Rodzaj dokumentu:	Oznaczenie dokumentu:	Wydanie:	Liczba załączników:	Strona:
Instrukcja	I - 264	6	0	1 (14)
Osoba odpowiedzialna za dokument:		Właściciel dokumentu:		Ważny od:
Wojciech Iwaszko		Arkadiusz Kurdej		2023-02-07

Instrukcja wdrażania i eksploatacji systemów OT

SPIS TREŚCI:

1 Cel 2
2 Zakres 2
3 Definicje 2
4 Materiały źródłowe, na podstawie których opracowano instrukcję 2
4.1 Zasady klasyfikacji systemów OT do stref bezpieczeństwa 3
4.2 Zasady połączeń struktur logicznych systemów OT 4
4.3 Zasady konfiguracji urządzeń sieciowych w systemach OT 4
4.4 Podstawowe zasady bezpieczeństwa dostępu do systemów OT 5
4.5 Zasady zdalnego dostępu do systemów OT 6
5 Wymagania eksploatacji systemów przemysłowych OT 7
5.1 Dodatkowe Wymagania dla stacji OPC/PI 8
5.2 Uruchomienie transmisji danych z systemu cyfrowego do systemu PI 8
6 Wymagania dla dostawców systemów OT 10
6.1 Wymagania ogólne 10
6.2 Wymagania szczegółowe 11
7 Zespół Nadzoru Systemów OT 13

1 Cel

Celem niniejszej Instrukcji jest określenie wytycznych dotyczących bezpieczeństwa i ciągłości działania systemów OT zawartych w „Polityce wdrażania i eksploatacji systemów OT", zarówno dla systemów nowych jak i już istniejących w zakładach PGNIG TERMIKA. Opracowanie niniejszej instrukcji ma na celu osiągnięcie niezbędnego poziomu organizacyjnego i technicznego, który:

- będzie gwarantował ochronę i bezpieczeństwo funkcjonowania systemów OT,
- zagwarantuje ciągłość działania systemów OT podczas normalnej eksploatacji oraz w sytuacjach kryzysowych,
- zapewni odpowiedni poziom bezpieczeństwa i poufności informacji systemów OT.

2 Zakres

Przedmiotowy dokument precyzuje szczegółowe wymagania związane z dostarczaniem i wdrażaniem oraz bieżącym utrzymaniem przemysłowych systemów sterowania OT w PGNiG TERMIKA.

3 Definicje

- **Bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji.
- **Poufność** – atrybut dostępności informacji wyłącznie dla osób, które zostały upoważnione do korzystania z danej informacji.
- **Dostępność** – atrybut informacji umożliwiający jej wykorzystanie przez upoważnioną osobę na uzasadnione żądanie w ustalonym czasie.
- **Systemy OT (Operational Technology**) – pojęcie określające ogół systemów sterowania automatyki przemysłowej.
- **CN (Corporate Network)** – sieć korporacyjna.
- **DCS (Distributed Control Systems)** – system sterowania i wizualizacji procesu przemysłowego posiadający wspólną bazę danych dla sterowania i wizualizacji.
- **ICS (Industrial Control Systems)** – przemysłowe systemy sterowania.
- **PCN (Process Control Network)** – sieć komputerowa systemów sterowania i produkcji.
- **DLC (Digital Logic Controlers)** – uniwersalne urządzenie mikroprocesorowe przeznaczone do sterowania pracą maszyny lub urządzenia technologicznego.
- **SCADA (Supervisory Control And Data Acquisition)** – system informatyczny nadzorujący przebieg procesu technologicznego lub produkcyjnego.
- **PGNiG TERMIKA** – PGNiG TERMIKA S.A.

4 Materiały źródłowe, na podstawie których opracowano instrukcję

Wytyczne zostały opracowane na podstawie następujących dokumentów:

- Polityka wdrażania i eksploatacji systemów OT w PGNIG TERMIKA.
- Norma PN-ISO/IEC 27001:2022 z 25 października 2022– norma określająca wymagania związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji.

- NIST 800-82 - Guide to Industrial Control Systems (ICS) Security – National Institute of Standards and Technology;
- NERC CIP – Critical Infrastructure Protection http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- Good Practice Guide, Process Control and SCADA Security, - Centre for the Protection of National Infrastructure;
- Narodowy Program Ochrony Infrastruktury Krytycznej Załącznik 1 - Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje – Rządowe Centrum Bezpieczeństwa (Rok 2020);
- Dyrektywa NIS i NIS2 (Network and Information Security), Wytyczne dotyczące bezpieczeństwa systemów OT.

Priorytetem planowanych działań modernizacyjno-odtworzeniowych i eksploatacyjnych jest zachowanie bezpieczeństwa i ciągłości działania systemów przy ograniczeniu kosztów usług zewnętrznych i kosztów eksploatacji. Zamiast dedykowanych dotychczas protokołów transmisji danych typu Modbus, DNP3.0, IEC61850, czy IEC-101/104, dostawcy rozwiązań systemowych typu ICS, DCS, SCADA, DLC stosują standardowe obecnie protokoły TCP/IP oraz ogólnodostępne systemy operacyjne i mechanizmy zdalnego dostępu. Rozwiązania takie zwiększają podatność systemów przemysłowych na zagrożenia w postaci sieciowych cyberataków z zewnątrz poprzez rozprzestrzeniające się wirusy, robaki sieciowe czy ograniczenie dostępu do sieci. Celem zachowania bezpieczeństwa i ciągłości działania jest określenie stref bezpieczeństwa i struktur połączeń systemów, a następnie wdrożenie niezbędnych wymagań bezpieczeństwa.

4.1 Zasady klasyfikacji systemów OT do stref bezpieczeństwa

W strefach bezpieczeństwa i między nimi należy wdrożyć odpowiednie mechanizmy kontroli, aby zapewnić wymagane bezpieczeństwo poszczególnych systemów przemysłowych oraz infrastruktury teleinformatycznej. W oparciu o przyjęte w PGNiG TERMIKA założenia oraz zgodnie z przyjętą „Polityką wdrażania i eksploatacji systemów OT”, systemy technologiczne należy przypisać do jednej z trzech newralgicznych stref bezpieczeństwa wg następujących wymagań:

a. **Strefa 1 — Critical Automation (Krytyczne systemy sterowania i automatyki)**
   Systemy teleinformatyczne używane do kontroli krytycznych procesów związanych z produkcją. Systemy w tej strefie działają w oparciu o oddzielną infrastrukturę sieciową. Systemy te należy chronić fizycznie przez mechanizmy o zwiększonym stopniu zabezpieczeń. Do systemów strefy 1 zaliczamy m.in.: serwer systemu automatyki, kontroler DCS, urządzenia sieciowe, zegar DCF/GPS, sterownik PLC, mechanizm zabezpieczający przesyłanie, system bezpieczeństwa narzędziowego SIS (Safety Instrumented System) itp.

b. **Strefa 2 — Critical Operation Control (Krytyczne funkcje kontroli eksploatacji urządzeń)**
   Systemy teleinformatyczne używane do kontrolowania procesu automatyzacji pracy systemów w strefie 1. Systemy w strefie 2 mają wpływ na niezawodność produkcji i działanie procesów krytycznych. Systemy te wspomagają funkcje operatorów w zakresie kontroli procesu produkcyjnego, umożliwiają również konfigurowanie

i optymalizowanie krytycznych systemów sterowania i automatyki. Systemy strefy 2 są chronione fizycznie przez mechanizmy o zwiększonym stopniu zabezpieczeń. Do systemów strefy 2 zaliczamy m.in.: serwer aplikacji produkcyjnej, system zarządzania energią EMS (Energy Management System), inżynierska stacja robocza, interfejs HMI (Human Machine Interface), stacja robocza operatora OWS (Operator Workstation), Zdalna jednostka terminalowa RTU (Remote Terminal Unit), serwer SCADA itp.

c. **Strefa 3 — Operation Support (Wsparcie eksploatacji)**
Systemy teleinformatyczne niemające wpływu na krytyczne funkcje kontroli i monitorowania urządzeń lub mające na nie niewielki wpływ. Systemy w strefie 3 wspierają proces eksploatacji i mogą pełnić rolę strefy buforowej między strefami krytycznymi (1 i 2) a strefami biznesowymi. Do strefy tej należy zaliczać również systemy niekrytyczne, pomocnicze funkcje sterowania i automatyki (systemy szkoleniowe i testowe). Do systemów strefy 3 zaliczamy m.in.: systemy antywłamaniowe, systemy gromadzenia i rejestrowania danych, systemy planowania i monitorowania produkcji, system monitorowania emisji, system monitorowania przemysłowego, terminalowy serwer zdalnego dostępu, systemy powiązane z obrotem handlowym itp.

Celem zastosowania ww. strefowego modelu ochrony jest separacja krytycznych systemów teleinformatycznych, zwiększanie poziomu ich bezpieczeństwa oraz kontrolowanie przepływu informacji i zarządzanie dostępem do nich. Niezbędne jest przypisanie poszczególnych systemów OT dla poszczególnych stref bezpieczeństwa dla wszystkich systemów technologicznych PGNIG TERMIKA. Kolejnym krokiem powinno być techniczne dostosowanie systemów OT do roli pełnionej w poszczególnych strefach.

4.2 Zasady połączeń struktur logicznych systemów OT

Realizacja połączeń systemów OT wymaga maksymalnego odseparowania struktury logicznej systemu OT od innych sieci korporacyjnych. Ze względów bezpieczeństwa wymaga się zastosowania poniższych konfiguracji:

a. Pojedynczy firewall: rozwiązanie należy zrealizować umieszczając firewall pomiędzy siecią korporacyjną oraz PCN.
b. Podwójny firewall: rozwiązanie należy zrealizować poprzez użycie dwóch urządzeń firewall ze zdefiniowaną i skonfigurowaną wspólną strefą zdemilitaryzowaną DMZ (Demilitarized Zone) umieszczoną pomiędzy siecią korporacyjną i produkcyjną.
c. Podwójne karty sieciowe: Rozwiązanie realizowane przez pojedynczy serwer OPC wyposażony w dwie karty sieciowe łączący PCN z siecią korporacyjną. Niedopuszczalne jest uruchomienie routingu pomiędzy interfejsami. Wymaga się zastosowania oprogramowania lokalnego firewall'a, blokującego ruch pakietów do PCN. Dopuszcza się tymczasowe bezpośrednie sprzęgnięcie dwóch interfejsów sieciowych od strony serwera OPC i klienta OPC (z pominięciem sieci) w przypadkach np.: awaryjnych, remontowych.

4.3 Zasady konfiguracji urządzeń sieciowych w systemach OT

a. Należy wykonać zmiany wszystkich ustawień fabrycznych na urządzeniach.

b. Reguły dostępu dla portów i usług pomiędzy OT a siecią zewnętrzną muszą zostać dokładnie zdefiniowane i udokumentowane. Odpowiedzialność za definicję reguł musi zostać przypisana do konkretnej osoby. Dopuszcza się TYLKO reguły statyczne.
c. Reguły systemu firewall muszą podlegać cyklicznym przeglądom. Podstawowa reguła na firewallu musi zostać ustawiona na DENY ALL, PERMIT NONE.
d. Ruch w sieci musi zostać zdefiniowany przy pomocy reguł ograniczających do określonego numeru bądź zakresu numerów IP oraz koniecznych portów TCP/UDP (Transmission Control Protocol / User Datagram Protocol).
e. Protokoły nieoparte na pakietach IP dla komunikacji z siecią zewnętrzną muszą być odrzucone. Należy stosować wyłącznie dozwolone protokoły międzystrefowe.
f. Zarządzanie firewallem należy realizować z wykorzystaniem oddzielnej, zabezpieczonej sieci lub sieci zaszyfrowanej co najmniej dwoma elementami autoryzacyjnymi.
g. Należy monitorować i rejestrować zdarzenia w systemie firewall w sposób ciągły. W przypadku braku wykonania monitorowania zdarzeń przez służby automatyki, należy zlecić realizację ww. rejestracji i monitorowania dostawcom systemu w ramach umów serwisowych i gwarancyjnych.
h. Zaleca się zainstalować osobne firewalle w każdej lokalizacji dla dostępu zdalnego.
i. Niedozwolone są jakiekolwiek połącznia modemowe, ftp lub telnet.
j. W zastosowanych przełącznikach sieciowych należy wydzielić i skonfigurować przynajmniej jeden port dla każdej z istniejących podsieci, którego zadaniem będzie przesyłanie kopii ruchu sieciowego (SPAN port/port mirroring). Dopuszcza się możliwość zastosowania usługi umożliwiającej agregację ruchu sieciowego z kilku podsieci do jednego portu (RSPAN). Funkcjonalność należy uruchomić zarówno w części operatorskiej systemu, jak i w części procesowej (na poziomie sterowników PLC i kontrolerów DCS).
k. Należy monitorować stan połączeń sieciowych oraz wybranych parametrów urządzeń sieciowych (np. obciążenie) za pomocą dostępnych protokołów typu SNMP czy Syslog. Informacje te powinny być wysyłane do zewnętrznego systemu monitorowania cyberbezpieczeństwa teleinformatycznego PGNIG Termika osobnym portem.

4.4 Podstawowe zasady bezpieczeństwa dostępu do systemów OT

Dostęp do oprogramowania systemu technologicznego OT będą posiadali tylko zdefiniowani użytkownicy z ograniczeniem wyłącznie do zespołu osób uprawnionych:

a. Dostęp ten wymaga ochrony hasłem. Stosowane hasła muszą spełniać przynajmniej następujące warunki: zachowanie długości od 8 do 25 znaków; wykorzystanie dużych i małych liter, liczb oraz symboli. W przypadku stacji operatorskich z uwagi na stabilność pracy systemu dopuszcza się uproszczenie ww. wymagań.
b. Należy przestrzegać bezwzględnego zakazu udostępniania haseł osobom trzecim.
c. Zawsze należy zmieniać domyślne konta oraz hasła dostarczone przez producentów.
d. Zaleca się przeprowadzać regularne audyty jakości haseł raz w roku.
e. Każdy z uprawnionych użytkowników musi posiadać nadany unikatowy identyfikator pozwalający na jego jednoznaczną identyfikację. W przypadku stacji operatorskich dopuszcza się uproszczenie ww. wymagań.

f. Konta w systemach należy przeglądać raz w roku pod kątem adekwatności uprawnień oraz zamykania kont starych i niewykorzystywanych.
g. Wymaga się, aby wszystkie nowo wdrażane systemy OT były chronione oprogramowaniem antywirusowym zalecanym przez producenta systemu. W przeciwnym przypadku należy wdrożyć inne rozwiązania minimalizujące możliwość zainfekowania systemów OT.

4.5 Zasady zdalnego dostępu do systemów OT

Dostęp zdalny może być wdrożony wyłącznie w przypadku wyraźnego uzasadnienia biznesowego. Dopuszcza się zdalny dostęp wyłącznie po podpisaniu oddzielnej umowy/porozumienia na usługę VPN z firmą obsługującą Spółkę pod kątem obsługi IT/OT, przy czym:

a. Wymagane jest odpowiednie uwierzytelnienie użytkowników posiadających dostęp zdalny, np. za pomocą mechanizmów silnego uwierzytelnienia, dodatkowych haseł, tokenów dostępowych, zewnętrznego oprogramowania (podwójny faktor uwierzytelniania). Wykorzystywany w PGNiG Termika SA system do obsługi zdalnych połączeń posiada możliwość uwierzytelniania użytkownika za pomocą biometryk w telefonach (Android oraz iOS) przypisanych numerem telefonu do konkretnych serwisantów. PGNiG Termika zastrzega możliwość uruchomienia tej funkcjonalności.
b. Połączenia zdalne realizowane będą poprzez infrastrukturę PGNiG Termika SA.
c. Należy wyznaczyć jedną stację, która pełniła będzie funkcje terminala przesiadkowego, do którego terminowane będzie połączenie zdalne, i z którego będzie istniała możliwość dostania się do dalszej części systemu. Stacja powinna być pod obsługą systemu Windows lub Linux.
d. W przypadku łączenia wielu instancji systemów DCS wspólną infrastrukturą sieciową, dopuszcza się stosowanie jednej wspólnej stacji przesiadkowej dla tych systemów.
e. Ze względu na niebezpieczeństwo utraty (kompromitacji) poświadczeń, na stacji przesiadkowej powinno znajdować się konto przeznaczone tylko i wyłącznie do logowania zdalnego, którego hasło automatycznie będzie zmieniane przez system zarządzający zdalnymi sesjami zainstalowany w PGNiG Termika SA.
f. Sesje VPN podlegają nagrywaniu i rejestracji.
g. Zalecane protokoły komunikacyjne to RDP i SSH.
h. Należy wyznaczyć osobę – Koordynatora nadzorującego zdalny dostęp, prowadzącego ewidencję wszystkich zdalnych dostępów (połączeń) do systemów i urządzeń technologicznych.
i. Zdalny dostęp dla podmiotów zewnętrznych do sieci OT musi być poprzedzony podpisaniem oświadczenia określającego obowiązki i odpowiedzialności stron w zakresie bezpieczeństwa.
j. Wymaga się, aby każde zdalne połączenie poprzedzone było zgłoszeniem e-mail lub uzgodnione telefonicznie (SMS) z Koordynatorem. Koordynator posiada możliwość akceptacji lub odrzucenia próby połączenia zdalnego.
k. Wymagane jest przeprowadzenie co rok w styczniu audytu/przeglądu wszystkich aktywnych dostępów zdalnych do systemów produkcyjnych. Wyniki audytu muszą

zostać przedstawione do zatwierdzenia i wiadomości Zespołu Nadzoru Systemów OT koordynującego bezpieczeństwo.

l. Dostęp zdalny powinien być ograniczony do wybranych systemów i urządzeń. Zdalny dostęp powinien wymuszać samoczynne rozłączenie połączenia po 2 godzinach aktywności/nieaktywności i wymusić ponowne logowanie.
m. Dla modernizowanych i nowobudowanych systemów OT dostawca systemu zabuduje wymaganą infrastrukturę na potrzeby zdalnego dostępu VPN zgodnie z obowiązującymi w PGNiG TERMIKA wymaganiami.
n. Imienne konta serwisantów nadawane są z okresem ważności do 12 miesięcy lecz nie dłużej niż do dnia 31 stycznia roku następnego . Konta posiadają włączoną funkcję cyklicznego wymuszania zmiany hasła.
o. Wymaga sią – nie rzadziej niż raz na trzy miesiące – wykonać przegląd dziennika zdarzeń systemów rejestrujących wyjątki, usterki, pod kątem liczby ataków z zewnątrz i bezpieczeństwa informacji.
p. Zabrania się wykorzystywania dla komputerowych systemów sterowania OT sieci bezprzewodowej (GSM, WIFI, Bluetooth itp). Wykorzystanie sieci bezprzewodowych dopuszcza się w uzasadnionych przypadkach wyłącznie dla wydzielonych od komputerowych systemów sterowania lokalnych sterowników w zakresie działania jednokierunkowym (nadawanie) w celach diagnostyczno-pomiarowych.

5 Wymagania eksploatacji systemów przemysłowych OT

Podczas bieżącej eksploatacji oraz wdrażając nowe rozwiązanie systemów technologicznych należy dokonać klasyfikacji systemu do odpowiedniej strefy oraz zastosować strategię zwaną „defense-in-depth” oznaczającą, że zastosowane zostanie wiele niezależnych zabezpieczeń na różnych warstwach systemu. Należy więc bezwzględnie stosować:

a. Maksymalne ograniczenie dostępu do logicznej struktury sieci systemów technologicznych wraz z mechanizmami uwierzytelniania i autoryzacji dla użytkowników.
b. Wykorzystywanie wielowarstwowej topologii sieci.
c. Wykonywanie kopii zapasowych nie rzadziej niż raz na kwartał oraz przed każdą zmianą / aktualizacją w systemie.
d. Szczepionki oprogramowania antywirusowego powinny być dostarczane po uprzednim ich przetestowaniu nie rzadziej, niż raz na miesiąc.
e. Ograniczenie fizycznego dostępu do sieci systemów technologicznych i urządzeń. Powinny być zastosowane wielorakie środki kontroli dostępu fizycznego, takie jak zamki, blokady, zamykane szafki i skrzynki, czytniki kart, ochrona, monitoring itp.
f. Ochronę poszczególnych komponentów systemów technologicznych i urządzeń, poprzez:
   - możliwie szybki sposób wdrażanie uprzednio przetestowanych poprawek zabezpieczeń,
   - możliwość wyłączenia wszystkich nieużywanych portów i usług. Porty aktywne dla potrzeb serwisowych należy zabezpieczyć fizycznie (zamek, blokada),
   - definiowanie użytkowników oraz ograniczenie ich uprawnień tylko do tych, które są wymagane do pełnionej roli,

- stosowanie mechanizmów kontroli bezpieczeństwa (zalecane przez producenta oprogramowanie antywirusowe, ograniczenie możliwości instalowania innych aplikacji typu OFFICE, OUTLOOK),
- rejestrowanie wszystkich zmian w systemach OT. Istotne i krytyczne zmiany muszą być autoryzowane przez osoby z „Zespołu Nadzoru Systemów OT" .

g. Należy opracować „Plan ciągłości działania" (BCP-Business Continuity Planning) dla każdego z systemów OT. Plan musi uwzględniać podstawowe i ogólne zasady postępowania w przypadku awarii lub uszkodzenia systemu.

5.1 Dodatkowe Wymagania dla stacji OPC/PI

a. Należy rozdzielać funkcjonalność, jaką pełnią stacje OPC, tak aby nie stanowiły integratora więcej niż dwóch sprzęgów systemów przemysłowych.
b. Należy usunąć rozwiązania poprzez wydzielenie funkcji OPC od innych funkcji systemowych, tak aby stacja systemowa OPC nie była również stacją inżynierską, na której prowadzone są prace konfiguracyjne systemu.
c. Dla nowych lub modernizowanych systemów należy separować sprzętowo funkcję serwera OPC PI i funkcję klienta OPC przez zastosowanie dwóch stacji. Dodatkowo wymaga się, aby dla nowych lub modernizowanych systemów dostarczono redundantne serwery OPC DA celem zapewnienia równoległego kanału przekazywania danych do systemu PI. Dopuszcza się dostawę jednego serwera OPC pod warunkiem uruchomienia przez dostawcę systemu dodatkowego redundantnego kanału danych (identycznego z protokołem danych udostępnianych z OPC) przekazywanych bezpośrednio z serwerów typu SCADA do systemu PI. Warunkiem jest dostępność danych na drugim protokole w standardzie OPC DA
d. Dostawa serwera/serwerów OPC możliwa jest przez dostawcę systemu typu SCADA wyłącznie po zatwierdzeniu jej parametrów prze PGNiG Serwis.
e. Zaleca się sukcesywną wymianę serwerów OPC i stacji OPC/PI na nowsze (co 6 lat – 8 lat) w miarę możliwości po dokonaniu okresowego przeglądu stacji i wpisaniu rekomendacji odnośnie ich modernizacji, tak aby zapewnić ciągłość bezpieczeństwa pracy oraz niezbędną aktualizację szczepionek systemu antywirusowego.

5.2 Uruchomienie transmisji danych z systemu cyfrowego do systemu PI

W ramach tego zadania do Wykonawców należy:

a. Dostarczenie /lub/ zaktualizowanie oprogramowania komunikacyjnego pomiędzy dostarczanym /lub/ modernizowanym systemem cyfrowym, a ogólnozakładowym systemem wizualizacji monitorującym produkcję PGNIG TERMIKA – PI (dostarczanym przez firmę OSISoft). W zakresie prac należy uwzględnić wszystkie zmiany konfiguracyjne niezbędne do odtworzenia funkcjonalności systemu sprzed modernizacji lub uruchomienia nowej instancji systemu PI. W przypadku rozbudowy systemu cyfrowego i zwiększonej liczby sygnałów Wykonawca odpowiednio dostosuje zakres w/w prac.
b. W celu podłączenia do systemu cyfrowego wydzielonej stacji, która będzie pełnić rolę stacji sprzęgającej OPC (serwera danych) do systemu PI, wykonawca przedstawi Zamawiającemu do akceptacji propozycję rozwiązania umożliwiającego posadowienie dodatkowej stacji buforującej dane do PI (min. 30 dni całkowicie zautomatyzowanej

archiwizacji buforowanych danych przekazywanych do klienta PI) po swojej stronie sieci LAN. Jako rozwiązanie standardowe dopuszcza się przekazywania danych w standardzie OPC DA. W przypadku pozytywnej opinii Zamawiającego, Wykonawca uruchomi bezpieczną redundantną (dwa niezależne kanały komunikacyjne z redundantnych serwerów OPC lub OPC i SCADA) transmisję danych do stacji sprzęgających i serwera systemu PI, z zachowaniem bezpieczeństwa architektury IT (dodatkowy router/firewall). Stacje sprzęgające wraz z systemem operacyjnym i licencjami systemu PI dostarczane są przez PGNiG Serwis.

c. Wykonanie i uruchomienie niezbędnego oprogramowania komunikacyjnego wynikającego z zabudowy nowego /lub/ modernizowanego systemu cyfrowego umożliwiającego przesyłanie danych pomiędzy systemem cyfrowym a stacjami sprzęgającymi i serwerem systemu PI. Typowo komunikacja taka realizowana jest w standardzie OPC. Oprogramowanie Wykonawcy powinno pracować na zasadach i z użyciem procedur określonych w systemie PI (do uzgodnienia z inżynierem PGNiG Serwis).
d. Przekazanie Zamawiającemu w formie edytowalnej ustalonej bazy i listy sygnałów (format *.xls, *.txt) zawierającą dane niezbędne do prawidłowego skonfigurowania sygnałów po stronie systemu PI (nazwa sygnału widoczna na serwerze OPC, opis, dla sygnałów analogowych: zakres i jednostki inżynierskie; dla sygnałów wielostanowych: znaczenie poszczególnych wartości itd.). W przypadku rozbudowy systemu cyfrowego Wykonawca uzgodni i dostarczy rozszerzoną liczbę sygnałów. W zależności od realizowanego projektu lista sygnałów jest każdorazowo ustalana indywidualnie (do uzgodnienia w trakcie realizacji).
e. Uwzględnienie wszystkich czynności, wykonywanych po stronie systemu cyfrowego oraz stacji sprzęgającej i buforującej, niezbędnych do poprawnego odebrania po stronie serwera systemu PI wszystkich sygnałów wymaganych do poprawnego funkcjonowania wizualizacji, obliczeń i raportów – zarówno uprzednio istniejących, jak i nowych.

Ponadto:

f. Jeśli zostało wykorzystane autorskie oprogramowanie komunikacyjne, do obowiązków Wykonawcy należy wykonanie dokumentacji powykonawczej oprogramowania wraz z instrukcją instalacji i konfiguracji oraz przekazanie Zamawiającemu kopii (2 egz.) oprogramowania w wersji instalacyjnej na nośnikach elektronicznych. Wykonawca przekazuje także Zamawiającemu instrukcję dodawania nowych sygnałów do sygnałów już wysyłanych do systemu PI oraz uruchamiania, serwisowania i diagnostyki sprzęgów.
g. Dostawca obligatoryjnie zobowiązany jest do dostawy na swój koszt narzędzi posadowionych na stacji sprzęgającej umożliwiających pobranie wybranych danych archiwalnych za wybrany okres z systemu cyfrowego w celu uzupełniania archiwum systemu PI danymi, które nie przesłały się automatycznie do serwera z powodu zakłóceń w transmisji danych. Wykonawca odpowiedzialny jest za poprawność i terminowość przekazywania danych do stacji sprzęgającej PI. Stacje sprzęgające PI będą realizowane, jako dwie fizyczne jednostki komputerowe, lub realizowane, jako jedna jednostka fizyczna, a druga zwirtualizowana. W przypadku przerwy (zaniku transmisji danych) z systemu cyfrowego do stacji OPC PI – Wykonawca jest

zobowiązany niezwłocznie przywrócić komunikację oraz odtworzyć i przywrócić wszystkie dane i wielkości przekazywane (zgodnie z uzgodniona listą sygnałów – ppkt. d) do systemu PI w okresie trwania Umowy i jej okresu gwarancyjnego.

h. W celu uzgodnienia wymagań technicznych dotyczących konfiguracji stacji sprzęgającej do PI, konfiguracji rozwiązań architektury IT oraz adresacji sieci należy kontaktować się ze specjalistami ds. systemów wsparcia produkcji: PI@serwis.pgnig.pl
i. W celu uzgodnienia wymagań technicznych dotyczących konfiguracji wizualizacji i synoptyk, zakresu danych (listy sygnałów) oraz licencji dla systemu PI należy kontaktować się ze specjalistami ds. systemów zarządzania produkcją: pditech@termika.pgnig.pl

6 Wymagania dla dostawców systemów OT

Dostawcom systemów technologicznych lub ich komponentów na etapach wdrażania, modernizacji i bieżącej eksploatacji (remonty) należy przedstawić szczegółowe wymagania związane z dostarczaniem i wdrażaniem przemysłowych systemów sterowania OT do PGNiG TERMIKA.

6.1 Wymagania ogólne

a. Wykonawca powinien być autorem wdrażanego systemu lub posiadać certyfikowany stopień partnerstwa. Osoby wdrażające system powinny posiadać stosowne zaświadczenia o odbytych kursach i szkoleniach z zakresu instalacji i konfiguracji systemu.
b. Wykonawca winien wykazać się posiadaniem w zespole wdrażającym co najmniej jedną osobą posiadającą świadectwo kwalifikacyjne „E” do 1 kV.
c. Przyjęte rozwiązanie powinno opierać się o standardy bezpieczeństwa opisane w NIST Special Publication 800-82 current Revision „Guide to Industrial Control Systems (ICS) Security”
d. Przed przystąpieniem do wdrażania oferowanego systemu Wykonawca winien przedstawić Zamawiającemu kompletną wykonawczą dokumentację techniczną zawierającą co najmniej:
   - opis funkcjonalny systemu,
   - schemat techniczny zawierający proponowaną strukturę połączeń wraz z opisem przyjętych oznaczeń i symboli,
   - schemat logicznych i fizycznych połączeń sieciowych, wraz z adresacją,
   - listę serwerów, stacji roboczych, przełączników sieciowych, routerów, konwerterów oraz innych wykorzystywanych urządzeń,
   - wykaz wykorzystywanego oprogramowania komercyjnego (systemy operacyjne i bazy danych oraz pozostałe aplikacje i ich wersje),
   - opis stosowanych zabezpieczeń zawierający listę wykorzystywanych protokołów sieciowych, portów, usług, sygnałów, zdarzeń i alarmów.
e. Opracować plan (harmonogram) dostarczania i wdrażania systemu z podziałem na kolejne etapy. Każdy etap powinien kończyć się testami i obustronnie podpisanym protokołem odbioru.
f. W przypadku modernizacji istniejącego systemu Wykonawca musi zapewnić jego bezawaryjną pracę i ciągłość działania. W przypadkach, gdy zajdzie potrzeba

chwilowego zatrzymania systemu, Wykonawca zagwarantuje ograniczenie niedyspozycyjności systemu do niezbędnego minimum. Każda przerwa w pracy systemu wymaga pisemnego zgłoszenia i zgody Zamawiającego.

g. Należy wskazać Koordynatora systemu odpowiedzialnego za bezpośredni kontakt z Zamawiającym oraz zdalny dostęp do systemów.

6.2 Wymagania szczegółowe

a. Wszystkie dostarczone przez Wykonawcę urządzenia i systemy powinny być zasilane z napięcia gwarantowanego 230V, 50Hz. W przypadku dostarczenia urządzeń zasilanych innym napięciem, Wykonawca dostarcza również dodatkowe urządzenia (przetwornice) dostosowujące napięcie zasilające np. 230V/24V.
b. Wszystkie systemy przetwarzania informacji należy zsynchronizować z jednym wzorcowym źródłem czasu.
c. Należy zapewnić maksymalne ograniczenie dostępu do istniejącej logicznej struktury sieci Zamawiającego. Jeśli całkowita separacja jest niemożliwa, należy zastosować strefy zdemilitaryzowane OT (DMZ OT) wykorzystując dostarczone zapory sieciowe. Połączenia takie winny być szczegółowo opisane w dokumentacji i monitorowane. W przypadku braku możliwości instalacji urządzenia typu Firewall, należy powiadomić Zamawiającego i przygotować rozwiązanie alternatywne. Zabrania się wykorzystywania dla komputerowych systemów sterowania OT sieci bezprzewodowej (GSM, WIFI, Bluetooth itp.).
d. Oferowany system powinien posiadać wbudowane mechanizmy uwierzytelniania (potwierdzenia tożsamości) i autoryzacji (potwierdzenia uprawnień) dla użytkowników. Na poziomie administratora powinna istnieć możliwość definiowania użytkowników oraz ograniczania ich uprawnień tylko do tych, które są wymagane do pełnionej roli. Dostęp do stacji i wykorzystanie stacji powinny być monitorowane i nadzorowane w celu wykrywania i rejestrowania zdarzeń.
e. Kluczowe punkty systemu muszą posiadać pełne redundantne rozwiązania w zakresie urządzeń i dróg transmisji zapewniające ciągłość jego pracy.
f. Okablowanie powinno być wykonane przy maksymalnym wykorzystaniu technologii światłowodowej spełniającej standard IEC 60793-2. Należy stosować światłowody wielomodowe (kable typu GI 62,5/125) i złącza LC. Okablowanie sieci LAN musi zagwarantować redundancję włókien światłowodowych. Wymaga się kładzenia okablowania wykorzystując istniejącą infrastrukturę Zamawiającego (strefy chronione, serwerownie, szafy, przepusty, kanały, wydzielone pomieszczenia itp.). W pozostałych przypadkach Wykonawca zobowiązany jest przedstawić i uzgodnić z Zamawiającym stosowny projekt tras kablowych i rozwiązań technicznych.
g. Węzłami sieci mogą być tylko przełączniki spełniające wymagania funkcjonalne zgodne ze standardem IEC 61850. Zgodnie z normą IEEE 802.1q i IEEE 802.1d przełącznik sieciowy powinien być zdolny do obsługi etykietowanych ramek Ethernet, do obsługi ramek z uwzględnieniem różnych priorytetów oraz powinien mieć możliwość tworzenia co najmniej 10 wirtualnych sieci LAN (VLAN). Zastosowanie urządzeń typu HUB jest zabronione.
h. Zastosowane routery na portach WAN muszą wspierać protokoły warstwy łącza danych: HDLC – High Level Data Link Control, LLC-2 – Logical Link Control type 2, PPP

– Point-to-Point Protocol, SLIP – Serial Line Internet Protocol. Na portach LAN router musi być zgodny ze standardem IEEE 802.3 (Ethernet). Wymagane jest, by wsparcie routera dla warstwy sieciowej obejmowało: IPv4 – Internet Protocol ver 4, NAT – Network Address Translation, IP Multicast, protokoły routing static i dynamic: RIP – Routing Information Protocol, RIP2, OSPF – Open Shorted Path First). Wymagane wsparcie routera dla wzajemnej komunikacji VLAN utworzonych w oparciu o standard IEEE 802.1q.

i. Dostarczone urządzenie typu Firewall musi realizować kontrolę dostępu na poziomie warstwy sieciowej, transportowej oraz aplikacji. Urządzenie musi działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie transparentnym (tzn. w warstwie 2 modelu OSI) oraz trybie pasywnego nasłuchu (tzn. TAP). Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN zgodnie z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać protokoły routingu dynamicznego (co najmniej OSPF). Ilość interfejsów urządzenia musi zapewnić możliwość utworzenia i podłączenia co najmniej stref: 1 x Inside, 1 x Outside, 2 x DMZ.
j. Wszystkie linki cyfrowe dochodzące do systemu DCS (pakiety danych) w standardach TCP/IP, MODBUS TCP i innych opartych o standard TCP/IP pochodzących z urządzeń i/lub sterowników PLC powinny być filtrowane (przynajmniej na poziomie 2 warstwy ISO/OSI – kart komunikacyjnych oraz usług DHCP, DNS i innych standardowo generowanych przez urządzenia sieciowe) przez firewall lub odpowiednio skonfigurowany router lub switch warstwy 3.
k. Urządzenia automatyki wyposażone w elektryczne porty LAN (Ethernet 10/100BaseT/TX) mogą być dołączone do portów światłowodowych typu 100Base-FX za pomocą konwerterów światłowodowych. Wymagane jest stosowanie światłowodów wielomodowych 62,5/125 oraz złącz LC.
l. Urządzenia automatyki wyposażone w elektryczne porty RS-232 lub RS-485 mogą być dołączone do portów światłowodowych przełączników sieci LAN przy wykorzystaniu konwerterów światłowodowych RS/LAN transformujących porty RS-232/RS-485 na porty LAN typu 100Base-FX.
m. Serwery wykorzystywane do instalacji systemów powinny spełniać zalecenia producenta systemu co do wydajności i pojemności oraz powinny być przystosowane do montażu w szafach typu rack.
n. Dla sieci LAN średni czas międzyawaryjny MTBF (Mean Time Between Failures) nie może być niższy niż 100 000 godz. (klasa R3). Dla urządzeń sieciowych (routery, firewall'e, przełączniki) wymaga się MTBF > 100 000 godz.
o. Dla sieci LAN i aktywnych urządzeń sieciowych wymaga się, by średni czas MTTR (Mean Time To Restoration) przywrócenia zdolności do działania nie przekraczał 12 godz., tzn. by spełniał on wymagania klasy M3.
p. Wymaga się, by średni czas MRT (Mean Repair Time) naprawy uszkodzonego elementu sieci LAN oraz urządzeń aktywnych nie przekraczał 6 godz., tzn. spełniał on wymagania klasy RT3.
q. Adresacja stacji roboczych i serwerów musi być stała, maksymalnie ograniczona maską sieci. Należy uruchomić tylko konieczne do prawidłowej eksploatacji protokoły, porty i usługi; pozostałe zaleca się wyłączyć lub dezaktywować.

r. System powinien umożliwiać śledzenie i monitorowanie parametrów pracy, a w tym w szczególności: wykorzystania procesora, pojemności twardych dysków, analizy dzienników zdarzeń oraz przepływności sieci; ww. parametry pracy powinny być dostępne dla zamawiającego w trybie online.
s. Należy wskazać oraz uzgodnić z Zamawiającym dostawcę instalowanego oprogramowania antywirusowego; szczepionki powinny być dostarczane po uprzednim ich przetestowaniu nie rzadziej, niż raz na miesiąc lub na żądanie Zamawiającego przez osoby uprawnione lub PGNIG Serwis. Stosowanie aplikacji szczepionek nie powinno być automatyczne, ale po uprzednim otrzymaniu pozwolenia od dostawcy. Serwer dystrybucyjny, jak i poszczególne stacje robocze, nie mogą mieć dostępu do sieci Internet.
t. Wykonawca winien dostarczyć dokumentację opisującą sposób wykonywania kopii zapasowych oraz ich odtwarzania przy założeniu, że będą one wykonywane nie rzadziej niż raz na kwartał oraz przed każdą zmianą / aktualizacją w systemie. Kopie należy przechowywać w bezpiecznym miejscu.
u. Wykonawca musi opracować procedury eksploatacyjne uwzględniające postępowanie w razie wystąpienia incydentów np. awaryjnych.
v. Wykonawca zapewni cykl szkoleń dla administratorów systemu oraz jego użytkowników uwzględniając zasady bezpiecznej eksploatacji systemu.
w. Po zakończeniu wdrożenia Wykonawca opracuje i dostarczy dokumentację powykonawczą i użytkową zawierającą pełny opis funkcjonalny i techniczny systemu wraz z jego topologią i konfiguracją.
x. Wszelkie zmiany wykonywane przez Wykonawcę w systemie na każdym etapie wdrażania i eksploatacji muszą być konsultowane z Zamawiającym; wprowadzone zmiany Wykonawca nanosi na dokumentacji powykonawczej i użytkowej.

Dostosowanie systemów do ww. wymagań i standardów dotyczy wszystkich nowo wdrażanych systemów przemysłowych OT. W przypadku systemów istniejących opisane wyżej wymagania należy wdrażać adekwatnie do zakresu realizowanych prac modernizacyjnych i remontowych.

7 Zespół Nadzoru Systemów OT

W celu zapewnienia weryfikacji proponowanych rozwiązań w zakresie wdrażanych, modernizowanych systemów należy powołać do życia „Zespoły Nadzoru Systemów OT". Zespoły należy powołać w obrębie każdego z wyznaczonych zakładów produkcyjnych. Rolą zespołu będzie weryfikacja zaproponowanych rozwiązań technicznych w celu zachowania bezpieczeństwa i ciągłości działania systemów. Zakłada się, że zgoda zespołu jest niezbędna do uruchomienia jakiekolwiek działania w obrębie systemów OT. Powołane Zespoły Nadzoru Systemami OT dla poszczególnych zakładów produkcyjnych PGNIG TERMIKA zajmują się:

a. EC Żerań:
    1. Wojciech Iwaszko - PGNIG TERMIKA a tel. (22)-587 8731
    2. Grzegorz Wajs - PGNIG TERMIKA tel. (22)-587 4796
    3. Piotr Ozga – PGNIG TERMIKA tel. (22)-587 8980

b. EC Pruszków:
    1. Wojciech Iwaszko - PGNIG TERMIKA tel. (22)-587 8731
    2. Wojciech Owczarek - PGNIG TERMIKA tel. (22)-587 5204
    3. Piotr Ozga – PGNIG TERMIKA tel. (22)-587 8980

c. C Wola:
    1. Wojciech Iwaszko - PGNIG TERMIKA tel. (22)-587 8731
    2. Mariusz Urbański - PGNIG TERMIKA tel. (22)-587 4769
    3. Piotr Ozga – PGNIG TERMIKA tel. (22)-587 8980

d. EC Siekierki:
    1. Wojciech Iwaszko - PGNIG TERMIKA tel. (22)-587 8731
    2. Adam Krzywiec - PGNIG TERMIKA tel. (22)-587 3701
    3. Piotr Ozga – PGNIG TERMIKA tel. (22)-587 8980

e. C Kawęczyn:
    1. Wojciech Iwaszko - PGNIG TERMIKA tel. (22)-587 8731
    2. Tomasz Wołukaniec - PGNIG TERMIKA tel. (22)-587 1714
    3. Piotr Ozga – PGNIG TERMIKA tel. (22)-587 8980