Cyberbezpieczeństwo

Biała księga: Koncepcja wielowarstwowej ochrony dla branży wodno-kanalizacyjnej

WinCC RT Professional

Wstęp

Niniejsza biała księga zawiera omówienie tematu bezpieczeństwa przemysłowego w branży wodno-kanalizacyjnej. Opisuje zagrożenia i ryzyko, na jakie narażone są systemy sterowania i automatyki przemysłowej w zakładach oczyszczania ścieków oraz przetwarzania wody. Wprowadza również najlepsze rozwiązania w celu zminimalizowania tych zagrożeń, aby osiągnąć poziom ochrony akceptowalny w zakresie ograniczeń ekonomicznych, jak i żądanego poziomu bezpieczeństwa. Obejmuje również potrzeby przeciwdziałania nieustannie rosnącym zagrożeniom ze strony postępującej digitalizacji, takim jak wszechobecny dostęp do Internetu oraz duże ilości wartościowych danych, które sprawiają, że cyberataki na niezabezpieczone instalacje są łatwiejsze i bardziej prawdopodobne.

STATUS: WYDANIE PIERWSZE

Wersja V1
01.04.2020

Dodatkowe informacje dotyczące bezpieczeństwa przemysłowego w Siemens można znaleźć pod adresem: https://www.siemens.com/industrialsecurity

Informacje przedstawione w niniejszej białej księdze są aktualne na marzec 2020 roku.

Wydawca
Siemens AG
Digital Industries

Gleiwitzer Str. 555
90475 Nuremberg, Germany

Pomoc

Wszelkie pytania związane z tą białą księgą proszę kierować do osoby kontaktowej w Siemens u przedstawiciela/w biurze sprzedaży bądź pod adres industrialsecurity.i@siemens.com.

Oświadczenie dotyczące bezpieczeństwa

Siemens zapewnia produkty i rozwiązania o funkcjach bezpieczeństwa przemysłowego wspierające bezpieczną pracę instalacji, systemów, maszyn i sieci.
Aby chronić urządzenia systemy, maszyny i sieci przed cyberzagrożeniami, konieczne jest wdrożenie - i ciągłe utrzymywanie - holistycznej, najnowocześniejszej koncepcji bezpieczeństwa przemysłowego. Produkty i rozwiązania Siemens stanowią tylko część takiej koncepcji.

W gestii klienta leży zabezpieczenie ich instalacji, systemów, maszyn i sieci przed nieupoważnionym dostępem. Systemy, maszyny i podzespoły powinny być podłączone do sieci zakładowej lub Internetu jedynie w niezbędnym zakresie i przy zachowaniu odpowiednich środków ochronnych (np. zastosowaniu zapory sieciowej i segmentacji sieci).

Więcej informacji odnośnie środków bezpieczeństwa przemysłowego, jakie można zastosować, dostępnych jest na stronie https://www.siemens.com/industrialsecurity.

Produkty i rozwiązania Siemens są stale rozwijane, by zwiększać ich bezpieczeństwo. Siemens gorąco zaleca, by stosować najnowsze aktualizacje produktów, i korzystać z nich gdy tylko zostaną udostępnione. Korzystanie

z wersji produktów, które nie są już wspierane oraz niezastosowanie najnowszych aktualizacji może zwiększyć ryzyko zostania ofiarą cyberataku.

Aby pozostać na bieżąco z aktualizacjami produktów, zapisz się do kanału RSS Siemens Industrial Security pod adresem: https://www.siemens.com/industrialsecurity.

Treść

1 Wstęp

Bezpieczne działanie infrastruktury wodno-kanalizacyjnej jest kluczowe dla wszystkich obszarów społecznych i przemysłowych.

W celu zapewnienia gwarantowanej dostawy wysokiej jakości wody pitnej, a także zgodnego z przepisami oczyszczania ścieków, Siemens wspiera konsultantów, integratorów systemów oraz przedsiębiorstwa zajmujące się dostawą wody i odbiorem ścieków, w projektowaniu, wdrażaniu i zarządzaniu bezpiecznymi rozwiązaniami automatyzacji.

Rosnący stopień cyfryzacji automatyki przemysłowej oraz systemów sterowania (IACS) jest powiązany ze ścisłą integracją, dużymi ilościami danych oraz stosowaniem otwartych standardów w celu zapewnienia niezbędnego bezpośredniego dostępu na wszystkich poziomach systemów. Powstałe w ten sposób ogromne zalety dla użytkowników skłoniły ekspertów do rozpoczęcia debaty o nowej rewolucji przemysłowej – „Industry 4.0".

Analogicznie – zastosowane w sektorze wodociągowym i odbioru ścieków – opracowano takie koncepcje jak „Water 4.0", które skupiając się na automatyzacji i cyfryzacji, jako kluczowych aspektach strategii wydajnego, zrównoważonego i elastycznego zarządzania wodą.

Ten trend wzajemnego łączenia systemów ma jednakże znaczącą wadę w postaci zwiększonej podatności na cyberataki z różnych stron.

Kompleksowa integracja oraz otwarte standardy komunikacyjne znacznie ułatwiają atakującym oraz programom szpiegowskim dostęp do systemu. Badania i potwierdzone zdarzenia pokazują, że nie tylko systemy sterowania – określane także jako technologia operacyjna – ale także obszary produkcyjne są uznawane za wartościowe cele różnego rodzaju ataków. Organizacje stojące za tego typu atakami stają się coraz bardziej agresywne w swoich działaniach, stosując coraz skuteczniejsze narzędzia i poświęcając więcej zasobów na poważne zakłócenie lub wyrządzenie szkody dla życia publicznego.

Traktowanie zaopatrzenia w wodę i odprowadzanie ścieków jako infrastrukturę krytyczną narzuca konieczność opracowania, wdrożenia i utrzymywania strategii środków technicznych i organizacyjnych w celu ochrony i zabezpieczenia funkcjonowania obiektów wodno-kanalizacyjnych.

Dzisiejsza rzeczywistość jest taka, że wszystkie systemy przemysłowe, administracyjne oraz infrastruktury są narażone na profesjonalnie przeprowadzane ataki. Zmiana rodzaju zagrożenia wymaga gruntownego przemyślenia sposobu zabezpieczenia informacji i obsługi, ochrony dostępu – a także całego procesu definiowania i wdrażania rozwiązań bezpieczeństwa przemysłowego. Nigdy do tej pory nie było tak ważne, by sprzedający, dostawcy rozwiązań oraz operatorzy systemów sterowania stawiali czoła związanym z tym zagrożeniom.

Stawianie czoła wyzwaniom cyberbezpieczeństwa oraz podejmowanie działań

Obiekty infrastruktury krytycznej wymagają specjalnych rozwiązań w zakresie systemów informatycznych (IT) oraz technologii operacyjnych (OT), które wymagają nieprzerwanej dostępności instalacji, obsługi krytycznych funkcji systemów sterowania i automatyki przemysłowej (IACS) oraz kompleksowej i stale aktualizowanej ochrony przed zagrożeniami. Wymogi te można spełnić, korzystając ze skoordynowanych, szeroko zróżnicowanych i kompleksowych koncepcji z podzespołami i systemami przeznaczonymi do użytku przemysłowego.

Pod tym względem wskazane jest wdrożenie tzw. koncepcji wielowarstwowej ochrony (Defence in Depth Concept), ustandaryzowanej normą IEC 62443 i dostarczanej przez firmę Siemens, jako czołowego dostawcę IACS w zakresie usług i rozwiązań.

Przy użyciu właściwych narzędzi, możliwe jest stałe monitorowanie bezpieczeństwa instalacji wodociągowych i kanalizacyjnych, wykrywając i zapobiegając atakom. Dostęp do systemu oraz komunikacja są analizowane i dokumentowane, by firmy były w stanie spełnić wymóg identyfikowania i zgłaszania zdarzeń związanych ze środowiskiem i bezpieczeństwem do odpowiednich władz.

Należy dokładnie skoordynować środki organizacyjne i techniczne: wszechstronna koncepcja bezpieczeństwa opiera się na ludziach, procesach i technologii działających w synergii, w celu osiągnięcia niezbędnego poziomu ochrony. Norma IEC 62443 dotyczy wszystkich zaangażowanych stron, czyli dostawców IACS, dostawców rozwiązań i usług, a także firmy obsługujące; definiuje obowiązki i odpowiednie połączenia organizacyjne, ponadto zapewnia ramy do definiowania, wdrażania, dokumentowania, testowania i utrzymywania środków organizacyjnych i technicznych.

Właściciel aktywów / firma obsługująca

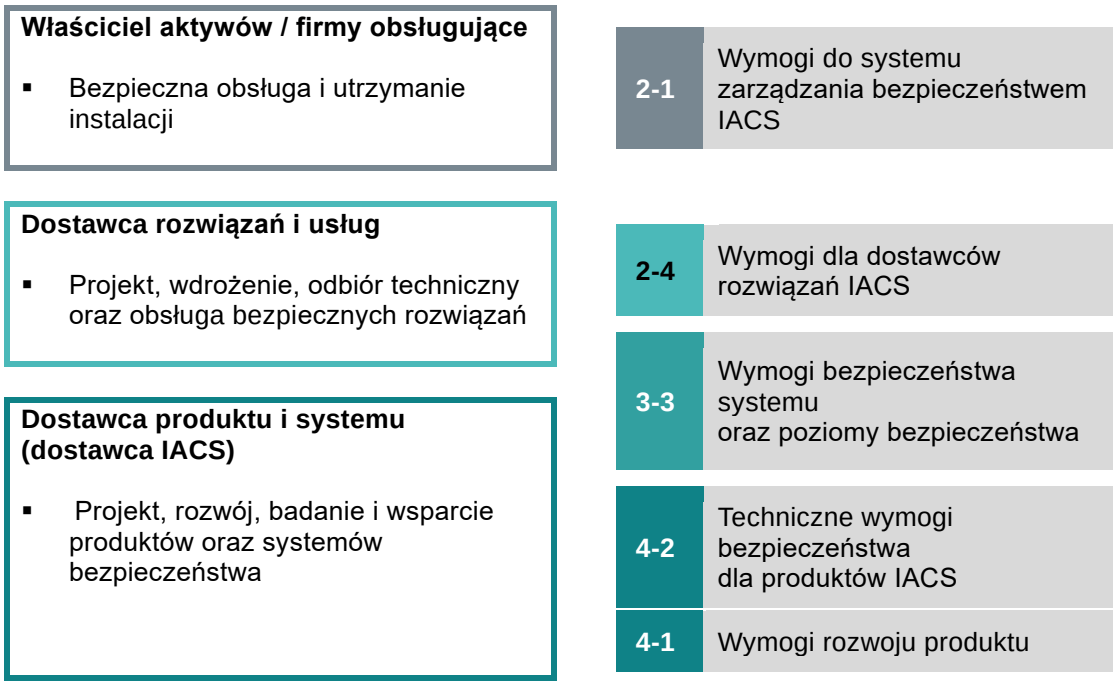
- Wdraża system zarządzania bezpieczeństwem informacji
- Określa cele ochrony dla danego zakładu
- Określa wymogi bezpieczeństwa dla danego zakładu
- Zarządza wprowadzaniem poprawek do systemu kontrolnego danego zakładu

Dostawca rozwiązań i usług

- Posiada (certyfikowany) proces tworzenia i zarządzania rozwiązaniem
- Projektuje bezpieczną architekturę systemu dla rozwiązania klienta, w tym także ocena zagrożeń i ryzyka (Threat and Risk Assessment - TRA)
- Przygotowuje stosowną dokumentację klienta
- Zarządzanie zdarzeniami i lukami w zabezpieczeniach podczas wykonywania projektu
- Zarządzanie wprowadzaniem poprawek do wszystkich produktów zastosowanych w rozwiązaniu podczas wykonywania projektu

Dostawca produktu i systemu (dostawca IACS)

- Posiada (certyfikowany) proces rozwoju dla zastosowanych produktów
- Rozwój produktów z funkcjonalnościami bezpieczeństwa
- Zarządzanie zdarzeniami i słabymi punktami
- Zarządzenie wprowadzaniem poprawek do produktów własnych



Ilustracja 1: Normy do definiowania wymogów dotyczących bezpieczeństwa dla dostawców produktów i systemów, integratorów systemów i/lub dostawców rozwiązań, a także właścicieli aktywów / firm obsługujących

Właściwa dokumentacja do cyberbezpieczeństwa w branży Woda i Ścieki

Niniejsza biała księga opisuje kompleksową koncepcję bezpieczeństwa dla automatyki przemysłowej oraz systemów sterowania, a także rozwiązań – zgodnych z IEC 62443 – do ochrony instalacji i sieci doprowadzenia wody i oczyszczania ścieków. Przypisuje ogólne wymagania do konkretnych celów ochrony i zagrożeń dla sektora wodnego; obejmuje system SCADA WinCC RT Professional, koncepcję sieci wraz ze zdalnym dostępem i telekontrolą, a także odnośne urządzenia zabezpieczające.

Aby uzyskać szczegółowe informacje techniczne i przykłady praktycznego zastosowania środków bezpieczeństwa dla instalacji zaopatrzenia w wodę i odprowadzania ścieków, należy odnieść się do wytycznych konfiguracji bezpieczeństwa dla systemów SCADA WinCC Professional, V7 oraz WinCC Open Architecture dostępnych od sierpnia 2020 roku.

Dodatkowe informacje dotyczące cyberbezpieczeństwa dostępne są pod adresem https://www.siemens.com/industrialsecurity

Motywacja

Jak wspomniano powyżej, rosnąca współpraca pomiędzy urządzeniami przemysłowymi i obiektami wpisującymi się w koncepcję „Industry 4.0”, bazujących na sieciach IT, niesie ze sobą liczne zagrożenia.

Do tej grupy zagrożeń zaliczają się nie tylko ataki, ale również pomyłki i skutki uboczne zmian w konfiguracji systemu, które wcześniej dotyczyły jedynie lokalnego obiektu, a teraz mogą wpływać na cały zakład, a nawet klientów globalnego systemu IT.

W odpowiedzi na te zagrożenia, władze ustawodawcze na całym świecie zdefiniowały zasoby kluczowe dla funkcjonowania społeczeństwa i gospodarki. Zasoby te, zwane „infrastrukturą krytyczną”, podlegają specjalnym przepisom, tj. konieczne jest utrzymanie bezpieczeństwa ich sieci na najwyższym poziomie oraz należy powiadomić instytucje rządowe o zdarzeniach związanych z cyberatakami.

Europejska dyrektywa 2008/114/WE została wydana w sprawie rozpoznania i wyznaczenia Europejskiej Infrastruktury Krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony. Kraje członkowskie wdrożyły te wytyczne do prawa krajowego w 2011 roku.

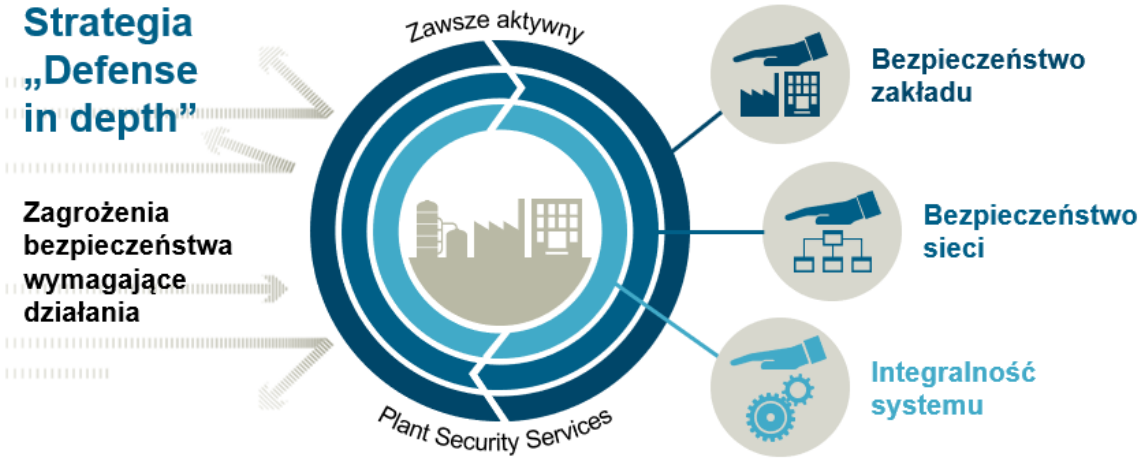
W Polsce infrastrukturę krytyczną reguluje ustawa o zarządzaniu kryzysowym (Dz. U. z 2013 r. poz. 1166 oraz z 2015 r. poz. 1485) oraz Narodowy Program Ochrony Infrastruktury Krytycznej. Istnieje również wiele innych norm, które można wykorzystać do sprawdzania czy infrastruktura krytyczna jest należycie zabezpieczona. W przypadku klientów przemysłowych, do zapewnienia żądanego poziomu bezpieczeństwa, powszechnie stosuje się normę IEC 62443.

Cel niniejszej białej księgi oraz wszystkich czynności zabezpieczających w infrastrukturze transportu publicznego można podsumować w następujących punktach:

- Ataki na urządzenia podłączone do sieci stają się coraz łatwiejsze i bardziej powszechne
- Przepisy tworzenia i utrzymywania tych infrastruktur w większości państw stają się coraz bardziej wymagające
- Ryzyko finansowe cyberataków wskutek przestarzałych zabezpieczeń, odszkodowań za poniesione straty oraz kar za zaniedbania w zakresie środków bezpieczeństwa istotnie wzrosły

2 Omówienie koncepcji firmy Siemens dla bezpieczeństwa przemysłowego

Wszystkie aspekty, począwszy od sieci publicznych i korporacyjnych, poprzez poziom instalacji, aż do obiektu, obejmując i) bezpieczeństwo instalacji i kontrolę dostępu fizycznego, ii) bezpieczeństwo sieci, iii) integralność systemu, muszą zostać uwzględnione jednocześnie, aby chronić instalacje wodno-kanalizacyjne przez wewnętrznymi i zewnętrznymi cyberatakami. Najodpowiedniejszym podejściem jest Strategia wielowarstwowej ochrony (Defence in Depth) zgodny z zaleceniami normy IEC 62443.



Ilustracja 2: Strategia wielowarstwowej ochrony (Defence in Depth Concept)

Strategia „Defence in Depth” składa się z wielowarstwowych elementów i środków ochronnych; elementy bezpieczeństwa instalacji, bezpieczeństwa sieci oraz integralności systemu tworzą podstawę koncepcji bezpieczeństwa przemysłowego, od interfejsu dla systemów zarządzania i administracji poprzez poziom operacyjny do poziomu maszyn.

Wszystkie trzy warstwy – wraz z odpowiednimi środkami technicznymi – są szczegółowo opisane w wytycznych konfiguracji bezpieczeństwa dla systemów Siemens SCADA (Security Configuration Guidelines for Siemens SCADA), wliczając w to ochronę dostępu fizycznego, środki organizacyjne, takie jak wytyczne i procesy, a również środki techniczne do zabezpieczania sieci i systemów przed nieupoważnionym dostępem, szpiegostwem i manipulacją. Zabezpieczenie na kilku poziomach oraz połączony efekt różnorodnych środków

ochronnych prowadzi do wyższego poziomu bezpieczeństwa, zmniejszenia ryzyka udanych ataków oraz finalnie do poprawy dostępności systemu.

Spójne wdrożenie strategii wielowarstwowej ochrony zapewnia firmom obsługującym i ich doradcom, w zakresie bezpieczeństwa, dodatkowe środki ochronne przed zagrożeniami związanymi z cyberbezpieczeństwem i możliwością przestrzegania ogólnych rekomendacji zespołu reagowania kryzysowego dla przemysłowych systemów sterowania (ICS-CERT).

ICS-CERT zaleca:

- Zminimalizować obecność w sieci wszystkich urządzeń systemu sterowania. Urządzenia krytyczne nie powinny mieć bezpośredniego dostępu do Internetu
- Umieścić sieci systemu sterowania oraz urządzenia zdalne za zaporami sieciowymi i odizolować je od sieci firmowej
- Korzystać z takich metod zabezpieczenia jak bezpieczna wirtualna sieć prywatna (VPN), jeśli wymagany jest zdalny dostęp lub komunikacja poprzez sieci publiczne. Należy pamiętać, że VPN jest tak samo bezpieczny, jak podłączone do niej urządzenia.

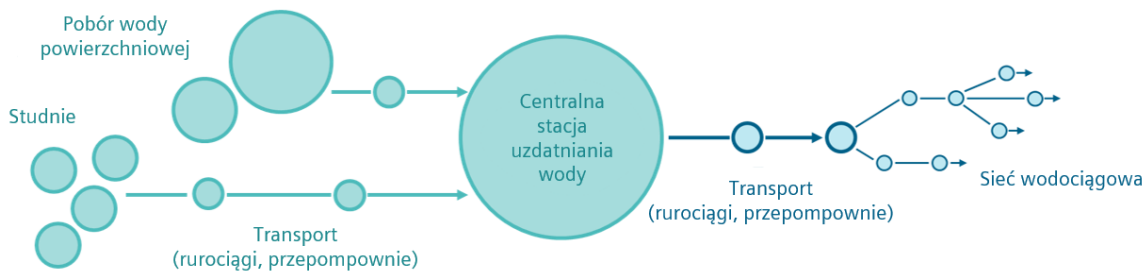
3 Stacje uzdatniania wody i oczyszczanie ścieków

Omówienie procesu

Zasadniczymi cechami systemów zaopatrzenia w wodę oraz odprowadzania ścieków to transport na duże odległości oraz zdecentralizowane i silnie rozgałęzione infrastruktury sieci wodociągowych i kanalizacyjnych.

Sieć wodociągowa

Zaopatrzenie w wodę obejmuje instalacje do produkcji wody pitnej oraz jej dystrybucję do podłączonych odbiorców domowych i przemysłowych. Pobór wody surowej obejmuje zarówno wody powierzchniowe, jak i studnie. Centralna stacja uzdatniania wody oczyszcza i przetwarza wodę do żądanej jakości, a na koniec dostarcza ją do sieci wodociągowej.

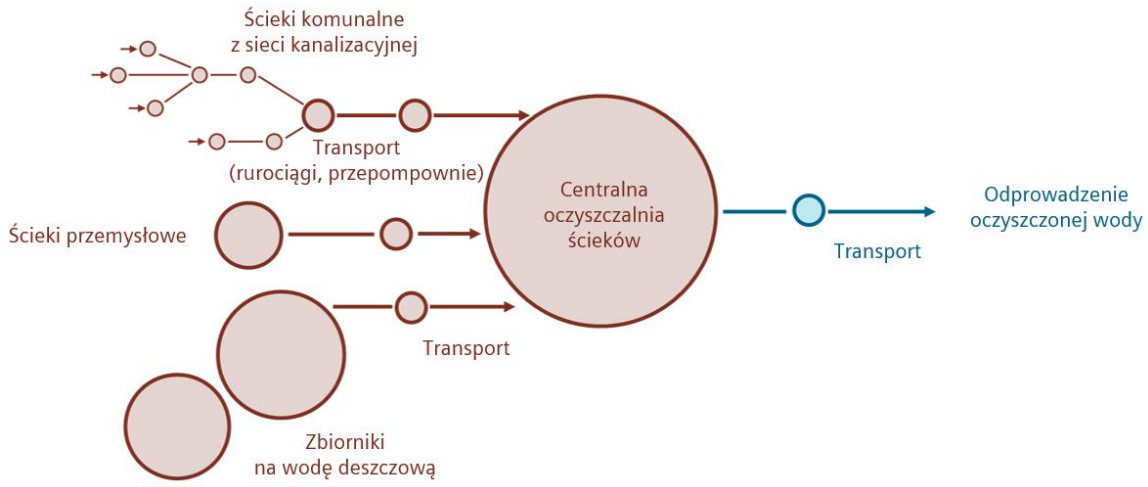


Ilustracja 3: Zaopatrzenie w wodę obejmuje pobór wody z różnych źródeł, centralną stację uzdatniania wody oraz transport i dystrybucję do sieci wodociągowej

Zakłady odsalania wody morskiej różnią się zasadniczo w zakresie centralnego przetwarzania; również są ujęte w następujących dokumentach.

Odprowadzanie ścieków

Odprowadzanie ścieków obejmuje odbieranie i przetwarzanie zanieczyszczonej wody z instalacji domowych i przemysłowych, wraz z późniejszym odprowadzeniem jej do naturalnych wód, minimalizując wpływ na środowisko naturalne. Ścieki są odbierane poprzez sieć kanalizacyjną, transportowane z użyciem pomp do centralnej oczyszczalni, a tam poddawane kilku procesom oczyszczania. Oczyszczona woda jest następnie transportowana do rzek lub morza poprzez dalsze przepompownie i rurociągi.



Ilustracja 4: Oczyszczanie ścieków obejmuje gromadzenie ścieków z różnych źródeł, centralną stację oczyszczania oraz transport i odprowadzenie czystej wody

Obiekty

Choć szczegóły procesów w dostawie świeżej wody, a oczyszczaniem ścieków istotnie się różnią, architektura automatyki i systemu sterowania, a także odnośnych mechanizmów komunikacji i kontroli, jest niemal identyczna, zwłaszcza w zakresie bezpieczeństwa.

Systemy automatyki przemysłowej i sterowania dla instalacji wodno-ściekowych często mają strukturę hierarchiczną. Obejmują one główne centrum sterowania, kilka lokalnych sterowni do poszczególnych zasobów, takich jak stacje uzdatniania wody lub ścieków, a także wiele stacji operatorskich na poziomie instalacji, np. przy każdej pompowni.

Zarówno centralna instalacja uzdatniania, jak i lokalne obiekty zajmujące się transportem i siecią są w pełni zautomatyzowane. Te drugie mają zazwyczaj postać zdalnie sterowanych podstacji przy użyciu telekontroli, częściowo za pośrednictwem publicznych sieci komunikacyjnych.

Poniższy ustęp zapewnia omówienie obiektów i ich funkcji.

Główne centrum sterowania

Główne centrum sterowania monitoruje i kontroluje jedną lub kilka instalacji wodociągowych/ kanalizacyjnych oraz sieci, które leżą w odpowiedzialności obsługującego podmiotu.

Główna instalacja/ instalacje

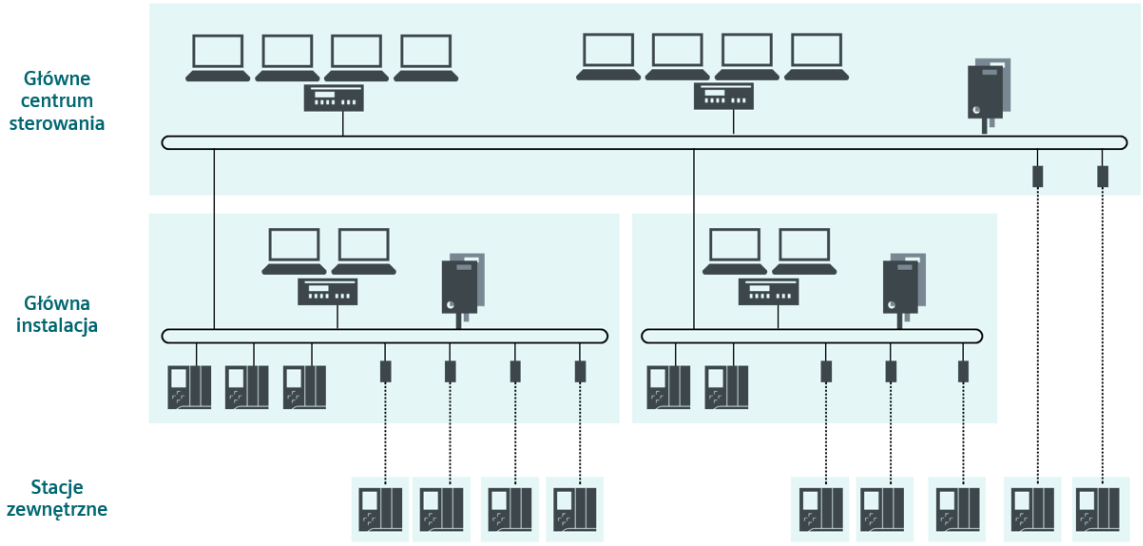
Główna instalacja zawiera najważniejsze jednostki procesowe, a także odpowiadające im systemy automatyki i sterowania (PLC, serwery, urządzenia komunikacyjne), w tym lokalną dyspozytornię instalacji do monitorowania i sterowania.

Jeśli dostępne jest centralne główne centrum sterowania, lokalna sterownia instalacji może być (tymczasowo) bezobsługowa i monitorowana zdalnie.

Stacje zewnętrzne

Stacje zewnętrzne znajdują się w różnych miejscach, takich jak studnie, zbiorniki wodne, przepompownie itp.

Zazwyczaj działają one samodzielnie i automatycznie. Zwykle są połączone poprzez prywatny WAN lub sieć publiczną.



Ilustracja 5: Typowa hierarchiczna architektura systemu sterowania w sieciach wodociągowych lub kanalizacyjnych obejmuje główne centrum sterowania, instalacje z lokalnymi centrami sterowania oraz stacje zewnętrzne

4 Schematy i środki bezpieczeństwa

Typowe konfiguracje systemu SCADA

W zależności od typu i wielkości instalacji, a także innych czynników wpływających, istnieją różne sposoby podejścia do przemysłowych systemów sterowania i automatyzacji (IACS) dostarczania wody lub odprowadzania ścieków. Siemens oferuje – w oparciu o SCADA WinCC RT Professional – skalowalne i elastyczne portfolio, począwszy od małych instalacji o lokalnym zakresie działania, poprzez większe oczyszczalnie wody i ścieków, aż po szeroko rozproszone sieci i główne centra sterowania do monitorowania i kontrolowania kilku instalacji obsługujących podmiotów.

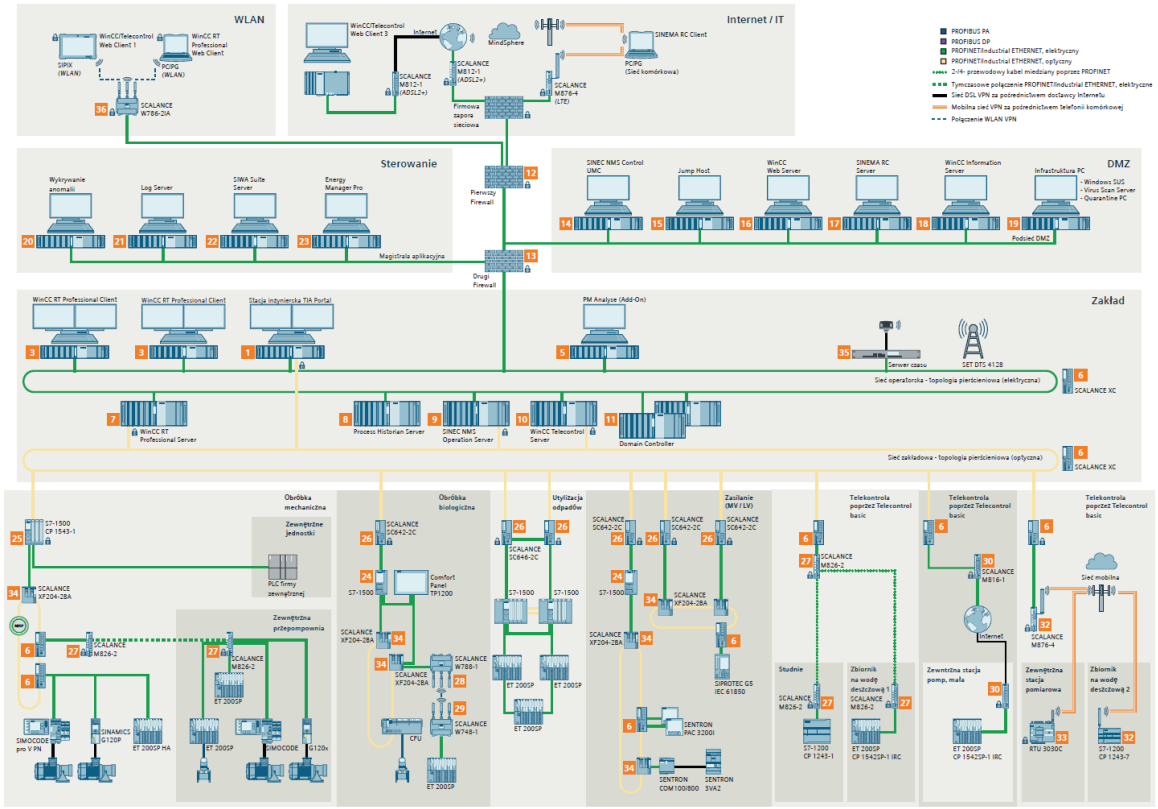
Scenariusze zagrożeń i ryzyka oraz wynikające z nich niezbędne środki ochronne są w dużej mierze identyczne dla różnych modeli systemu sterowania; zostaną one przedstawione poniżej w ogólnym zarysie. Do każdego systemu sterowania dołączona jest konkretna dokumentacja, opisująca szczegółowo różne formy mechanizmów bezpieczeństwa.

Przedstawione przykłady opierają się na systemie oczyszczania ścieków wraz z podstacjami. Choć zagrożenia i ryzyko w instalacjach wodociągowych i kanalizacyjnych mogą się różnić, proponowane środki bezpieczeństwa (ochrona dostępu, szyfrowanie danych, DMZ / zapory sieciowe, szyfrowana komunikacja / VPN itp.) są identyczne na poziomie produktu i systemu.

Przedstawiona architektura systemu sterowania może zostać wykorzystana jako ogólny schemat, zapewniający w dużej mierze ustandaryzowaną architekturę bezpieczeństwa, która została uważnie zaprojektowana przez ekspertów firmy Siemens z zakresu automatyzacji i bezpieczeństwa – ze szczególnym uwzględnieniem przemysłu wodociągowego i kanalizacyjnego.

Schematy przedstawiają najczęściej stosowaną architekturę poszczególnych jednostek procesowych. Zastosowanie konkretnej konfiguracji dla danego typu jednostki procesowej jest przydatne, lecz nie jest konieczne. Możliwe jest na przykład zaprojektowanie w identyczny sposób wszystkich jednostek, w celu ograniczenia różnorodności [1].

[1] Oznacza to taki sam sterownik i rozdzielnię dla każdej maszyny; taki sam sterownik, protokół telekontroli i router dla każdej jednostki zdalnej.



Ilustracja 6: Architektura systemu oparta na WinCC Professional

Strefy bezpieczeństwa

Strefa bezpieczeństwa to fizyczne lub logiczne grupowanie zasobów (PLC, stacje operatorskie i inżynierskie, urządzenia komunikacyjne itp.), niezbędnych do obsługi procesów przemysłowych i funkcji sterowniczych, dzielących wspólne ryzyko i słabe punkty, ze wspólnymi konsekwencjami naruszenia bezpieczeństwa. Z tego względu mają wspólne wymogi bezpieczeństwa oraz cechy, takie jak polityka bezpieczeństwa czy kontrola dostępu.

Definicja stref bezpieczeństwa systemu sterowania jest dostosowywana do wymagań dotyczących ekspozycji i bezpieczeństwa dla danych procesów i funkcji.

Dla każdej strefy konieczne jest określenie wymogów dotyczących bezpieczeństwa oraz poziomów tolerowanego ryzyka. Dokumentacja obejmuje zakres funkcjonalności strefy, jej poziom bezpieczeństwa oraz zagrożenia i ryzyko. Stanowi ona wytyczne dla środków bezpieczeństwa, jakie należy zastosować w celu zabezpieczenia zasobów, funkcji oraz kontrolowanego procesu.

Koncepcja ta zapewnia wielopoziomowe podejście do bezpieczeństwa, które uwzględnia strategię „Defence-in-Depth”.

Główne strefy bezpieczeństwa przemysłowych systemów sterowania i automatyzacji (IACS) dla obiektów wodno-ściekowych to:

1 – Sterownia

Budynek / strefa sterowni obejmuje stacje inżynierskie i operatorskie, zapewniające funkcjonalność monitorowania i kontroli. Zawiera również dodatkowe serwery infrastrukturalne, na przykład zarządzanie siecią, kontroler domeny oraz serwer czasu.

Ponadto, może także obejmować serwery do przetwarzania danych i informacji, na przykład do monitorowania jakości i energii. Funkcje te zazwyczaj nie są tak krytyczne, lecz można zabezpieczyć je, korzystając z tej samej infrastruktury ochronnej.

2 – Centralna instalacja

Strefa ta obejmuje najważniejsze i krytyczne podsystemy IACS do bezpiecznego działania oraz dostępności systemu i procesu. Dotyczy to systemów automatyki / sterowników, systemów IO oraz oprzyrządowania, a także napędów i urządzeń zabezpieczających.

W tej strefie obowiązuje najwyższy stopień ochrony, zarówno fizycznie/ technicznie, jak i organizacyjnie.

3 – Strefa zdemilitaryzowana

Strefa zdemilitaryzowana (DMZ; określana także jako sieć obwodowa) to podsieć, która oddziela sieć zakładową (m.in. sterowanie) (OT) od sieci biurowej (IT).

Systemy i aplikacje umieszczone w DMZ mają dostęp do wewnętrznej i zewnętrznej sieci, przez co są najbardziej narażone na ataki. Dlatego, dane przychodzące, jak i wychodzące przechodzą przez urządzenia zabezpieczające w sieci obwodowej, co ogranicza połączenia do wymaganego minimum.

4 ...8 – Zewnętrzne / zdalne stacje

Strefa ta obejmuje szeroko rozproszone, zewnętrzne/ zdalne stacje, połączone poprzez prywatne WAN lub infrastrukturę sieci publicznej, w tym także połączenia radiowe oraz technologie telekontroli. Jako że stacje zazwyczaj znajdują się w nienadzorowanych i częściowo dostępnych publicznie obszarach, wymogi dotyczące bezpieczeństwa są wyższe i obejmują fizyczną ochronę dostępu, a także monitorowanie pod względem ingerencji. W sytuacjach nadzwyczajnych możliwe jest tymczasowe obsługiwanie poszczególnych podstacji lokalnie, bez połączenia sieciowego z głównym systemem sterowania.

Zasadniczo, komunikacja ze strefy centralnej instalacji do stacji zewnętrznych – tzw. łącznik – jest uznawany za odrębną strefę bezpieczeństwa, która obejmuje infrastrukturę sieci publicznej. Jako że ta ostatnia nie leży w odpowiedzialności dostawcy IACS ani dostawcy rozwiązań i usług, lecz podmiotu obsługującego oraz dostawcy usług internetowych, nie została tutaj uwzględniona.

9 – Dostęp WLAN

Jeśli – zwłaszcza przy czynnościach związanych z serwisem i utrzymaniem – na terenie zakładu wykorzystywane są urządzenia mobilne, wymagany jest dostęp bezprzewodowy.

Jako że połączenie bezprzewodowe może być wystawione na działanie publicznej infrastruktury komunikacyjnej, urządzenia w tej strefie uznaje się za „niezaufane".

10 – Firmowy system informatyczny / Internet

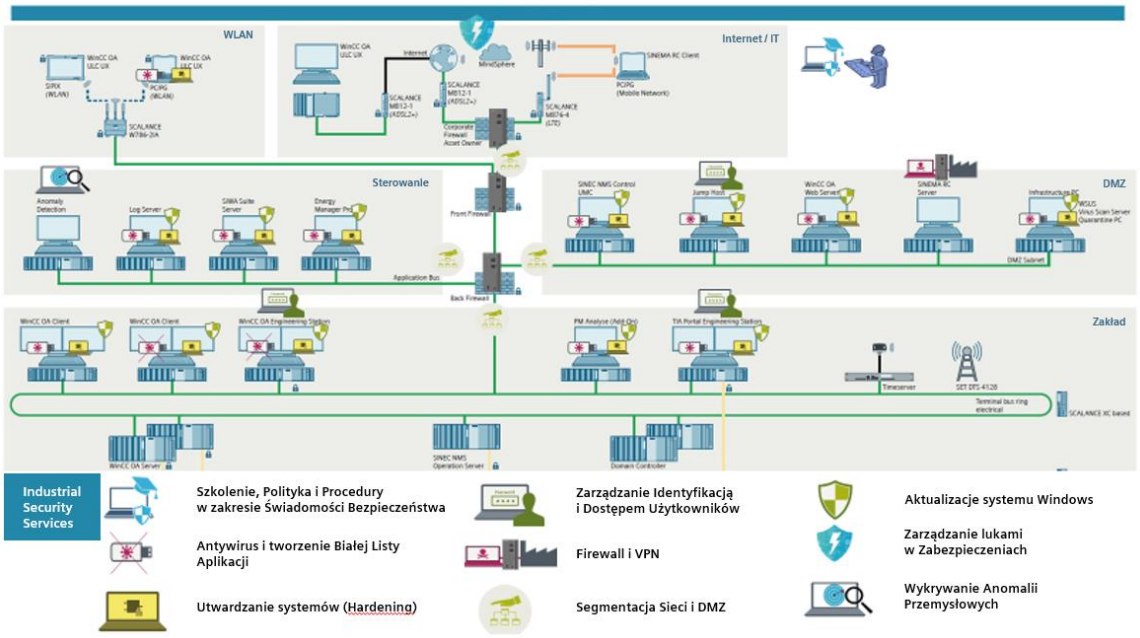
Strefy zewnętrzne nie są obsługiwane przez IACS. Urządzenia w tych strefach mają najniższy poziom bezpieczeństwa, mają dostęp do Internetu i są najbardziej narażone na atak. Uznaje się je za „niezaufane", więc komunikacja jest ograniczona do połączeń z DMZ.

Separacja części produkcyjnych – Komórki bezpieczeństwa

Jednostka procesowa to fizyczna lub logiczna grupa zasobów, powiązanych procesów, które mogą działać przez określony czas bez podłączenia do reszty instalacji, tj. jednostka procesowa musi móc pozostać operacyjnie niezależna przez pewien czas. Jednostka operacyjna może odpowiadać komórce bezpieczeństwa, jeśli zastosowano odpowiednią politykę bezpieczeństwa i środki ochronne, które obejmują kontrolę fizycznego dostępu, dostępu do komputera i sieci ze stosownym uwierzytelnianiem i autoryzacją, a także monitorowanie i kontrolę procesu.

Strategia podziału instalacji na poszczególne części zwiększa ogólną dostępność całego systemu, ponieważ ogranicza to zagrożenie i zdarzenia związane z bezpieczeństwem do najbliższego otoczenia, tj. do jednej komórki.

W obiektach wodno-kanalizacyjnych, komórki bezpieczeństwa zazwyczaj odpowiadają poszczególnym jednostkom procesowym, takim jak obróbka mechaniczno-biologiczna w instalacji centralnej oraz segmenty sieci kanalizacyjnej i przepompownie w zewnętrznych/ zdalnych stacjach.



Ilustracja 7: Przykład wdrożenia portfolio Siemens Industrial Security w W&WW

Zagrożenia i ryzyko

Wszystkie środki związane z bezpieczeństwem wywodzą się ze szczegółowej analizy ryzyka i zagrożeń (TRA – Threat and Risk Assessment) zgodnie z normą IEC 62443.

Dokument ten opiera się na ogólnym TRA, który uwzględnia standardowe instalacje wodno-kanalizacyjne oraz typowe środowiska operacyjne.

W oparciu o te analizy, opracowano specjalne schematy (referencyjne architektury systemu), aby wdrożyć ogólne środki bezpieczeństwa, które skupiają się na ochronie sieci i dostępu do systemu.

Jednakże, dla każdej instalacji, zalecane jest specjalne TRA, które jest zwykle wymagane. TRA, architektura systemu sterowania oraz środki do wdrożenia mogą zatem opierać się na tych ogólnych rozwiązaniach, aby zminimalizować nakład sił na adaptację.

Poniższe główne zagrożenia zidentyfikowano i oceniono, biorąc pod uwagę cele ochrony oraz planowane środowisko operacyjne.

Fizyczny dostęp

Fizyczny dostęp do instalacji, sieci i części instalacji stanowi największe zagrożenie. Niekontrolowany dostęp oznacza uzyskanie pełnej kontroli nad instalacją.

Rozproszone stacje nie pozwalają na łatwe zabezpieczenie, ani monitorowanie poprzez regularną fizyczną obecność. Fizyczny dostęp jest zazwyczaj

ograniczony poprzez środki, podobne jak w głównym zakładzie. Ponadto, stacje zdalne są zazwyczaj zaprojektowane do pracy niezależnej i automatycznej.

Wprowadzenie złośliwego oprogramowania poprzez przenośne nośniki danych

Przenośne nośniki danych są częstym sposobem na wprowadzenie złośliwego oprogramowania. Jeśli pracownik nie jest świadomy ryzyka, może podłączyć (osobisty) pendrive do komputera w sieci biurowej lub automatyki i w ten sposób narazić system na zagrożenie. Ryzyko wprowadzenia w ten sposób złośliwego oprogramowania jest poważne, ponieważ środki bezpieczeństwa w sektorze prywatnym są na ogół na bardzo niskim poziomie.

Wtargnięcie poprzez dostęp zdalny / Internet

Rozlegle rozproszone systemy sterowania wymagają dostępu poprzez komunikację zdalną po sieci publicznej, w tym bezprzewodową komunikację radiową, którą można wykorzystać do cyberataków. Przede wszystkim pierwsza zapora sieciowa jest narażona na atak. Zdalny dostęp może stanowić zagrożenie, jeśli nie zostanie należycie zaprojektowany i zarządzany.

Błędy ludzkie i sabotaż

Brak świadomości lub ignorancja w zakresie wysokiego ryzyka pewnych działań to najpowszechniejsze powody wewnętrznych ataków. Wyraźnie określone wytyczne są często celowo ignorowane, ponieważ wymagają poświęcenia nieco więcej wysiłku.

W dużych firmach może występować poważna różnica w znajomości zagadnienia bezpieczeństwa teleinformatycznego pomiędzy pracownikami różnych działów. Niezadowoleni pracownicy mogą celowo przeprowadzić atak.

Usterki techniczne

Nigdy nie jest możliwe całkowite wykluczenie błędów oprogramowania i sprzętu. Wystąpienie usterek sprzętu spowodowanych trudnymi warunkami środowiskowymi (brud, temperatura, wilgoć itp.) jest bardzo prawdopodobne, jeśli nie zostaną zastosowane stosowne środki ostrożności. Usterki mogą prowadzić do awarii lub nieprawidłowego działania systemu.

Portfolio i środki bezpieczeństwa przemysłowego

Schematy systemów sterowania i automatyki przemysłowej zapewniają kluczowe funkcje bezpieczeństwa poprzez produkty zabezpieczające (wzmocnienie urządzenia itp.), na poziomie systemowym (strefy bezpieczeństwa i komórki, izolacja stref i komórek, ochrona poprzez zapory sieciowe itp.), a także dobrą podstawę do wprowadzania dalszych środków przez dostawcę usług i rozwiązań IACS i/ lub klienta końcowego (użytkownicy, role

i konta, zarządzanie siecią, tunele VPN po sieciach publicznych, zarządzanie bezpieczeństwem i aktualizacją wirusów itp.).

Poniższa lista przedstawia przegląd dostępnych środków bezpieczeństwa:

1. Wzmocnienie systemu operacyjnego, np. poprzez dedykowaną wersję systemu, politykę bezpieczeństwa.

   Centralny system operacyjny oraz zarządzanie wprowadzaniem poprawek do IACS.

   Centralne zarządzanie aktualizacją antywirusów, zabezpieczenie punktów końcowych, lista zaufanych aplikacji.
2. Centralne zarządzanie wprowadzaniem poprawek oprogramowania do sieci SCALANCE oraz urządzeń zabezpieczających poprzez SINEC NMS.
3. Aktualizacja oprogramowania sterownika SIMATIC.
4. Centralna identyfikacja i zarządzanie dostępem poprzez Windows Domain Controller dla użytkowników i kont Windows, polityka haseł, uporządkowane role IACS oraz konta poprzez SIMATIC Logon.
5. Kopia zapasowa i przywracanie systemu operacyjnego (serwer kopii jest zależny od projektu).
6. Kopia zapasowa danych / projekty IACS i przywracanie danych poprzez SIMATIC Manager (serwer kopii jest zależny od projektu).
7. Bezpieczeństwo sieci i sieci centralnej oraz zarządzanie urządzeniami i kopia zapasowa poprzez SINEC NMS (serwer kopii jest zależny od projektu).
8. Strefy bezpieczeństwa i komórki, strefa i ochrona komórki poprzez segmentację sieci, zapory sieciowe.

   Szyfrowana komunikacja pomiędzy różnymi strefami bezpieczeństwa / komórkami.

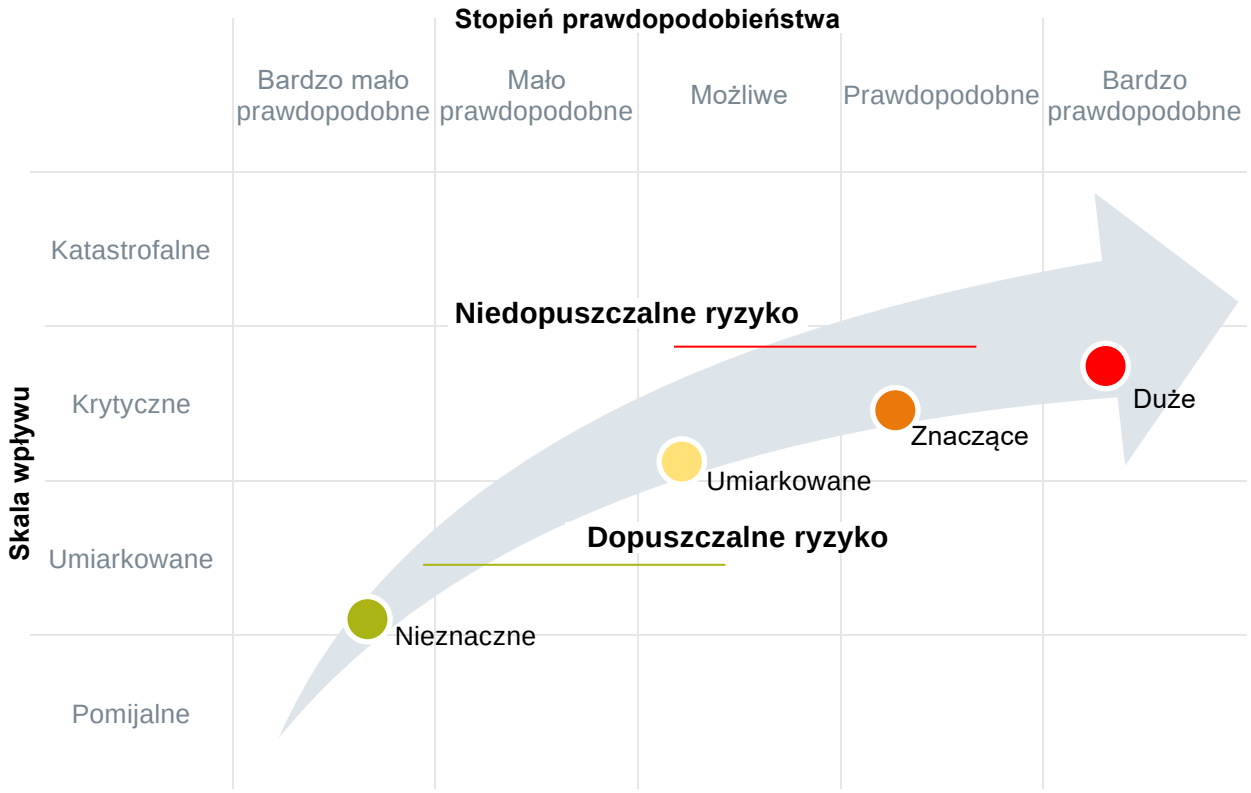
   Ograniczenie adresów IP, ograniczenie usług / portów, kontrola pakietów dla wszystkich zapór sieciowych.
9. Szyfrowane IPSec VPN do komunikacji zdalnej.
10. Szyfrowany WLAN, tunel warstwy 2, WLAN iPFC.
11. Field Interface Security dla S7-1200 i S7-1500: komunikacja do dedykowanych interfejsów urządzeń, ograniczone do działania IO; inne polecenia komunikacji są odrzucane.
12. Rejestrowanie komunikacji sieciowej; dla urządzeń SCALANCE centralnie poprzez SINEC NMS.
13. Centralne, pasywne wykrywanie anomalii do komunikacji opartej na głębokiej inspekcji pakietu.
14. Serwer kwarantannowy jako centralny punkt transferu danych, np. do konfiguracji danych inżynierskich.

5 Zarządzanie bezpieczeństwem przemysłowym

Większość celów związanych z bezpieczeństwem i ochroną można osiągnąć jedynie poprzez połączenie środków technicznych i organizacyjnych.

Te drugie obejmują ustanowienie procesu zarządzania bezpieczeństwem w organizacji. Pierwszym krokiem podczas określania wymaganych czynności jest przeanalizowanie i ocenienie znaczenia określonych zagrożeń i ryzyka. Istotność zidentyfikowanego zagrożenia zależy od skutków – na przykład na dostawę wody – powiązanych z prawdopodobieństwem wystąpienia. Błędy w analizie zagrożenia i ryzyka (TRA) mają bezpośredni wpływ na możliwość osiągnięcia celów w zakresie bezpieczeństwa i ochrony. Może prowadzić to do nieskutecznych, niedostatecznych lub drogich środków. Możliwe jest także, że słabe punkty nie zostały zidentyfikowane i skorygowane.

Podczas planowania nowego obiektu należy wykonać analizę zagrożenia i ryzyka na bardzo wczesnej fazie planowania. Jest to idealny moment na identyfikację ryzyka, klasyfikację i definicję planu wprowadzenia środków cyberbezpieczeństwa. Zgodnie z tym podejściem, możliwe jest osiągnięcie konceptu oszczędnego i „zabezpieczonego w fazie projektu".



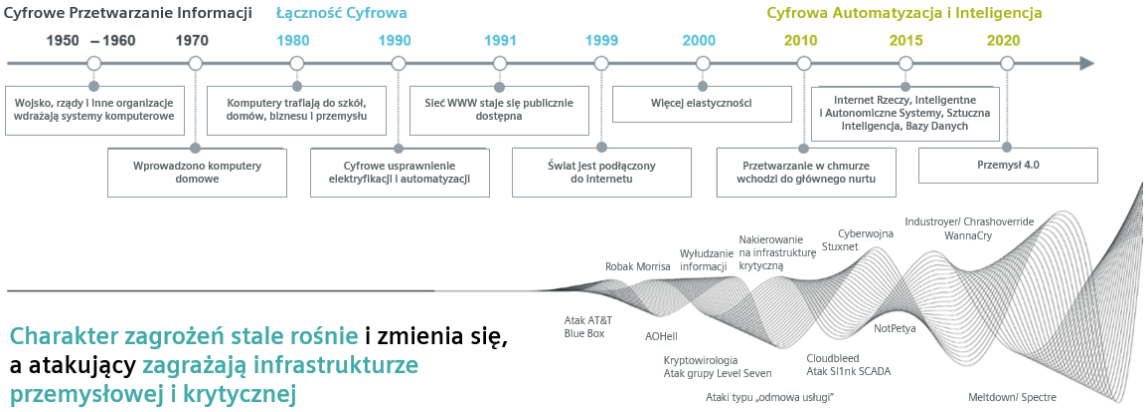
Ilustracja 8: Tablica decyzyjna oceny ryzyka stosowana w połączeniu z uprzednią analizą ryzyka danej instalacji. Ryzyko związane z obsługą należy regularnie kontrolować

Analiza ryzyka zapewnia cele w zakresie bezpieczeństwa i ochrony tworzące podstawę określonych środków organizacyjno-technicznych. Środki te należy skontrolować lub przetestować po wprowadzeniu w życie. Ocena ryzyka powinna być przeprowadzana regularnie, a także w przypadku zmian technicznych lub organizacyjnych, wpływających na oryginalne TRA.

Projekty, w tym środki bezpieczeństwa przedstawione powyżej, opierają się na drobiazgowej ocenie zagrożeń i ryzyka dla „ogólnych" obiektów wodociągowych i kanalizacyjnych; w przypadku indywidualnych obiektów i rozwiązań, wymagane są konkretne oceny i odpowiednie zmiany w projektach oraz środkach.

6 Bezpieczeństwo przemysłowe przez cały okres eksploatacji instalacji wodno-kanalizacyjnych

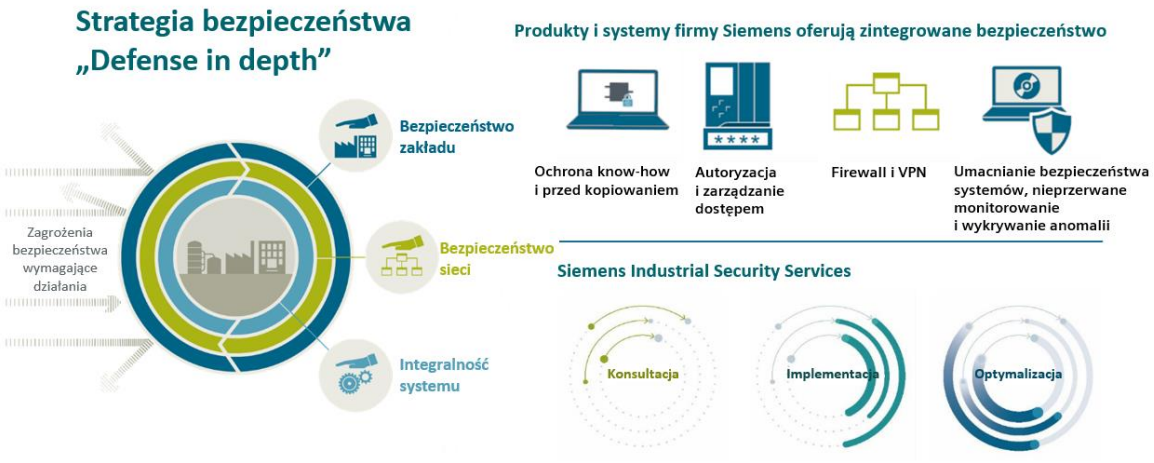
Kilka lat temu, bezpieczeństwo placówek przemysłowych opierało się na ochronie sterowania urządzeń peryferyjnych. Nowe zagrożenia okazały się być abstrakcyjne i teoretyczne, przy czym niewielu klientów końcowych i operatorów było zainteresowanych tymi kwestiami.



Ilustracja 9: Zdarzenia związane z cyberbezpieczeństwem w infrastrukturze krytycznej i przemysłowej

Doniesienia mediów o zdarzaniach związanych z bezpieczeństwem przyciągnęły zwiększoną uwagę. Stało się jasne, że systemy sterowania i automatyka przemysłowa oraz obiekty infrastruktury również mogą podlegać cyberatakom. Podatność na atak i możliwe konsekwencje mogą być poważne, dlatego też ochrona przed atakami – wraz z postępującą cyfryzacją – to nieodzowny czynnik wymagający uwagi.

Siemens – jako dostawca systemów sterowania i automatyki przemysłowej – stoi w dobrej pozycji, by wesprzeć integratorów systemów i podmioty obsługujące w dążeniu do spełnienia tych stale rosnących wymagań. Ograniczenie ryzyka jest możliwe poprzez wdrożenie wymogów i środków bezpieczeństwa na etapie projektowania, rozwoju i obsługi, a także poprzez zastosowanie holistycznego konceptu bezpieczeństwa.



Ilustracja 10: Portfolio bezpieczeństwa przemysłowego: koncept, produkty i usługi

Sama warstwa inżynieryjno-technologiczna nie wystarczy – konieczne jest również wdrożenie środków procesowych i organizacyjnych wraz z ich stałą adaptacją.

Dzięki wielu latom doświadczenia, Siemens jest silnym partnerem także w zakresie bezpieczeństwa przemysłowego do instalacji wodociągowych i kanalizacyjnych. Siemens oferuje szerokie portfolio produktów i usług związanych z bezpieczeństwem, a także skuteczne rozwiązania bezpieczeństwa przemysłowego.

Usługi bezpieczeństwa przemysłowego (Industrial Security Services)

Dedykowane usługi bezpieczeństwa wspierają konsultantów, integratorów systemów, generalnych wykonawców oraz podmioty obsługujące podczas projektowania i obsługi bezpiecznego środowiska automatyzacji.
Ten wspomagany proces rozciąga się od oceny ryzyka, organizacji i istniejących środków po projekt i wdrożenie bezpiecznego działania automatyki do ciągłego monitorowania i optymalizacji stanu bezpieczeństwa przemysłowego.

Ilustracja 11: Portfolio usług bezpieczeństwa przemysłowego

Konsultacja w zakresie bezpieczeństwa

Faza konsultacji pozwala na przejrzystość statusu bezpieczeństwa instalacji oraz identyfikuje słabe punkty i zagrożenia. Niezbędne środki są podsumowane w planie działania, przedstawiając, w jaki sposób można podnieść status bezpieczeństwa instalacji do żądanego poziomu. Jako przykład mogą służyć IEC 62443 lub ISO 27001, w których określono działania dla konkretnych instalacji wodociągowych lub kanalizacyjnych, mające na celu zapewnienie zgodności z odnośnymi częściami normy. Ocena ta może również zostać wykorzystana podczas fazy planowania, by określić wymagane działania i środki w celu osiągnięcia żądanego poziomu bezpieczeństwa.

Usługi skanowania pozwalają osiągnąć przejrzystość istniejących urządzeń automatyki, a wraz z monitorowaniem stanu bezpieczeństwa i zarządzaniem słabymi punktami, stanowią ciągłą kontrolę w ramach zdefiniowanych poziomów bezpieczeństwa.

Ilustracja 12: Proces rozwoju produktów Siemens, certyfikat TÜV IEC 62443-4-1

Wdrożenie bezpieczeństwa

Następnym krokiem jest wdrożenie proponowanych środków, stanowiących odpowiedź na zidentyfikowane słabe strony. Zasoby obejmują warstwę sprzętową (np. zapory sieciowe) oraz warstwę programową (np. antywirus, biała lista i detekcja anomalii). Dotyczy to również jednoznacznych instrukcji i wytycznych dla bezpieczeństwa IT oraz OT.

Większość tych środków została już uwzględniona podczas fazy projektów przedstawionej powyżej.

Rozwiązania bezpieczeństwa są skuteczne jedynie przy odpowiednim przeszkoleniu personelu. Należy stale kłaść nacisk na świadomość i zrozumienie pracownika, poprzez warsztaty, szkolenia sieciowe lub równoważne środki.

Optymalizacja bezpieczeństwa

Kolejnym kluczowym aspektem usług Siemens w tym zakresie jest wsparcie klienta w ciągłym monitorowaniu instalacji przemysłowych, a także zarządzaniu słabymi punktami i wprowadzaniem poprawek.

Strategia wielowarstwowej ochrony „Defence in Depth" tworzy odpowiednią podstawę do optymalizacji bezpieczeństwa w środowiskach automatyzacji. Usługi bezpieczeństwa przemysłowego Siemens (Industrial Security Services) zapewniają wsparcie przedsiębiorstw we wdrażaniu odpowiednich środków. Wszechstronny zakres usług, od oceny bezpieczeństwa do ciągłego monitorowania, pomaga klientom ograniczyć potencjalne zagrożenie związane z instalacjami wodociągowymi lub kanalizacyjnymi.

7 Podsumowanie

Uznanie doprowadzenia wody i oczyszczanie ścieków za infrastrukturę krytyczną narzuca konieczność rozwoju strategii bezpieczeństwa i podjęcia środków zaradczych, w celu zapewnienia ciągłej ochrony i bezpiecznego działania instalacji oraz sieci wodno-kanalizacyjnych.

Siemens zapewnia wszystkie elementy wymagane do wprowadzenia strategii bezpieczeństwa i osiągnięcia żądanego poziomu bezpieczeństwa przy użyciu odpowiednich produktów, systemów, rozwiązań i usług.

Mimo iż większość obecnych norm narzuca obowiązek regularnego podejmowania działań i przeprowadzania audytów jedynie na dużych obiektach, znaczenie małych i średnich instalacji i sieci wodno-kanalizacyjnych jest równie ważne i powinny się one opierać na tej samej kompleksowej metodologii.

W przypadku zastosowania właściwych narzędzi, możliwe jest stałe monitorowanie bezpieczeństwa instalacji wodociągowych i kanalizacyjnych, wykrywając, analizując i dokumentując próby ataków.

Aby wspólnie określić następny ważny krok, należy skontaktować się z lokalnym przedstawicielem handlowym firmy Siemens.