SIEMENS
Ingenuity for life

Bezpieczeństwo przemysłowe

Cyberbezpieczeństwo zdalnego dostępu

Biała księga

Wersja 06/2020

siemens.com/telecontrol

Spis treści

1. Wymogi dotyczące wodociągów/przetwarzania ścieków 3

2. IEC 62443: Ukierunkowane środki cyberbezpieczeństwa 5

2.1 Certyfikacja cyklu życia produktu zgodnie z IEC 62443-4-1 6

2.2 Wymogi produkcyjne zgodnie z IEC 62443-4-2 7

2.3 Analiza systemowa zgodnie z IEC 62443-3 10

3. Stała aktywność: Powiadomienia i aktualizacje bezpieczeństwa przemysłowego 11

4. Ocena bezpieczeństwa zgodnie z IEC 62443 / ISO 27001 ze strony Siemens 11

5. Podsumowanie 12

6. Źródła 12

Wstęp

Podstawą niezawodności dostaw wody jest bezpieczeństwo samych obiektów, oprócz ich rzeczywistej funkcjonalności, należy zagwarantować ich bezpieczeństwo pod kątem zagrożeń w kwestii cyberbezpieczeństwa. W wielu krajach obowiązują wytyczne i wymogi prawne, obligujące operatorów tzw. infrastruktury krytycznej do stosownego zabezpieczenia i wzmocnienia ich systemów, wg przyjętych standardów.
Podstawy ogólnego podejścia do zagadnienia cyberbezpieczeństwa zostały ujęte w międzynarodowej normie IEC 62443.

Cyberbezpieczeństwo

1. Wymogi dotyczące wodociągów/ przetwarzania ścieków

Dla funkcjonowania społeczeństwa niezbędna jest niezawodna i bezpieczna infrastruktura publiczna, np. w zakresie dostawy wody i elektryczności. Ze względu na postępującą cyfryzację i związane z tym trendy stosowania standardowych usług informatycznych, powszechną dostępność telefonii komórkowej oraz internetu, rosnące zagęszczenie sieci, lub użytkowanie usług opartych na chmurze, wzrasta ryzyko cyberataku na obiekty infrastruktury publicznej.
Zagrożenia obejmują szpiegostwo oraz manipulację przy poufnych danych, a także sabotaż całej produkcji lub procesu.

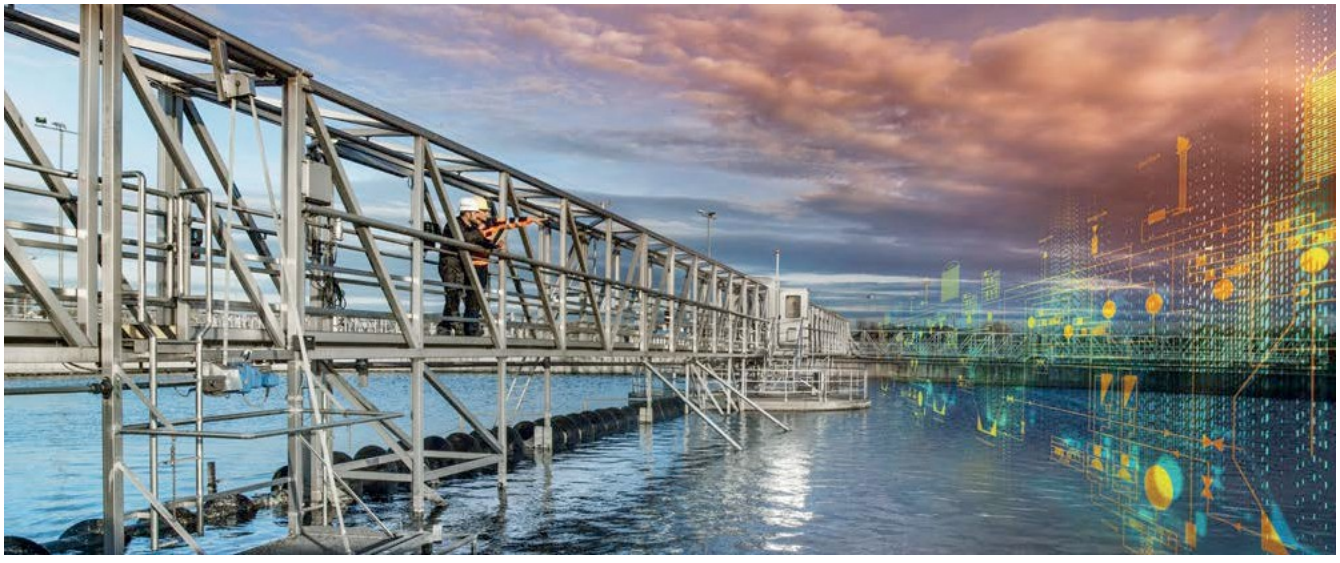
Działalność w Niemczech

W związku z tym w Niemczech uchwalono ustawę o bezpieczeństwie teleinformatycznym, z niemieckim Urzędem Federalnym ds. Bezpieczeństwa Informacji (Bundesamt für Sicherheit in der Informationstechnik – BSI) stanowiącym centralny punkt kontaktowy. Ustawa o bezpieczeństwie teleinformatycznym zobowiązuje operatorów tzw. infrastruktury krytycznej do odpowiedniego zabezpieczenia systemów informatycznych, podzespołów i procesów, a także do dostarczania dowodu zgodności z wymaganiami do BSI co najmniej co 2 lata.

https://www.bsi.bund.de

Zgodnie z obowiązującymi przepisami, za infrastrukturę krytyczną uznaje się te sektory, które są niezbędne do utrzymania ważnych funkcji społecznych, zdrowia, bezpieczeństwa oraz dobrobytu społecznego lub ekonomicznego. Obejmuje to dostęp do wody, elektryczności, pożywienia, transportu i ruchu drogowego, zdrowia, usług informatycznych i telekomunikacyjnych, a także media i kulturę. Tyczy się to obiektów dostarczających usługi do co najmniej 500 000 osób. W przypadku sektora wodnego, generuje to również parametr 22 milionów m^3 wody (tłoczonej, dystrybuowanej, usuwanej lub oczyszczanej).

https://www.kritis.bund.de



Ochrona infrastruktury krytycznej w zakresie

Cyberbezpieczeństwo

W ramach pomocy dla operatorów infrastruktury krytycznej w zakresie zapewnienia zgodności z wymogami prawnymi, niemieckie związki przemysłowe zdefiniowały wytyczne i instrukcje dla norm bezpieczeństwa w danym przemyśle. W przypadku sektora wodnego (zaopatrzenie w wodę pitną oraz utylizacja ścieków), operatorzy mogą liczyć na wsparcie określonych przepisów dotyczących konfiguracji środków ochrony działania obiektu [1, 2]. Obejmuje to między innymi konfigurację i obsługę tzw. „systemu zarządzania bezpieczeństwem informacji" (ISMS), który ma na celu zapewnienie zgodności z aktualnym stanem wiedzy w zakresie bezpieczeństwa informacji, co z kolei wiąże się z wymogiem cyklicznych testów.

W wytycznych do norm przemysłowych wprowadzono zalecenie, by stosować ISMS oparte na ISO 27001. Co więcej, operatorzy infrastruktury krytycznej muszą ustanowić punkt kontaktowy czynny 24/7, za pomocą którego można w dowolnej chwili komunikować się z władzami, a także przez który zgłaszane będą zdarzenia związane z bezpieczeństwem teleinformatycznym. Ogólnie rzecz biorąc, konieczne jest wprowadzenie środków bezpieczeństwa informatycznego, by zapewnić „dostępność systemów i danych, spójność przetwarzanych informacji oraz systemów, autentyczność pochodzenia danych i informacji".

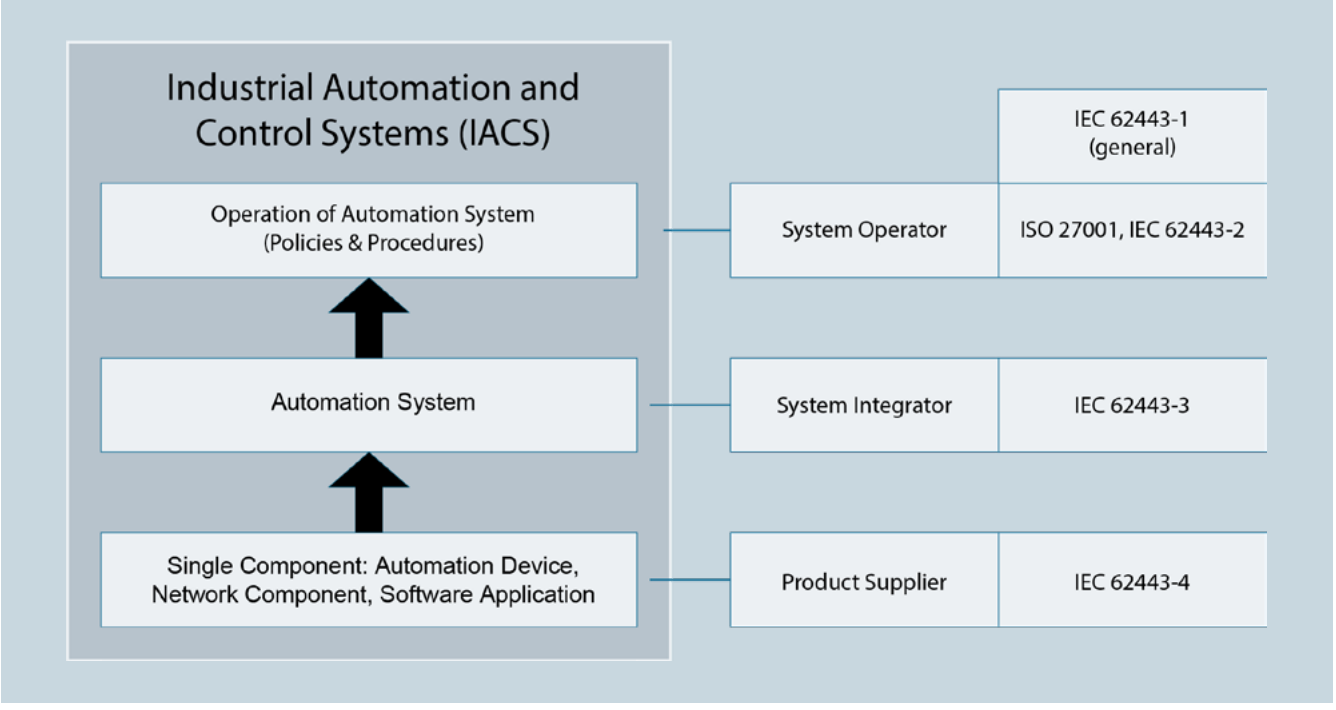
Podczas gdy wyżej wymienione normy ISO są na ogół skierowane do operatorów systemów informatycznych, dodatkowo stosowana jest norma IEC 62443 dla dedykowanych systemów przemysłowych. Stała się ona w ostatnich latach główną serią norm dla cyberbezpieczeństwa przemysłowego, przy czym jest kompatybilna z ISO 27001.

W innych krajach Unii Europejskiej, a także na całym świecie, trwają prace zapoczątkowane przez rządy i stosowne organy publiczne, mające na celu określenie podstawy dla stosownych środków ochronnych w ważnych obszarach. Tworzone są wytyczne i uchwalane są prawa mające na celu ochronę infrastruktury krytycznej, a tym samym ludności - zapewniając funkcjonowanie społeczeństwa. Oprócz ochrony fizycznej, głównym problemem ponownie staje się zabezpieczenie przed cyberatakami. Z tego względu podstawę ogólnego podejścia do zagadnienia cyberbezpieczeństwa systemów i obiektów również zostały ujęte w międzynarodowej normie IEC 62443.

Cyberbezpieczeństwo

2. IEC 62443: Ukierunkowane środki cyberbezpieczeństwa

Norma IEC 62443, składająca się z kilku części, podejmuje zagadnienie cyberbezpieczeństwa „przemysłowych systemów automatyzacji i sterowania" (IACS). Została ona opracowana wyłącznie dla środowiska przemysłowego i jego konkretnych wymogów i obejmuje wszystkie obszary przemysłu, od produkcji jednostkowej, poprzez przemysł przetwórczy, aż do rozproszonych systemów zasilających. Zawarte w niej szeregi norm odnoszą się nie tylko do operatorów systemów, lecz także do integratorów/użytkowników systemów, a także dostawców produktów/producentów podzespołów i usług. W związku z tym, firma Siemens opracowała wszechstronną strategię cyberbezpieczeństwa, która pomaga spełnić wymagania BSI oraz norm przemysłu wodociągowego/kanalizacyjnego – skutecznie chroniąc cały obiekt lub system przed atakami.



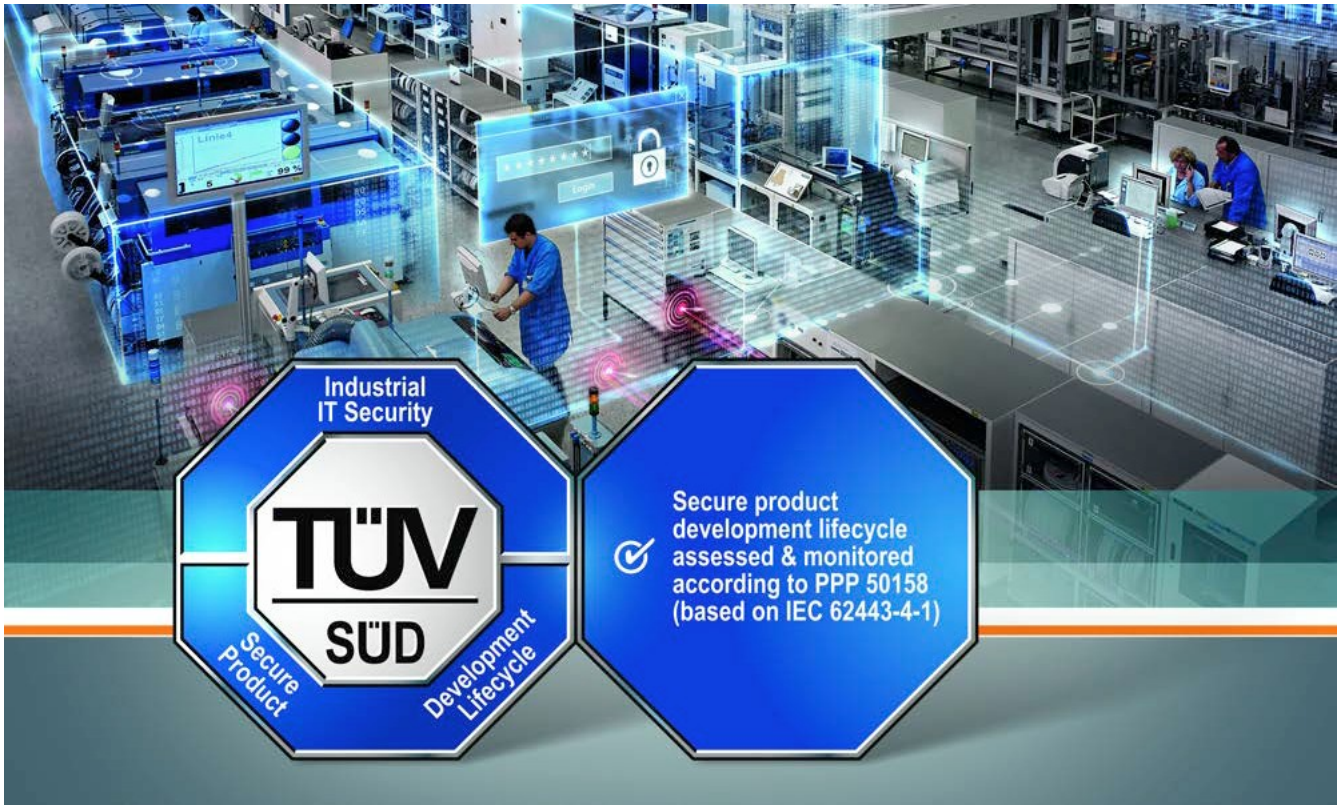
Przegląd normy IEC

Cyberbezpieczeństwo

2.1 Certyfikacja cyklu życia produktu zgodnie z IEC 62443-4-1

Część 4-1 normy IEC 62443 definiuje sposób wykorzystania podzespołów wyprodukowanych przez dostawcę produktów. Nie ma znaczenia, czy jest to podzespół z dedykowanymi funkcjami bezpieczeństwa, taki jak zapora sieciowa, przełącznik czy element automatyki. Tylko w przypadku, gdy połączenie wszystkich podzespołów, tj. cały system, opiera się na niezawodnej i bezpiecznej podwalinie, możliwe jest utworzenie skutecznego konceptu ochrony. Dlatego też, w sierpniu 2016 roku, Siemens był pierwszą firmą, która otrzymała od TÜV SÜD (Niemcy) certyfikat oparty na IEC 62443-4-1 za nadzór procesu rozwoju produktów z zakresu techniki napędowej i automatyzacji, w tym także oprogramowania przemysłowego.

Norma obejmuje między innymi następujące aspekty związane z bezpieczeństwem cyklu życia produktu: umiejętności i doświadczenie, kontrola procesu i jakości, aspekty związane z bezpieczeństwem podzespołów firm zewnętrznych, bezpieczna architektura i projekt, zarządzanie słabymi punktami bezpieczeństwa, zapewnienie aktualizacji zabezpieczeń, a także zarządzanie poprawkami i zmianami. Uwzględniając te aspekty, już podczas fazy rozwoju produktu zachowywana jest szczególna uwaga w celu uniknięcia słabych punktów i wykluczenia lub zminimalizowania zagrożeń związanych z bezpieczeństwem poprzez wybranie stosownej architektury systemu. Jeśli mimo to w oprogramowaniu wystąpią słabe punkty, użytkownicy zostaną aktywnie poinformowani oraz udostępnione zostaną odpowiednie środki zaradcze lub poprawki bezpieczeństwa.



TÜV SÜD IEC 62443-4-1 dla Siemens

2.2 Wymogi produkcyjne zgodnie z IEC 62443-4-2

Choć normy przemysłowe dla wodociągów/kanalizacji głównie odnoszą się do obsługi ISMS a tym samym narzucając zgodność z instrukcjami roboczymi i procesowymi, zastosowane podzespoły muszą obsługiwać podstawowe funkcje techniczne pozwalające operatorowi infrastruktury krytycznej na spełnienie wymagań norm.

Portfolio IRC (IRC: ang. Industrial Remote Communication, przemysłowa komunikacja zdalna) w zakresie sterowania zdalnego od firmy Siemens obsługuje niezbędne funkcje bezpieczeństwa (zgodnie z częścią 3 normy IEC 62443). Poniżej zamieszczono przykłady ważnych funkcji, które wspierają bezpieczne działanie obiektu lub systemu w celu spełnienia niezbędnych wymogów bezpieczeństwa. Kompletna analiza i projekt obiektu bądź systemu powinny stanowić część oceny bezpieczeństwa; patrz rozdział 4 „Ocena bezpieczeństwa zgodnie z IEC 62443 / ISO 27001 ze strony Siemens" niniejszego dokumentu.

1. Oprogramowanie sprzętowe podpisane cyfrowo w celu ochrony przed zmanipulowanymi aktualizacjami

2. Bezpieczna transmisja e-mail poprzez zabezpieczone połączenia

3. Bezpieczne szyfrowanie na całej drodze przesyłu przy pomocy OpenVPN/IPsec

4. Zdarzenia bezpieczeństwa pozwalają na śledzenie zdarzeń systemowych związanych z bezpieczeństwem

5. Ograniczony obszar ataku poprzez dezaktywację nieużywanych usług

6. Zabezpieczenie podzespołów jako część konceptu obrony w głąb

Cyberbezpieczeństwo

1. **Oprogramowanie sprzętowe podpisane cyfrowo w celu ochrony przed zmanipulowanymi aktualizacjami**
   W celu zabezpieczenia podzespołów automatyki przez niebezpiecznym oprogramowaniem szpiegowskim oraz fałszywymi lub zmodyfikowanymi aktualizacjami, wszelkie aktualizacje są podpisane cyfrowo. Za sprawą automatycznie uruchamianej weryfikacji podpisu podczas procesu aktualizacji, zapewniane są zarówno autentyczność, jak i spójność stosownych plików. W przypadku wykrycia nieprawidłowości podczas procesu, jest on automatycznie przerywany, by zachować spójność samego podzespołu. Zmodyfikowane wersje oprogramowania, oprogramowanie szpiegowskie lub inne pakiety danych nie zostały podpisane przez Siemens, wobec czego nie zostaną uruchomione na podzespole.
   Siemens wspiera także tę funkcjonalność dla następujących modułów sterowania zdalnego:
   SIMATIC CP 1243-1, CP 1243-8 IRC, CP 1243-7 LTE, CP 1542SP-1 IRC, TIM 1531 IRC oraz RTU3000C.

2. **Bezpieczna transmisja e-mail poprzez zabezpieczone połączenia**
   Do przesyłania informacji z podzespołu automatyzacji, np. modułu sterowania zdalnego SIMATIC RTU3000C, do zdefiniowanego odbiorcy przy zachowaniu poufności, zalecane jest korzystanie z szyfrowanego połączenia. Przy pomocy uprzednio zaimportowanego cyfrowego certyfikatu możliwe jest szyfrowanie e-maili wysyłanych poprzez STARTTLS. Pozwala to na bezpieczne przesłanie krytycznych zdarzeń systemu oraz komunikatów diagnostycznych i danych procesu do żądanego odbiorcy. Oprócz szyfrowanej transmisji, możliwe jest zabezpieczenie hasłem skompresowanych załączników. Pozwala to na celowe ograniczenie dostępu do przesyłanych danych, zależnie od aplikacji i obszaru odpowiedzialności.
   Siemens wspiera także tę funkcjonalność dla następujących modułów sterowania zdalnego:
   SIMATIC CP 1243-1, CP 1243-8 IRC, CP 1243-7 LTE, CP 1542SP-1 IRC, TIM 1531 IRC oraz RTU3000C.

3. **Bezpieczne szyfrowanie na całej drodze przesyłu przy pomocy OpenVPN/IPsec**
   Do bezpiecznej komunikacji ze zdalnym komponentem służy transmisja po wirtualnej sieci prywatnej (VPN). Za sprawą autoryzacji uczestników opartej na certyfikatach oraz szyfrowaniu na całej drodze przesyłu, możliwa jest także bezpieczna transmisja informacji i konfiguracji po sieci publicznej. Dzięki zastosowaniu OpenVPN możliwe jest nawiązanie bezpiecznego połączenia tunelowego pomiędzy SIMATIC RTU3000C a dowolnym serwerem OpenVPN. Poprzez takie połączenie można przesyłać nie tylko protokoły sterowania zdalnego, ale także konfiguracje, aktualizacje oprogramowania, synchronizację czasu oraz informacje rejestru. W połączeniu z rozwiązaniami połączenia zdalnego SINEMA od Siemens, zastosowanie OpenVPN pozwala na ustanowienie kompleksowego rozwiązania zdalnego dostępu ze szczegółową ochroną dostępu.
   Siemens wspiera także tę funkcjonalność dla następujących modułów sterowania zdalnego:
   SIMATIC CP 1243-1, CP 1243-8 IRC, CP 1243-7 LTE, CP 1542SP-1 IRC, TIM 1531 IRC w połączeniu z wyposażeniem bezpieczeństwa Siemens oraz RTU3000C.

4. **Zdarzenia bezpieczeństwa pozwalają na śledzenie zdarzeń systemowych związanych z bezpieczeństwem**
   Aby utrzymać przejrzystość czynności związanych z bezpieczeństwem w obrębie całej sieci oraz na poszczególnych urządzeniach końcowych, podzespoły systemowe, takie jak CP 1243-8 IRC, obsługują rejestrowanie tzw. zdarzeń bezpieczeństwa. Dzięki tym zarejestrowanym zdarzeniom możliwe jest śledzenie nieupoważnionych zmian w konfiguracji, dostępu do systemu lub naruszeń integralności. Uwzględniając aktualne przepisy o ochronie danych, zarejestrowane zdarzenia można przesłać do aplikacji bezpieczeństwa wyższego poziomu oraz systemów analizy/archiwizacji, korzystając z Syslog. W połączeniu z bezpiecznym szyfrowaniem połączenia, zdarzenia są przesyłane do żądanych odbiorów w zabezpieczony sposób.
   Siemens wspiera także tę funkcjonalność dla następujących modułów sterowania zdalnego:
   SIMATIC CP 1243-1, CP 1243-8 IRC, CP 1243-7 LTE, CP 1542SP-1 IRC, TIM 1531 IRC w połączeniu z wyposażeniem bezpieczeństwa Siemens do komórek sieci oraz RTU3000C.

Cyberbezpieczeństwo

5. **Ograniczony obszar ataku poprzez dezaktywację nieużywanych usług**
   Aby utrzymać możliwie najmniejszy obszar podatny na atak w środowisku procesowym możliwe jest stałe dezaktywowanie nieużywanych lub zbędnych usług sieciowych, korzystając ze stosownych interfejsów konfiguracyjnych. Przykładowo, dostęp do zarządzania podzespołem opartego na sieci można ograniczyć do bezpiecznego protokołu HTTPS. Żądania po niezabezpieczonym wariancie HTTP są przekazywane do HTTPS lub odrzucane.
   Siemens stosuje to podejście we wszystkich produktach SIMATIC do sterowania zdalnego.

6. **Zabezpieczenie podzespołów jako część konceptu „obrony w głąb"**
   Aby zabezpieczyć system automatyzacji w sposób kompleksowy przed cyberatakami, należy skonfigurować go zgodnie z zaleceniami normy IEC 62443 jako część konceptu obrony w głąb. W przypadku podstawowego zabezpieczenia sieci, firma Siemens oferuje rozległe portfolio, dzięki któremu możliwa jest ochrona systemów w sposób modułowy i oparty na rzeczywistych potrzebach. Przykładowo, dzięki SCALANCE S, dostępne są urządzenie bezpieczeństwa przemysłowego, pozwalające na kontrolowanie i monitorowanie ruchu danych do i z chronionej komórki sieci. Koncept ten pozwala na połączenie różnych środków bezpieczeństwa i tym samym zabezpieczenie nie tylko „wszerz", lecz również „w głąb".

   Więcej informacji o koncepcie ochrony „obrona w głąb" od Siemens można znaleźć pod adresem:
   www.siemens.com/industrialsecurity

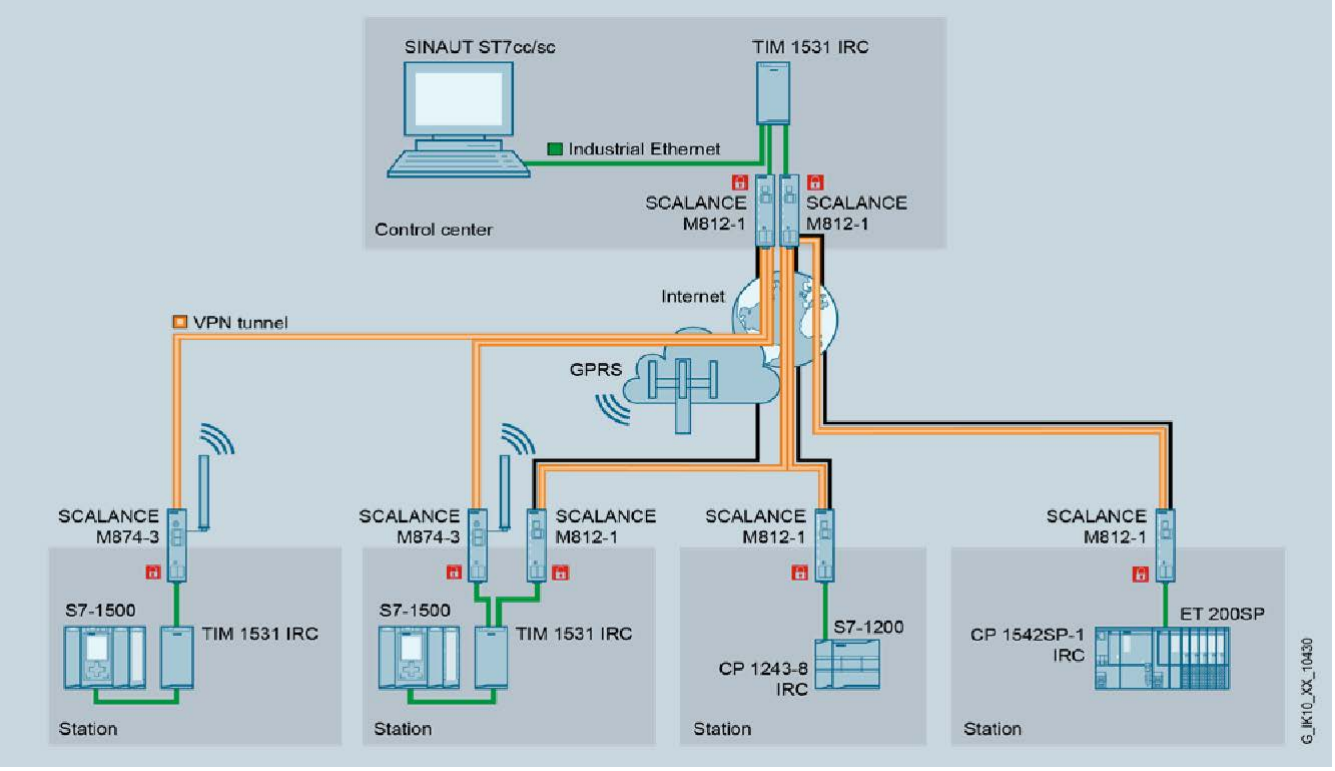
2.3 Analiza systemowa zgodnie z IEC 62443-3

W oparciu o koncept modułowej i zależnej od rzeczywistych potrzeb ochrony, rozwiązanie dla całego systemu lub obiektu może kompensować pewne brakujące właściwości techniczne poszczególnych podzespołów. Jeśli, przykładowo, komponent automatyzacji nie jest wyposażony w zintegrowaną funkcjonalność zapory sieciowej, może zostać ona zapewniona przez urządzenie bezpieczeństwa przemysłowego wyższego stopnia, takie jak SCALANCE S stojące powyżej SIMATIC TIM 1531 IRC, dzięki czemu połączenie tych podzespołów spełnia wymagania dotyczące bezpieczeństwa przemysłowego. W obrębie sieci systemu automatyzacji może występować wielka różnorodność kombinacji opcji tworzenia sieci.

W celu wsparcia koncepcji utworzenia bezpiecznych rozwiązań automatyzacji, Siemens udostępnia udokumentowane konfiguracje próbne (projekty), które zostały sporządzone zgodnie z normą IEC 62443 i tym samym stanowią bezpieczne rozwiązanie z perspektywy IT/OT. Dostępna jest dokumentacja oparta na systemach Siemens SCADA SIMATIC WinCC PROFESSIONAL/TIA, WinCC V7 oraz WinCC Open Architecture, a także oparta na systemach sterowania Siemens SIMATIC PCS 7.

Jako część konfiguracji próbnej, poniższa ilustracja przedstawia przykład bezpiecznej konfiguracji sterowania zdalnego, opartego na portfolio SIMATIC od firmy Siemens. Jednostki zdalnego dostępu (RTU), a także stacja nadrzędna w sterowni składają się ze sterowników rodziny SIMATIC S7-1200 (sterownik Basic), ET 200SP (sterownik rozproszony) oraz S7-1500 (sterownik Advanced). Połączenie ze sterownią odbywa się poprzez sieć publiczną przy użyciu modułów sterowania zdalnego SIMATIC oraz routerów przemysłowych SCALANCE (DSL i sieci komórkowe). Bezpieczne połączenia ze stacji do centralnej sterowni są wykonywane poprzez tunele VPN (OpenVPN). Funkcje bezpieczeństwa są wykonywane bezpośrednio przez moduł sterowania zdalnego lub w połączeniu z urządzeniami SCALANCE.

https://www.siemens.de/telecontrol



Bezpieczne rozwiązanie zdalnego sterowania z użyciem

Cyberbezpieczeństwo

3. Stała aktywność: Powiadomienia i aktualizacje bezpieczeństwa przemysłowego

Zagadnienie bezpieczeństwa przemysłowego to bardzo dynamiczne i złożone środowisko. Produkty, systemy, a także technologie, które dziś są uznawane za bezpieczne, jutro mogą być już przestarzałe i niebezpieczne. Dlatego konieczne jest stałe monitorowanie i dostosowywanie środków bezpieczeństwa, by stosowane produkty były zawsze aktualne w zakresie bezpieczeństwa. W tym celu „Siemens ProductCERT" analizuje wszystkie wykryte i zgłoszone problemy związane z bezpieczeństwem w produktach, rozwiązaniach i usług firmy Siemens – po czym publikuje zalecenia dotyczące stwierdzonych słabych punktów zabezpieczeń. Zalecenia dotyczące bezpieczeństwa zawierają informacje o sposobie postępowania ze słabymi punktami i zapewniają niezbędne kroki do bezpiecznej obsługi produktów i rozwiązań firmy Siemens. Często oferowane są aktualizacje programu lub oprogramowania sprzętowego bądź podjęcie odpowiednich działań. Możliwe jest zapisanie się do porad dotyczących bezpieczeństwa i wyświetlania ich przy pomocy kanału RSS, by użytkowane produkty Siemens były zawsze aktualne.

Więcej informacji:
https://new.siemens.com/global/de/produkte/services/cert.html#Benachrichtigungen

4. Ocena bezpieczeństwa zgodnie z IEC 62443 / ISO 27001 ze strony Siemens

Aby móc przestrzegać i wprowadzać w życie wszystkie istotne punkty oraz środki dla bezpieczeństwa teleinformatycznego i bezpiecznego działania obiektu, zalecana jest kompleksowa analiza bezpieczeństwa. Analiza bezpieczeństwa ze strony firmy Siemens obejmuje kontrolę i analizę wszystkich aspektów bezpieczeństwa w obiektach produkcyjnych. Przeprowadzona ocena zapewnia przejrzystość i przedstawia kompleksowy przegląd rzeczywistego stanu bezpieczeństwa systemu automatyzacji. Jest to warunek wstępny do rozpoznania konieczności działania w zakresie bezpieczeństwa przemysłowego oraz podjęcia środków w celu wyeliminowania luk w bezpieczeństwie.

Oceny opierają się na normach IEC 62443 lub ISO 27001. Analizie podlegają aspekty takie jak architektura sieci obiektu, przepływ danych, systemy produkcyjne oraz procesy, a także sami pracownicy:

- Kontrola bezpieczeństwa przemysłowego:
  Wynikiem jest raport z zaleceniami dotyczącymi środków do zmniejszenia ryzyka.
- Ocena IEC 62443 / ISO 27001:
  Wynikiem jest raport z zaleceniami dotyczącymi eliminacji zidentyfikowanych luk w bezpieczeństwie.
- Ocena ryzyka i podatności na uszkodzenia:
  W tym kroku zagrożenia są identyfikowane, analizowane, klasyfikowane i oceniane. Stanowi to podstawę do stworzenia mapy drogowej opartej na ryzyku i zależnej od bezpieczeństwa danego obiektu, która jest dostosowywana do klienta i jego placówki - zapewniając wszechstronny i jednolity poziom bezpieczeństwa.

Kontakt:
www.siemens.de/industrial-security-services

5. Podumowanie

Holistyczne podejście systemowe jest niezbędne w przypadku bezpieczeństwa teleinformatycznego oraz ochrony przed atakami na maszyny i obiekty w infrastrukturze publicznej, zwłaszcza gdy chodzi o ochronę infrastruktury krytycznej, np. przemysłu wodociągowego i kanalizacyjnego. Z tego względu norma IEC 62443 stała się głównym wyznacznikiem zasad.

Oprócz właściwości produktu związanych z bezpieczeństwem, w tym certyfikowanego procesu produkcji produktu, integratorzy systemów, a także operatorzy obiektów są szczególnie zobowiązani do zapewnienia zgodności z wymogami dotyczącymi bezpieczeństwa narzucanymi np. przez BSI. Firma Siemens oferuje kompletną gamę rozwiązań oraz usług pozwalających na określenie słabych punktów i wzmocnienie obiektu, by - oprócz faktycznej funkcjonalności - spełniały także wszystkie przyszłe wymogi bezpieczeństwa.

www.siemens.de/industrial-security

6. Źródła

[1] Zestaw reguł DWA: Broszura DWA-M 1060, bezpieczeństwo teleinformatyczne – standard przemysłowy dla wodociągów/kanalizacji (Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e.V. [Niemieckie Zrzeszenie Gospodarki Wodnej, Ścieków i Odpadów – Stowarzyszenie zarejestrowane]: DWA), 08/2017. [https://www.dwa.de]

[2] Zestaw reguł DVGW: Nota techniczna - broszura, DVGW W 1060 (M), bezpieczeństwo teleinformatyczne – standard przemysłowy dla wodociągów/kanalizacji (Deutscher Verein des Gas- und Wasserfaches e.V. [Niemieckie Zrzeszenie Aplikacji branży gazowej i gospodarki wodnej – Stowarzyszenie zarejestrowane]), 08/2017. [https://www.dvgw-regelwerk.de]

Dodatkowe informacje

Opublikowane przez Siemens AG

Digital Industries
P.O. Box 48 48
90026 Norymberga,
Niemcy

Article No. DIFA-B10092-00-7600

Z zastrzeżeniem zmian i błędów. Informacje zawarte w niniejszym dokumencie zawierają jedynie ogólne opisy i/lub cechy wydajności, które w przypadku faktycznego użytkowania nie zawsze mają zastosowanie zgodne z opisem lub mogą ulec zmianie w wyniku dalszego rozwoju produktów.
Żądane właściwości użytkowe są wiążące tylko w przypadku wyraźnego uzgodnienia w umowie.

Uwagi dotyczące bezpieczeństwa

Siemens zapewnia produkty i rozwiązania o funkcjach bezpieczeństwa przemysłowego wspierające bezpieczną pracę instalacji, rozwiązań, maszyn, wyposażenia i/lub sieci. Stanowią one ważne składniki holistycznego podejścia do bezpieczeństwa przemysłowego. Mając to na uwadze, produkty i rozwiązania Siemens są stale rozwijane.
Firma Siemens zaleca regularne kontrole aktualizacji produktów.

Aby zapewnić bezpieczne działanie produktów i rozwiązań Siemens, konieczne jest zastosowanie odpowiednich działań profilaktycznych (np. koncept ochrony komórki) oraz zintegrowanie poszczególnych podzespołów w ogólny koncept bezpieczeństwa przemysłowego najnowszej generacji. Należy również uwzględnić zastosowane produkty firm trzecich. Aby uzyskać więcej informacji na temat bezpieczeństwa przemysłowego, wejdź na:

www.siemens.com/industrial-security

Aby otrzymywać informacje o aktualizacjach produktów niezwłocznie po ich opublikowaniu, zapisz się na newsletter produktowy. Aby uzyskać więcej informacji, wejdź na:

http://support.automation.siemens.com