygujących do celów audytu.

6.3.6 Wykrywanie i ochrona przed malwarem

1. Dostawca/Wykonawca powinien ujawnić istnienie i przyczyny wszelkich znanych lub zidentyfikowanych kodów typu backdoor.
2. Dostawca/Wykonawca powinien spełnić jeden z dwóch warunków:

a. Zapewnić system wykrywania złośliwego oprogramowania oparty na hoście dla sieci systemu sterowania. Dostawca/Wykonawca sprawdza poprawność działania systemu w celu wykrycia szkodliwego oprogramowania hosta, poddania kwarantannie (zamiast automatycznego usuwania) podejrzanych plików oraz dostarczenia schematu aktualizacji podpisów. Dostawca/Wykonawca testuje również najważniejsze aktualizacje aplikacji do wykrywania złośliwego oprogramowania i dostarcza dane dotyczące pomiaru wydajności dotyczące wpływu zastosowania aplikacji do wykrywania złośliwego oprogramowania w aktywnym

systemie. Pomiary obejmują między innymi wykorzystanie sieci, wykorzystanie procesora, wykorzystanie pamięci i wszelkie inne wpływy na normalne przetwarzanie komunikacji.

b. Jeżeli Dostawca/Wykonawca nie dostarcza rzeczywistego schematu wykrywania szkodliwego oprogramowania hosta, Dostawca/Wykonawca powinien zaproponować produkty służące do wykrywania złośliwego oprogramowania i dostarczyć wskazówki dotyczące konfiguracji wykrywania złośliwego oprogramowania, które będą działać z produktami dostawców/wykonawców.

3. Dostawca/Wykonawca w ramach FAT i SAT powinien rejestrować pomiary wydajności systemu, które obejmują system z wykrywaniem złośliwego oprogramowania i bez niego.
4. Dostawca/Wykonawca w ramach FAT i SAT powinien udokumentować wszystkie znane lub zidentyfikowane backdoory.
5. Dostawca/Wykonawca powinien przechowywać logi aplikacji wykrywających złośliwe oprogramowanie przez okres określony w umowie/zamówieniu dla potencjalnych działań śledczych i sądowych.
6. Dostawca/Wykonawca powinien aktualizować oprogramowanie do wykrywania złośliwego oprogramowania zgodnie z wymaganiami, aby było skuteczne w przypadku najnowszego złośliwego oprogramowania. Wraz ze zmianą wariantów złośliwego oprogramowania należy zastosować nowe, bardziej precyzyjne lub dostrojone sygnatury.
7. Dostawca/Wykonawca powinien ujawniać istnienie i przyczyny wszelkich znanych lub zidentyfikowanych kodów typu backdoor.

6.4 Urządzenia końcowe

6.4.1 Intelligent Electronic Devices (IED)

1. Dostawca/Wykonawca powinien zapewnić bezpieczeństwo fizyczne i cyberbezpieczne funkcje obejmujące między innymi uwierzytelnianie, szyfrowanie, kontrolę dostępu, rejestrowanie zdarzeń i komunikacji, monitorowanie i alarmowanie w celu ochrony urządzenia i komputera konfiguracyjnego przed nieautoryzowanymi modyfikacjami lub użyciem.
2. Dostawca/Wykonawca powinien wyraźnie zidentyfikować cechy ochrony fizycznej i cyberbezpieczne funkcje oraz dostarczyć metodologię utrzymania tych funkcji, w tym metody zmiany ustawień z ustawień domyślnych producenta bądź Dostawcy/Wykonawcy.
3. Dostawca/Wykonawca powinien sprawdzić, czy dodanie funkcji bezpieczeństwa nie wpływa negatywnie na łączność, opóźnienia, przepustowość i czas reakcji, w tym podczas SAT, gdy jest podłączony do istniejącego sprzętu.

4. Dostawca/Wykonawca powinien usunąć lub wyłączyć wszystkie składniki oprogramowania, które nie są wymagane do działania i konserwacji urządzenia przed FAT. Dostawca/Wykonawca powinien dostarczyć dokumentację dotyczącą tego, co zostało usunięte i / lub wyłączone.
5. Dostawca/Wykonawca powinien zapewnić odpowiednie aktualizacje oprogramowania i usług, aby złagodzić wszystkie luki w zabezpieczeniach związane z dostarczanym urządzeniem i powinien utrzymać ustalony poziom bezpieczeństwa systemu, w okresie ustalonym w umowie/zamówieniu.
6. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację potwierdzającą, że system przyrządowy bezpieczeństwa (SIS/ESD) będzie certyfikowany po włączeniu urządzeń zabezpieczających.
7. Dostawca/Wykonawca powinien podczas FAT i SAT zweryfikować i udokumentować fizyczne bezpieczeństwo i cyberbezpieczeństwo, w tym między innymi uwierzytelnianie, szyfrowanie, kontrolę dostępu, rejestrację zdarzeń i komunikacji, monitorowanie i alarmowanie w celu ochrony urządzenia i komputera konfiguracyjnego przed nieautoryzowanymi modyfikacjami lub użyciem.
8. Dostawca/Wykonawca podczas FAT powinien zweryfikować i dostarczyć dokumentację, potwierdzającą że wszystkie zatwierdzone aktualizacje i poprawki bezpieczeństwa są zainstalowane i przetestowane.
9. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację, potwierdzającą że całe nieużywane oprogramowanie i usługi zostały usunięte lub wyłączone.
10. Dostawca/Wykonawca podczas SAT powinien sprawdzić i dostarczyć dokumentację potwierdzającą, że wszelkie domyślne konta, nazwy użytkowników, hasła, ustawienia zabezpieczeń, kody bezpieczeństwa i inne metody dostępu zostały zmienione, wyłączone lub usunięte.
11. Dostawca/Wykonawca powinien podczas SAT zweryfikować za pomocą skanów bezpieczeństwa cybernetycznego i dostarczyć dokumentację potwierdzającą, że dodanie funkcji bezpieczeństwa nie wpływa negatywnie na odpowiednią łączność, opóźnienie, przepustowość, czas odpowiedzi i przepustowość.
12. Dostawca/Wykonawca powinien zapewnić przez okres ustalony w umowie/zamówieniu, aktualizacje i poprawki dla urządzeń, gdy zidentyfikowane zostaną kwestie bezpieczeństwa w celu utrzymania ustalonego poziomu bezpieczeństwa systemu.
13. Dostawca/Wykonawca powinien utworzyć linię bazową zaktualizowanej komunikacji i konfiguracji systemu, w tym między innymi funkcje bezpieczeństwa cybernetycznego, oprogramowanie, protokoły, porty i usługi oraz udostępni dokumentację opisującą wszelkie zmiany.

14. Dostawca/Wykonawca powinien zweryfikować uprawnienia i ustawienia zabezpieczeń w systemie bazowym przed dostarczeniem uaktualnień w celu utrzymania ustalonego poziomu bezpieczeństwa systemu.
15. Dostawca/Wykonawca powinien udokumentować wszystkie uzupełnienia i zmiany w systemie kontroli w okresie gwarancyjnym/konserwacyjnym

6.4.2 Remote Terminal Units (RTU)

1. Dostawca/Wykonawca powinien zapewnić bezpieczeństwo fizyczne i cyberbezpieczne funkcje obejmujące między innymi uwierzytelnianie, szyfrowanie, kontrolę dostępu, rejestrowanie zdarzeń i komunikacji, monitorowanie i alarmowanie w celu ochrony urządzenia i komputera konfiguracyjnego przed nieautoryzowanymi modyfikacjami lub użyciem.
2. Dostawca/Wykonawca powinien wyraźnie zidentyfikować cechy ochrony fizycznej i cyberbezpieczne funkcje oraz dostarczyć metodologię utrzymania tych funkcji, w tym metody zmiany ustawień z ustawień domyślnych producenta bądź Dostawcy/Wykonawcy.
3. Dostawca/Wykonawca powinien sprawdzić, czy dodanie funkcji bezpieczeństwa nie wpływa negatywnie na łączność, opóźnienia, przepustowość i czas reakcji, w tym podczas SAT, gdy jest podłączony do istniejącego sprzętu.
4. Dostawca/Wykonawca powinien usunąć lub wyłączyć wszystkie składniki oprogramowania, które nie są wymagane do działania i konserwacji urządzenia przed FAT. Dostawca/Wykonawca powinien dostarczyć dokumentację dotyczącą tego, co zostało usunięte i / lub wyłączone.
5. Dostawca/Wykonawca powinien zapewnić odpowiednie aktualizacje oprogramowania i usług, aby złagodzić wszystkie luki w zabezpieczeniach związane z dostarczanym urządzeniem i powinien utrzymać ustalony poziom bezpieczeństwa systemu, w okresie ustalonym w umowie/zamówieniu.
6. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację potwierdzającą, że system przyrządowy bezpieczeństwa (SIS/ESD) będzie certyfikowany po włączeniu urządzeń zabezpieczających.
7. Dostawca/Wykonawca powinien podczas FAT i SAT zweryfikować i udokumentować fizyczne bezpieczeństwo i cyberbezpieczeństwo, w tym między innymi uwierzytelnianie, szyfrowanie, kontrolę dostępu, rejestrację zdarzeń i komunikacji, monitorowanie i alarmowanie w celu ochrony urządzenia i komputera konfiguracyjnego przed nieautoryzowanymi modyfikacjami lub użyciem.
8. Dostawca/Wykonawca podczas FAT powinien zweryfikować i dostarczyć dokumentację, potwierdzającą że wszystkie zatwierdzone aktualizacje i poprawki bezpieczeństwa są zainstalowane i przetestowane.

9. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację, potwierdzającą że całe nieużywane oprogramowanie i usługi zostały usunięte lub wyłączone.
10. Dostawca/Wykonawca podczas SAT powinien sprawdzić i dostarczyć dokumentację potwierdzającą, że wszelkie domyślne konta, nazwy użytkowników, hasła, ustawienia zabezpieczeń, kody bezpieczeństwa i inne metody dostępu zostały zmienione, wyłączone lub usunięte.
11. Dostawca/Wykonawca powinien podczas SAT zweryfikować za pomocą skanów bezpieczeństwa cybernetycznego i dostarczyć dokumentację potwierdzającą, że dodanie funkcji bezpieczeństwa nie wpływa negatywnie na odpowiednią łączność, opóźnienie, przepustowość, czas odpowiedzi i przepustowość.
12. Dostawca/Wykonawca powinien zapewnić przez okres ustalony w umowie/zamówieniu, aktualizacje i poprawki dla urządzeń, gdy zidentyfikowane zostaną kwestie bezpieczeństwa w celu utrzymania ustalonego poziomu bezpieczeństwa systemu.
13. Dostawca/Wykonawca powinien utworzyć linię bazową zaktualizowanej komunikacji i konfiguracji systemu, w tym między innymi funkcje bezpieczeństwa cybernetycznego, oprogramowanie, protokoły, porty i usługi oraz udostępni dokumentację opisującą wszelkie zmiany.
14. Dostawca/Wykonawca powinien zweryfikować uprawnienia i ustawienia zabezpieczeń w systemie bazowym przed dostarczeniem uaktualnień w celu utrzymania ustalonego poziomu bezpieczeństwa systemu.
15. Dostawca/Wykonawca powinien udokumentować wszystkie uzupełnienia i zmiany w systemie kontroli w okresie gwarancyjnym/konserwacyjnym.

6.4.3 Sterowniki PLC

1. Dostawca/Wykonawca powinien zapewnić bezpieczeństwo fizyczne i cyberbezpieczne funkcje obejmujące między innymi uwierzytelnianie, szyfrowanie, kontrolę dostępu, rejestrowanie zdarzeń i komunikacji, monitorowanie i alarmowanie w celu ochrony urządzenia i komputera konfiguracyjnego przed nieautoryzowanymi modyfikacjami lub użyciem.
2. Dostawca/Wykonawca powinien wyraźnie zidentyfikować cechy ochrony fizycznej i cyberbezpieczne funkcje oraz dostarczyć metodologię utrzymania tych funkcji, w tym metody zmiany ustawień z ustawień domyślnych producenta bądź Dostawcy/Wykonawcy.
3. Dostawca/Wykonawca powinien sprawdzić, czy dodanie funkcji bezpieczeństwa nie wpływa negatywnie na łączność, opóźnienia, przepustowość i czas reakcji, w tym podczas SAT, gdy jest podłączony do istniejącego sprzętu.
4. Dostawca/Wykonawca powinien usunąć lub wyłączyć wszystkie składniki oprogramowania, które nie są wymagane do działania i konserwacji urządzenia przed FAT.

Dostawca/Wykonawca powinien dostarczyć dokumentację dotyczącą tego, co zostało usunięte i / lub wyłączone.

5. Dostawca/Wykonawca powinien zapewnić odpowiednie aktualizacje oprogramowania i usług, aby złagodzić wszystkie luki w zabezpieczeniach związane z dostarczanym urządzeniem i powinien utrzymać ustalony poziom bezpieczeństwa systemu, w okresie ustalonym w umowie/zamówieniu.
6. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację potwierdzającą, że system przyrządowy bezpieczeństwa (SIS/ESD) będzie certyfikowany po włączeniu urządzeń zabezpieczających.
7. Dostawca/Wykonawca powinien podczas FAT i SAT zweryfikować i udokumentować fizyczne bezpieczeństwo i cyberbezpieczeństwo, w tym między innymi uwierzytelnianie, szyfrowanie, kontrolę dostępu, rejestrację zdarzeń i komunikacji, monitorowanie i alarmowanie w celu ochrony urządzenia i komputera konfiguracyjnego przed nieautoryzowanymi modyfikacjami lub użyciem.
8. Dostawca/Wykonawca podczas FAT powinien zweryfikować i dostarczyć dokumentację, potwierdzającą że wszystkie zatwierdzone aktualizacje i poprawki bezpieczeństwa są zainstalowane i przetestowane.
9. Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację, potwierdzającą że całe nieużywane oprogramowanie i usługi zostały usunięte lub wyłączone.
10. Dostawca/Wykonawca podczas SAT powinien sprawdzić i dostarczyć dokumentację potwierdzającą, że wszelkie domyślne konta, nazwy użytkowników, hasła, ustawienia zabezpieczeń, kody bezpieczeństwa i inne metody dostępu zostały zmienione, wyłączone lub usunięte.
11. Dostawca/Wykonawca powinien podczas SAT zweryfikować za pomocą skanów bezpieczeństwa cybernetycznego i dostarczyć dokumentację potwierdzającą, że dodanie funkcji bezpieczeństwa nie wpływa negatywnie na odpowiednią łączność, opóźnienie, przepustowość, czas odpowiedzi i przepustowość.
12. Dostawca/Wykonawca powinien zapewnić przez okres ustalony w umowie/zamówieniu, aktualizacje i poprawki dla urządzeń, gdy zidentyfikowane zostaną kwestie bezpieczeństwa w celu utrzymania ustalonego poziomu bezpieczeństwa systemu.
13. Dostawca/Wykonawca powinien utworzyć linię bazową zaktualizowanej komunikacji i konfiguracji systemu, w tym między innymi funkcje bezpieczeństwa cybernetycznego, oprogramowanie, protokoły, porty i usługi oraz udostępni dokumentację opisującą wszelkie zmiany.

14. Dostawca/Wykonawca powinien zweryfikować uprawnienia i ustawienia zabezpieczeń w systemie bazowym przed dostarczeniem uaktualnień w celu utrzymania ustalonego poziomu bezpieczeństwa systemu.
15. Dostawca/Wykonawca powinien udokumentować wszystkie uzupełnienia i zmiany w systemie kontroli w okresie gwarancyjnym/konserwacyjnym.

6.4.4 Czujniki (Sensory), Urządzenia/elementy wykonawcze (Aktuatory) i Przyrządy pomiarowe

1. Dostawca/Wykonawca powinien zapewnić bezpieczeństwo fizyczne i cyberbezpieczne funkcje obejmujące między innymi uwierzytelnianie, szyfrowanie, kontrolę dostępu, rejestrowanie zdarzeń i komunikacji, monitorowanie i alarmowanie w celu ochrony urządzenia i komputera konfiguracyjnego przed nieautoryzowanymi modyfikacjami lub użyciem.
2. Dostawca/Wykonawca powinien wyraźnie zidentyfikować cechy ochrony fizycznej i cyberbezpieczne funkcje oraz dostarczyć metodologię utrzymania tych funkcji, w tym metody zmiany ustawień z ustawień domyślnych producenta bądź Dostawcy/Wykonawcy.
3. Dostawca/Wykonawca powinien zapewnić bezpieczne interfejsy komunikacyjne (szeregowe, Ethernetowe i bezprzewodowe), w tym możliwość filtrowania i monitorowania komunikacji. Przy czym nie należy używać komunikacji bezprzewodowej.
4. Dostawca/Wykonawca powinien sprawdzić, czy dodanie funkcji bezpieczeństwa nie wpływa negatywnie na łączność, opóźnienia, przepustowość i czas reakcji, w tym podczas SAT, gdy jest podłączony do istniejącego sprzętu.
5. W przypadku stosowania urządzeń „inteligentnych” Dostawca/Wykonawca powinien usunąć lub wyłączyć wszystkie składniki oprogramowania, które nie są wymagane do działania i konserwacji urządzenia przed FAT. Dostawca/Wykonawca powinien dostarczyć dokumentację dotyczącą tego, co zostało usunięte i / lub wyłączone.
6. W przypadku stosowania urządzeń „inteligentnych” Dostawca/Wykonawca powinien zapewnić odpowiednie aktualizacje oprogramowania i usług, aby złagodzić wszystkie luki w zabezpieczeniach związane z dostarczanym urządzeniem i powinien utrzymać ustalony poziom bezpieczeństwa systemu, w okresie ustalonym w umowie/zamówieniu.
7. W przypadku stosowania urządzeń „inteligentnych” Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację potwierdzającą, że system przyrządowy bezpieczeństwa (SIS/ESD) będzie certyfikowany po włączeniu urządzeń zabezpieczających.
8. Dostawca/Wykonawca powinien podczas FAT i SAT zweryfikować i udokumentować fizyczne bezpieczeństwo i cyberbezpieczeństwo, w tym między innymi uwierzytelnianie, szyfrowanie, kontrolę dostępu, rejestrację zdarzeń i komunikacji, monitorowanie i alarmowanie w celu ochrony urządzenia i komputera konfiguracyjnego przed nieautoryzowanymi modyfikacjami lub użyciem.

9. Dostawca/Wykonawca podczas FAT powinien zweryfikować i dostarczyć dokumentację, potwierdzającą że wszystkie zatwierdzone aktualizacje i poprawki bezpieczeństwa są zainstalowane i przetestowane.
10. W przypadku stosowania urządzeń „inteligentnych" Dostawca/Wykonawca powinien zweryfikować i dostarczyć dokumentację, potwierdzającą że całe nieużywane oprogramowanie i usługi zostały usunięte lub wyłączone.
11. W przypadku stosowania urządzeń „inteligentnych" Dostawca/Wykonawca podczas SAT powinien sprawdzić i dostarczyć dokumentację potwierdzającą, że wszelkie domyślne konta, nazwy użytkowników, hasła, ustawienia zabezpieczeń, kody bezpieczeństwa i inne metody dostępu zostały zmienione, wyłączone lub usunięte.
12. Dostawca/Wykonawca powinien podczas SAT zweryfikować za pomocą skanów bezpieczeństwa cybernetycznego i dostarczyć dokumentację potwierdzającą, że dodanie funkcji bezpieczeństwa nie wpływa negatywnie na odpowiednią łączność, opóźnienie, przepustowość, czas odpowiedzi i przepustowość.
13. Dostawca/Wykonawca powinien utworzyć linię bazową zaktualizowanej komunikacji i konfiguracji systemu, w tym między innymi funkcje bezpieczeństwa cybernetycznego, oprogramowanie, protokoły, porty i usługi oraz udostępni dokumentację opisującą wszelkie zmiany.
14. Dostawca/Wykonawca powinien zweryfikować uprawnienia i ustawienia zabezpieczeń w systemie bazowym przed dostarczeniem uaktualnień w celu utrzymania ustalonego poziomu bezpieczeństwa systemu.
15. Dostawca/Wykonawca powinien udokumentować wszystkie uzupełnienia i zmiany w systemie kontroli w okresie gwarancyjnym/konserwacyjnym.

7. Spis rysunków