Kancelaria Prezesa
Rady Ministrów

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA
NSC 800-82 wer. 1.0

21 grudnia 2022

Przewodnik w zakresie bezpieczeństwa systemów sterowania przemysłowego

Systemy kontroli nadzorczej i pozyskiwania danych (SCADA), rozproszone systemy sterowania (DCS) oraz inne konfiguracje systemów sterowania, takie jak programowalne sterowniki logiczne (PLC)

Publikacja dostępna pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

DEPARTAMENT CYBERBEZPIECZEŃSTWA

PREAMBUŁA

Szanowni Państwo,

oddajemy w Państwa ręce zestaw publikacji specjalnych - Narodowe Standardy Cyberbezpieczeństwa, o których mowa w interwencji 2.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń. Standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST) i posiadają mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, na których oparte jest zarządzanie bezpieczeństwem informacji w podmiotach krajowego systemu cyberbezpieczeństwa.

Standardy stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę stosowaną w tym zakresie w administracji federalnej USA.

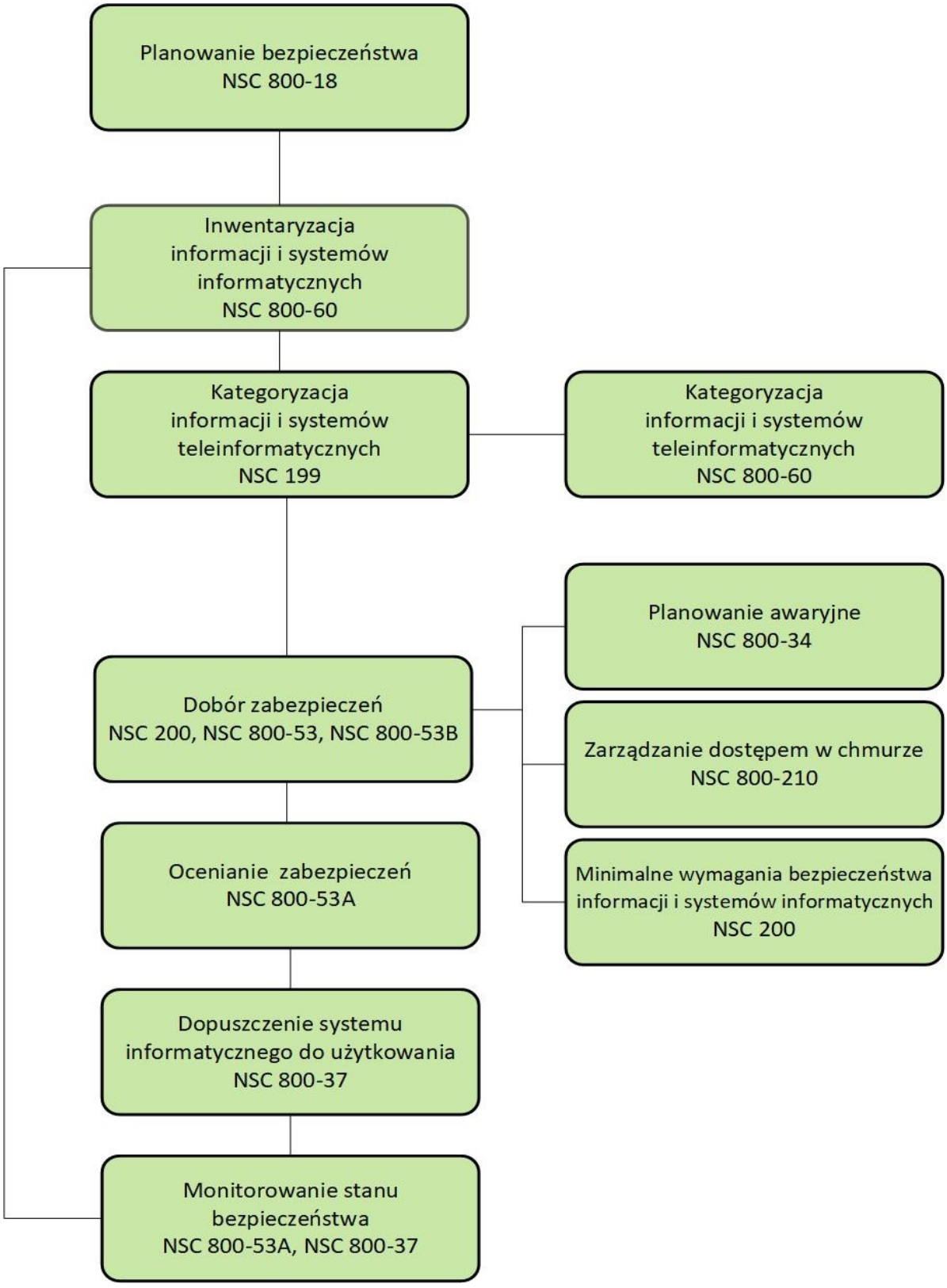
Zestaw publikacji specjalnych obejmuje następujące pozycje:

- NSC 199, Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199.
- NSC 200, Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200.
- NSC 800-18, Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych – na podstawie NIST SP 800-18.
- NSC 800-30, Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30.
- NSC 800-34, Poradnik planowania awaryjnego – na podstawie NIST SP 800-34.
- NSC 800-37, Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37.
- NSC 800-39, Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39.

- NSC 800-53, Zabezpieczenia i ochrona prywatności w systemach informacyjnych oraz organizacjach – na podstawie NIST SP 800-53.
- NSC 800-53A, Ocenianie środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych oraz organizacjach. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A.
- NSC 800-53B, Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B.
- NSC 800-60, Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60.
- NSC 800-61, Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61.
- NSC 800-210, Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej – na podstawie NIST SP 800-210.

W oparciu o te publikacje można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę.

Cykl zarządzania bezpieczeństwem informacji bazujący na publikacjach NIST wykorzystuje następujące dokumenty:



Cykl zarządzania bezpieczeństwem informacji

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował szereg standardów i wytycznych w celu zapewnienia jednolitego podejścia do problematyki bezpieczeństwa informacji i systemów informacyjnych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji i systemów informacyjnych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością działalności i majątku organizacji, osób fizycznych i państwa. Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informacyjnych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych. Dzięki jednolitemu podejściu do zarządzania ryzykiem ułatwia także wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznym i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (m. in. ISO[1]), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania tych innych standardów.

Publikacje NIST co do zasady nie są objęte restrykcjami wynikającymi z autorskich praw majątkowych. Są powszechnie dostępne oraz dopuszczone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejściem do zagadnień związanych z bezpieczeństwem informacji i systemów informacyjnych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem.

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST, jako godne zaufania i rekomendują stosowanie ich przez polskie

[1] International Organization for Standardization (ISO) - Międzynarodowa Organizacja Normalizacyjna– organizacja pozarządowa zrzeszająca krajowe organizacje normalizacyjne.

podmioty przy opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

Podmioty, urządzenia lub materiały prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Celem ich wskazania nie jest nakłanianie do korzystania z ww. podmiotów, urządzeń lub materiałów lub ich poparcie. Wskazanie ich nie ma również na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w danej dziedzinie.

W niniejszej publikacji mogą znajdować się odniesienia do innych opracowywanych przez nas publikacji. Informacje tu zawarte, w tym koncepcje, praktyki i metodologie, mogą być wykorzystywane przez organizacje jeszcze przed ukończeniem innych towarzyszących temu standardowi publikacji. W związku z tym, do czasu ukończenia każdej publikacji powinny obowiązywać dotychczasowe wymagania, wytyczne i procedury, jeśli takie istnieją. W ramach planowanych przez Państwa prac zalecamy śledzenie naszych prac publikacyjnych.

Aktualne informacje o prowadzonych przez nas pracach dostępne są pod adresem:

 Narodowe Standardy Cyberbezpieczeństwa

Jesteśmy również otwarci na wszelkie Państwa sugestie, które pomogą nam w dalszych pracach nad standardami cyberbezpieczeństwa i zachęcamy do kontaktu.

 +48222455922

 sekretariat.dc@mc.gov.pl

Niniejsza publikacja NSC 800-82, ***Przewodnik w zakresie bezpieczeństwa systemów sterowania przemysłowego***, została opracowana za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-82 rev. 2, *Guide to Industrial Control Systems (ICS) Security*.

Tam, gdzie to było możliwe i nie budziło kontrowersji, nazwy ról i kluczowych uczestników procesu zarządzania ryzykiem zostały podane w języku polskim. Pozostałe role i funkcje zostały przedstawione w języku angielskim. Do wszystkich tych ról / funkcji zastosowano akronimy terminologii angielskiej.

Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie NSC 7298, ***Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa***.

Spis treści

Spis ilustracji

Spis tabel

STRESZCZENIE

Niniejszy dokument zawiera rekomendacje dotyczące bezpieczeństwa systemów sterowania przemysłowego (*ang. Industrial Control Systems - ICS*) obejmujące systemy kontroli nadzorczej i pozyskiwania danych (*ang. Supervisory Control and Data Acquisition - SCADA*), rozproszone systemy sterowania (*ang. Distributed Control Systems - DCS*) oraz inne konfiguracje systemów sterowania, takie jak programowalne sterowniki logiczne (*ang. Programmable Logic Controllers - PLC*), które są często spotykane w sektorach sterowania przemysłowego.

ICS są zwykle używane w branży elektrycznej, wodnokanalizacyjnej, ropy naftowej i gazu ziemnego, transportowej, chemicznej, farmaceutycznej, celulozowo-papierniczej, żywnościowej oraz produkcji jednostkowej (np. motoryzacyjna, lotnicza i środków trwałych).

Systemy SCADA są zwykle używane do sterowania rozproszonymi aktywami przy użyciu scentralizowanej akwizycji danych i kontroli nadzorczej.

Systemy DCS są generalnie wykorzystywane do sterowania systemami produkcyjnymi w obrębie lokalnego obszaru, takiego jak fabryka, przy użyciu środków nadzorczych i regulacyjnych.

Sterowniki PLC są generalnie używane do sterowania dyskretnego w konkretnych zastosowaniach i zapewniają sterowanie regulacyjne. Systemy sterowania są niezbędne do funkcjonowania przemysłu oraz infrastruktur krytycznych, które często są w dużym stopniu połączone i wzajemnie zależne. Należy zauważyć, że znaczna część krajowej infrastruktury krytycznej jest własnością prywatną i jest eksploatowana przez podmioty prywatne. Podmioty realizujące zadania publiczne również obsługują wiele z wyżej wymienionych systemów ICS i obejmują na przykład kontrolę ruchu lotniczego lub obsługę logistyki (np. obsługę sortowanie przesyłek pocztowych, obsługę magazynów).

Niniejszy dokument zawiera przegląd tych systemów ICS i typowych topologii tych systemów, identyfikuje typowe zagrożenia i podatności oraz przedstawia zalecane środki bezpieczeństwa w celu zmniejszenia związanego z nimi poziomów ryzyka.

Początkowo ICS w niewielkim stopniu przypominały tradycyjne systemy informacyjne (*ang. information technology - IT*), ponieważ były to odizolowane systemy wykorzystujące zastrzeżone protokoły sterowania przy użyciu specjalistycznego sprzętu i oprogramowania (a jeszcze wcześniej przekaźników elektromagnetycznych – skąd wywodzi się kod drabinkowy, jeszcze niekiedy wykorzystywany do programowania PLC). Wiele komponentów ICS znajdowało się w fizycznie zabezpieczonych obszarach i elementy te nie były połączone z sieciami lub systemami informacyjnymi. Powszechnie dostępne, tanie urządzenia wykorzystujące protokół internetowy (*ang. Internet Protocol - IP*) zastępują obecnie rozwiązania dedykowane do specyficznego zastosowania, co zwiększa prawdopodobieństwo wystąpienia luk i incydentów w zakresie cyberbezpieczeństwa. Ponieważ ICS przyjmują rozwiązania informacyjne w celu zapewnienia łączności z korporacyjnymi systemami biznesowymi i możliwości zdalnego dostępu, a także są projektowane i wdrażane z wykorzystaniem standardowych komputerów, systemów operacyjnych (*ang. operating systems - OS*) i protokołów sieciowych, zaczynają przypominać systemy informacyjne. Integracja ta wspiera nowe możliwości IT, ale zapewnia znacznie mniejszą izolację ICS od świata zewnętrznego niż poprzednie systemy, co stwarza większą potrzebę zabezpieczenia tych systemów. Coraz częstsze korzystanie z sieci bezprzewodowych naraża wdrożenia ICS na większe ryzyko ze strony przeciwników, którzy znajdują się w stosunkowo bliskiej odległości, ale nie mają bezpośredniego fizycznego dostępu do sprzętu. O ile rozwiązania w zakresie bezpieczeństwa zostały opracowane z myślą o rozwiązaniu tych problemów w typowych systemach informacyjnych, o tyle przy wprowadzaniu tych samych rozwiązań do środowisk ICS należy zachować szczególne środki ostrożności. W niektórych przypadkach potrzebne są nowe rozwiązania w zakresie bezpieczeństwa, dostosowane do środowiska ICS.

Mimo podobieństwa niektórych cech, ICS posiadają również cechy różniące je od tradycyjnych systemów przetwarzania informacji. Wiele z tych różnic wynika z faktu, że logika wykonywana w ICS ma bezpośredni wpływ na otaczającą nas rzeczywistość. Niektóre z tych cech charakteryzują się znacznym zagrożeniem dla zdrowia i bezpieczeństwa ludzi oraz poważnymi szkodami dla środowiska naturalnego, a także istotnymi reperkusjami finansowymi, takimi jak straty w produkcji, negatywny wpływ

na gospodarkę narodową oraz ujawnienie informacji podlegających prawu własności intelektualnej. ICS mają wyjątkowe wymagania dotyczące wydajności i niezawodności i często wykorzystują systemy operacyjne i aplikacje, które mogą być uznane za niekonwencjonalne przez typowy personel IT. Ponadto, cele bezpieczeństwa i wydajności czasami kolidują między sobą w projektowaniu i działaniu systemów sterowania.

Programy cyberbezpieczeństwa ICS powinny być zawsze częścią szerszych programów bezpieczeństwa i niezawodności ICS zarówno w zakładach przemysłowych, jak i programów cyberbezpieczeństwa przedsiębiorstw, ponieważ cyberbezpieczeństwo jest niezbędne do bezpiecznego i niezawodnego działania nowoczesnych procesów przemysłowych. Zagrożenia systemów sterowania mogą pochodzić z wielu źródeł, w tym z wrogich państw, grup terrorystycznych, niezadowolonych pracowników, złośliwych intruzów, zawiłości procesów produkcyjnych, wypadków i klęsk żywiołowych, a także złośliwych lub przypadkowych działań osób wewnętrznych. Cele bezpieczeństwa ICS są zazwyczaj zgodne z priorytetem dostępności i integralności, a dopiero w dalszej kolejności poufności.

Możliwe incydenty, które mogą dotyczyć ICS, są następujące:

- Zablokowany lub opóźniony przepływ informacji przez sieci ICS, co może zakłócić działanie ICS.
- Nieuprawnione zmiany instrukcji, poleceń lub progów alarmowych, które mogłyby spowodować uszkodzenie, wyłączenie sprzętu, oddziaływanie na środowisko i/lub zagrożenie życia ludzkiego.
- Niepoprawne informacje wysyłane do operatorów systemu, albo w celu ukrycia nieautoryzowanych zmian, albo w celu skłonienia operatorów do podjęcia niewłaściwych działań, które mogą mieć różne negatywne skutki.
- Zmodyfikowane oprogramowanie ICS lub ustawienia konfiguracyjne lub oprogramowanie ICS zainfekowane złośliwym oprogramowaniem, co może mieć różne negatywne skutki.

- Zakłócanie działania systemów zabezpieczeń sprzętu, co może zagrażać urządzeniom kosztownym i trudnym do wymiany.
- Zakłócanie działania systemów bezpieczeństwa, które może zagrażać życiu ludzkiemu.

Główne cele bezpieczeństwa odnoszące się do ICS powinny obejmować następujące elementy:

- **Ograniczenie logicznego dostępu do sieci ICS i aktywności sieciowej.** Obejmuje to, przykładowo, stosowanie jednokierunkowych bram (diod danych), architektury sieciowej strefy zdemilitaryzowanej (DMZ) z zaporami sieciowymi (może to zapobiec bezpośredniemu przechodzeniu ruchu sieciowego między sieciami korporacyjnymi i ICS) oraz posiadanie oddzielnych mechanizmów uwierzytelniania i poświadczeń dla użytkowników sieci korporacyjnych i sieci ICS. System ICS powinien również korzystać z wielowarstwowej topologii sieci, w której najbardziej krytyczna komunikacja odbywa się w najbardziej bezpiecznej i niezawodnej warstwie.
- **Ograniczenie fizycznego dostępu do sieci i urządzeń systemu ICS.** Nieuprawniony dostęp fizyczny do komponentów może spowodować poważne zakłócenia w funkcjonowaniu systemu ICS. Należy stosować kombinację fizycznych środków kontroli dostępu, takich jak zamki, czytniki kart i/lub personel ochrony.
- **Ochrona poszczególnych komponentów ICS przed exploitami.** Obejmuje to wdrażanie poprawek bezpieczeństwa w możliwie najszybszy sposób, po przetestowaniu ich w warunkach roboczych; wyłączenie wszystkich nieużywanych portów i usług oraz zapewnienie, że pozostaną one wyłączone; ograniczenie uprawnień użytkowników ICS tylko do tych, które są wymagane dla roli każdej osoby; śledzenie i monitorowanie ścieżek audytu; oraz stosowanie środków bezpieczeństwa, takich jak oprogramowanie antywirusowe i oprogramowanie do sprawdzania integralności plików, tam gdzie jest to technicznie wykonalne, w celu zapobiegania, powstrzymywania, wykrywania i ograniczania szkodliwego oprogramowania (*ang. malware*).

- **Ograniczenie nieautoryzowanej modyfikacji danych.** Obejmuje to dane w tranzycie (przynajmniej przez granice sieci) i w spoczynku.
- **Wykrywanie zdarzeń i incydentów bezpieczeństwa.** Wykrywanie zdarzeń bezpieczeństwa, które jeszcze nie przerodziły się w incydenty, może pomóc atakowanym przerwać łańcuch ataku, zanim napastnicy osiągną swoje cele. Obejmuje to zdolność do wykrywania uszkodzonych komponentów ICS, niedostępnych usług i wyczerpanych zasobów, które są ważne dla zapewnienia prawidłowego i bezpiecznego funkcjonowania ICS.
- **Utrzymanie funkcjonalności w niekorzystnych warunkach.** Wymaga to zaprojektowania systemu ICS w taki sposób, aby każdy krytyczny komponent miał swój redundantny odpowiednik. Dodatkowo, w przypadku awarii komponentu, powinien on ulec awarii w sposób, który nie generuje niepotrzebnego ruchu w ICS lub innych sieciach lub nie powoduje problemu w innym miejscu, takiego jak zdarzenie kaskadowe. ICS powinien również umożliwiać stopniową degradację, taką jak przejście od "normalnej pracy" z pełną automatyzacją do "pracy awaryjnej" (z większym zaangażowaniem operatorów i ograniczoną automatyzacją), do "pracy ręcznej" bez automatyzacji.
- **Przywracanie systemu po wystąpieniu incydentu.** Wymagane jest opracowanie planu reagowania na incydenty, ponieważ występowanie incydentów jest nieuniknione. Główną cechą dobrego programu bezpieczeństwa jest szybkość przywracania systemu po wystąpieniu incydentu.

W celu właściwego podejścia do kwestii bezpieczeństwa w ICS, konieczne jest, aby wielofunkcyjny zespół ds. cyberbezpieczeństwa dzielił się swoją różnorodną wiedzą i doświadczeniem w celu oceny i ograniczania ryzyka odnoszącego się do ICS. Zespół ds. cyberbezpieczeństwa powinien składać się co najmniej z członka personelu informacyjnego organizacji, inżyniera sterowania, operatora systemu sterowania, eksperta ds. bezpieczeństwa sieci i systemu, członka kadry zarządzającej oraz członka działu bezpieczeństwa fizycznego. Dla zapewnienia ciągłości i kompletności, zespół ds. cyberbezpieczeństwa powinien skonsultować się również z dostawcą systemu sterowania i/lub integratorem systemu. Zespół ds. bezpieczeństwa cybernetycznego

powinien ściśle współpracować z zarządcą obiektu (np. kierownikiem obiektu) oraz CIO, CSO [2], którzy ponoszą pełną odpowiedzialność za cyberbezpieczeństwo systemu ICS oraz za wszelkie incydenty związane z bezpieczeństwem, niezawodnością lub uszkodzeniem sprzętu, spowodowane bezpośrednio lub pośrednio przez cyberincydenty. Skuteczny program cyberbezpieczeństwa ICS powinien stosować strategię znaną jako „obrona w głąb" (*ang. „defense-in-depth"*), polegającą na warstwowym stosowaniu mechanizmów bezpieczeństwa w taki sposób, aby zminimalizować wpływ awarii jednego z mechanizmów. Organizacje nie powinny polegać na zasadzie „bezpieczeństwo przez niejawność" (*ang. „security by obscurity"*).

W typowym systemie ICS oznacza to strategię "obrona w głąb", która obejmuje:

- Opracowanie zasad (polityki) bezpieczeństwa, procedur, materiałów szkoleniowych i edukacyjnych, które mają zastosowanie konkretnie do ICS.
- Rozważanie zasad i procedur bezpieczeństwa ICS w oparciu o poziom zagrożenia komunikowany przez właściwe organy rządowe, wdrażanie coraz bardziej zaostrzonych procedur bezpieczeństwa w miarę wzrostu poziomu zagrożenia.
- Uwzględnienie kwestii bezpieczeństwa w całym cyklu życia ICS, od projektu architektury, poprzez zamówienia, instalację, konserwację, aż po wycofanie z eksploatacji.
- Wdrożenie topologii sieci ICS, która ma wiele warstw, z najbardziej krytyczną komunikacją odbywającą się w najbardziej bezpiecznej i niezawodnej warstwie.
- Zapewnienie logicznej separacji między sieciami korporacyjnymi i ICS (np. zapory sieciowe z filtrowaniem typu *Stateful Packet Inspection* (*Stateful Firewall*)[3], bramy jednokierunkowe).
- Zastosowanie architektury sieciowej DMZ (tzn. uniemożliwienie bezpośredniego ruchu pomiędzy sieciami korporacyjnymi i ICS).

[2] Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie NSC 7298, Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.

[3] Funkcja zapór sieciowych zwiększająca bezpieczeństwo w sieci LAN.

- Zapewnienie, że krytyczne komponenty są redundantne i znajdują się w redundantnych sieciach.
- Projektowanie systemów krytycznych pod kątem stopniowej degradacji (tolerancja uszkodzeń) w celu zapobiegania katastrofalnym zdarzeniom kaskadowym.
- Wyłączenie nieużywanych portów i usług w urządzeniach ICS po przeprowadzeniu testów w celu upewnienia się, że nie będzie to miało wpływu na działanie ICS.
- Ograniczenie fizycznego dostępu do sieci i urządzeń ICS.
- Ograniczenie uprawnień użytkowników ICS tylko do tych, które są wymagane do wykonywania pracy przez każdą osobę (tj. ustanowienie kontroli dostępu opartej na rolach i skonfigurowanie każdej roli w oparciu i zasadę najmniejszych uprawnień).
- Stosowanie oddzielnych mechanizmów uwierzytelniania i poświadczeń dla użytkowników sieci ICS i sieci korporacyjnej (tzn. konta sieci ICS nie korzystają z kont użytkowników sieci korporacyjnej).
- Wykorzystanie nowoczesnych technologii, takich jak karty inteligentne do weryfikacji tożsamości osobistej (*ang. Personal Identity Verification - PIV*).
- Wdrożenie środków bezpieczeństwa, tam gdzie jest to technicznie wykonalne, takich jak oprogramowanie wykrywające włamania, oprogramowanie antywirusowe i oprogramowanie sprawdzające integralność plików, w celu zapobiegania, powstrzymywania, wykrywania i ograniczania wprowadzania, narażania i rozprzestrzeniania złośliwego oprogramowania do/ wewnątrz / i z ICS.
- Stosowanie technik bezpieczeństwa, takich jak szyfrowanie lub haszowanie kryptograficzne, do przechowywania danych ICS i komunikacji, jeśli uznano to za stosowne.
- Szybkie wdrażanie poprawek bezpieczeństwa po przetestowaniu wszystkich poprawek w warunkach roboczych na systemie testowym, jeśli to możliwe, przed ich instalacją w ICS.
- Śledzenie i monitorowanie ścieżek audytu w krytycznych obszarach systemu ICS.

- Stosowanie w miarę możliwości niezawodnych i bezpiecznych protokołów i usług sieciowych.

National Institute of Standards and Technology (NIST), we współpracy ze społecznością ICS z sektora publicznego i prywatnego, opracował szczegółowe wytyczne dotyczące stosowania w odniesieniu do ICS zabezpieczeń zawartych w publikacji specjalnej NIST (SP) 800-53 rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations* [22]. Dokument ten rekomendowany jest do zastosowania w Polsce jako Narodowy Standard Cyberbezpieczeństwa NSC 800-53 wer. 2, *Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji*.

Podczas, gdy szereg zabezpieczeń zawartych w NIST SP 800-53 rev. 5 ma wprost zastosowanie do ICS, tak jak to zapisano w tym standardzie, to jednak wiele zabezpieczeń wymaga specyficznej dla ICS interpretacji i/lub rozszerzenia poprzez dodanie do zabezpieczenia jednego lub więcej z poniższych elementów:

- **Wytyczne uzupełniające dotyczące ICS** dostarczają organizacjom dodatkowych informacji na temat stosowania zabezpieczeń opisanych w NIST SP 800-53 i ich rozszerzeń w przypadku stosowania tych zabezpieczeń w ICS oraz środowisk, w których działają te wyspecjalizowane systemy. Wytyczne uzupełniające dostarczają również informacji o tym, dlaczego dane zabezpieczenie lub jego rozszerzenie może nie mieć zastosowania w niektórych środowiskach ICS i może podlegać dostosowaniu (tj. zastosowania wytycznych dotyczących zakresu i/lub zabezpieczeń kompensacyjnych). Wytyczne uzupełniające dotyczące ICS nie zastępują oryginalnych zabezpieczeń występujących w NIST SP 800-53, lecz je uszczegóławiają.
- **Wytyczne rozszerzające dotyczące ICS** , które zapewniają ulepszenia w stosunku do zabezpieczeń oryginalnych, które mogą być wymagane dla niektórych systemów ICS.
- **Wytyczne uzupełniające rozszerzenie dotyczące ICS**, które zawierają wytyczne dotyczące tego, w jaki sposób rozszerzone zabezpieczenie ma zastosowanie lub nie ma zastosowania w środowiskach ICS.

Najskuteczniejszą metodą zabezpieczenia ICS jest zebranie zalecanych praktyk branżowych i zaangażowanie się w proaktywny, wspólny wysiłek kierownictwa, inżyniera sterowania i operatora, organizacji IT oraz zaufanego doradcy ds. automatyki. Ten zespół powinien czerpać z bogactwa informacji dostępnych z bieżących działań rządowych, grup przemysłowych, dostawców i organizacji normalizacyjnych wymienionych w Załączniku D.

1. WSTĘP

1.1. Cel i zakres

Celem niniejszego dokumentu jest przedstawienie rekomendacji dotyczących bezpieczeństwa systemów sterowania przemysłowego (ICS), w tym systemów kontroli nadzorczej i pozyskiwania danych (SCADA), rozproszonych systemów sterowania (DCS) oraz innych systemów realizujących funkcje sterowania. Dokument zawiera ogólny zarys ICS, przegląd typowych topologii i architektury systemów, identyfikuje znane zagrożenia i podatności tych systemów oraz przedstawia zalecane środki zaradcze w celu zmniejszenia związanego z nimi ryzyka. Dodatkowo, przedstawiono nakładkę zabezpieczeń dostosowaną do ICS, opartą na NIST SP 800-53 Rev. 4[4] (polski standard: NSC 800-53 wer. 1) [22], w celu zapewnienia dostosowania zabezpieczeń do unikatowych cech domeny ICS. Struktura dokumentu dostarcza kontekstu dla nakładki, ale nakładka jest przeznaczona do samodzielnego wykonywania.

ICS są zwykle używane w branży elektrycznej, wodnokanalizacyjnej, ropy naftowej i gazu ziemnego, transportowej, chemicznej, farmaceutycznej, celulozowo-papierniczej, żywnościowej oraz produkcji jednostkowej (np. motoryzacyjna, lotnicza i środków trwałych). Ponieważ istnieje wiele różnych typów ICS i różnym poziomie potencjalnego ryzyka i wpływu, dokument ten zawiera listę wielu różnych metod i technik zabezpieczania ICS. Dokument ten nie powinien być wykorzystywany wyłącznie jako lista kontrolna do zabezpieczenia konkretnego systemu. Zachęca się czytelników do przeprowadzenia szacowania ryzyka w swoich systemach oraz do dostosowania zalecanych wytycznych i rozwiązań w celu spełnienia konkretnych wymogów bezpieczeństwa, biznesowych i operacyjnych. Zakres zastosowania podstawowych koncepcji zabezpieczania systemów sterowania przedstawionych w tym dokumencie stale się rozszerza.

[4] Nakładka zabezpieczeń oparta na NIST SP 800-53 Rev. 5 przedstawiona jest w NSC 800-53 wer. 2.

1.2. Grupa docelowa

Niniejszy dokument obejmuje szczegóły specyficzne dla ICS. Czytelnicy tego dokumentu powinni być zaznajomieni z ogólnymi koncepcjami bezpieczeństwa komputerowego oraz protokołami komunikacyjnymi używanymi w sieciach. Dokument ten ma charakter techniczny, jednak zapewnia on podstawy niezbędne do zrozumienia omawianych tematów..

Grupa docelowa jest zróżnicowana i obejmuje następujące osoby:

- Inżynierowie, integratorzy i architekci systemów sterowania, którzy projektują lub wdrażają bezpieczne systemy ICS.
- Administratorzy systemów, inżynierowie i inni specjaliści technologii informacyjnych (IT), którzy administrują, wprowadzają poprawki lub zabezpieczają ICS.
- Konsultanci ds. bezpieczeństwa, którzy przeprowadzają oceny bezpieczeństwa i testy penetracyjne ICS.
- Kierownicy, którzy są odpowiedzialni za ICS.
- Kierownictwo wyższego szczebla, które poszukuje możliwości zrozumienia implikacji i konsekwencji uzasadnienia i zastosowania programu cyberbezpieczeństwa ICS w celu złagodzenia wpływu na funkcjonowanie przedsiębiorstwa.
- Naukowcy i analitycy, którzy próbują zidentyfikować unikatowe potrzeby bezpieczeństwa ICS.
- Sprzedawcy opracowujący produkty, które zostaną wdrożone jako część systemu ICS.

1.3. Struktura dokumentu

Pozostała część niniejszej publikacji została podzielona na następujące główne rozdziały:

- W rozdziale 2 przedstawiono przegląd ICS, w tym porównanie ICS z systemami informacyjnymi.
- W rozdziale 3 przedstawiono omówienie zarządzania ryzykiem ICS i jego szacowanie.
- Rozdział 4 zawiera przegląd rozwoju i wdrożenia programu bezpieczeństwa ICS w celu ograniczenia ryzyka związanego z podatnościami zidentyfikowanymi w Załączniku C.
- Rozdział 5 zawiera zalecenia dotyczące integracji bezpieczeństwa z architekturami sieciowymi typowymi dla ICS, z naciskiem na praktyki segregacji sieci.
- W rozdziale 6 przedstawiono podsumowanie zabezpieczeń zarządczych, operacyjnych i technicznych zidentyfikowanych w publikacji specjalnej NIST SP 800-53 rev. 4 (NSC 800-53 wer. 1) oraz wstępne wytyczne dotyczące stosowania tych środków bezpieczeństwa w odniesieniu do ICS.

Dokument zawiera również poniższe załączniki z materiałami pomocniczymi:

- Załącznik a - przedstawia listę akronimów i skrótów użytych w niniejszym dokumencie.
- Załącznik B - zawiera słowniczek terminów używanych w niniejszym dokumencie.
- Załącznik C - przedstawia listę zagrożeń, podatności i incydentów związanych z ICS.
- Załącznik D - prezentuje wykaz działań związanych z bezpieczeństwem ICS.
- Załącznik E- zawiera wykaz możliwości i narzędzi w zakresie bezpieczeństwa ICS.
- Załącznik F - przedstawia listę odniesień wykorzystanych przy opracowywaniu niniejszego dokumentu.
- Załącznik G - zawiera nakładkę na ICS z wykazem środków bezpieczeństwa, rozszerzeń i dodatkowych rekomendacji, które mają zastosowanie w szczególności do ICS.

2. PRZEGLĄD SYSTEMÓW STEROWANIA PRZEMYSŁOWEGO

System sterowania przemysłowego (ICS) jest terminem ogólnym, który obejmuje kilka rodzajów systemów sterowania, w tym systemy kontroli nadzorczej i pozyskiwania danych (*SCADA*), rozproszone systemy sterowania (*DCS*) oraz inne konfiguracje systemów sterowania, takie jak programowalne sterowniki logiczne (*PLC*), które są często spotykane w sektorach sterowania przemysłowego.

ICS składa się z kombinacji komponentów sterujących (np. elektrycznych, mechanicznych, hydraulicznych, pneumatycznych), które działają razem, aby osiągnąć cel przemysłowy (np. produkcję, transport materii lub energii). Część systemu zajmująca się głównie wytwarzaniem produktu wyjściowego jest określana jako proces. Część kontrolna systemu obejmuje specyfikację pożądanego wyniku lub wydajności. Sterowanie może być w pełni zautomatyzowane lub może obejmować człowieka w pętli. Systemy mogą być skonfigurowane do działania w pętli otwartej, zamkniętej i w trybie ręcznym. W systemach sterowania z otwartą pętlą wyjście jest kontrolowane przez ustalone ustawienia. W systemach sterowania z zamkniętą pętlą wyjście ma wpływ na wejście w taki sposób, aby utrzymać pożądany cel. W trybie ręcznym system jest całkowicie kontrolowany przez człowieka. Część systemu zajmująca się głównie utrzymaniem zgodności ze specyfikacjami jest określana mianem kontrolera (lub sterowania). Typowy system ICS może zawierać liczne pętle sterowania, interfejsy człowiek-maszyna (*ang. Human Machine Interfaces - HMI*) oraz narzędzia zdalnej diagnostyki i konserwacji zbudowane z wykorzystaniem szeregu protokołów sieciowych. Mikroukłady sterujące procesami przemysłowymi są zwykle stosowane w przemyśle elektrycznym, wodno-kanalizacyjnym, paliwowym i gazowym, chemicznym, transportowym, farmaceutycznym, celulozowo-papierniczym, spożywczym i produkcji napojów oraz w produkcji jednostkowej (np. W przemyśle samochodowym, lotniczym i dóbr trwałych).

ICS mają kluczowe znaczenie dla funkcjonowania krajowych infrastruktur krytycznych, które często są w dużym stopniu połączone i wzajemnie zależne. Należy zauważyć, że znaczna część krajowej infrastruktury krytycznej jest własnością prywatną i jest eksploatowana przez podmioty prywatne. Podmioty realizujące zadania publiczne

również obsługują wiele z wyżej wymienionych procesów przemysłowych, jak również kontrolę ruchu lotniczego. Niniejszy rozdział zawiera przegląd systemów SCADA, DCS i PLC, łącznie z typowymi topologiami i komponentami. Aby ułatwić zrozumienie tych systemów, zaprezentowano kilka diagramów przedstawiających topologię sieci, połączenia, komponenty i protokoły typowe dla każdego systemu. Przykłady te stanowią jedynie próbę określenia pojęć topologii. Rzeczywiste implementacje ICS mogą być hybrydami, które zacierają granicę między systemami DCS i SCADA. Należy zauważyć, że diagramy w tej sekcji nie koncentrują się na zabezpieczeniu ICS. Architektura bezpieczeństwa i zabezpieczenia są omówione odpowiednio w rozdziałach 5 i 6 niniejszego dokumentu.

2.1. Ewolucja systemów sterowania przemysłowego

Wiele z dzisiejszych systemów ICS powstało w wyniku wprowadzenia funkcji informacyjnych do istniejących systemów fizycznych, często zastępując lub uzupełniając fizyczne mechanizmy sterowania. Na przykład, wbudowane cyfrowe układy sterowania zastąpiły analogowo-mechaniczne układy sterowania w maszynach wirujących i silnikach. Ulepszenia w zakresie kosztów i wydajności sprzyjały tej ewolucji, czego wynikiem jest wiele dzisiejszych "inteligentnych" technologii, takich jak inteligentna sieć elektryczna, inteligentny transport, inteligentne budynki i inteligentna produkcja. Chociaż zwiększa to powiązania i krytyczność tych systemów, stwarza to również większe zapotrzebowanie na ich zdolność do adaptacji, odporność, bezpieczeństwo i ochronę.

Inżynieria systemów ICS stale ewoluuje w celu zapewnienia nowych możliwości przy jednoczesnym zachowaniu typowego dla tych systemów długiego cyklu życia. Wprowadzenie możliwości informacyjnych do systemów fizycznych powoduje powstawanie nowych zachowań, które mają wpływ na bezpieczeństwo. Modele i analizy inżynieryjne ewoluują, aby uwzględnić te nowe właściwości, w tym współzależności w zakresie bezpieczeństwa, ochrony, prywatności i wpływu na środowisko.

2.2. Sektory przemysłowe związane z systemem ICS i ich współzależności

Systemy sterowania są stosowane w wielu różnych sektorach krytycznych, w tym w produkcji, dystrybucji i transporcie przemysłu i infrastrukturach.

2.2.1. Przemysł wytwórczy

Produkcja stanowi duży i zróżnicowany sektor przemysłowy z wieloma różnymi procesami, które można sklasyfikować jako produkcję opartą na *procesach i* produkcję *dyskretną*.

W przemyśle wytwórczym *opartym na procesach* produkcyjnych wykorzystuje się zazwyczaj dwa główne procesy [1]:

- **Procesy produkcji ciągłej.** Procesy te przebiegają w sposób ciągły, często z przejściami w celu wytworzenia różnych gatunków produktu. Typowe ciągłe procesy produkcyjne obejmują przepływ paliwa lub pary w elektrowni, ropy naftowej w rafinerii oraz destylację w zakładach chemicznych.
- **Procesy produkcji seryjnej.** Procesy te mają odrębne etapy przetwarzania, prowadzone na pewnej ilości materiału. Proces wsadowy ma wyraźny etap początkowy i końcowy, z możliwością krótkich operacji w stanie ustalonym podczas etapów pośrednich. Typowe procesy produkcji wsadowej obejmują produkcję żywności.

Branże produkcyjne oparte na produkcji *dyskretnej* zazwyczaj wykonują serię czynności na pojedynczym urządzeniu w celu stworzenia produktu końcowego. Montaż części elektronicznych i mechanicznych oraz obróbka mechaniczna części są typowymi przykładami tego typu przemysłu.

Zarówno branże oparte na procesach, jak i te oparte na produkcji dyskretnej wykorzystują te same rodzaje systemów sterowania, czujników i sieci. Niektóre zakłady stanowią hybrydę produkcji dyskretnej i procesowej.

2.2.2. Branża dystrybucyjna

ICS są wykorzystywane do sterowania zasobów rozproszonych geograficznie, często rozrzuconych na tysiącach kilometrów kwadratowych, w tym systemów dystrybucji, takich jak systemy dystrybucji wody i odprowadzania ścieków, systemy nawadniania rolnictwa, rurociągi ropy naftowej i gazu ziemnego, sieci elektroenergetyczne i systemy transportu kolejowego.

2.2.3. Różnice między produkcyjnymi i dystrybucyjnymi systemami ICS

Chociaż systemy sterowania stosowane w przemyśle produkcyjnym i dystrybucyjnym są bardzo podobne w działaniu, to jednak różnią się pod pewnymi względami. Branże produkcyjne są zazwyczaj zlokalizowane w obrębie ograniczonej fabryki lub zakładu, w porównaniu z rozproszonymi geograficznie branżami dystrybucyjnymi. Komunikacja w przemyśle produkcyjnym odbywa się zazwyczaj za pomocą technologii sieci lokalnych (*ang. local area network - LAN*), które są zazwyczaj bardziej niezawodne i szybsze w porównaniu z komunikacją na duże odległości za pomocą sieci rozległych (*ang. wide-area network - WAN*) i technologii bezprzewodowych/ częstotliwości radiowych (*ang. wireless / radio frequency - RF*) stosowanych w przemyśle dystrybucyjnym. ICS stosowane w branżach dystrybucyjnych są zaprojektowane tak, aby radzić sobie z wyzwaniami związanymi z komunikacją na duże odległości, takimi jak opóźnienia i utrata danych spowodowane różnymi wykorzystywanymi mediami komunikacyjnymi. Stosowane środki bezpieczeństwa mogą się różnić w zależności od typu sieci.

2.2.4. Współzależności między ICS a infrastrukturą krytyczną

Infrastrukturę krytyczną często określa się mianem "system systemów" (*ang. „system of systems" –SoS*) ze względu na współzależności występujące pomiędzy poszczególnymi sektorami przemysłu, a także wzajemne powiązania pomiędzy partnerami biznesowymi [8] [9]. Infrastruktury krytyczne są ze sobą silnie powiązane i wzajemnie zależne w złożony sposób, zarówno fizycznie, jak i za pośrednictwem wielu technologii informacyjnych i telekomunikacyjnych. Incydent w jednej infrastrukturze może

bezpośrednio lub pośrednio wpłynąć na inne infrastruktury poprzez kaskadowe i eskalowane awarie.

Zarówno branża przesyłu jak i dystrybucji energii elektrycznej wykorzystuje rozproszoną geograficznie technologię sterowania SCADA do obsługi wzajemnie połączonych i dynamicznych systemów składających się z tysięcy publicznych i prywatnych przedsiębiorstw użyteczności publicznej oraz wspólnot dostarczających energię elektryczną do użytkowników końcowych. Niektóre systemy SCADA monitorują i sterują dystrybucją energii elektrycznej poprzez zbieranie danych z odległych geograficznie obiektowych stacji kontrolnych i wydawanie im poleceń ze scentralizowanej lokalizacji.

Systemy SCADA są również wykorzystywane do monitorowania i kontroli dystrybucji wody, ropy naftowej i gazu ziemnego, w tym rurociągów, statków, ciężarówek i systemów kolejowych, a także systemów zbierania ścieków.

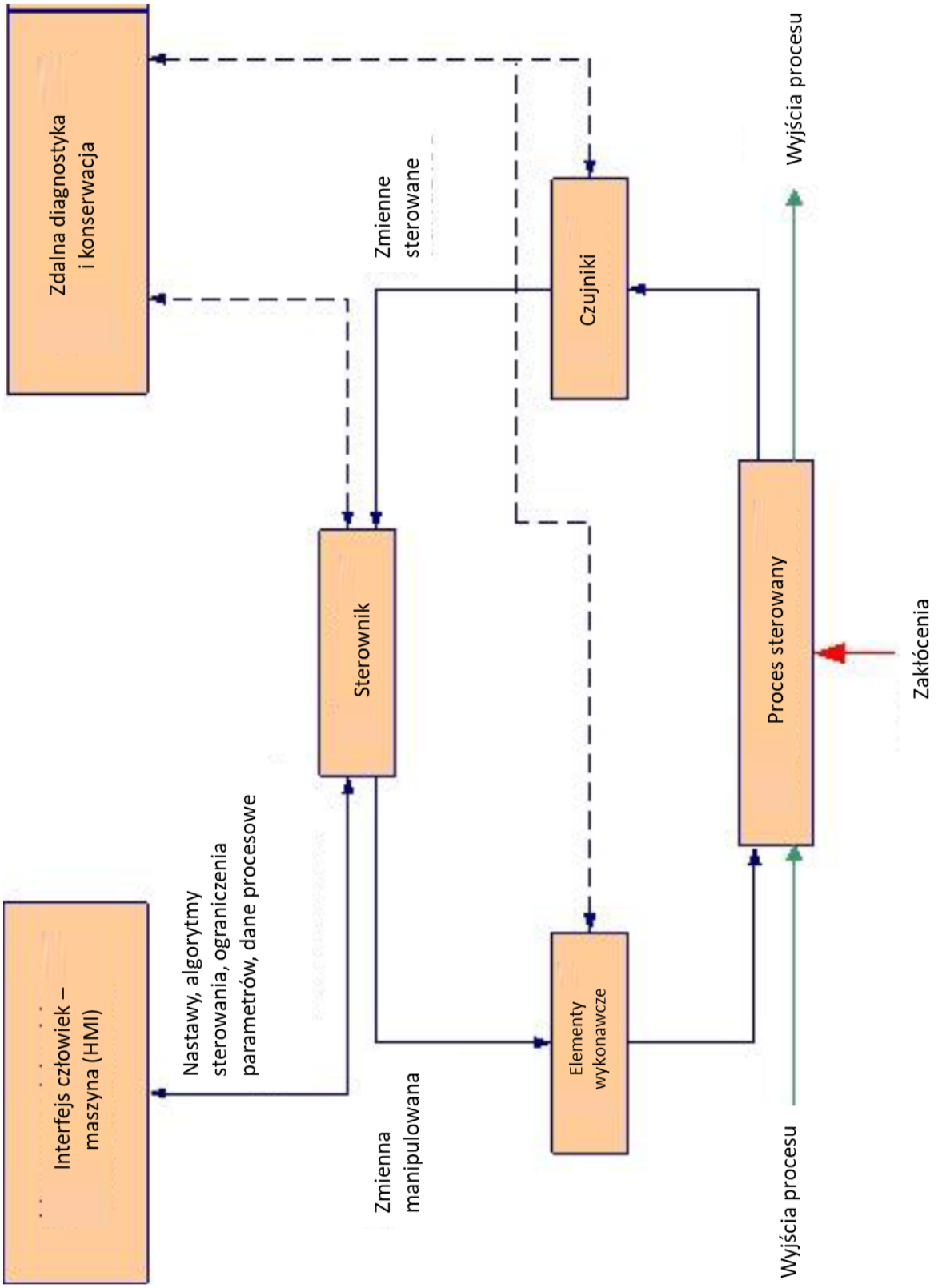
Systemy SCADA i DCS są często połączone w sieć. Tak jest w przypadku centrów sterowania energią elektryczną i obiektów wytwarzających energię elektryczną. Mimo, że praca instalacji wytwarzającej energię elektryczną jest kontrolowana przez DCS, DCS musi komunikować się z systemem SCADA, aby skoordynować produkcję z zapotrzebowaniem na przesył i dystrybucję.

Zakłócenia w dostawie energii elektrycznej są często uważane za jedno z najbardziej powszechnych źródeł zakłóceń współzależnych infrastruktur krytycznych. Przykładowo, awaria kaskadowa może zostać zainicjowana przez zakłócenie sieci łączności radiowej systemu SCADA wykorzystywanego w przesyle energii elektrycznej. Brak możliwości monitorowania i sterowania mógłby spowodować wyłączenie dużej jednostki prądotwórczej, co doprowadziłoby do utraty mocy w podstacji przesyłowej. Utrata ta mogłaby spowodować poważną nierównowagę, wywołując awarię kaskadową w całej sieci energetycznej. Mogłoby to spowodować przerwy w dostawie energii elektrycznej na dużym obszarze, które mogłyby potencjalnie wpłynąć na produkcję ropy naftowej i gazu ziemnego, działalność rafinerii, systemy uzdatniania wody, systemy odprowadzania ścieków oraz systemy transportu rurociągowego, które są uzależnione od sieci elektroenergetycznej.

2.3. Działanie i komponenty ICS

Podstawowe działanie systemu ICS przedstawiono na rysunku 2-1 [2]. Niektóre procesy krytyczne mogą również obejmować systemy bezpieczeństwa. Kluczowe komponenty obejmują następujące elementy:

- Typowy system ICS zawierający liczne pętle sterowania, interfejsy ludzkie oraz narzędzia zdalnej diagnostyki i konserwacji zbudowane z wykorzystaniem szeregu protokołów sieciowych w warstwowych architekturach sieciowych. Pętla sterowania wykorzystuje czujniki, siłowniki i sterowniki (np. PLC) do manipulowania określonym kontrolowanym procesem. Czujnik jest urządzeniem, które dokonuje pomiaru określonej wielkości fizycznej a następnie przesyła do sterownika te informacje, jako zmienne dane sterowania. Sterownik interpretuje nadsyłane dane i generuje odpowiednie zmienne sterowania w oparciu o algorytm sterowania i zadane docelowe wartości, które przekazuje do elementów wykonawczych. Elementy wykonawcze, takie jak zawory regulacyjne, wyłączniki, przełączniki i silniki są wykorzystywane do bezpośredniej manipulacji procesem na podstawie poleceń sterownika.
- Monitorowanie i konfigurowanie punktów nastaw, algorytmów sterowania oraz regulowanie i ustalanie parametrów w sterowniku przez operatorów i inżynierów używających stosownych interfejsów. Interfejs obsługiwany przez człowieka wyświetla również informacje o stanie procesu i informacje historyczne. Narzędzia diagnostyczne i konserwacyjne są wykorzystywane do zapobiegania, identyfikacji i usuwania skutków nieprawidłowego działania lub awarii.
- Pętle regulacyjne, czasami zagnieżdżone kaskadowo - w takim przypadku wartość zadana dla jednej pętli jest oparta na zmiennej procesowej określonej przez inną pętlę. Pętle poziomu nadzorczego i pętle niższego poziomu działają w sposób ciągły przez cały czas trwania procesu z czasami cyklu rzędu od milisekund do minut.



Rysunek 2-1. Działanie systemu sterowania przemysłowego ICS.

W celu ułatwienia prowadzenia dalszych rozważań, w niniejszym rozdziale zdefiniowano kluczowe komponenty ICS, które są wykorzystywane w sterowaniu i tworzeniu sieci. Niektóre z tych komponentów mogą być opisane jako ogólnie stosowane w systemach SCADA, DCS i PLC, podczas gdy inne są unikalne dla jednego z nich. Słownik terminów w załączniku B zawiera bardziej szczegółowy wykaz komponentów sterowania i sieci. Dodatkowo, Rysunek 2-5 i Rysunek 2-6 przedstawiają przykłady wdrożenia systemu SCADA. Rysunek 2-7 przedstawia przykład wdrożenia systemu DCS. Rysunek 2-8 ilustruje przykład wdrożenia sterownika PLC, który zawiera te komponenty.

2.3.1. Czynniki związane z projektowaniem systemu ICS

W rozdziale 2.3 przedstawiono podstawowe komponenty ICS, jednak konstrukcja ICS, w tym to, czy zastosowana zostanie topologia oparta na SCADA, DCS czy PLC, zależy od wielu czynników. W niniejszej sekcji określono kluczowe czynniki, które wpływają na decyzje projektowe dotyczące właściwości sterowania, komunikacji, niezawodności i redundancji systemu ICS. Ponieważ czynniki te w dużym stopniu wpływają na projekt systemu ICS, pomogą one również w określeniu potrzeb bezpieczeństwa systemu.

- **Wymagania dotyczące taktowania.** Procesy ICS mają szeroki zakres wymagań związanych z czasem, w tym bardzo dużą szybkość, spójność, regularność i synchronizację. Ludzie mogą nie być w stanie niezawodnie i konsekwentnie spełnić tych wymagań, konieczne może być zastosowanie zautomatyzowanych sterowników. Niektóre systemy mogą wymagać, aby obliczenia były wykonywane jak najbliżej czujników i elementów wykonawczych, aby zmniejszyć opóźnienia w komunikacji i na czas wykonać niezbędne czynności sterowania.
- **Rozproszenie geograficzne.** Systemy mają różny stopień rozproszenia, począwszy od małego systemu (np. lokalny proces sterowany za pomocą PLC) do dużych, rozproszonych systemów (np. rurociągi naftowe, sieć energoelektryczna). Większe rozproszenie wiąże się zazwyczaj z koniecznością zapewnienia komunikacji rozległej (np. linie dzierżawione, komutacja łączy i komutacja pakietów) oraz komunikacji mobilnej.

- **Hierarchia.** Sterowanie nadzorcze jest stosowane w celu zapewnienia centralnej lokalizacji, która może agregować dane z wielu lokalizacji, aby wspierać decyzje dotyczące sterowania w oparciu o bieżący stan systemu. Często stosuje się sterowanie hierarchiczne/scentralizowane, aby zapewnić operatorom kompleksowy wgląd w cały system.
- **Złożoność sterowania.** Często funkcje sterowania mogą być realizowane przez proste sterowniki i wstępnie ustawione algorytmy. Jednak bardziej złożone systemy (np. kontrola ruchu lotniczego) wymagają jednak od operatorów zapewnienia, że wszystkie działania związane ze sterowaniem są odpowiednie dla osiągnięcia większych celów systemu.
- **Dostępność.** Wymagania dotyczące dostępności (tzn. niezawodności) systemu są również ważnym czynnikiem projektowym. Systemy o wysokich wymaganiach dotyczących dostępności/czasu pracy mogą wymagać większej redundancji lub alternatywnych wdrożeń we wszystkich obszarach komunikacji i sterowania.
- **Wpływ awarii.** Awaria funkcji sterowania może mieć bardzo różne skutki w różnych dziedzinach. Systemy o większym wpływie często wymagają możliwości kontynuowania działania dzięki nadmiarowym układom sterowania lub możliwości działania w stanie awaryjnym. Projekt musi uwzględniać te wymagania.
- **Ochrona.** Ważnym czynnikiem przy projektowaniu systemu są również wymagania dotyczące ochrony. Systemy muszą być w stanie wykrywać niebezpieczne warunki i uruchamiać działania mające na celu sprowadzenie stanów niebezpiecznych do bezpiecznych. W większości operacji krytycznych dla bezpieczeństwa, nadzór i kontrola człowieka nad potencjalnie niebezpiecznym procesem jest istotną częścią systemu ochrony.

2.3.2. Systemy SCADA

Systemy SCADA są wykorzystywane do sterowania rozproszonymi zasobami, gdzie scentralizowane pozyskiwanie danych jest równie ważne jak sterowanie [3], [4]. Systemy te są stosowane w systemach dystrybucji, takich jak systemy dystrybucji wody i gromadzenia nieczystości, rurociągi ropy naftowej i gazu ziemnego, systemy przesyłu

i dystrybucji energii elektrycznej oraz systemy transportu kolejowego i innego transportu publicznego. Systemy SCADA integrują systemy akwizycji danych z systemami transmisji danych i oprogramowaniem HMI w celu zapewnienia scentralizowanego systemu monitorowania i sterowania wieloma wejściami i wyjściami procesowymi. Systemy SCADA są zaprojektowane do zbierania informacji z terenu, przekazywania ich do centralnego obiektu obliczeniowego i wyświetlania informacji operatorowi w formie graficznej lub tekstowej, co pozwala na monitorowanie lub sterowanie całym systemem z centralnej lokalizacji w czasie zbliżonym do rzeczywistego. W zależności od stopnia zaawansowania i konfiguracji danego systemu, sterowanie każdym pojedynczym systemem, operacją lub zadaniem może być zautomatyzowane lub może być wykonywana za pomocą poleceń operatora.

Typowy sprzęt obejmuje serwer sterujący umieszczony w centrum sterowania, urządzenia komunikacyjne (np. radio, linia telefoniczna, kabel lub satelita) oraz jeden lub więcej geograficznie rozproszonych punktów obiektowych składających się ze zdalnych jednostek końcowych (*ang. Remote Terminal Units - RTU*) i/lub sterowników PLC, które sterują elementami wykonawczymi i/lub monitorują czujniki. Serwer sterujący przechowuje i przetwarza informacje z wejść i wyjść RTU, podczas gdy RTU lub PLC steruje procesem lokalnym. Sprzęt komunikacyjny umożliwia dwukierunkowe przesyłanie informacji i danych pomiędzy serwerem sterowania a RTU lub PLC. Oprogramowanie jest zaprogramowane tak, aby informowało system o tym, co i kiedy należy monitorować, jakie zakresy parametrów są dopuszczalne i jaką odpowiedź inicjować na zmiany parametrów poza dopuszczalne wartości. Inteligentne urządzenie elektroniczne (*ang. Intelligent Electronic Device - IED*), takie jak przekaźnik zabezpieczający, może komunikować się bezpośrednio z serwerem sterowania, lub może być odpytywane przez lokalny RTU w celu zebrania danych i przekazania ich do serwera sterowania. Urządzenia IED stanowią bezpośredni interfejs do sterowania i monitorowania urządzeń i czujników. Urządzenia IED mogą być bezpośrednio odpytywane i sterowane przez serwer sterujący. W większości przypadków posiadają lokalne oprogramowanie, które pozwala na działanie IED bez bezpośrednich poleceń z centrum sterowania. Systemy SCADA są zazwyczaj projektowane jako systemy

odporne na błędy ze znaczną redundancją wbudowaną w system. Redundancja może nie być wystarczającym środkiem zaradczym w obliczu złośliwego ataku.

Rysunek 2-2 przedstawia komponenty i ogólną konfigurację systemu SCADA. W centrum sterowania znajduje się serwer sterujący i routery komunikacyjne. Inne komponenty dany centrum sterowania to interfejs HMI, stacje robocze inżynierów oraz rejestrator historii danych, które są połączone siecią LAN. Centrum sterowania gromadzi i rejestruje informacje zebrane przez obiekty terenowe, wyświetla informacje na panelu HMI i może generować działania na podstawie wykrytych zdarzeń. Centrum sterowania jest również odpowiedzialne za scentralizowane alarmowanie, analizę trendów i raportowanie. Stanowisko obiektowe steruje lokalnie elementami wykonawczymi i monitoruje czujniki (należy pamiętać, że czujniki i elementy wykonawcze są pokazane tylko na Rysunku 2-5). Obiekty terenowe są często wyposażone w funkcję zdalnego dostępu umożliwiającą operatorom wykonywanie zdalnej diagnostyki i napraw, zwykle za pośrednictwem oddzielnego modemu telefonicznego lub połączenia WAN. Do przesyłania informacji między centrum sterowania a obiektami terenowe wykorzystuje się standardowe (*ang. standard*) i zastrzeżone (ang. *proprietary*) protokoły komunikacyjne[5] działające za pośrednictwem komunikacji szeregowej i sieciowej, wykorzystujące techniki telemetryczne, takie jak linia kablowa, światłowód oraz transmisja radiowa, np. komunikacja rozgłoszeniowa, mikrofalowa lub satelitarna.

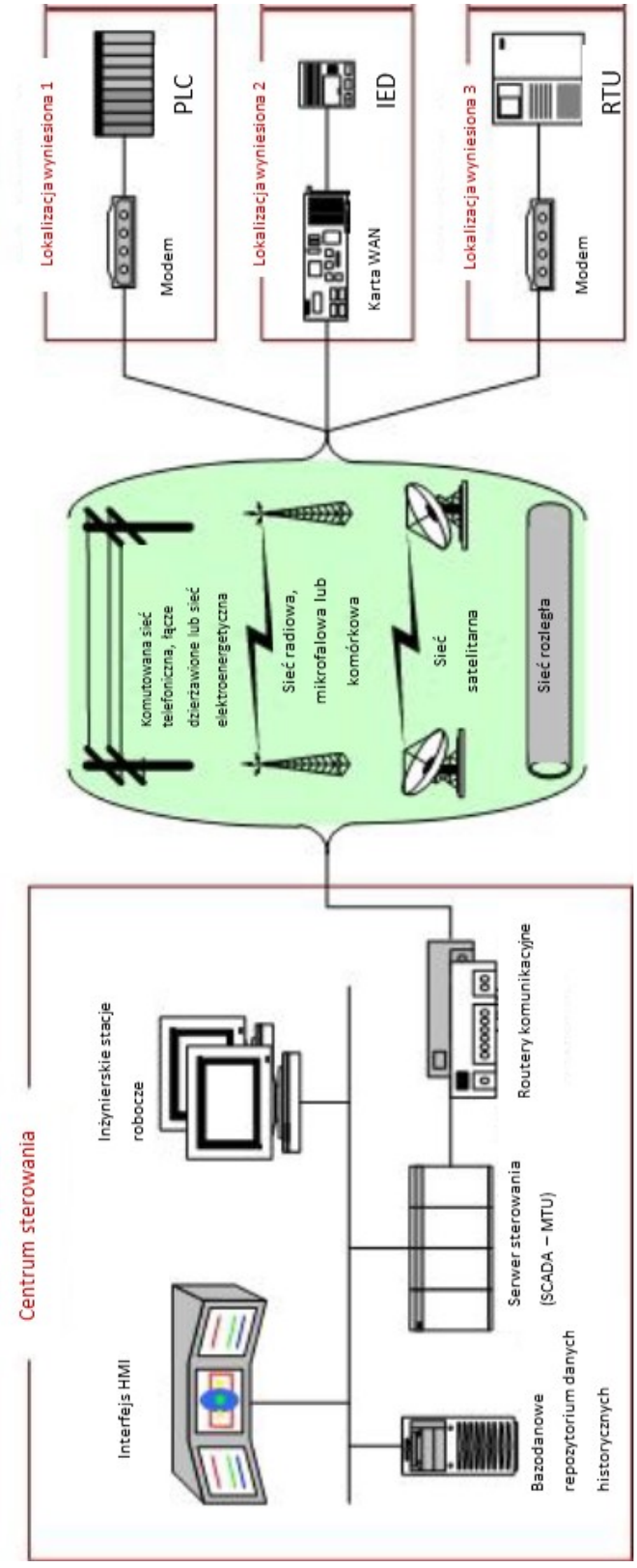
Topologie komunikacyjne SCADA różnią się w zależności od implementacji. Na rysunku 2-3 pokazane są różne stosowane topologie, w tym: punkt-punkt, szeregowa, szeregowo-gwiaździsta i wielopunktowa [5].

Połączenie punkt-punkt jest funkcjonalnie najprostszym typem; jest jednak kosztowne ze względu na indywidualne kanały potrzebne do każdego połączenia.

[5] Główna różnica między protokołem zastrzeżonym a standardowym polega na tym, że protokoły zastrzeżone są zazwyczaj opracowywane przez jednego sprzedawcę w celu wykorzystania ich w jego własnych produktach. Natomiast protokoły standardowe są publikowanymi otwartymi standardami, które każdy sprzedawca może stosować w swoich produktach.

W konfiguracji szeregowej liczba używanych kanałów jest zredukowana, jednak współdzielenie kanałów ma wpływ na wydajność i złożoność operacji SCADA.

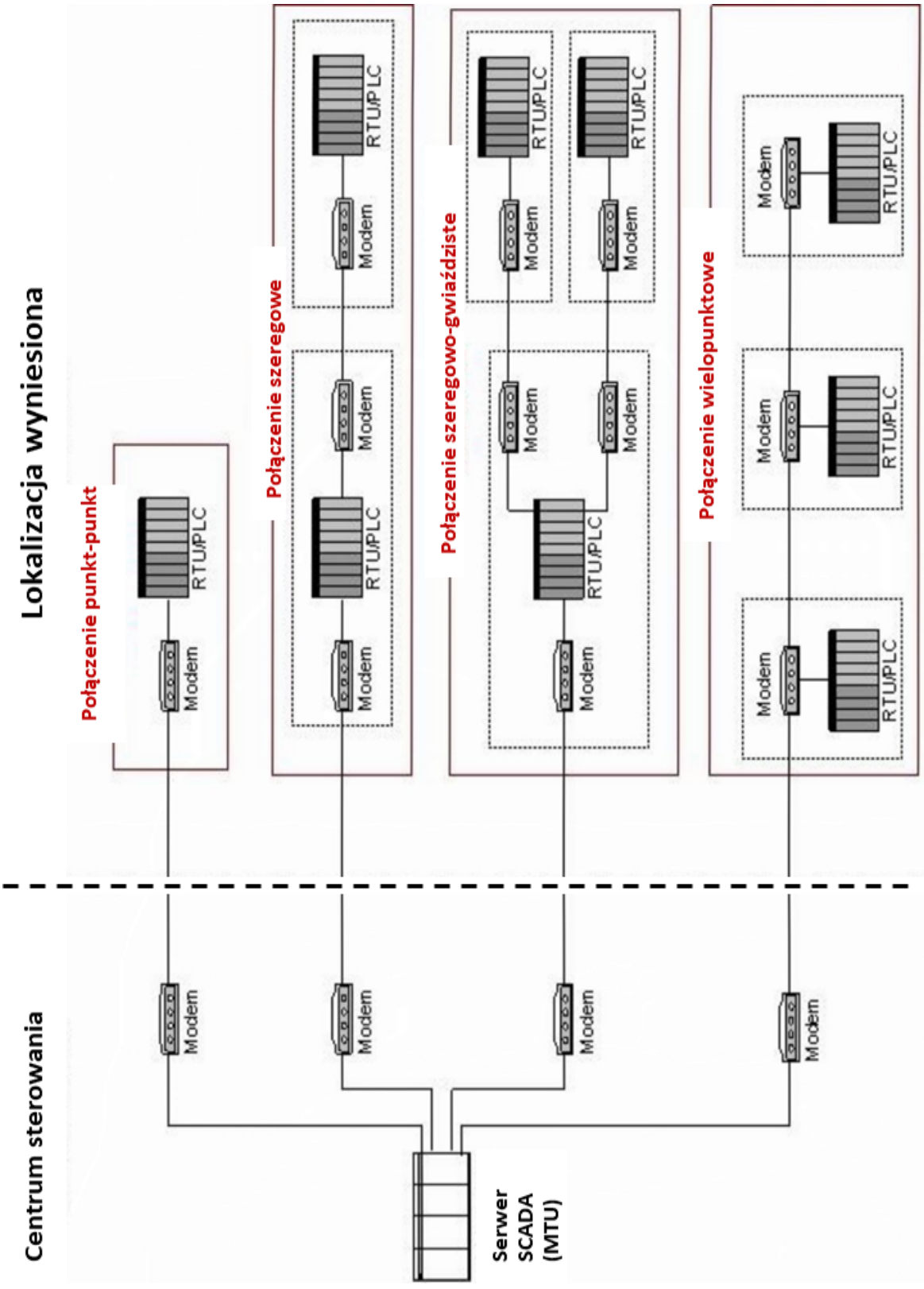
Podobnie, wykorzystanie w konfiguracjach szeregowo-gwiaździstych i wielopunktowych jednego kanału na urządzenie powoduje zmniejszenie wydajności i zwiększenie złożoności systemu.



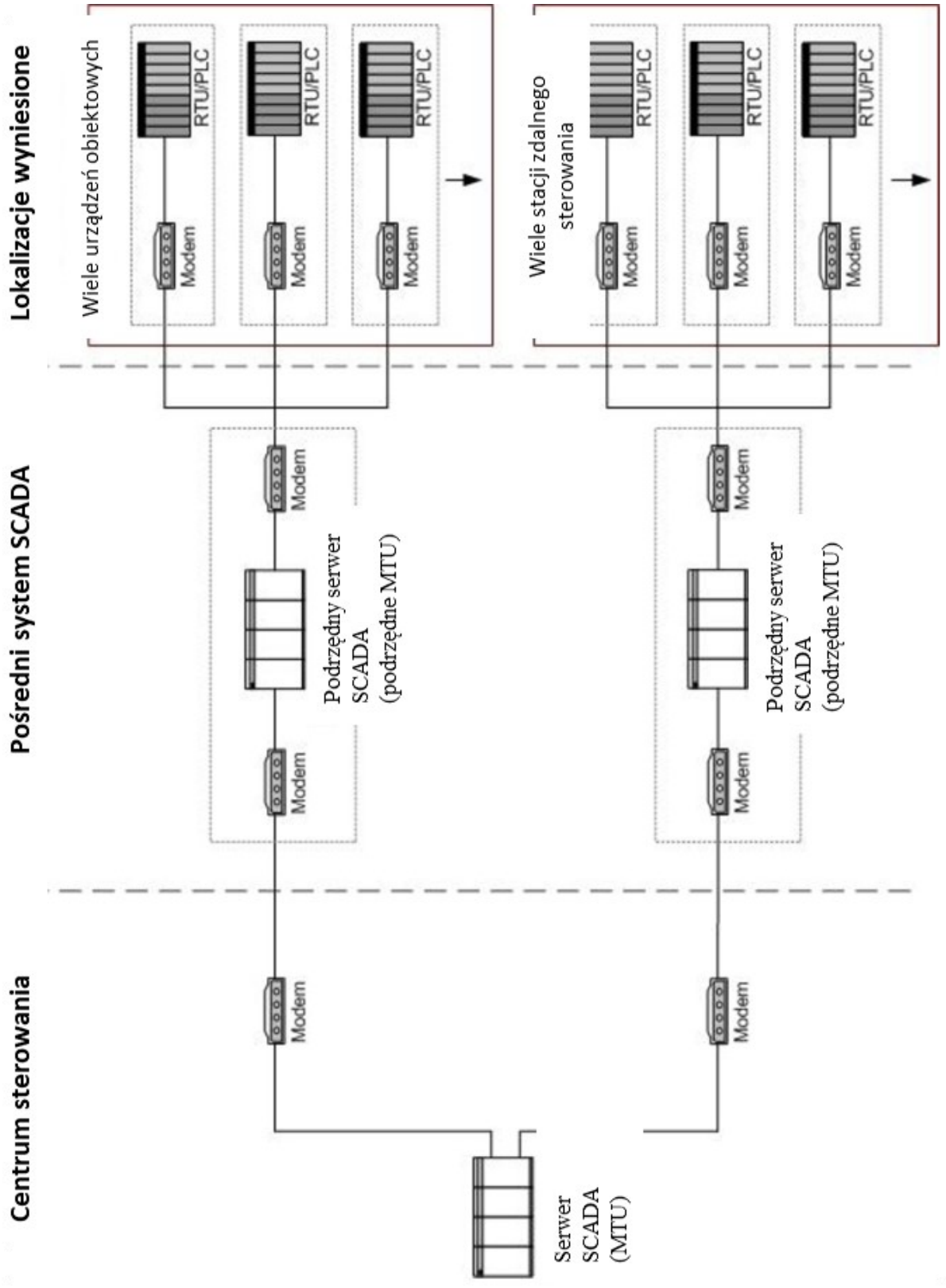
Rysunek 2-2. Schemat ogólny systemu SCADA.

Cztery podstawowe topologie z rysunku 2-3 mogą być dalej rozbudowywane przy użyciu dedykowanych urządzeń do zarządzania wymianą komunikatów oraz przełączania komunikatów i buforowania. Duże systemy SCADA, zawierające setki RTU, często stosują podrzędny serwer sterowania, aby odciążyć serwer główny. Ten typ topologii pokazano na rysunku 2-4.

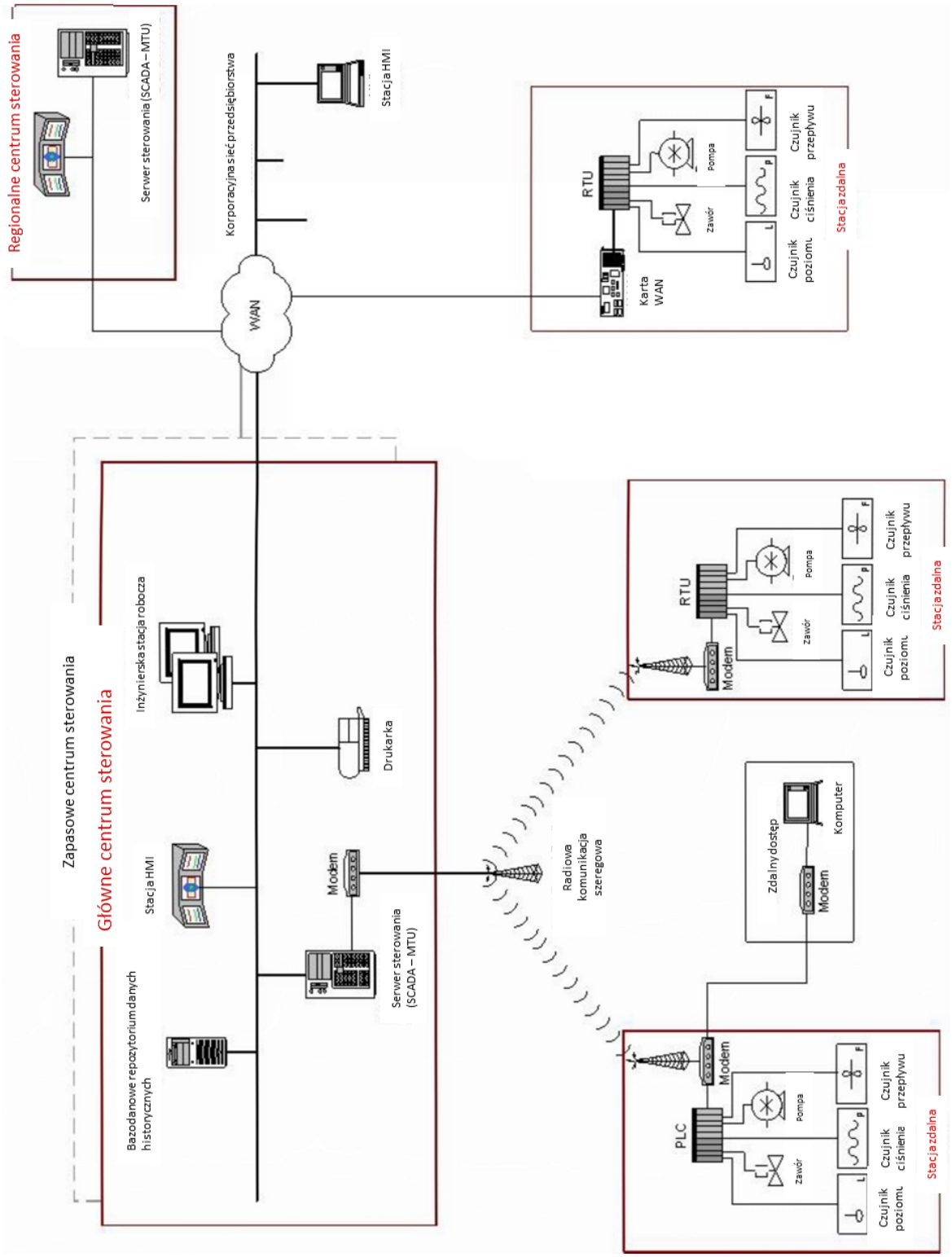
Rysunek 2-5 przedstawia przykład wdrożenia systemu SCADA. Ten konkretny system SCADA składa się z głównego centrum sterowania i trzech lokalizacji obiektowych. Zapasowe centrum sterowania zapewnia redundancję w przypadku awarii głównego centrum sterowania. Połączenia typu punkt-punkt są używane do komunikacji pomiędzy centrum sterowania a lokalizacjami obiektowymi, przy czym dwa połączenia wykorzystują telemetrię radiową. Trzecia lokalizacja obiektowa jest lokalna w stosunku do centrum sterowania i do komunikacji wykorzystuje sieć WAN. Regionalne centrum sterowania znajduje się powyżej głównego centrum sterowania celem wyższego poziomu sterowania nadzorczego. Sieć korporacyjna ma dostęp do wszystkich centrów sterowania poprzez sieć WAN, a do placówek obiektowych można uzyskać zdalny dostęp w celu rozwiązywania problemów i przeprowadzania czynności konserwacyjnych. Główne centrum sterowania odpytuje urządzenia obiektowe i dane w określonych odstępach czasu (np. 5 sekund, 60 sekund) i może wysyłać nowe punkty nastaw do urządzenia obiektowego, jeśli jest to wymagane. Oprócz odpytywania i wydawania poleceń wysokiego poziomu, serwer sterujący obserwuje również przerwania priorytetowe pochodzące z obiektowych systemów alarmowych.



Rysunek 2-3. Podstawowe topologie komunikacyjne SCADA.

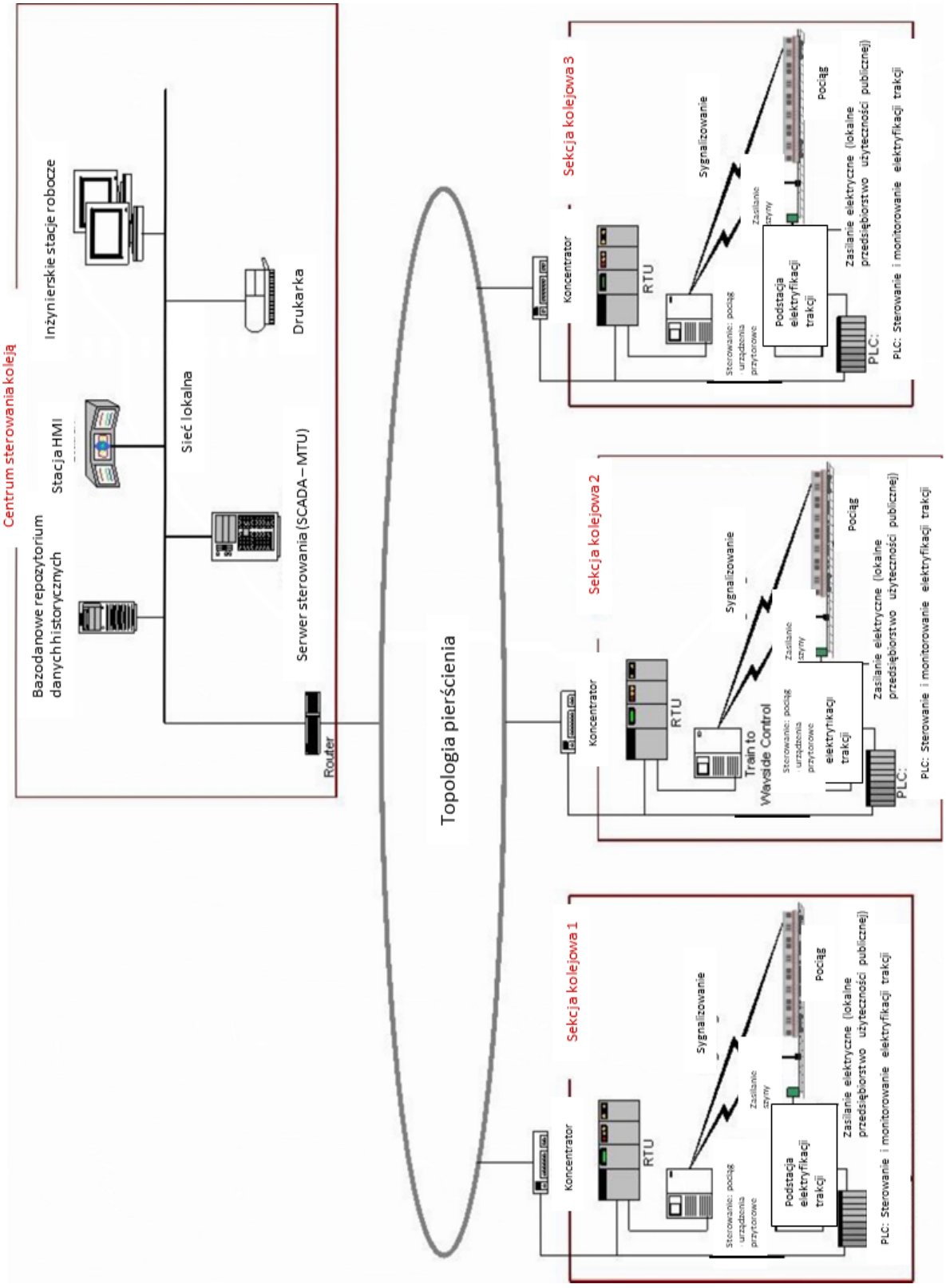


Rysunek 2-4. Topologia komunikacyjna dużego systemu SCADA.



Rysunek 2-5. Przykład wdrożenia systemu SCADA (monitorowanie i sterowanie dystrybucją).

Na rysunku 2-6 przedstawiono przykładowe wdrożenie monitorowania i sterowania ruchem kolejowym. Przykład ten obejmuje centrum sterowania ruchem kolejowym, w którym znajduje się system SCADA oraz trzy sekcje systemu kolejowego. System SCADA wyszukuje w sekcjach kolejowych takie informacje, jak stan pociągów, systemy sygnalizacyjne, systemy elektryfikacji trakcji oraz automaty biletowe. Informacje te są również przekazywane do konsoli operatora na stacji HMI w centrum sterowania ruchem kolejowym. System SCADA monitoruje również dane wejściowe operatora w centrum sterowania ruchem kolejowym i przekazuje wysokopoziomowe polecenia operatora do składowych sekcji kolejowych. Ponadto system SCADA monitoruje warunki na poszczególnych odcinkach torów i wydaje polecenia oparte na tych warunkach (np. zatrzymanie pociągu, aby uniemożliwić mu wjazd na obszar, który w oparciu o monitorowanie stanu został uznany za uszkodzony lub zajęty przez inny pociąg).



Rysunek 2-6. Przykład wdrożenia systemu SCADA (monitorowanie i sterowanie ruchem kolejowym).

2.3.3. Rozproszone systemy sterowania

Systemy DCS są wykorzystywane do sterowania systemami produkcyjnymi w obrębie tej samej lokalizacji geograficznej, w takich gałęziach przemysłu jak rafinerie ropy naftowej, oczyszczanie wody i ścieków, zakłady produkcji energii elektrycznej, zakłady produkcji chemicznej, produkcja samochodów oraz zakłady przetwórstwa farmaceutycznego. Systemy te są zazwyczaj systemami sterowania procesami lub systemami sterowania dyskretnego.

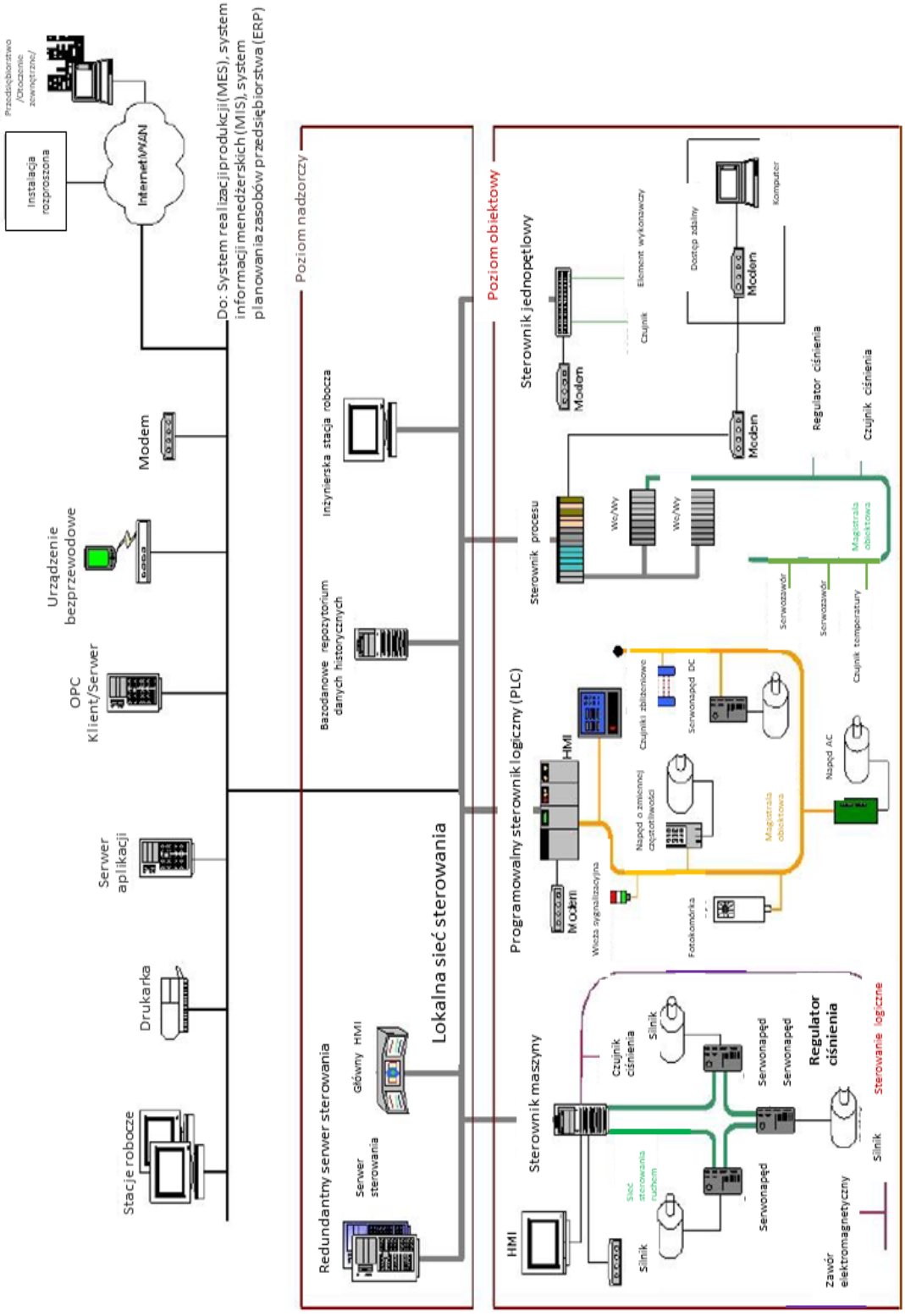
DCS są zintegrowane jako architektura sterowania zawierająca poziom sterowania nadzorczego nadzorujący wiele zintegrowanych podsystemów, które są odpowiedzialne za kontrolę szczegółów lokalnego procesu. System DCS wykorzystuje scentralizowaną pętlę sterowania, aby pośredniczyć w pracy sterowników zlokalizowanych w grupy , które współdzielą całościowe zadania związane z realizacją całego procesu produkcyjnego [6]. Sterowanie produktem i procesem jest zazwyczaj osiągane poprzez zastosowanie pętli sterowania ze sprzężeniem zwrotnym lub sprzężeniem wyprzedzającym, dzięki czemu kluczowe warunki produktu i/lub procesu są automatycznie utrzymywane wokół pożądanej wartości zadanej. Aby osiągnąć pożądaną tolerancję produktu i/lub procesu wokół określonej wartości zadanej, w terenie stosowane są sterowniki konkretnych procesów lub bardziej wydajne sterowniki PLC, które są dostrajane w celu zapewnienia pożądanej tolerancji, jak również szybkości autokorekty podczas zaburzeń procesu. Dzięki modułowej budowie systemu produkcyjnego, system DCS zmniejsza wpływ pojedynczej usterki na cały system. W wielu nowoczesnych systemach DCS jest sprzężony z siecią korporacyjną, aby zapewnić podgląd produkcji w działalności biznesowej.

Przykładowa implementacja przedstawiająca komponenty i ogólną konfigurację systemu DCS przedstawiona została na rysunku 2-7. System DCS obejmuje cały zakład, od procesów produkcyjnych na najniższym poziomie, aż po warstwę korporacji lub przedsiębiorstwa. W tym przykładzie sterownik nadzorczy (serwer sterowania) komunikuje się ze swoimi jednostkami podrzędnymi za pośrednictwem sieci sterowania. Nadzorca wysyła wartości zadane i żąda danych z rozproszonych sterowników obiektowych. Sterowniki rozproszone sterują swoimi elementami

wykonawczymi procesu w oparciu o polecenia serwera sterowania i informacje zwrotne z czujników procesu.

Rysunek 2-7 przedstawia przykłady sterowników niskiego poziomu, które można znaleźć w systemie DCS. Przedstawione urządzenia sterujące obejmują sterownik PLC, sterownik procesu, sterownik jednopętlowy i sterownik maszyny. Sterownik jednopętlowy łączy czujniki i elementy wykonawcze za pomocą okablowania punkt-punkt, podczas gdy pozostałe trzy urządzenia obiektowe do łączenia czujników i elementów wykonawczych procesu wykorzystują sieci magistrali obiektowej. Sieci magistrali obiektowej eliminują konieczność okablowania punkt-punkt pomiędzy sterownikiem a poszczególnymi czujnikami polowymi i elementami wykonawczymi. Dodatkowo, magistrala polowa umożliwia większą funkcjonalność niż tylko sterowanie, w tym diagnostykę urządzeń polowych i może realizować algorytmy sterowania w obrębie magistrali obiektowej, unikając w ten sposób kierowania sygnału z powrotem do sterownika PLC dla każdej operacji sterowania. W sieciach sterowania i sieciach magistrali obiektowej często stosowane są standardowe protokoły komunikacji przemysłowej opracowane przez grupy branżowe, takie jak Modbus i Fieldbus [7].

Oprócz pętli sterowania na poziomie nadzorczym i na poziomie obiektowym (terenowym) mogą istnieć również pośrednie poziomy sterowania. Na przykład, w przypadku systemu DCS sterującego pracą zakładu produkującego części dyskretne, może występować nadzorca poziomu pośredniego dla każdej komórki w obrębie zakładu. Nadzorca ten obejmowałby komórkę produkcyjną zawierającą sterownik maszyny obrabiającej element oraz sterownik robota obsługującego surowiec i produkty końcowe. Może istnieć kilka takich komórek, które zarządzają sterownikami na poziomie polowym pod główną pętlą sterowania systemu DCS.



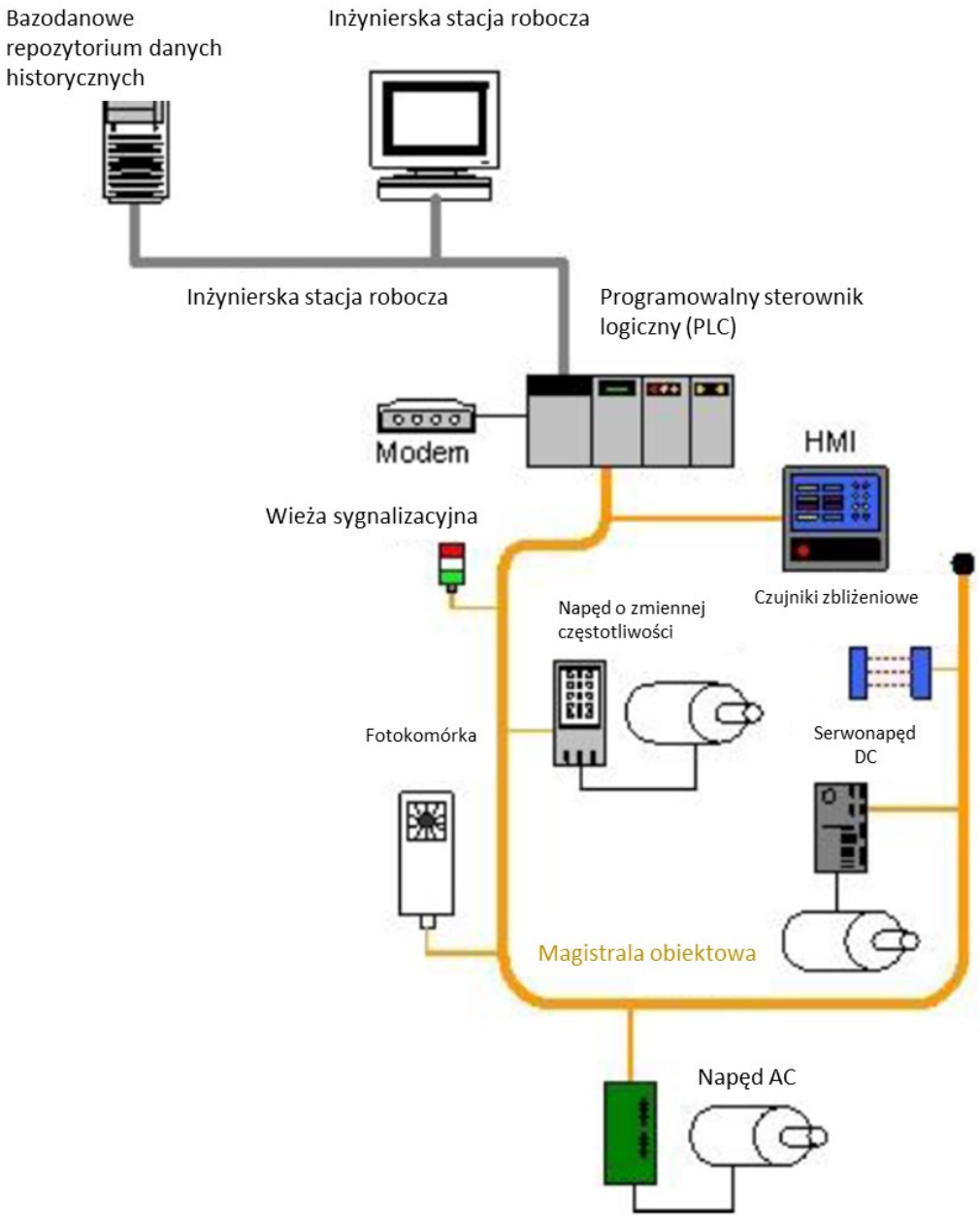
Rysunek 2-7. Przykład wdrożenia systemu DCS.

2.3.4. Systemy oparte na programowalnych sterownikach logicznych

Sterowniki PLC są wykorzystywane zarówno w systemach SCADA jak i DCS jako elementy sterujące w ogólnym systemie hierarchicznym, aby zapewnić lokalne zarządzanie procesami poprzez sterowanie ze sprzężeniem zwrotnym, jak opisano w powyższych rozdziałach. W przypadku systemów SCADA, mogą one zapewniać taką samą funkcjonalność jak RTU. W przypadku zastosowania w systemach DCS, sterowniki PLC są implementowane jako sterowniki lokalne w ramach schematu sterowania nadzorczego.

Oprócz stosowania sterowników PLC w systemach SCADA i DCS, sterowniki PLC są również wdrażane jako podstawowe sterowniki w mniejszych konfiguracjach systemów sterowania w celu zapewnienia operacyjnego sterowania procesami dyskretnymi, takimi jak linie montażowe samochodów i sterowanie dmuchawami pyłu węglowego w elektrowniach. Topologie te różnią się od SCADA i DCS tym, że zazwyczaj nie posiadają centralnego serwera sterowania i interfejsu HMI, a zatem przede wszystkim zapewniają sterowanie w pętli zamkniętej bez bezpośredniego udziału człowieka. Sterowniki PLC posiadają programowalną przez użytkownika pamięć do przechowywania instrukcji w celu realizacji określonych funkcji, takich jak sterowanie we/wy, logika, taktowanie, liczenie, regulacja proporcjonalno-całkująco-różniczkująca (*ang. proportional-integral-derivative – PID*), komunikacja, arytmetyka oraz przetwarzanie danych i plików.

Rysunek 2-8 przedstawia sterowanie procesem produkcyjnym przez sterownik PLC za pośrednictwem sieci Fieldbus. Sterownik PLC jest dostępny za pośrednictwem interfejsu programistycznego umieszczonego na stacji roboczej inżyniera, a dane są przechowywane w historii danych, połączonym w sieci LAN.



Rysunek 2-8. Przykład wdrożenia systemu sterowania PLC.

2.4. Porównanie bezpieczeństwa systemów ICS i IT

Systemy ICS kontrolują świat fizyczny a systemy informacyjne zarządzają danymi. ICS mają wiele cech, które różnią je od tradycyjnych systemów informacyjnych, w tym różne rodzaje ryzyka i priorytety. Niektóre z nich stanowią znaczne zagrożenie dla zdrowia i bezpieczeństwa ludzi, poważne szkody dla środowiska oraz reperkusje finansowe, takie jak straty w produkcji i negatywny wpływ na gospodarkę narodową.

ICS mają inne wymagania dotyczące wydajności i niezawodności, a także wykorzystują systemy operacyjne i aplikacje, które mogą być uważane za niekonwencjonalne w typowym środowisku systemów IT. Środki bezpieczeństwa (zabezpieczenia) muszą być wdrożone w taki sposób, aby utrzymać integralność systemu podczas normalnych operacji, jak również w czasie cyberataku [17].

Początkowo ICS w niewielkim stopniu przypominały systemy IT, ponieważ były to odizolowane systemy wykorzystujące zastrzeżone protokoły sterowania przy użyciu specjalistycznego sprzętu i oprogramowania. Powszechnie dostępne, niedrogie urządzenia wykorzystujące sieć Ethernet i protokoły internetowe (IP) zastępują obecnie starsze, zastrzeżone technologie, co zwiększa możliwość wystąpienia podatności i incydentów w zakresie cyberbezpieczeństwa. Ponieważ ICS przyjmują rozwiązania informacyjne w celu promowania łączności korporacyjnej i możliwości zdalnego dostępu, a także są projektowane i wdrażane z wykorzystaniem standardowych komputerów, systemów operacyjnych (OS) i protokołów sieciowych, zaczynają przypominać systemy informacyjne. Integracja ta wspiera nowe możliwości IT, ale powoduje znacznie mniejszą izolację ICS od świata zewnętrznego niż poprzednie systemy, co stwarza większą potrzebę zabezpieczenia tych systemów. Podczas, gdy zabezpieczenia zostały zaprojektowane w celu rozwiązania tych problemów w typowych systemach IT, należy podjąć specjalne środki ostrożności przy wprowadzaniu tych samych rozwiązań do środowisk ICS. W niektórych przypadkach potrzebne są nowe rozwiązania w zakresie bezpieczeństwa, dostosowane do środowiska ICS.

Środowiska, w których funkcjonują systemy ICS i IT, ulegają ciągłym zmianom. Środowiska operacyjne obejmują, ale nie ograniczają się do: przestrzeni zagrożeń, podatności, misji/funkcji biznesowych, procesów misji/biznesu, architektur bezpieczeństwa korporacyjnego i informacyjnego, technologii informacyjnych, personelu, obiektów, relacji w łańcuchu dostaw, ładu/kultury organizacyjnej, procesów zaopatrzenia/nabywania, polityk/procedur organizacyjnych, założeń organizacyjnych, ograniczeń, tolerancji na ryzyko oraz priorytetów/wyborów).

Poniżej wymieniono kilka specyficznych czynników, które należy wziąć pod uwagę przy rozważaniach dotyczących bezpieczeństwa ICS:

- **Wymagania dotyczące terminowości i wydajności.** ICS są na ogół krytyczne czasowo, przy czym kryterium akceptowalnych poziomów opóźnień i zakłóceń jest dyktowane przez poszczególne indywidualne instalacje. Niektóre systemy wymagają niezawodnych, deterministycznych odpowiedzi. Wysoka przepustowość nie ma zazwyczaj zasadniczego znaczenia dla ICS. z kolei systemy informacyjne wymagają zazwyczaj dużej przepustowości i zazwyczaj są w stanie wytrzymać pewien poziom opóźnień i zakłóceń. W przypadku niektórych systemów ICS czas reakcji automatycznej lub reakcji systemu na interakcję człowieka jest bardzo krytyczny. Niektóre ICS są zbudowane na systemach operacyjnych czasu rzeczywistego (*ang. real-time operating system - RTOS*), gdzie czas rzeczywisty odnosi się do wymogów terminowości. Jednostki czasu rzeczywistego są bardzo zależne od aplikacji i muszą być jednoznacznie określone.
- **Wymagania dotyczące dostępności.** Wiele procesów ICS ma charakter ciągły. Nieoczekiwane przestoje systemów sterujących procesami przemysłowymi są niedopuszczalne. Przestoje często muszą być zaplanowane z kilkudniowym lub tygodniowym wyprzedzeniem. Wyczerpujące testy przedwdrożeniowe są niezbędne do zapewnienia wysokiej dostępności (tzn. niezawodności) ICS. Systemów sterowania często nie da się łatwo zatrzymać i uruchomić bez wpływu na produkcję. W niektórych przypadkach wytwarzane produkty lub używany sprzęt są ważniejsze niż przekazywane informacje. W związku z tym stosowanie typowych strategii informacyjnych, takich jak ponowne uruchomienie komponentu, jest zwykle rozwiązaniem nie do przyjęcia ze względu na niekorzystny wpływ na wymagania dotyczące wysokiej dostępności, niezawodności i zdolność utrzymania systemu ICS. Niektóre systemy ICS wykorzystują nadmiarowe komponenty, często działające równolegle, w celu zapewnienia ciągłości działania w przypadku niedostępności komponentów podstawowych.
- **Wymagania dotyczące zarządzania ryzykiem. W** typowym systemie informacyjnym najważniejszymi problemami są zazwyczaj poufność i integralność danych.

W przypadku ICS najważniejszymi kwestiami są: bezpieczeństwo ludzi i odporność na awarie (aby zapobiec utracie życia lub zagrożeniu zdrowia lub zaufania publicznego), zgodność z przepisami, utrata sprzętu, utrata własności intelektualnej, utracone lub uszkodzone produkty. Personel odpowiedzialny za obsługę, zabezpieczenie i obsługę ICS musi rozumieć istotny związek między bezpieczeństwem a ochroną. Wszelkie środki bezpieczeństwa, które zmniejszają bezpieczeństwo, są nie do przyjęcia.

- **Skutki fizyczne.** Urządzenia obiektowe ICS (np. PLC, stacja operatorska, sterownik DCS) są bezpośrednio odpowiedzialne za sterowanie procesami fizycznymi. ICS mogą mieć bardzo złożone interakcje z procesami fizycznymi i ich konsekwencjami w domenie ICS, które mogą przejawiać się w zdarzeniach fizycznych. Zrozumienie tych potencjalnych skutków fizycznych często wymaga komunikacji pomiędzy ekspertami w dziedzinie systemów sterowania oraz w danej dziedzinie fizycznej.
- **Obsługiwanie systemu.** Systemy operacyjne (OS) i sieci sterowania ICS często różnią się od odpowiedników informacyjnych, wymagając innych zestawów umiejętności, doświadczenia i poziomu wiedzy specjalistycznej. Sieci sterowania są zazwyczaj zarządzane przez inżynierów sterowania a nie przez personel IT. Założenia, że różnice nie są istotne, mogą mieć katastrofalne skutki dla działania systemu.
- **Ograniczenia zasobów.** ICS i ich systemy operacyjne działające w czasie rzeczywistym, są często systemami o ograniczonych zasobach, które nie obejmują typowych współczesnych funkcji bezpieczeństwa IT. W starszych systemach często brakuje zasobów typowych dla nowoczesnych systemów informacyjnych. Wiele systemów może nie posiadać pożądanych funkcji, takich jak możliwości szyfrowania, rejestrowania błędów i ochrony hasłem. Bezkrytyczne stosowanie praktyk bezpieczeństwa IT w ICS może powodować zakłócenia w dostępności i czasie reakcji. W komponentach ICS może nie być dostępnych zasobów obliczeniowych, aby wyposażyć te systemy w aktualne funkcje bezpieczeństwa. Dodanie zasobów lub funkcji może okazać się niemożliwe.

- **Komunikacja.** Protokoły komunikacyjne i media wykorzystywane przez środowiska ICS do sterowania urządzeniami obiektowymi i komunikacji wewnątrz procesowej, różnią się zazwyczaj od większości środowisk informacyjnych i mogą być prawnie zastrzeżone.
- **Zarządzanie zmianami.** Zarządzanie zmianami ma nadrzędne znaczenie dla zachowania integralności zarówno systemów informacyjnych, jak i sterowania. Nieuaktualnione oprogramowanie stanowi jedną z największych podatności systemu na ataki. Aktualizacje oprogramowania w systemach IT, w tym poprawki bezpieczeństwa, są zazwyczaj stosowane w odpowiednim czasie w oparciu o właściwą politykę i procedury bezpieczeństwa. Ponadto, procedury te są często zautomatyzowane przy użyciu narzędzi serwerowych. Aktualizacje oprogramowania w ICS nie zawsze mogą być wdrażane na czas. Aktualizacje te przed wdrożeniem muszą być dokładnie przetestowane zarówno przez dostawcę aplikacji sterowania przemysłowego, jak i przez użytkownika końcowego aplikacji. Ponadto właściciel ICS musi zaplanować i stworzyć harmonogram wyłączenia ICS z kilkudniowym/tygodniowym wyprzedzeniem. ICS może również wymagać przedłużenia ważności w ramach procesu aktualizacji. Innym problemem jest to, że wiele systemów ICS wykorzystuje starsze wersje systemów operacyjnych, które nie są już wspierane przez producenta. W związku z tym mogą nie być dostępne uaktualnienia. Zarządzanie zmianami dotyczy również sprzętu i oprogramowania firmowego. Proces zarządzania zmianą, gdy jest stosowany do ICS, wymaga starannej oceny przez ekspertów ICS (np. inżynierów sterowania) współpracujących z personelem bezpieczeństwa i IT.
- **Zarządzane wsparciem.** Typowe systemy informacyjne pozwalają na zróżnicowane formy wsparcia, być może obsługując różne, ale wzajemnie połączone architektury technologiczne. W przypadku ICS wsparcie serwisowe jest czasami zapewniane przez jednego dostawcę, który może nie dysponować zróżnicowanym i interoperacyjnym rozwiązaniem wsparcia od innego dostawcy. W niektórych przypadkach rozwiązania zabezpieczające innych firm nie są dozwolone ze względu na umowy licencyjne i serwisowe dostawców ICS, a utrata wsparcia serwisowego

może nastąpić, jeśli aplikacje innych firm zostaną zainstalowane bez potwierdzenia lub zgody dostawcy.

- **Żywotność komponentów.** Typowe komponenty IT mają okres eksploatacji rzędu 3-5 lat, przy czym okres ten jest krótki ze względu na szybki rozwój technologii. W przypadku ICS, gdzie technologia została w wielu przypadkach opracowana do bardzo specyficznego zastosowania i wdrożenia, okres eksploatacji wdrożonej technologii wynosi często od 10 do 15 lat a czasami dłużej.
- **Lokalizacja komponentów.** Większość komponentów IT i niektóre ICS są zlokalizowane w obiektach biznesowych i komercyjnych fizycznie dostępnych za pomocą lokalnego transportu. Odległe lokalizacje mogą być wykorzystywane jako obiekty zapasowe. Rozproszone komponenty ICS mogą być odizolowane, odległe i aby do nich dotrzeć może być wymagany duży wysiłek logistyczny. Lokalizacja komponentów musi również uwzględniać niezbędne fizyczne i środowiskowe środki bezpieczeństwa.

W tabeli 2-1 zestawiono niektóre typowe różnice między systemami IT a ICS.

Tabela 2-1. Podsumowanie różnic między systemami IT a ICS.

Kategoria	System informacyjny	System sterowania przemysłowego
Wymagania dotyczące wydajności	Praca w czasie nieokreślonym.	Praca w czasie rzeczywistym.
	Konsekwentna reakcja.	Reakcja krytyczna czasowo.
	Wymagana wysoka przepustowość.	Akceptowalna umiarkowana przepustowość.
	Akceptowalne wysokie opóźnienie i jitter.	Niedopuszczalne wysokie opóźnienie i/lub jitter.
	Mniej krytyczna interakcja w sytuacji awaryjnej.	Krytyczna interakcja na międzyludzkie i inne sytuacje awaryjne.
	Wdrożona ścisła kontrola dostępu w stopniu niezbędnym do zapewnienia bezpieczeństwa.	Rygorystycznie kontrolowany dostęp do ICS, nie utrudniający lub zakłócający interakcji człowiek – maszyna.
Wymagania dotyczące dostępności (niezawodności)	Odpowiedzi, takie jak ponowne uruchomienie systemu, mogą być dopuszczalne.	Odpowiedzi, takie jak ponowne uruchomienie systemu, mogą być niedopuszczalne ze względu na wymagania dotyczące dostępności procesu.
	Niedostępność może być tolerowana, w zależności od wymagań operacyjnych systemu.	Wymagania dotyczące dostępności mogą nakazywać stosowanie systemów redundantnych.
		Wyłączenia muszą być zaplanowane z kilkudniowym/tygodniowym wyprzedzeniem.

Kategoria	System informacyjny	System sterowania przemysłowego
		Wysoka dostępność wymaga przeprowadzania szczegółowych testów przedwdrożeniowych.
Wymagania w zakresie zarządzania ryzykiem	Zarządzanie danymi.	Sterowanie światem fizycznym.
	Najważniejsza jest poufność i integralność danych.	Najważniejsze jest bezpieczeństwo ludzi a następnie ochrona procesu.
	Odporność na błędy jest mniej ważna - chwilowe przestoje nie stanowią poważnego ryzyka.	Odporność na błędy jest niezbędna, nawet chwilowe przestoje mogą być nie do zaakceptowania.
	Głównym skutkiem ryzyka jest opóźnienie operacji biznesowych.	Główne skutki ryzyka to niezgodność z przepisami, wpływ na środowisko, utrata życia, sprzętu lub produkcji.
Działanie systemu	Systemy przeznaczone są do pracy z typowymi systemami operacyjnymi.	Różniące się i ewentualnie chronione prawem systemy operacyjne, często bez wbudowanych funkcji bezpieczeństwa.
	Aktualizacje są proste dzięki dostępności zautomatyzowanych narzędzi wdrożeniowych.	Zmiany w oprogramowaniu muszą być wprowadzane ostrożnie, zazwyczaj przez producentów oprogramowania, ze względu na wyspecjalizowane algorytmy sterowania i być może zmodyfikowanego sprzętu i oprogramowania.

Kategoria	System informacyjny	System sterowania przemysłowego
Ograniczenia zasobów	Systemy są wyposażone w wystarczające zasoby do obsługi dodawania aplikacji stron trzecich, takich jak rozwiązania w zakresie bezpieczeństwa.	Systemy są zaprojektowane do obsługi zamierzonego procesu przemysłowego i mogą nie mieć wystarczającej ilości pamięci i zasobów obliczeniowych, aby wspierać dodanie funkcji bezpieczeństwa.
Komunikacja	Stosowane są standardowe protokoły komunikacyjne.	Stosowanych jest wiele chronionych prawem oraz standardowych protokołów komunikacyjnych.
	Wykorzystywane są głównie sieci przewodowe z możliwością korzystania z lokalnych sieci bezprzewodowymi.	Stosowanych jest kilka rodzajów mediów komunikacyjnych, w tym dedykowane przewodowe i bezprzewodowe (radiowe i satelitarne).
	Mają zastosowanie typowe praktyki sieciowe IT.	Sieci są złożone i czasami wymagają wiedzy specjalistycznej inżynierów sterowania.
Zarządzanie zmianami	Zmiany w oprogramowaniu są wprowadzane w odpowiednim czasie przy zachowaniu zasad i procedur bezpieczeństwa. Procedury te są często zautomatyzowane.	Zmiany w oprogramowaniu muszą być dokładnie testowane i wdrażane przyrostowo w całym systemie, aby zapewnić utrzymanie integralności systemu sterowania. Wyłączenia systemów ICS często muszą być zaplanowane z kilkudniowym lub tygodniowym wyprzedzeniem.

Kategoria	System informacyjny	System sterowania przemysłowego
		W systemach ICS mogą być używane systemy operacyjne, które nie są już wspierane.
Zarządzanie wsparciem	Możliwe stosowanie zróżnicowanych rodzajów wsparcia	Wsparcie serwisowe jest zazwyczaj świadczone przez jednego dostawcę.
Czas życia systemu	Żywotność rzędu 3 do 5 lat.	Żywotność rzędu 10 do 15 lat.
Lokalizacja komponentów	Komponenty są zazwyczaj lokalne i łatwo dostępne.	Komponenty mogą być odizolowane, odległe i wymagać dużego wysiłku fizycznego, aby uzyskać do nich dostęp.

Podsumowując, różnice operacyjne i różnice ryzyka pomiędzy systemami ICS a IT stwarzają potrzebę zwiększenia stopnia zaawansowania w stosowaniu strategii cyberbezpieczeństwa i strategii operacyjnych. Wielofunkcyjny zespół inżynierów sterowania, operatorów systemów sterowania oraz specjalistów ds. bezpieczeństwa IT musi ściśle współpracować w celu zrozumienia możliwych implikacji instalacji, obsługi i konserwacji rozwiązań bezpieczeństwa w połączeniu z obsługą systemu sterowania. Specjaliści IT pracujący z ICS muszą zrozumieć wpływ technologii bezpieczeństwa informacji na niezawodność przed ich wdrożeniem. Niektóre systemy operacyjne i aplikacje działające w ICS mogą nie działać prawidłowo z komercyjnymi rozwiązaniami cyberbezpieczeństwa IT dostępnymi w sprzedaży (*ang. commercial-off-the-shelf - COTS*) ze względu na specjalistyczną architekturę środowiska ICS.

2.5. Inne rodzaje systemów sterowania

Chociaż niniejszy dokument zawiera wytyczne dotyczące zabezpieczenia ICS, inne rodzaje systemów sterowania mają podobne cechy i wiele z zaleceń zawartych w tym przewodniku ma zastosowanie i może być wykorzystywanych jako punkt odniesienia do ochrony tych systemów przed cyberzagrożeniami. Na przykład, mimo, że wiele

systemów budowlanych, transportowych, medycznych, ochrony i logistycznych wykorzystuje inne protokoły, porty i usługi, a także jest skonfigurowanych i działa w innych trybach niż ICS, mają one podobne cechy do tradycyjnych ICS [18].

Przykłady niektórych z tych systemów i protokołów obejmują:

Inne rodzaje systemów sterowania

- Zaawansowana infrastruktura pomiarowa.
- Systemy automatyki budynków.
- Systemy nadzoru telewizji przemysłowej (*ang. Closed-Circuit Television - CCTV*).
- Monitoring dwutlenku węgla CO_2.
- Systemy podpisu cyfrowego.
- Systemy zarządzania cyfrowym obrazem wideo.
- Elektroniczne systemy ochrony.
- Systemy zarządzania kryzysowego.
- Systemy zarządzania energią.
- Systemy sterowania oświetleniem zewnętrznym.
- Systemy sygnalizacji pożaru.
- Systemy tryskaczy przeciwpożarowych.
- Systemy sterowania oświetleniem wewnętrznym.
- Systemy wykrywania włamań.
- Systemy fizycznej kontroli dostępu.
- Bezpieczeństwo publiczne/Radiotelefony.
- Systemy geotermalnej energii odnawialnej.
- Systemy fotowoltaicznej energii odnawialnej.
- Systemy kontroli zaciemnienia.
- Systemy oddymiania i oczyszczania.

- System transportu pionowego (windy i schody ruchome).
- Systemy sterowania urządzeniami laboratoryjnymi.
- Systemy zarządzania informacją laboratoryjną (ang. Laboratory Information Management Systems - LIMS).

Protokoły/porty i usługi

- Modbus: urządzenia nadrzędne/podrzędne (*ang. Master/Slave*) - Port 502.
- BACnet[6] : urządzenia nadrzędne/podrzędne - Port 47808.
- LonWorks/LonTalk[7]: połączenie równorzędne (*ang. Peer to Peer*) - Port 1679.
- DNP3: Urządzenie nadrzędne/podrzędne - port 19999 w przypadku korzystania z zabezpieczenia warstwy transportowej (*ang. Transport Layer Security - TLS*), port 20000 w przypadku niekorzystania z TLS.
- 802.x - połączenie równorzędne (Peer to Peer).
- ZigBee - połączenie równorzędne (Peer to Peer).
- Bluetooth - urządzenia nadrzędne/podrzędne (Master/Slave).

Zabezpieczenia przedstawione w Załączniku G niniejszego standardu są na tyle ogólne i elastyczne, że można je wykorzystać do oceny innych rodzajów systemów sterowania, ale eksperci merytoryczni powinni je przejrzeć i odpowiednio dostosować, aby uwzględnić wyjątkowość innych rodzajów systemów sterowania. Nie ma „jednego rozwiązania pasującego do wszystkiego", a ryzyko może nie być takie samo, nawet w obrębie danej grupy. Na przykład, w budynku znajduje się wiele różnych podsystemów, takich jak automatyka budynku, sygnalizacja pożaru, fizyczna kontrola dostępu, oznakowanie cyfrowe, telewizja przemysłowa itp. Systemy bezpieczeństwa o znaczeniu krytycznym dla życia, takie jak alarm przeciwpożarowy i system kontroli dostępu fizycznego, mogą spowodować, że poziom wpływu będzie „wysoki", podczas gdy pozostałe systemy będą miały zazwyczaj poziom „niski". Organizacja może

[6] http://www.bacnet.org/

[7] http://en.wikipedia.org/wiki/LonWorks

zdecydować się na indywidualną ocenę każdego podsystemu, lub zdecydować się na zastosowanie podejścia zagregowanego. Ocena systemów sterowania powinna być połączona z oceną wpływu na działalność, planem awaryjnym i planem reagowania na incydenty, aby zapewnić, że krytyczne funkcje i operacje organizacji mogą zostać przywrócone i odtworzone zgodnie z czasem odzyskiwania (*ang. Recovery Time Objectives – RTO*).

3. ZARZĄDZANIE I SZACOWANIE RYZYKA ICS

3.1. Zarządzanie ryzykiem

Organizacje realizując swoje cele biznesowe codziennie zarządzają ryzykiem. Ryzyko to może, przykładowo, obejmować ryzyko finansowe, ryzyko awarii sprzętu oraz ryzyko związane z bezpieczeństwem personelu. Organizacje muszą opracować procesy pozwalające szacować ryzyko związane z ich działalnością oraz zdecydować, jak radzić sobie z tym ryzykiem w oparciu i priorytety organizacyjne oraz ograniczenia zarówno wewnętrzne, jak i zewnętrzne. Zarządzanie ryzykiem jest prowadzone jako interaktywny, ciągły proces w ramach wykonywania normalnych operacji. Organizacje wykorzystujące ICS historycznie zarządzały ryzykiem poprzez dobre praktyki w zakresie ochrony i inżynierii. Oceny ochrony są dobrze ugruntowane w większości sektorów i są często włączane do wymogów regulacyjnych. Zarządzanie ryzykiem związanym z bezpieczeństwem informacji stanowi dodatkowy wymiar, który może mieć charakter uzupełniający. Proces i ramy zarządzania ryzykiem przedstawione w tej sekcji mogą być stosowane do każdego szacowania ryzyka, w tym zarówno ochrony, jak i bezpieczeństwa informacji.

Proces zarządzania ryzykiem powinien być stosowany w całej organizacji, z wykorzystaniem podejścia trójwarstwowego w celu uwzględnienia ryzyka na (I) poziomie organizacji; (II) poziomie misji/procesu biznesowego; oraz (III) poziomie systemu informacyjnego (IT oraz ICS). Proces zarządzania ryzykiem jest prowadzony w sposób płynny na wszystkich trzech poziomach, a jego ogólnym celem jest ciągłe doskonalenie działań związanych z ryzykiem oraz efektywna komunikacja między poziomami i wewnątrz poziomów pomiędzy wszystkimi zainteresowanymi stronami, które mają wspólny interes w zapewnianiu powodzenia misji/biznesu organizacji.

W rozdziale tym skupiono się przede wszystkim na rozważaniach dotyczących ICS na poziomie systemu informacyjnego, należy jednak zauważyć, że działania, informacje i artefakty związane z zarządzaniem ryzykiem na każdym poziomie mają wpływ na pozostałe poziomy i są dla nich źródłem informacji. Rozdział 6 rozszerza przedstawione tu koncepcje i poziomy kategorii zabezpieczeń i przedstawia specyficzne dla ICS

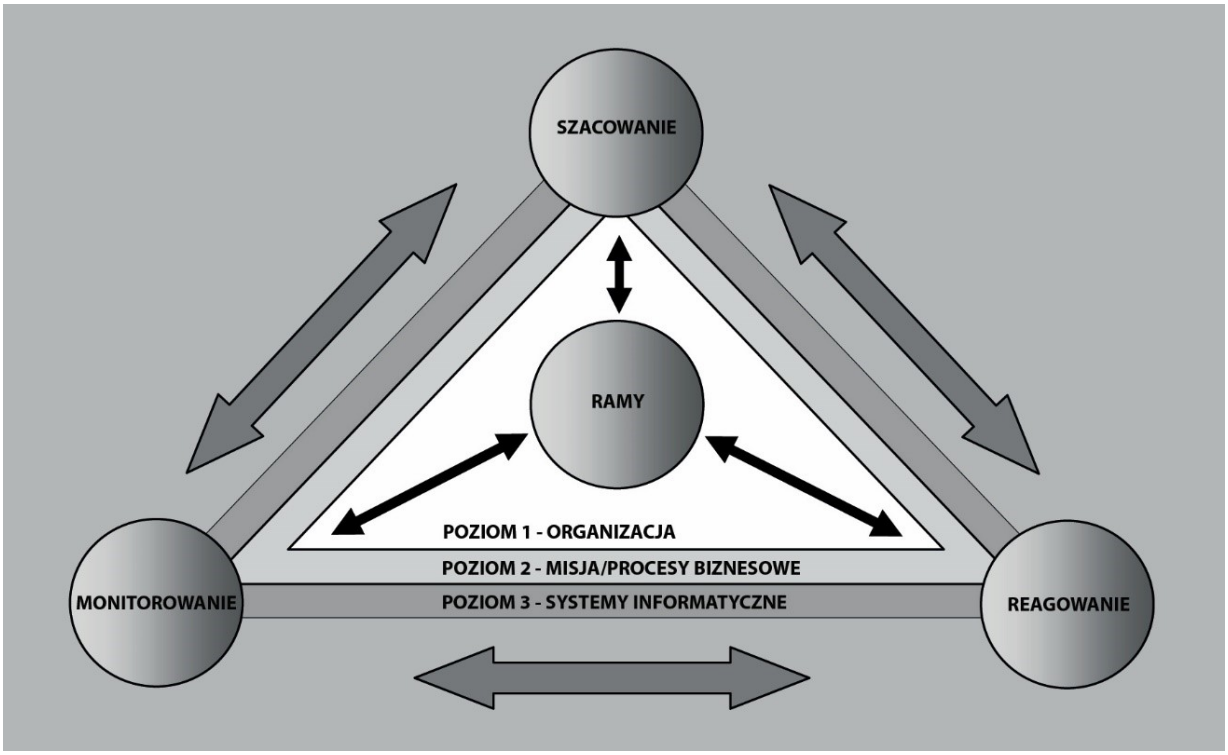
zalecenia rozszerzające kategorie zabezpieczeń. W całym poniższym omówieniu zarządzania ryzykiem zostaną przedstawione uwarunkowania związane z ICS oraz omówiony zostanie wpływ, jaki te względy mają na proces zarządzania ryzykiem.[8]

3.2. Wprowadzenie do procesu zarządzania ryzykiem

Jak pokazano na rysunku 3-1, proces zarządzania ryzykiem składa się z czterech elementów: *określania ram*, *szacowania*, *reagowania i monitorowania*. Działania te są współzależne i w organizacji często występują jednocześnie. Na przykład, wyniki komponentu monitorującego będą wykorzystane w elemencie określającym ramy. Ponieważ środowisko, w którym działają organizacje, stale się zmienia, zarządzanie ryzykiem musi być procesem ciągłym, w którym wszystkie komponenty działają na bieżąco. Ważne jest, aby pamiętać, że komponenty te mają zastosowanie do zarządzania każdym ryzykiem, niezależnie od tego, czy jest to ryzyko związane z bezpieczeństwem informacji, bezpieczeństwem fizycznym, ochroną czy ryzykiem finansowym.

[8] Więcej informacji na temat procesu zarządzania ryzykiem można znaleźć w publikacjach:

- NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission and Information System View [20]; (polskie opracowanie: NSC 800-39, Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego);
- NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations. a System Life Cycle Approach for Security and Privacy. [21] (polskie opracowanie: NSC 800-37, Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu);
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems (polskie opracowanie: NSC 199, Standardy Kategoryzacji Bezpieczeństwa);
- NIST Special Publication 800-30, Guide for Conducting Risk Assessments (polskie opracowanie: NSC 800-30, Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne).



Rysunek 3-1. Proces zarządzania ryzykiem stosowany na wszystkich poziomach.

Komponent „ramy” (komponent ramowy, komponent tworzenia ram) w procesie zarządzania ryzykiem polega na opracowaniu ram dla podejmowanych decyzji w zakresie zarządzania ryzykiem. Poziom ryzyka, który organizacja jest skłonna zaakceptować, to *tolerancja na ryzyko.*

Komponent „ramy” powinien obejmować przegląd istniejącej dokumentacji, takiej jak wcześniejsze szacowania ryzyka. Mogą istnieć powiązane działania, takie jak planowanie zarządzania klęskami żywiołowymi w całej społeczności, które również należy wziąć pod uwagę, ponieważ mają one wpływ na wymagania, które muszą być uwzględnione w szacowaniu ryzyka.

Zalecenia i wytyczne dotyczące ICS

Ochrona systemów ICS jest dla operatorów głównym czynnikiem, który bezpośrednio wpływa na decyzje dotyczące projektowania i eksploatacji systemów. Ochronę można zdefiniować jako "brak warunków, które mogą spowodować śmierć, obrażenia, chorobę zawodową, uszkodzenie lub utratę sprzętu lub własności, lub szkodę dla środowiska" . Częścią komponentu tworzenia ram dla organizacji ICS jest określenie,

jak te wymagania współgrają z bezpieczeństwem informacji. Na przykład, jeśli wymagania ochrony są sprzeczne z dobrymi praktykami bezpieczeństwa, jak organizacja będzie decydować pomiędzy tymi dwoma priorytetami? Większość operatorów ICS odpowiedziałaby, że ochrona jest głównym czynnikiem branym pod uwagę – komponent tworzenia ram czyni takie założenia jednoznacznymi, tak aby istniała zgodność w całym procesie i w organizacji.

Innym istotnym problemem dla operatorów ICS jest dostępność usług świadczonych przez ICS. System ICS może być częścią infrastruktury krytycznej (na przykład systemów wodnych lub energetycznych), w przypadku której istnieje znacząca potrzeba ciągłego i niezawodnego działania. W związku z tym systemy ICS mogą mieć ścisłe wymagania dotyczące dostępności lub odtwarzania. Takie założenia powinny być opracowane i określone w komponencie ramowym. W przeciwnym razie organizacja może podjąć decyzje dotyczące ryzyka, które spowodują niezamierzone konsekwencje dla tych, którzy są zależni od świadczonych usług.

Fizyczne środowisko operacyjne to kolejny aspekt kształtowania ryzyka, który organizacje powinny rozważyć podczas pracy z ICS. Systemy ICS często mają specyficzne wymagania środowiskowe (np. proces produkcyjny może wymagać precyzyjnej temperatury) lub mogą być związane ze swoim fizycznym środowiskiem działania. Takie wymagania i ograniczenia powinny być wyraźnie określone w komponencie ramowym, tak aby ryzyka wynikające z tych ograniczeń mogły być zidentyfikowane i rozważone.

Szacowanie ryzyka wymaga, aby organizacje zidentyfikowały swoje zagrożenia i podatności, szkody, jakie te zagrożenia i podatności mogą wyrządzić organizacji oraz prawdopodobieństwo wystąpienia niekorzystnych zdarzeń wynikających z tych zagrożeń i podatności.

Zalecenia i wytyczne dotyczące ICS

Przy ocenie wpływu potencjalnego incydentu ICS na misję organizacji, ważne jest, aby wśród innych możliwości uwzględnić wpływ na fizyczny proces/system, wpływ na zależne systemy/procesy oraz wpływ na środowisko fizyczne. Dodatkowo, zawsze należy rozważyć potencjalny wpływ na bezpieczeństwo.

Komponent reagowania opiera się na koncepcji spójnej, ogólnoorganizacyjnej reakcji na identyfikowane ryzyka. Reakcja na identyfikację ryzyka (w przeciwieństwie do reakcji na incydent) wymaga, aby organizacje najpierw rozważyły możliwe kierunki działań w celu zaadresowania ryzyka, oceniły te możliwości w świetle tolerancji organizacji na ryzyko, przy uwzględnieniu innych czynników określonych podczas etapu tworzenia ram, a następnie wybrały optymalną alternatywę dla organizacji. Element reakcji obejmuje wdrożenie wybranego sposobu działania w celu rozwiązania problemu zidentyfikowanego ryzyka: *akceptacja*, *unikanie*, *łagodzenie*, *współdzielenie*, *przekazywanie* lub dowolna kombinacja tych opcji[9].

Zalecenia i wytyczne dotyczące ICS

W przypadku ICS dostępne reakcje na ryzyko mogą być ograniczone przez wymagania systemowe, potencjalny niekorzystny wpływ na działalność operacyjną lub reżimami zgodności z przepisami. Przykładem współdzielenia ryzyka jest sytuacja, w której przedsiębiorstwa energetyczne zawierają umowy o "użyczeniu" pracowników liniowych w sytuacjach awaryjnych, co skraca czas trwania skutków zdarzenia do akceptowalnego poziomu.

Monitorowanie jest czwartym elementem działań związanych z zarządzaniem ryzykiem. Organizacje muszą na bieżąco monitorować ryzyko, w tym: wdrażanie wybranych strategii zarządzania ryzykiem, zmiany w otoczeniu, które mogą wpłynąć na kalkulację ryzyka, oraz skuteczność i efektywność działań ograniczających ryzyko. Działania

[9] Dodatkowe informacje na temat akceptowania, unikania, ograniczania, dzielenia się lub przenoszenia ryzyka można znaleźć w publikacji NSC 800-39.

w ramach komponentu monitorowania mają wpływ na wszystkie pozostałe komponenty.

3.3. Szczególne rozważania dotyczące przeprowadzania szacowania ryzyka

Charakter systemu ICS powoduje, że podczas przeprowadzania przez organizację szacowania ryzyka, mogą pojawić się dodatkowe czynniki, które nie występują podczas przeprowadzania szacowania ryzyka tradycyjnego systemu informacyjnego. Ponieważ wpływ incydentu w ICS może obejmować zarówno skutki fizyczne, jak i cyfrowe, szacowanie ryzyka musi uwzględniać te potencjalne skutki. W tym rozdziale zostaną dokładniej przeanalizowane następujące kwestie:

- Wpływ na bezpieczeństwo i wykorzystanie ocen bezpieczeństwa.
- Fizyczny wpływ cyberincydentu na ICS, w tym na większe środowisko fizyczne; wpływ na kontrolowany proces oraz fizyczny wpływ na sam ICS.
- Konsekwencje dla szacowania ryzyka związanego z analogowymi elementami sterowania w ramach ICS.

3.3.1. Bezpieczeństwo w ramach szacowania ryzyka ochrony informacji w systemach ICS

Kultura ochrony i ocen ochrony jest dobrze ugruntowana w większości społeczności użytkowników ICS. Szacowanie ryzyka w zakresie bezpieczeństwa informacji powinno być postrzegane jako uzupełniające w stosunku do szacowania ryzyka w odniesieniu do biznesu/ misji organizacji, chociaż mogą one wykorzystywać różne podejścia i obejmować różne obszary. Oceny ochrony dotyczą przede wszystkim świata fizycznego. Szacowanie ryzyka w zakresie bezpieczeństwa informacji dotyczy przede wszystkim świata cyfrowego. Jednak w środowisku ICS elementy fizyczne i cyfrowe są ze sobą powiązane i mogą się w znacznym stopniu nakładać.

Ważne jest, aby podczas przeprowadzania szacowania ryzyka w zakresie bezpieczeństwa informacji organizacje uwzględniały wszystkie aspekty zarządzania ryzykiem dla bezpieczeństwa (np. określanie ram ryzyka, tolerancje ryzyka), a także

wyniki oceny bezpieczeństwa. Pracownicy odpowiedzialni za szacowanie ryzyka związanego z bezpieczeństwem informacji muszą być w stanie zidentyfikować zagrożenia, które mogą mieć wpływ na bezpieczeństwo, i poinformować o nich. Z kolei pracownicy odpowiedzialni za ocenę bezpieczeństwa muszą znać potencjalne skutki fizyczne i prawdopodobieństwo ich wystąpienia, które zostały określone w procesie szacowania ryzyka w zakresie bezpieczeństwa informacji.

3.3.2. Potencjalne skutki fizyczne incydentu ICS

Ocena potencjalnych szkód fizycznych spowodowanych cyberincydentem powinna uwzględniać: (I) sposób, w jaki incydent mógłby manipulować działaniem czujników i elementów wykonawczych, aby wpłynąć na środowisko fizyczne; (II) nadmiarowe mechanizmy zabezpieczeń istniejące w ICS, zapobiegające takiemu wpływowi; oraz (III) sposób, w jaki incydent fizyczny mógłby powstać w oparciu o te warunki.

Zdarzenie fizyczne może negatywnie wpłynąć na otaczający świat na wiele sposobów, w tym poprzez uwolnienie materiałów niebezpiecznych (np. zanieczyszczeń, ropy naftowej), niszczące siły kinetyczne (np. eksplozje) oraz narażenie na działanie źródeł energii (np. elektryczności, pary).

Zdarzenie fizyczne może mieć negatywny wpływ na ICS i infrastrukturę wspierającą, różne procesy realizowane przez ICS lub większe środowisko fizyczne. Ocena potencjalnych oddziaływań fizycznych powinna obejmować wszystkie elementy systemu ICS, począwszy od oceny potencjalnych oddziaływań na zestaw czujników i elementów wykonawczych. Każda z tych dziedzin zostanie dokładniej przeanalizowana poniżej.

Ocena wpływu cyberincydentu na środowisko fizyczne powinna koncentrować się na potencjalnych szkodach dla bezpieczeństwa ludzi, środowiska naturalnego i innych infrastruktur krytycznych. Wpływ na bezpieczeństwo ludzi powinien być oceniany na podstawie tego, czy możliwe jest wystąpienie obrażeń, chorób lub śmierci w wyniku nieprawidłowego działania ICS. Ocena ta powinna uwzględniać wszelkie wcześniej przeprowadzone przez organizację oceny wpływu na bezpieczeństwo, dotyczące zarówno pracowników, jak i ogółu społeczeństwa. Konieczne może być również

uwzględnienie oddziaływań na środowisko. Analiza ta powinna uwzględniać wszelkie dostępne oceny oddziaływania na środowisko wykonane przez organizację w celu określenia, jak zdarzenie może wpłynąć na zasoby naturalne i dzikie zwierzęta w krótkim lub długim okresie. Ponadto, należy zauważyć, że ICS może nie być zlokalizowany w jednym, kontrolowanym miejscu i może być rozmieszczony na dużym obszarze fizycznym i narażony na oddziaływanie niekontrolowanego środowiska. Wreszcie, wpływ na środowisko fizyczne powinien obejmować zbadanie zakresu, w jakim incydent może uszkodzić infrastrukturę zewnętrzną w stosunku do ICS (np. wytwarzanie/dostarczanie energii elektrycznej, infrastruktura transportowa i usługi wodne).

3.3.3. Skutki fizycznego zakłócenia procesu systemu ICS

Oprócz wpływu na środowisko fizyczne w szacowaniu ryzyka należy również ocenić potencjalne skutki wpływu na proces fizyczny realizowany przez rozpatrywany ICS, a także na inne systemy. Zdarzenie, które oddziałuje na system ICS i zakłóca zależny od niego proces, może mieć wpływ kaskadowy na inne powiązane procesy ICS oraz na zależność ogółu społeczeństwa od powstających produktów i usług. Oddziaływanie na powiązane procesy ICS może obejmować zarówno systemy i procesy wewnątrz organizacji (np. proces produkcyjny, który zależy od procesu sterowanego przez rozważany system), jak i systemy i procesy zewnętrzne w stosunku do organizacji (np. zakład energetyczny sprzedający wytworzoną energię pobliskiemu przedsiębiorstwu).

Cyberincydent może również negatywnie wpłynąć na fizyczny system ICS. Tego typu oddziaływanie obejmuje przede wszystkim fizyczną infrastrukturę organizacji (np. zbiorniki, zawory, silniki), a także cyfrowe i analogowe mechanizmy sterowania (np. kable, sterowniki PLC, manometr). Uszkodzenia ICS lub instalacji fizycznej mogą powodować krótko- lub długoterminowe przerwy w pracy w zależności od stopnia incydentu. Przykładem cyberincydentu mającego wpływ na ICS jest złośliwe oprogramowanie Stuxnet, które spowodowało fizyczne uszkodzenie wirówek, a także zakłóciło zależne od nich procesy.

3.3.4. Uwzględnienie analogowych aspektów w ocenie wpływu na system ICS

Wpływu na ICS nie można odpowiednio określić skupiając się jedynie na cyfrowych aspektach systemu, ponieważ często występują mechanizmy analogowe, które zapewniają odporność na błędy i uniemożliwiają ICS działanie poza dopuszczalnymi parametrami. Dlatego też mechanizmy te mogą pomóc w ograniczeniu negatywnego wpływu, jaki może mieć incydent cyfrowy na ICS i powinny zostać uwzględnione w procesie szacowania ryzyka. Na przykład, ICS często posiadają analogowe mechanizmy zabezpieczające, które mogą zapobiec działaniu ICS poza bezpieczną granicą, a tym samym ograniczyć skutki ataku (np. mechaniczny nadciśnieniowy zawór bezpieczeństwa). Ponadto mechanizmy analogowe (np. mierniki, alarmy) mogą być wykorzystywane do obserwacji fizycznego stanu systemu, aby zapewnić operatorom wiarygodne dane, jeśli odczyty cyfrowe są niedostępne lub zakłócone.

Tabela 3-1 zawiera kategoryzację analogowych mechanizmów sterowania, które mogą być dostępne w celu zmniejszenia wpływu incydentu ICS.

Tabela 3-1. Kategorie analogowych komponentów sterowania systemu ICS.

Typ systemu	Opis
Wyświetlacze analogowe lub alarmy	Mechanizmy analogowe, które mierzą i wyświetlają stan systemu fizycznego (np. temperaturę, ciśnienie, napięcie, prąd) i mogą dostarczyć operatorowi dokładnych informacji w sytuacjach, gdy wyświetlacze cyfrowe są niedostępne lub zakłócone. Informacje te mogą być przekazywane operatorowi na niektórych niecyfrowych wyświetlaczach (np. termometrach, manometrach) oraz poprzez alarmy dźwiękowe.
Mechanizmy sterowania ręcznego	Mechanizmy sterowania ręcznego (np. ręczne sterowanie zaworami, fizyczne wyłączniki) zapewniają operatorom możliwość ręcznego sterowania napędem bez polegania na cyfrowym systemie sterowania. Zapewnia to możliwość sterowania napędem nawet w przypadku niedostępności lub uszkodzenia systemu sterowania.

Typ systemu	Opis
Analogowe systemy sterowania	Analogowe systemy sterowania wykorzystują niecyfrowe czujniki i siłowniki do monitorowania i sterowania procesem fizycznym. Mogą one być w stanie zapobiec wprowadzeniu procesu fizycznego w niepożądany stan w sytuacjach, gdy cyfrowy system sterowania jest niedostępny lub uszkodzony. Sterowniki analogowe obejmują urządzenia takie jak regulatory, urządzenia zarządzające i przekaźniki elektromechaniczne.

Określenie potencjalnego wpływu, jaki cyberincydent może mieć na ICS, powinno obejmować analizę wszystkich niecyfrowych mechanizmów sterujących oraz stopnia, w jakim mogą one złagodzić potencjalne negatywne skutki w ICS. Rozważając możliwe skutki łagodzące niecyfrowych mechanizmów sterowania, należy wziąć pod uwagę wiele czynników, takich, jak:

- Niecyfrowe mechanizmy sterujące mogą wymagać dodatkowego czasu i znacznego zaangażowania człowieka w celu wykonania niezbędnych funkcji monitorowania lub sterowania. Na przykład, takie mechanizmy mogą wymagać od operatorów udania się do odległych miejsc w celu przeprowadzenia pewnych funkcji sterowania. Mechanizmy takie mogą być również uzależnione od czasu reakcji człowieka, który może być wolniejszy niż w przypadku sterowania automatycznego.
- Systemy ręczne i analogowe mogą nie zapewniać możliwości monitorowania lub sterowania z taką samą dokładnością i niezawodnością jak cyfrowy system sterowania. Może to stwarzać ryzyko, jeśli główny system sterowania jest niedostępny lub uszkodzony z powodu obniżenia jakości, bezpieczeństwa lub wydajności systemu. Na przykład, cyfrowy/numeryczny przekaźnik zabezpieczający zapewnia większą dokładność i niezawodność wykrywania usterek niż przekaźniki analogowe/statyczne, dlatego też system może wykazywać większe prawdopodobieństwo wystąpienia fałszywego zadziałania przekaźnika, jeśli przekaźniki cyfrowe nie będą dostępne.

3.3.5. Uwzględnienie wpływu systemów bezpieczeństwa

Systemy bezpieczeństwa mogą również ograniczyć wpływ cyberincydentu na ICS. Systemy bezpieczeństwa są często wdrażane w celu realizacji określonych funkcji monitorowania i zabezpieczeń, aby zapewnić bezpieczeństwo ludzi, środowiska, procesów i ICS. Chociaż systemy te są tradycyjnie wdrażane jako w pełni redundantne w stosunku do głównego ICS, mogą one nie zapewniać pełnej redundancji w przypadku cyberincydentów, zwłaszcza ze strony zaawansowanego napastnika. Należy ocenić wpływ wdrożonych zabezpieczeń na system, aby stwierdzić, czy nie mają one negatywnego wpływu na ten system.

3.3.6. Uwzględnienie rozprzestrzeniania się wpływu na systemy połączone

Ocena wpływu zdarzenia musi również uwzględniać sposób, w jaki wpływ danego ICS może rozprzestrzeniać się na połączony ICS lub system fizyczny. System ICS może być połączony z innymi systemami w taki sposób, że awarie w jednym systemie lub procesie mogą łatwo przenosić się na inne systemy wewnątrz lub na zewnątrz organizacji. Rozprzestrzenianie się skutków może wystąpić zarówno ze względu na zależności fizyczne, jak i logiczne. Właściwe przekazywanie wyników szacowania ryzyka operatorom połączonych lub współzależnych systemów i procesów jest jednym ze sposobów łagodzenia takich oddziaływań.

Logiczne uszkodzenie połączonego ICS mogłoby nastąpić, gdyby cyberincydent rozprzestrzenił się na połączone systemy sterowania. Przykładem może być rozprzestrzenienie się wirusa lub robaka do połączonego ICS, a następnie oddziaływanie na ten system. Uszkodzenia fizyczne mogłyby również rozprzestrzenić się na inne połączone ze sobą ICS. Jeśli incydent ma wpływ na środowisko fizyczne ICS, może mieć także wpływ na inne powiązane domeny fizyczne. Oddziaływanie może na przykład spowodować zagrożenie fizyczne, które spowoduje degradację pobliskich środowisk fizycznych. Ponadto oddziaływanie może także pogorszyć funkcjonowania współdzielonych zasobów (np. zasilania energetycznego) lub spowodować niedobór materiałów potrzebnych do późniejszego etapu procesu przemysłowego.

4. OPRACOWANIE I WDROŻENIE PROGRAMU BEZPIECZEŃSTWA ICS

W rozdziale 2 omówiono istotne różnice operacyjne pomiędzy systemami ICS i IT, natomiast w rozdziale 3 - zarządzanie i szacowanie ryzyka. Niniejszy rozdział łączy te dwa zagadnienia poprzez omówienie sposobu, w jaki organizacje powinny opracowywać i wdrażać program bezpieczeństwa ICS. Plany i programy bezpieczeństwa ICS powinny być spójne i zintegrowane z istniejącymi doświadczeniami, programami i praktykami bezpieczeństwa IT, ale muszą uwzględniać specyficzne wymagania i cechy technologii środowisk ICS. Organizacje powinny regularnie przeglądać i aktualizować swoje plany i programy bezpieczeństwa ICS w celu odzwierciedlenia zmian w technologiach, operacjach, normach i przepisach, a także potrzeb bezpieczeństwa konkretnych obiektów.

W rozdziale tym przedstawiono przegląd rozwoju i wdrażania programu bezpieczeństwa ICS. W sekcji 4.1 opisano sposób tworzenia uzasadnienia biznesowego dla programu bezpieczeństwa ICS, w tym sugerowaną zawartość uzasadnienia biznesowego. W sekcjach od 4.2 do 4.5 omówiono opracowanie kompleksowego programu bezpieczeństwa ICS i przedstawiono informacje na temat kilku głównych etapów wdrażania programu. Informacje i konkretnych środkach bezpieczeństwa, które mogą być wdrożone w ramach programu bezpieczeństwa, znajdują się w rozdziale 6.

Skuteczne włączenie bezpieczeństwa do systemów ICS wymaga zdefiniowania i realizacji kompleksowego programu, który obejmuje wszystkie aspekty bezpieczeństwa, począwszy od określenia celów, poprzez codzienną eksploatację i bieżący audyt zgodności i doskonalenia. Należy wyznaczyć kierownika ds. bezpieczeństwa informacji w ICS posiadającego odpowiedni zakres obowiązków, odpowiedzialność i uprawnienia. W tej części opisano podstawowy proces tworzenia programu bezpieczeństwa, obejmujący następujące elementy:

- Opracowanie uzasadnienia biznesowego dotyczącego bezpieczeństwa.
- Stworzenie i przeszkolenie zespołu wielofunkcyjnego.

- Określenie statutu i zakresu.
- Określenie szczegółowych zasad i procedur dotyczących ICS.
- Wdrożenie ram zarządzania ryzykiem związanym z bezpieczeństwem systemów ICS:
  - ✓ określenie i inwentaryzacja aktywów ICS;
  - ✓ opracowanie planu bezpieczeństwa systemów ICS;
  - ✓ przeprowadzenie szacowania ryzyka;
  - ✓ określenie zabezpieczeń ograniczających ryzyko;
  - ✓ zapewnienie szkoleń i podnoszenie świadomości personelu ICS w zakresie bezpieczeństwa.

Bardziej szczegółowe informacje na temat poszczególnych kroków znajdują się w dokumencie ISA-62443-2-1, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program* [34].

Zaangażowanie w program bezpieczeństwa zaczyna się na poziomie najwyższego kierownictwa organizacji. Kierownictwo wyższego szczebla musi zademonstrować wyraźne zobowiązanie do zapewnienia bezpieczeństwa informacji. Bezpieczeństwo informacji jest odpowiedzialnością biznesową ponoszoną przez wszystkich członków przedsiębiorstwa, a w szczególności przez członków wiodących zespołów biznesowych, procesowych i zarządczych. Programy bezpieczeństwa informacji z odpowiednim finansowaniem i widocznym wsparciem na najwyższym szczeblu ze strony liderów organizacji mają większe szanse na osiągnięcie zgodności, sprawniejsze funkcjonowanie i większy sukces niż programy, którym tego wsparcia brakuje.

Za każdym razem, gdy projektowany i instalowany jest nowy system, konieczne jest poświęcenie czasu na uwzględnienie kwestii bezpieczeństwa w całym cyklu życia, od architektury, poprzez zakupy, instalację, obsługę, aż po wycofanie z eksploatacji. Istnieje poważne ryzyko związane z wdrażaniem systemów do produkcji w oparciu o założenie, że zostaną one zabezpieczone później. Jeżeli nie ma wystarczającej ilości czasu i zasobów, aby odpowiednio zabezpieczyć system przed wdrożeniem, jest mało

prawdopodobne, że później będzie wystarczająca ilość czasu i zasobów, aby zająć się bezpieczeństwem.

Projektowanie i wdrażanie nowego systemu są dość rzadkie. Znacznie częściej przeprowadzana jest modernizacja, rozbudowa lub aktualizacja istniejącego systemu. Zawarte w całym dokumencie informacje, odnoszą się do zarządzania ryzykiem w istniejącym systemie ICS. Tworzenie Programu Bezpieczeństwa ICS i zastosowanie go w istniejących systemach jest znacznie bardziej złożone i wymagające więcej nakładów pracy.

4.1. Uzasadnienie biznesowe zapewnienia bezpieczeństwa

Pierwszym krokiem w procesie wdrażania programu bezpieczeństwa informacji odnoszącego się do systemu ICS jest opracowanie przekonującego uzasadnienia biznesowego odnoszącego się do unikatowych potrzeb organizacji. Uzasadnienie biznesowe powinno uwzględniać kwestie biznesowe kierownictwa wyższego szczebla a jednocześnie opierać się na doświadczeniach osób, które już mają do czynienia z zagrożeniami. Uzasadnienie biznesowe przedstawia wpływ biznesowy i finansowe przesłanki stworzenia zintegrowanego programu bezpieczeństwa informacji. Powinno ono zawierać szczegółowe informacje na temat następujących kwestii:

- Korzyści, w tym zwiększona niezawodność i dostępność systemu sterowania, wynikające z utworzenia zintegrowanego programu bezpieczeństwa.
- Priorytetyzacji potencjalnych kosztów i scenariuszy szkód, jeśli program bezpieczeństwa informacji w ICS nie zostanie wdrożony.
- Wysokopoziomowego przeglądu procesów wymaganych do wdrożenia, obsługi, monitorowania, przeglądu, utrzymania i doskonalenia programu bezpieczeństwa informacji.
- Kosztów i zasobów wymaganych do opracowania, wdrożenia i utrzymania programu bezpieczeństwa.

Przed przedstawieniem uzasadnienia biznesowego kierownictwu, powinien istnieć dobrze przemyślany i opracowany plan wdrożenia obejmujący koszty zabezpieczeń. Na przykład, samo żądanie zainstalowania zapory sieciowej nie jest wystarczające.

4.1.1. Korzyści

Polityka odpowiedzialnego zarządzania ryzykiem stanowi, że zagrożenie dotyczące ICS powinno być mierzone i monitorowane w celu ochrony interesów pracowników, wspólnoty, udziałowców, klientów, sprzedawców, społeczeństwa i państwa. Analiza ryzyka umożliwia wyważenie kosztów i korzyści tak, aby można było podejmować świadome decyzje dotyczące działań ochronnych. Poza redukcją ryzyka, zachowanie należytej staranności i wykazywanie się odpowiedzialnością pomaga organizacjom w:

- Poprawie bezpieczeństwa, niezawodności i dostępności systemów sterowania.
- Podnoszeniu morale pracowników, ich lojalności i chęci pozostania w firmie.
- Zmniejszaniu niepokoju społeczności.
- Zwiększeniu zaufania inwestorów.
- Zmniejszeniu odpowiedzialności prawnej.
- Spełnieniu wymagań prawnych.
- Wzmocnieniu wizerunku i reputacji firmy.
- Wspomaganiu ochrony ubezpieczeniowej i kosztów.
- Poprawie relacji inwestorskich i finansowych.

Solidny program zarządzania bezpieczeństwem i ochroną informacji ma fundamentalne znaczenie dla zrównoważonego modelu biznesowego.

Poprawa bezpieczeństwa systemów sterowania oraz polityki bezpieczeństwa, specyficzne dla systemów sterowania, mogą potencjalnie zwiększyć niezawodność i dostępność tych systemów. Obejmuje to również minimalizację niezamierzonego wpływu na bezpieczeństwo informacji systemu sterowania, wynikającego z niewłaściwego testowania, polityk i niewłaściwie skonfigurowanych systemów.

4.1.2. Potencjalne konsekwencje

Znaczenie procesu ustanawiania bezpieczeństwa systemów powinno być jeszcze bardziej podkreślane w miarę jak wzrasta zależność biznesu od wzajemnych zależności z tym stanem. Ataki typu odmowa świadczenia usługi (*ang. Denial of Service - DoS*) i złośliwe oprogramowanie (*ang. malware*) np. robaki, wirusy, stały się zbyt powszechne i już wywierały wpływ na ICS. Cyberataki mogą mieć znaczące skutki fizyczne i następcze. Zarządzanie ryzykiem omówiono w rozdziale 3. Główne kategorie wpływu (skutków) są następujące:

- **Skutki fizyczne.** Obejmują zbiór bezpośrednich konsekwencji awarii ICS. Potencjalne skutki i nadrzędnym znaczeniu obejmują obrażenia ciała i utratę życia. Inne skutki obejmują utratę mienia (w tym danych) i potencjalne szkody w środowisku.
- **Skutki ekonomiczne.** Są efektem wtórnym w stosunku do skutków fizycznych wynikających z incydentu ICS. Wpływ fizyczny może powodować konsekwencje w działaniu systemu, które z kolei powodują większe straty ekonomiczne dla obiektu, organizacji lub innych osób zależnych od ICS. Niedostępność infrastruktury krytycznej (np. zasilania elektrycznego, transportu) może mieć skutki ekonomiczne daleko wykraczające poza systemy, które uległy bezpośrednim i fizycznym uszkodzeniom. Skutki te mogą mieć negatywny wpływ na gospodarkę lokalną, regionalną, krajową a nawet globalną.
- **Skutki społeczne.** Kolejny efekt wtórny, występujący jako konsekwencja wynikająca z utraty zaufania narodowego lub publicznego do organizacji, jest często pomijany. Jest to jednak bardzo realny skutek, która może wynikać z incydentu ICS.

Program kontroli takiego ryzyka jest omówiony w rozdziale 3. Należy zauważyć, że pozycje na tej liście nie są niezależne. W rzeczywistości każda z nich może prowadzić do drugiej. Na przykład, uwolnienie materiału niebezpiecznego może prowadzić do obrażeń lub śmierci. Przykłady potencjalnych konsekwencji incydentu ICS są wymienione poniżej:

- Wpływ na bezpieczeństwo narodowe - ułatwienie przeprowadzenia aktu terrorystycznego.
- Zmniejszenie lub utrata produkcji w jednym zakładzie lub w wielu zakładach jednocześnie.
- Obrażenia lub śmierć pracowników.
- Obrażenia lub śmierć osób w społeczności.
- Uszkodzenie sprzętu.
- Uwolnienie, przekierowanie lub kradzież materiałów niebezpiecznych.
- Szkody w środowisku naturalnym.
- Naruszenie wymogów regulacyjnych.
- Skażenie (*ang. contamination*) produktu.
- Odpowiedzialność prawna w sprawach karnych lub cywilnych.
- Utrata informacji niejawnych.
- Utrata wizerunku marki lub zaufania klientów.

Niepożądane incydenty każdego rodzaju obniżają wartość organizacji, ale incydenty związane z bezpieczeństwem i ochroną mogą mieć, w porównaniu do innych rodzajów incydentów, bardziej długotrwały negatywny wpływ na wszystkich interesariuszy - pracowników, udziałowców, klientów i społeczności, w których działa organizacja.

Lista potencjalnych skutków biznesowych powinna zostać uszeregowana pod względem ważności, tak aby skupić się na konkretnych skutkach biznesowych, które kierownictwo wyższego szczebla uzna za najbardziej przekonujące. Pozycje o najwyższym priorytecie przedstawione na liście uszeregowanych pod względem ważności skutków biznesowych należy ocenić w celu uzyskania szacunkowej oceny rocznego wpływu na działalność, najlepiej, ale niekoniecznie, w kategoriach finansowych.

Wykazanie należytej staranności jest wymagane przez większość wewnętrznych i zewnętrznych firm audytorskich, aby zadowolić udziałowców i innych interesariuszy

organizacji. Wdrażając kompleksowy program bezpieczeństwa informacji, kierownictwo zachowuje należytą staranność.

4.1.3. Źródła informacji na temat budowania uzasadnienia biznesowego

Istotne zasoby informacji pomocnych w formułowaniu uzasadnienia biznesowego można znaleźć w źródłach zewnętrznych należących do innych organizacji działających w podobnych branżach - indywidualnie lub w ramach wymiany informacji, organizacji handlowych i standaryzacyjnych, firm konsultingowych oraz w zasobach wewnętrznych w powiązanych programach zarządzania ryzykiem, inżynieryjnych i operacyjnych. Organizacje zewnętrzne mogą często dostarczyć przydatnych wskazówek dotyczących tego, jakie aspekty wpłynęły na wsparcie ich wysiłków przez kierownictwo i jakie zasoby wewnątrz organizacji okazały się najbardziej pomocne. W różnych branżach czynniki te mogą być inne, ale mogą być zbliżone do ról, jakie mogą być pełnione przez innych specjalistów ds. zarządzania ryzykiem. Załącznik D zawiera listę i krótki opis niektórych bieżących działań w zakresie bezpieczeństwa ICS.

Wewnętrzne zasoby w ramach powiązanych działań zarządzających ryzykiem (np. bezpieczeństwo informacji, ochrona zdrowia, bezpieczeństwo i ryzyko środowiskowe, bezpieczeństwo fizyczne, ciągłość działania) mogą zapewnić znaczącą pomoc w oparciu o ich doświadczenia z powiązanymi incydentami występującymi w organizacji. Informacje te są pomocne z punktu widzenia priorytetyzacji zagrożeń i szacowania wpływu na działalność firmy. Zasoby te mogą również zapewnić wgląd w to, którzy menedżerowie koncentrują się na zajmowaniu się poszczególnymi rodzajami ryzyka, a tym samym, którzy menedżerowie mogą być najbardziej odpowiedni lub najbardziej otwarci na pełnienie roli lidera. Zasoby wewnętrzne w zakresie inżynierii systemów sterowania i działalności operacyjnej, mogą zapewnić wgląd w szczegóły dotyczące sposobu wdrażania systemów sterowania w organizacji, np.:

- W jaki sposób dzielone i rozdzielane są sieci.
- Jakiego rodzaju połączenia zdalnego dostępu są zazwyczaj stosowane.

- Jak zazwyczaj projektowane są systemy sterowania wysokiego ryzyka lub systemy bezpieczeństwa.
- Jakie środki zaradcze w zakresie bezpieczeństwa są powszechnie stosowane.

4.1.4. Przedstawianie argumentów biznesowych kierownictwu organizacji

W rozdziale 3 przedstawiono podejście trójwarstwowe, które uwzględnia ryzyko na: (I) poziomie organizacji; (II) poziomie misji/procesu biznesowego; oraz (III) poziomie systemu informacyjnego. Proces zarządzania ryzykiem jest realizowany w sposób płynny na wszystkich trzech poziomach, a jego ogólnym celem jest ciągłe doskonalenie działań organizacji związanych z ryzykiem oraz efektywna komunikacja między poziomowa i wewnątrzpoziomowa pomiędzy wszystkimi uczestnikami, którzy mają wspólny interes w powodzeniu misji/biznesu organizacji.

Dla powodzenia programu bezpieczeństwa ICS decydujące znaczenie ma to, aby kierownictwo szczebla organizacyjnego włączyło się do programu bezpieczeństwa ICS i uczestniczyło w nim aktywnie. Kierownictwo poziomu 1 organizacji, które obejmuje zarówno operacje IT jak i ICS, ma perspektywę i kompetencje do uświadomienia sobie ryzyka i wzięcia odpowiedzialności.

Kierownictwo biznesowe poziomu 1 będzie odpowiedzialne za zatwierdzanie i prowadzenie polityki bezpieczeństwa informacji, przydzielanie ról i obowiązków związanych z bezpieczeństwem oraz wdrażanie programu bezpieczeństwa informacji w całej organizacji. Finansowanie całego programu może być zwykle realizowane etapami. Na początek działań związanych z bezpieczeństwem informacji mogą być wymagane pewne środki finansowe, ale dodatkowe środki można uzyskać w późniejszym czasie, gdy lepiej poznane zostaną podatności na zagrożenia bezpieczeństwa i potrzeby programu oraz opracowane zostaną dodatkowe strategie. Ponadto należy rozważyć koszty (zarówno bezpośrednie, jak i pośrednie) związane z modernizacją ICS pod kątem bezpieczeństwa wobec przyjętych na początku działań związanych z bezpieczeństwem.

Często dobrym sposobem na uzyskanie poparcia kierownictwa dla rozwiązania problemu, jest oparcie uzasadnienia biznesowego na skutecznym, rzeczywistym

przykładzie pochodzącym od strony trzeciej. W uzasadnieniu biznesowym należy przedstawić kierownictwu, że inna organizacja miała ten sam problem a następnie przedstawić, że znalazła rozwiązanie i jak je zrealizowała. Zwykle motywuje to kierownictwo do postawienia pytania, jakie jest to rozwiązanie i jak można je zastosować w ich organizacji.

4.2. Zbudowanie i przeszkolenie zespołu wielofunkcyjnego

Istotne jest, aby wielofunkcyjny zespół ds. bezpieczeństwa informacji dzielił się swoją różnorodną wiedzą i doświadczeniem w celu oceny i ograniczania ryzyka w ICS. Zespół ds. bezpieczeństwa informacji powinien składać się co najmniej z członka personelu informacyjnego organizacji, inżyniera sterowania, operatora systemu sterowania, ekspertów ds. bezpieczeństwa oraz członka personelu zarządzającego ryzykiem w przedsiębiorstwie. Wiedza i umiejętności z zakresu bezpieczeństwa powinny obejmować architekturę i projektowanie sieci, procesy i praktyki bezpieczeństwa oraz projektowanie i obsługę bezpiecznej infrastruktury. Współczesne przekonanie, że zarówno ochrona, jak i bezpieczeństwo są właściwościami wyłaniającymi się z połączonych systemów sterowania cyfrowego, sugeruje włączenie do zespołu eksperta ds. bezpieczeństwa. Dla zachowania spójności i kompleksowości w skład zespołu ds. bezpieczeństwa informacji powinien wchodzić także dostawca systemu sterowania i/lub integrator systemu.

Zespół ds. bezpieczeństwa informacji powinien podlegać bezpośrednio kierownikowi ds. bezpieczeństwa informacji na poziomie misji/procesu biznesowego lub organizacji, który z kolei podlega odpowiednio menedżerowi misji/procesu biznesowego (np. zarządcy obiektu) lub dyrektorowi ds. bezpieczeństwa informacji w przedsiębiorstwie (np. CIO/CSO). Ostateczne uprawnienia i odpowiedzialność spoczywają na funkcji zarządzającej ryzykiem (RE) poziomu 1, która zapewnia kompleksowe, ogólnoorganizacyjne podejście do zarządzania ryzykiem. Funkcja zarządzania ryzykiem (RE) współpracuje z kierownictwem najwyższego szczebla w celu zaakceptowania poziomu ryzyka szczątkowego i odpowiedzialności za bezpieczeństwo informacji w ICS. Rozliczalność na poziomie kierownictwa pozwala zapewnić stałe ich zaangażowanie w działania związane z bezpieczeństwem informacji.

Chociaż inżynierowie automatycy będą odgrywać znaczącą rolę w zabezpieczaniu ICS, nie będą w stanie tego zrobić bez współpracy i wsparcia ze strony działu IT i kierownictwa. Dział IT ma często wieloletnie doświadczenie w zakresie bezpieczeństwa, które w dużej mierze można wykorzystać w systemach ICS. Ponieważ środowisko inżynierów automatyków i informatyków często znacznie się różni, ich integracja będzie niezbędna do opracowania wspólnego projektu i działania w zakresie bezpieczeństwa.

4.3. Zdefiniowanie statutu i zakresu

Zarządzający bezpieczeństwem informacji powinien ustanowić politykę organizacyjną, która określa podstawowe zasady bezpieczeństwa informacji oraz role, obowiązki i zakres odpowiedzialności właścicieli systemów, osób zarządzających misjami/procesami biznesowymi i użytkowników. Menedżer odpowiedzialny za bezpieczeństwo informacji powinien określić i udokumentować cel programu bezpieczeństwa, organizacje biznesowe, których ten program dotyczy, wszystkie zaangażowane systemy i sieci komputerowe, wymagany budżet i zasoby oraz podział obowiązków. Zakres ten może również obejmować wymagania biznesowe, szkoleniowe, audytowe, prawne i regulacyjne, a także harmonogramy i zakresy odpowiedzialności. Strategia bezpieczeństwa informacji w organizacji jest składnikiem architektury bezpieczeństwa informacji, która jest częścią architektury korporacyjnej, omówionej w rozdziale 3. Możliwe, że istnieje już program bezpieczeństwa informacji lub jest on opracowywany dla informacyjnych systemów biznesowych organizacji. Menedżer odpowiedzialny za bezpieczeństwo informacji w systemach ICS powinien określić, które z istniejących praktyk należy wykorzystać, a które są specyficzne dla danego systemu sterowania. W dłuższej perspektywie łatwiej będzie uzyskać pozytywne rezultaty, jeśli zespół będzie mógł dzielić się zasobami z innymi osobami w organizacji, których cele są zbieżne.

4.4. Zdefiniowanie specyficznych dla ICS polityk i procedur bezpieczeństwa

Polityka i procedury są podstawą każdego udanego programu bezpieczeństwa. Tam, gdzie jest to możliwe, polityki i procedury bezpieczeństwa specyficzne dla ICS powinny być zintegrowane z istniejącymi politykami i procedurami operacyjnymi/zarządzania. Polityki i procedury pomagają zapewnić, że środki bezpieczeństwa są zarówno spójne, jak i aktualne, aby chronić przed zmieniającymi się zagrożeniami. Załącznik C wskazuje, że brak polityki bezpieczeństwa jest istotną podatnością na zagrożenia. Załącznik G - nakładka ICS - zawiera wiele zaleceń dotyczących polityki bezpieczeństwa informacji w zakresie ICS. Po przeprowadzeniu analizy ryzyka związanego z bezpieczeństwem informacji menedżer ds. bezpieczeństwa informacji powinien przeanalizować istniejące polityki bezpieczeństwa, aby sprawdzić, czy w odpowiedni sposób uwzględniają one zagrożenia dla ICS. W razie potrzeby należy zweryfikować istniejące zasady lub stworzyć nowe.

Jak omówiono w rozdziale 3, członkowie kierownictwa poziomu 1 są odpowiedzialni za opracowanie i ogłoszenie poziomu ryzyka tolerowanego przez organizację - poziomu ryzyka, który organizacja jest skłonna zaakceptować - co pozwala menedżerowi bezpieczeństwa informacji określić poziom ograniczania ryzyka, który należy podjąć w celu zmniejszenia ryzyka szczątkowego do akceptowalnego poziomu. Opracowanie polityk bezpieczeństwa powinno być oparte na ocenie ryzyka, która określi priorytety i cele bezpieczeństwa dla organizacji, tak aby ryzyko związane z zagrożeniami było wystarczająco ograniczone. Należy opracować procedury wspierające polityki, tak aby były one w pełni i prawidłowo wdrożone w systemie ICS. Procedury bezpieczeństwa powinny być dokumentowane, testowane i okresowo aktualizowane w odpowiedzi na zachodzące zmiany w polityce, technologii i zagrożeniach.

4.5. Wdrożenie ram zarządzania ryzykiem związanych z bezpieczeństwem ICS

Z abstrakcyjnego punktu widzenia zarządzanie ryzykiem związanym z ICS to kolejne niebezpieczeństwo dodane do list zagrożeń, z którymi mierzy się organizacja (np. finansowe, bezpieczeństwa, informacyjne, środowiskowe). W każdym przypadku kierownictwo odpowiedzialne za misję lub proces biznesowy ustanawia i prowadzi program zarządzania ryzykiem w koordynacji z funkcji zarządzającą ryzykiem (RE) najwyższego szczebla. Publikacja NSC 800-39 (bazująca na Specjalnej publikacji NIST 800-39, *Managing Information Security Risk-Organization, Mission, and Information System View* [20]) stanowi podstawę takiego programu zarządzania ryzykiem. Podobnie, jak w przypadku innych obszarów misji/procesów biznesowych, personel zajmujący się ICS wykorzystuje swoją specjalistyczną wiedzę merytoryczną do ustanowienia i prowadzenia zarządzania ryzykiem w zakresie bezpieczeństwa ICS oraz do komunikacji z kierownictwem przedsiębiorstwa w celu wspierania skutecznego zarządzania ryzykiem w całym przedsiębiorstwie. Standard NSC 800-37 (bazujący na Specjalnej Publikacji NIST 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* [21]), przedstawia ramy zarządzania ryzykiem i omawia proces ich wdrażania. Poniższe rozdziały podsumowują ten proces oraz zastosowanie RMF do środowiska ICS.

Proces RMF obejmuje zestaw ściśle określonych zadań związanych z ryzykiem, które mają być wykonywane przez wyznaczone osoby lub grupy w ramach precyzyjnie zdefiniowanych ról organizacyjnych (np. funkcje zarządzające ryzykiem (RE), osoba autoryzująca (AO), pełnomocnik osoby autoryzującej (AODR), CIO, SISO, architekt korporacyjny, architekt bezpieczeństwa informacji, właściciel informacji lub władający informacją (IO/S), właściciel systemu informacyjnego (ISO/SO), dostawca zabezpieczeń wspólnych, ISSO, oceniający środki bezpieczeństwa)[10]. Wiele ról związanych z zarządzaniem ryzykiem ma swoje odpowiedniki zdefiniowane w rutynowych

[10] Definicje ról organizacyjnych – patrz: NSC 800-37, NSC 7298.

procesach cyklu życia systemu. Zadania RMF są wykonywane równolegle z procesami cyklu życia systemu lub jako ich część, z uwzględnieniem odpowiednich zależności.

Organizacje mogą również skorzystać z dokumentu ISA-62443-2-1, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*, który przedstawia inne spojrzenie na elementy systemu zarządzania cyberbezpieczeństwem w środowisku automatyki przemysłowej i systemów sterowania [34]. Dostarcza on wskazówek, jak spełnić wymagania dotyczące poszczególnych elementów. Rozdziały od 4 do 6 w sposób najbardziej zbliżony odpowiadają zaleceniom NSC 800-39; pozostałe rozdziały nawiązują do innych publikacji specjalnych NIST oraz do nakładki ICS zawartej w Załączniku G niniejszego dokumentu. We wszystkich tych wytycznych uznano, że nie ma jednego uniwersalnego rozwiązania; przy dostosowywaniu wytycznych do potrzeb konkretnej organizacji należy raczej kierować się wiedzą dotyczącą danej branży.

4.5.1. Kategoryzacja aktywów systemów i sieci ICS

Zespół ds. bezpieczeństwa informacji powinien zdefiniować, zinwentaryzować i skategoryzować aplikacje i systemy komputerowe wchodzące w skład ICS, a także sieci wchodzące w skład ICS i łączące się z nimi. Należy skupić się na systemach, a nie tylko urządzeniach i uwzględnić sterowniki PLC, DCS, SCADA oraz systemy oparte na instrumentach, które wykorzystują urządzenia monitorujące, takie jak HMI (*ang. Human-Machine Interface*). Należy udokumentować zasoby, które wykorzystują protokół routowany lub są dostępne przez dial-up. Zespół powinien przeglądać i aktualizować listę zasobów ICS corocznie oraz po każdym dodaniu lub usunięciu zasobu.

Istnieje kilka komercyjnych narzędzi do inwentaryzacji IT w przedsiębiorstwie, które mogą zidentyfikować i udokumentować cały sprzęt i oprogramowanie znajdujące się w sieci. Przed użyciem tych narzędzi do identyfikacji zasobów ICS należy zachować ostrożność. Zespoły powinny najpierw przeprowadzić ocenę sposobu działania tych narzędzi i wpływu, jaki mogą one mieć na podłączone urządzenia sterujące. Ocena narzędzi może obejmować testowanie w podobnych, nieprodukcyjnych środowiskach systemów sterowania w celu upewnienia się, że narzędzia nie mają negatywnego

wpływu na systemy produkcyjne. Wpływ może wynikać z charakteru informacji lub natężenia ruchu sieciowego. O ile wpływ ten może być dopuszczalny w systemach informacyjnych, o tyle może być niedopuszczalny w ICS.

Zautomatyzowany system zarządzania zasobami (np. komputerowy system zarządzania utrzymaniem ruchu (*Computerized Maintenance Management System - CMMS*), komputerowo wspomagany system zarządzania obiektami (*Computer Aided Facility Management System - CAFM*), model informacji o budynku (*Building Information Model - BIM*), system informacji geoprzestrzennej (*Geospatial Information System - GIS*), system wymiany informacji o budynkach i ich eksploatacji (*Construction-Operations Building information exchange data - COBie*), system wymiany informacji o zarządzaniu automatyką budynkową (*Building Automation Management information exchange - BAMie*), system zarządzania utrzymaniem ruchu (*Sustainment Management Systems - SMS Builder*) pozwala organizacji na dokładne ewidencjonowanie tego, co znajduje się w systemie, zarówno pod kątem bezpieczeństwa, jak i ze względów budżetowych.

4.5.2. Wybór zabezpieczeń systemu ICS

Środki bezpieczeństwa wyłonione na podstawie kategoryzacji bezpieczeństwa ICS są udokumentowane w planie bezpieczeństwa, w celu przedstawienia przeglądu wymogów bezpieczeństwa dla programu bezpieczeństwa informacji ICS oraz opisania istniejących lub planowanych środków bezpieczeństwa służących spełnieniu tych wymogów. Opracowywanie planów bezpieczeństwa jest omówione w standardzie NSC 800-18 (bazującym na specjalnej publikacji NIST 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems [19]). Plan bezpieczeństwa może być pojedynczym dokumentem lub zbiorem wszystkich dokumentów odnoszących się do problemów bezpieczeństwa systemu oraz planów przeciwdziałania tym problemom. Oprócz zabezpieczeń, standard NSC 800-53 wer. 1 (bazujący na specjalnej publikacja NIST 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations [20]), zawiera programy zarządzania bezpieczeństwem informacji (*Program Management - PM*), które są zazwyczaj wdrażane na poziomie organizacji, a nie poszczególnych systemów informacyjnych. W tym

rozdziale omówiono, w jaki sposób organizacja ustanawia i wdraża zabezpieczenia programu zarządzania bezpieczeństwem.

Skuteczne wdrożenie zabezpieczeń systemów informacyjnych organizacji zależy od skutecznego wdrożenia programu zarządzania środkami bezpieczeństwa w całej organizacji. Sposób, w jaki organizacje wdrażają kontrole zarządzania programem zależy od specyficznych cech organizacji, w tym na przykład od wielkości, złożoności i misji/wymagań biznesowych danej organizacji. Zabezpieczenia programu zarządzania uzupełniają środki bezpieczeństwa i koncentrują się na programowych, ogólnoorganizacyjnych wymaganiach dotyczących bezpieczeństwa informacji, które są niezależne od konkretnego systemu informacyjnego i są niezbędne do zarządzania programami bezpieczeństwa informacji. Organizacje dokumentują zabezpieczenia związane z programem zarządzania w planie programu bezpieczeństwa informacji. Plan programu bezpieczeństwa informacji obejmujący całą organizację uzupełnia indywidualne plany bezpieczeństwa opracowane dla każdego systemu informacyjnego organizacji. Plany bezpieczeństwa dla poszczególnych systemów informacyjnych oraz program bezpieczeństwa informacji łącznie obejmują całość środków bezpieczeństwa stosowanych przez organizację.

4.5.3. Przeprowadzenie szacowania ryzyka

Ponieważ każda organizacja dysponuje ograniczonym zestawem zasobów, powinna ocenić wpływ zdarzeń niepożądanych na działalność organizacji (tj. misję, funkcje, wizerunek i reputację), aktywa organizacji, osoby, inne organizacje i państwo (np. przy użyciu standardu NSC 199, bazującego na FIPS 199 [15] lub bardziej szczegółowego podejścia). Jak omówiono w rozdziale 3, organizacje mogą doświadczać konsekwencji/skutków zdarzeń niepożądanych na poziomie pojedynczego systemu ICS (np. brak wymaganego działania), na poziomie misji/procesu biznesowego (np. brak pełnej realizacji celów misji/procesu biznesowego) oraz na poziomie organizacyjnym (np. brak zgodności z wymogami prawnymi lub regulacyjnymi, pogorszenie reputacji lub relacji z innymi podmiotami albo podważenie długoterminowej rentowności). Zdarzenie niepożądane może mieć wiele konsekwencji i różne rodzaje wpływu, na różnych poziomach i w różnych ramach czasowych. NSC 800-53 i nakładka ICS

przedstawiona w Załączniku G zawierają podstawowe środki bezpieczeństwa, które wynikają z tego określenia wpływu.

Organizacja może przeprowadzić szczegółowe szacowanie ryzyka systemów o największym poziomie wpływu oraz systemów o mniejszym wpływie, jeśli uzna to za rozsądne i jeśli pozwolą na to zasoby. Szacowanie ryzyka pomoże zidentyfikować wszelkie słabości, które przyczyniają się do powstawania ryzyka związanego z bezpieczeństwem informacji, oraz sposoby ograniczania tego ryzyka. Szacowanie ryzyka przeprowadza się wielokrotnie w trakcie cyklu życia systemu. Zakres tematyczny i poziom szczegółowości zależą od stopnia zaawansowania systemu.

4.5.4. Wdrażanie zabezpieczeń

Organizacje powinny przeanalizować szczegółowe oszacowanie ryzyka oraz wpływ na działalność organizacji (tj. misję, funkcje, wizerunek i reputację), aktywa organizacji, osoby, inne organizacje i państwo, a także ustalić priorytety wyboru środków ograniczających ryzyko. Organizacje powinny skupić się na ograniczaniu ryzyka o największym potencjalnym poziomie wpływu. Wdrożenie środków bezpieczeństwa jest zgodne z architekturą korporacyjną organizacji i architekturą bezpieczeństwa informacji.

Zabezpieczenia mające na celu ograniczenie konkretnego ryzyka mogą być różne dla różnych typów systemów. Na przykład zabezpieczenia uwierzytelniania użytkowników mogą być inne dla ICS niż dla korporacyjnych systemów wynagrodzeń i systemów handlu elektronicznego. Menedżer odpowiedzialny za bezpieczeństwo informacji w ICS powinien udokumentować i przedstawić wybrane zabezpieczenia wraz z procedurami ich stosowania. Niektóre rodzaje ryzyka można ograniczyć za pomocą gotowych rozwiązań - tanich i wartościowych praktyk, które mogą znacznie zmniejszyć ryzyko. Przykładem takich rozwiązań jest ograniczenie dostępu do Internetu i wyeliminowanie dostępu do poczty elektronicznej na stacjach sterowania lub konsolach operatorów. Organizacje powinny jak najszybciej zidentyfikować, ocenić i wdrożyć odpowiednie szybkie rozwiązania w celu zmniejszenia ryzyka związanego z bezpieczeństwem i osiągnięcia szybkich korzyści. Departament Energii USA (*Department of Energy - DOE*) opublikował dokument "21 kroków do poprawy

cyberbezpieczeństwa sieci SCADA" (*21 Steps to Improve Cyber Security of SCADA Networks* [33]), który może być wykorzystany jako punkt wyjścia do opracowania konkretnych działań mających na celu zwiększenie bezpieczeństwa systemów SCADA i innych systemów ICS.

5. ARCHITEKTURA BEZPIECZEŃSTWA ICS

Podczas projektowania architektury sieciowej na potrzeby wdrożenia systemu ICS, zwykle zaleca się oddzielenie sieci ICS od sieci korporacyjnej. Specyfika ruchu sieciowego w tych dwóch sieciach jest inna: dostęp do Internetu, FTP, poczta elektroniczna i dostęp zdalny są zwykle dozwolone w sieci korporacyjnej, ale nie powinny być dozwolone w sieci ICS. W sieci korporacyjnej mogą nie obowiązywać rygorystyczne procedury zabezpieczeń zmian w sprzęcie sieciowym, konfiguracji i oprogramowaniu. Jeśli ruch sieciowy pochodzący z sieci ICS jest transmitowany przez sieć korporacyjną, może zostać przechwycony lub stać się przedmiotem ataków DoS lub typu Man-in-the-Middle [5.14]. Dzięki wydzieleniu osobnych sieci problemy z bezpieczeństwem i wydajnością w sieci korporacyjnej nie powinny mieć wpływu na sieć ICS.

Względy praktyczne, takie jak koszt instalacji ICS lub utrzymanie jednorodnej infrastruktury sieciowej, często oznaczają, że wymagane jest połączenie między ICS a siecią korporacyjną. Takie połączenie stanowi istotne zagrożenie dla bezpieczeństwa i powinno być chronione za pomocą urządzeń ochrony brzegowej. Jeśli sieci muszą być połączone, zdecydowanie zaleca się, aby dozwolone były tylko minimalne (pojedyncze, jeśli to możliwe) połączenia oraz, aby połączenie odbywało się przez zaporę sieciową i strefę zdemilitaryzowaną (DMZ). DMZ to oddzielny segment sieci, który łączy się bezpośrednio z zaporą sieciową. W tym segmencie sieci umieszcza się serwery zawierające dane z systemu ICS, które muszą być dostępne z sieci korporacyjnej. Tylko te systemy powinny być dostępne z sieci korporacyjnej. W przypadku wszelkich połączeń zewnętrznych należy zezwolić na minimalny dostęp przez zaporę sieciową, w tym na otwarcie tylko tych portów, które są wymagane do określonej komunikacji. W kolejnych rozdziałach omówiono szczegółowo wspomniane uwarunkowania strukturalne. Zalecane praktyki ICS-CERT można znaleźć na stronie http://ics-cert.us-cert.gov/Recommended-Practices.

5.1. Segmentacja i segregacja sieci

W tym rozdziale omówiono partycjonowanie ICS do domen bezpieczeństwa i oddzielenie ICS od innych sieci, takich jak sieć korporacyjna. Przedstawiono także przykładową architekturę bezpieczeństwa. Należy przeprowadzić analizę ryzyka operacyjnego, aby określić krytyczne części każdej sieci ICS i sposobu działania oraz pomóc w zdefiniowaniu, które części ICS należy poddać segmentacji. Segmentacja sieci polega na podzieleniu sieci na mniejsze sieci. Na przykład jedna duża sieć ICS jest dzielona na wiele sieci ICS, przy czym podział ten opiera się na takich czynnikach, jak uprawnienia do zarządzania, jednolita polityka i poziom zaufania, krytyczność funkcjonalna oraz ilość ruchu komunikacyjnego przekraczającego granicę domeny. Segmentacja i wydzielenie sieci jest jedną z najskuteczniejszych koncepcji architektonicznych, jakie organizacja może wdrożyć w celu ochrony swoich systemów ICS. Segmentacja tworzy domeny bezpieczeństwa lub obszary zamknięte, które są zwykle definiowane jako zarządzane przez ten sam organ, egzekwujące tę samą politykę i posiadające jednolity poziom zaufania. Segmentacja może ograniczyć do minimum sposób i poziom dostępu do informacji wrażliwych, komunikacji w ramach systemów ICS i konfiguracji sprzętu, a także znacznie utrudnić działanie potencjalnym złośliwym cyberprzestępcom oraz ograniczyć skutki błędów i zdarzeń niezwiązanych z działalnością złośliwą. Praktycznym aspektem przy definiowaniu domeny bezpieczeństwa jest ilość ruchu komunikacyjnego przekraczającego granicę domeny, ponieważ ochrona domeny zazwyczaj polega na badaniu ruchu granicznego i określaniu, czy jest on dozwolony.

Celem segmentacji i segregacji sieci jest zminimalizowanie dostępu do informacji wrażliwych dla tych systemów i osób, które tego dostępu nie potrzebują, przy jednoczesnym zapewnieniu, że organizacja może nadal efektywnie funkcjonować. Można to osiągnąć za pomocą różnych technik i technologii, w zależności od architektury i konfiguracji sieci.

Tradycyjnie segmentacja i segregacja sieci jest realizowana na bramie dostępowej pomiędzy domenami. Środowiska ICS często mają wiele dobrze zdefiniowanych domen, takich jak operacyjne sieci LAN, sterujące sieci LAN i operacyjne strefy DMZ,

a także bramy do domen nie związanych z ICS i mniej godnych zaufania, takich jak Internet i korporacyjne sieci LAN. Jeśli weźmie się pod uwagę ataki wewnętrzne, socjotechnikę, urządzenia mobilne oraz inne podatności i warunki predysponujące omówione w Załączniku C, ochrona bram domenowych jest rozsądna i warta rozważenia.

Segregacja sieci polega na opracowaniu i egzekwowaniu zestawu reguł zabezpieczających, określających, jaki rodzaj komunikacji jest dozwolony przez bramę. Reguły zazwyczaj opierają się na tożsamości źródła i miejsca docelowego oraz na typie lub zawartości przesyłanych danych.

Prawidłowe wdrożenie segmentacji i segregacji sieci minimalizuje sposób i poziom dostępu do informacji wrażliwych. Można to osiągnąć za pomocą różnych technologii i metod. W zależności od architektury i konfiguracji sieci, najczęściej stosowane technologie i metody obejmują:

- Logiczną separację sieci wymuszoną przez szyfrowanie lub partycjonowanie wymuszone przez urządzenia sieciowe:
  - ✓ Wirtualne sieci lokalne (*ang. Virtual Local Area Networks - VLANS*).
  - ✓ Szyfrowane wirtualne sieci prywatne (*ang. Virtual Private Networks - VPNs*) wykorzystujące mechanizmy kryptograficzne do rozdzielenia ruchu połączonego w jednej sieci.
  - ✓ Jednokierunkowe bramy ograniczające komunikację między połączeniami wyłącznie w jednym kierunku, co powoduje segmentację sieci.
- Fizyczną separację sieci w celu całkowitego uniemożliwienia wzajemnego przekazywania ruchu pomiędzy domenami.
- Filtrowanie ruchu sieciowego, wykorzystujące różne technologie w poszczególnych warstwach sieci i pozwalające na egzekwowanie wymogów i domen bezpieczeństwa:
  - ✓ Filtrowanie w warstwie sieciowej, które ogranicza możliwość komunikowania się systemów z innymi w sieci na podstawie informacji o adresie IP i trasie.

- ✓ Filtrowanie na podstawie informacji o stanie, które ogranicza możliwość komunikowania się systemów z innymi w sieci na podstawie ich zamierzonej funkcji lub bieżącego stanu działania.
- ✓ Filtrowanie na poziomie portów i/lub protokołów, które ogranicza liczbę i rodzaj usług, z których każdy system może korzystać w celu komunikowania się z innymi w sieci.
- ✓ Filtrowanie aplikacji, które zazwyczaj filtruje zawartość komunikacji między systemami w warstwie aplikacji. Obejmuje to zapory sieciowe na poziomie aplikacji, serwery proxy i filtry treści.

Niektórzy producenci wytwarzają produkty do filtrowania protokołów ICS na poziomie aplikacji, które sprzedają jako zapory ICS.

Niezależnie od technologii wybranej do wdrożenia segmentacji i segregacji sieci, istnieją cztery powszechne obszary, które pozwalają wdrożyć koncepcję obrony dogłębnej (*defense-in-depth*) poprzez zapewnienie właściwej segmentacji i segregacji sieci:

- Stosowanie technologii segmentacji i segregacji nie tylko w warstwie sieciowej. Każdy system i sieć powinny być podzielone na segmenty i odseparowane, jeśli to możliwe, począwszy od warstwy łącza danych do warstwy aplikacji włącznie.
- Stosowanie zasady minimalnych uprawnień (*ang. least privilege*) i zasady wiedzy koniecznej (*ang. need to know*). Jeśli system nie musi komunikować się z innym systemem, nie powinien być do tego dopuszczony. Jeśli system nie musi komunikować się z innym systemem, nie powinien mieć takiej możliwości. Jeśli system musi współpracować z innym systemem tylko za pośrednictwem określonego portu lub protokołu, albo musi przesyłać ograniczony zestaw danych oznaczonych etykietami lub o stałym formacie, powinien zostać objęty takimi ograniczeniami.
- Rozdzielanie informacji i infrastruktury w oparciu o wymagania dotyczące bezpieczeństwa. Może to obejmować stosowanie różnego sprzętu lub platform w zależności od różnych środowisk zagrożeń i ryzyka, w których działa każdy system

lub segment sieci. Najbardziej krytyczne komponenty wymagają surowszego odizolowania od innych komponentów. Oprócz separacji sieci w celu osiągnięcia wymaganej izolacji można zastosować wirtualizację.

- Wdrażanie „białej listy" (*ang. whitelisting*)[11] zamiast „czarnej listy" (*ang. blacklisting*); czyli przyznawanie dostępu do powszechnie znanych dobrych rozwiązań, a nie odmawianie dostępu do znanych złych. Zestaw aplikacji działających w ICS jest zasadniczo statyczny, co sprawia, że "biała lista" staje się bardziej praktyczna. Zwiększa to również możliwości organizacji w zakresie analizowania zawartości plików logów.

5.2. Ochrona granic systemu

Urządzenia ochrony granic systemów zabezpieczają przepływ informacji między połączonymi domenami bezpieczeństwa w celu ochrony ICS przed złośliwymi atakami cyberprzestępców oraz błędami i zdarzeniami niezwiązanymi ze złośliwym działaniem. Przekazywanie informacji między systemami reprezentującymi różne domeny bezpieczeństwa o różnych politykach bezpieczeństwa wiąże się z ryzykiem, że takie przekazywanie informacji naruszy jedną lub więcej polityk bezpieczeństwa domeny. Urządzenia ochrony granic są kluczowymi elementami szczegółowych rozwiązań architektonicznych, które egzekwują określone polityki bezpieczeństwa. Organizacje mogą odizolować komponenty ICS i systemów biznesowych wykonujące różne misje i/lub funkcje biznesowe. Taka izolacja ogranicza przepływ nieautoryzowanych informacji pomiędzy komponentami systemu, a także umożliwia wdrożenie wyższych poziomów ochrony dla wybranych komponentów. Rozdzielenie komponentów systemu za pomocą mechanizmów ochrony brzegowej umożliwia zwiększenie poziomu ochrony poszczególnych komponentów oraz skuteczniejsze zabezpieczanie przepływów informacji między tymi komponentami.

[11] „Biała lista" to lista lub rejestr podmiotów (użytkownik lub proces działający w imieniu użytkownika), które otrzymują określony przywilej, usługę, mobilność, dostęp lub uznanie. Tylko te podmioty, które znajdują się na liście będą akceptowane, zatwierdzane lub uznawane (tzn. dozwolone). „Biała lista" jest przeciwieństwem „czarnej listy", czyli praktyki identyfikowania tych, którzy są odrzucani, nierozpoznawani lub wykluczani (tzn. podmiotów niedozwolonych).

Zabezpieczenia brzegowe obejmują bramy, routery, zapory, osłony, systemy wirtualizacji i sieciowe systemy analizy złośliwego kodu, systemy wykrywania włamań (sieciowe i na hoście), szyfrowane tunele, zarządzane interfejsy, bramy e-mail, bramy jednokierunkowe (np. diody danych). Urządzenia ochrony granic określają, czy transfer danych jest dozwolony, najczęściej poprzez analizę danych lub powiązanych metadanych.

Architekci bezpieczeństwa sieci i systemów ICS muszą zdecydować, które domeny mają mieć możliwość bezpośredniej komunikacji, jakie zasady regulują dozwoloną komunikację, jakie urządzenia mają być używane do egzekwowania zasad oraz jaką topologię należy zastosować, aby zapewnić i wdrożyć te decyzje, które są zwykle oparte na relacjach zaufania między domenami. Zaufanie obejmuje poziom kontroli, jaką organizacja sprawuje nad domeną zewnętrzną (np. inną domeną w tej samej organizacji, zakontraktowanym dostawcą usług, Internetem).

Urządzenia ochrony granic są rozmieszczone zgodnie z architekturą bezpieczeństwa organizacji. Popularną konstrukcją architektoniczną jest strefa zdemilitaryzowana (DMZ), czyli segment hosta lub sieci umieszczony jako "strefa neutralna" między domenami bezpieczeństwa. Jej celem jest egzekwowanie zasad bezpieczeństwa informacji obowiązujących w domenie ICS w odniesieniu do zewnętrznej wymiany informacji oraz zapewnienie domenom zewnętrznym ograniczonego dostępu przy jednoczesnym chronieniu domeny ICS przed zagrożeniami zewnętrznymi.

Dodatkowe względy architektoniczne i funkcje, które mogą być realizowane przez urządzenia ochrony granic podczas komunikacji między domenami, obejmują:

- Odmawianie domyślnego ruchu komunikacyjnego i zezwalanie na ruch komunikacyjny w drodze wyjątku (tj. odmowa wszystkim, zezwolenie na podstawie wyjątku). Polityka „odmowa dostępu dla wszystkich, zezwolenie w drodze wyjątku” (*ang. deny-all, permit-by-exception*) zapewnia, że dozwolone są tylko te połączenia, które zostały zatwierdzone. Jest to znane jako polityka białej listy (*ang. white-listing*).
- Wdrażanie serwerów proxy, które działają jako pośrednik dla zewnętrznych domen żądających dostępu do zasobów systemu informacyjnego (np. plików, połączeń lub

usług) od domeny ICS. Zewnętrzne żądania ustanowione poprzez początkowe połączenie z serwerem proxy są oceniane w celu zarządzania złożonością i zapewnienia dodatkowej ochrony poprzez ograniczenie bezpośredniego połączenia.

- Zapobieganie nieautoryzowanej eksfiltracji informacji. Techniki te obejmują np. zapory sieciowe z dogłębną inspekcją pakietów oraz bramy XML. Urządzenia te weryfikują przestrzeganie formatów i specyfikacji protokołów w warstwie aplikacji i służą do wykrywania podatności, które nie mogą być wykryte przez urządzenia działające w warstwie sieciowej lub transportowej. Ograniczona liczba formatów, a zwłaszcza zakaz stosowania dowolnego tekstu w wiadomościach e-mail, ułatwia stosowanie takich technik na granicach obszarów systemów ICS.
- Zezwolenie na komunikację tylko pomiędzy autoryzowanymi i uwierzytelnionymi parami adresów źródłowych i docelowych przez jedną lub więcej organizacji, systemów, aplikacji i osób.
- Rozszerzenie koncepcji DMZ na inne oddzielne podsieci, na przykład, w celu izolowania ICS i zapobiegania odkryciu przez przeciwników technik analitycznych i kryminalistycznych organizacji.
- Egzekwowanie fizycznej kontroli dostępu w celu ograniczenia autoryzowanego dostępu do komponentów ICS.
- Ukrywanie adresów sieciowych komponentów ICS przed ich rozpoznaniem (np. adres sieciowy nie jest publikowany lub nie jest wprowadzany do systemów nazw domen), co wymaga posiadania wcześniejszej wiedzy w celu uzyskania dostępu.
- Wyłączenie usług i protokołów kontroli i rozwiązywania problemów, zwłaszcza tych wykorzystujących wiadomości rozgłoszeniowe, które mogą ułatwić eksplorację sieci.
- Konfigurowanie urządzeń ochrony granic tak, aby po wystąpieniu usterki przechodziły do określonego stanu. Przewidywane stany awaryjne ICS wymagają zrównoważenia wielu czynników, w tym bezpieczeństwa i ochrony.

- Konfiguracja domen bezpieczeństwa z oddzielnymi adresami sieciowymi (tzn. jako rozłączne podsieci).
- Wyłączenie informacji zwrotnej (np. tryb „bez odpowiedzi”[12], *ang. none-verbose mode*) dla nadawców, gdy wystąpi błąd w formacie walidacji protokołu, aby uniemożliwić uzyskanie informacji przez osoby niepowołane.
- Wdrażanie jednokierunkowego przepływu danych, szczególnie pomiędzy różnymi domenami bezpieczeństwa.
- Wprowadzenie pasywnego monitorowania sieci ICS w celu wykrywania anomalii w komunikacji i przekazywania ostrzeżeń.

5.3. Zapory sieciowe

Zapory sieciowe to urządzenia lub systemy kontrolujące przepływ ruchu sieciowego pomiędzy sieciami stosującymi różne podejścia do bezpieczeństwa. W większości współczesnych zastosowań, zapory sieciowe i środowiska zaporowe są omawiane w kontekście łączności z Internetem i zestawu protokołów UDP/IP. Jednak zapory sieciowe mogą być stosowane w środowiskach sieciowych, które nie obejmują lub nie wymagają łączności z Internetem. Na przykład, wiele sieci korporacyjnych stosuje zapory sieciowe w celu ograniczenia możliwości łączenia się z sieciami wewnętrznymi obsługującymi bardziej wrażliwe funkcje, takie jak działy księgowości lub personalne.

Zapory sieciowe mogą dodatkowo ograniczyć wewnętrzną komunikację ICS między funkcjonalnymi podsieciami bezpieczeństwa i urządzeniami. Stosując zapory sieciowe do nadzorowania łączności z tymi obszarami, organizacja może zapobiegać nieautoryzowanemu dostępowi do poszczególnych systemów i zasobów znajdujących się w bardziej wrażliwych obszarach.

Istnieją trzy ogólne klasy zapór sieciowych[13]:

[12] Tryb odpowiedzi na błędne zapytanie ukrywający szczegóły powodu odrzucenia zapytania.

[13] Publikacja specjalna NIST SP 800-41 Revision 1, *Guidelines on Firewalls and Firewall Policy* [85], zawiera ogólne wytyczne dotyczące wyboru zapór sieciowych oraz polityki zapór sieciowych.

- **Zapora sieciowa z filtrowaniem pakietów**. Najbardziej podstawowy typ zapory sieciowej nazywany jest filtrem pakietów. Zapory sieciowe z filtrami pakietów są w istocie urządzeniami routingowymi, które zawierają funkcje kontroli dostępu do adresów systemowych i sesji komunikacyjnych. Kontrola dostępu jest regulowana przez zestaw dyrektyw określanych zbiorczo jako zestaw reguł. W swojej najbardziej podstawowej formie, filtry pakietów działają w warstwie 3 (sieciowej) modelu OSI (*ang. Open Systems Interconnection*), ISO/IEC 7498. Ten rodzaj zapory, przed przekazaniem pakietu dalej, sprawdza podstawowe informacje zawarte w każdym pakiecie, takie jak adresy IP, pod kątem przyjętego zestawu kryteriów. W zależności od pakietu i kryteriów, zapora może odrzucić pakiet, przekazać go dalej lub wysłać komunikat do inicjatora. Ten typ zapory może zapewnić wysoki poziom bezpieczeństwa, ale może mieć wpływ na koszty ogólne i opóźnienia w działaniu sieci.
- **Zapory sieciowe z inspekcją stanu pakietów (*ang. Stateful Inspection Firewalls*)**. Zapory sieciowe z inspekcją stanu pakietów to filtry pakietów, które dodatkowo uwzględniają dane modelu OSI warstwy 4 (transport). Zapory sieciowe z inspekcją pakietów filtrują pakiety w warstwie 3 (sieciowej), określają, czy pakiety sesji są legalne i oceniają zawartość pakietów również w warstwie transportowej (np. TCP, UDP). Inspekcja stanu pakietów śledzi aktywne sesje i wykorzystuje te informacje do określenia, czy pakiety powinny być przekazywane dalej, czy blokowane. Oferuje ona wysoki poziom bezpieczeństwa i dobrą wydajność, ale może być droższa i bardziej skomplikowana w administrowaniu. Mogą być wymagane dodatkowe zestawy reguł dla aplikacji ICS.
- **Zapora sieciowa typu serwer-proxy *(ang. Application-Proxy Gateway)***.Ta klasa zapór sieciowych analizuje pakiety w warstwie aplikacji i filtruje ruch w oparciu o określone reguły aplikacyjne, takie jak wybrane aplikacje (np. przeglądarki) lub protokoły (np. FTP). Zapory tego typu mogą być bardzo skuteczne w zapobieganiu atakom na usługi zdalnego dostępu i konfiguracji świadczone przez komponenty ICS. Oferują one wysoki poziom bezpieczeństwa, ale mogą mieć wpływ na obciążenie sieci i opóźnienia w jej działaniu, co może być niedopuszczalne w środowisku ICS.

W środowisku ICS, zapory sieciowe są najczęściej wdrażane pomiędzy siecią ICS a siecią korporacyjną [34]. Odpowiednio skonfigurowane mogą w znacznym stopniu ograniczyć niepożądany dostęp do i z komputerów hosta systemu sterowania i sterowników, poprawiając tym samym bezpieczeństwo. Mogą one również potencjalnie poprawić szybkość reakcji sieci sterowania poprzez usunięcie z sieci ruchu, który nie jest niezbędny. Odpowiednio zaprojektowane, skonfigurowane i utrzymywane dedykowane sprzętowe zapory sieciowe mogą w znacznym stopniu przyczynić się do zwiększenia bezpieczeństwa współczesnych środowisk ICS.

Zapory sieciowe udostępniają szereg narzędzi do egzekwowania polityki bezpieczeństwa, których nie można zrealizować lokalnie na obecnie dostępnych na rynku urządzeniach do sterowania procesami, w tym możliwość:

- Blokowania całej komunikacji z wyjątkiem specjalnie włączonej komunikacji między urządzeniami w niechronionej sieci LAN a chronionymi sieciami ICS. Blokowanie może być oparte np. na parach źródłowych i docelowych adresów IP, usługach, portach, stanie połączenia oraz określonych aplikacjach lub protokołach obsługiwanych przez zaporę. Blokowanie może dotyczyć zarówno pakietów przychodzących, jak i wychodzących, co jest pomocne w ograniczaniu komunikacji wysokiego ryzyka, takiej jak poczta elektroniczna.
- Wymuszenia bezpiecznego uwierzytelniania wszystkich użytkowników, którzy chcą uzyskać dostęp do sieci ICS. Istnieje możliwość zastosowania różnych poziomów ochrony metod uwierzytelniania, w tym prostych haseł, haseł złożonych, technologii uwierzytelniania wielopoziomowego, tokenów, biometrii i kart inteligentnych. Wyboru konkretnej metody należy dokonać w oparciu o podatność chronionej sieci ICS, a nie na podstawie metody dostępnej na poziomie urządzenia.
- Wymuszenia autoryzacji miejsc docelowych. Użytkownikom można ograniczyć dostęp i zezwolić na dostęp tylko do tych węzłów w sieci sterowania, które są niezbędne do wykonywania ich zadań. Zmniejsza to potencjał użytkowników do celowego lub przypadkowego uzyskania dostępu i kontroli nad urządzeniami, do których nie są upoważnieni, ale zwiększa złożoność procesu szkolenia pracowników w trakcie pracy lub szkolenia przekwalifikowującego.

- Rejestrowania przepływu informacji w celu monitorowania ruchu, analizy i wykrywania włamań.
- Zezwolenia ICS na wdrożenie zasad operacyjnych odpowiednich dla ICS, które jednak mogą nie być odpowiednie dla sieci informacyjnej, takich jak zakaz mniej bezpiecznej komunikacji, np. za pośrednictwem poczty elektronicznej oraz zezwolenia stosowania łatwych do zapamiętania nazw użytkowników i haseł grupowych.
- Projektowania z udokumentowanymi i minimalnymi (pojedynczymi, jeśli to możliwe) połączeniami, które umożliwiają oddzielenie sieci ICS od sieci korporacyjnej, jeśli taka decyzja zostanie podjęta, w przypadku poważnych cyberincydentów.

Inne możliwe wdrożenia obejmują użycie zapór sieciowych opartych na hostach lub małych, samodzielnych zapór sprzętowych instalowanych przed lub w poszczególnych urządzeniach sterujących. Stosowanie zapór na poszczególnych urządzeniach może powodować znaczne koszty zarządzania, zwłaszcza w przypadku zarządzania zmianami w konfiguracji zapór, jednak praktyka ta upraszcza również indywidualne zestawy reguł konfiguracyjnych.

Wdrażając zapory sieciowe w środowiskach ICS należy zwrócić uwagę na kilka kwestii, a w szczególności na:

- Możliwe wprowadzenie opóźnienia do komunikacji w systemie sterowania.
- Brak doświadczenia w projektowaniu zestawów reguł odpowiednich dla aplikacji przemysłowych. Zapory sieciowe stosowane do ochrony systemów sterowania powinny być tak skonfigurowane, aby domyślnie nie zezwalały na ruch przychodzący lub wychodzący. Domyślna konfiguracja powinna być modyfikowana tylko wtedy, gdy konieczne jest zezwolenie na połączenia do lub z zaufanych systemów w celu wykonania autoryzowanych funkcji ICS.

Zapory sieciowe wymagają ciągłego wsparcia, konserwacji i tworzenia kopii zapasowych konfiguracji. Zestawy reguł muszą być weryfikowane, aby upewnić się, że zapewniają odpowiednią ochronę w świetle stale zmieniających się zagrożeń bezpieczeństwa. Należy monitorować możliwości systemu (np. przestrzeń dyskową na

logi zapory), aby upewnić się, że zapora wykonuje swoje zadania związane z gromadzeniem danych, i że można na niej polegać w przypadku naruszenia bezpieczeństwa. Monitorowanie w czasie rzeczywistym zapór sieciowych i innych czujników bezpieczeństwa jest konieczne do szybkiego wykrywania i inicjowania reakcji na cyberincydenty.

5.4. Logicznie odseparowana sieć sterowania

Sieć ICS powinna być co najmniej logicznie oddzielona od sieci korporacyjnej przy użyciu fizycznie oddzielnych urządzeń sieciowych. W zależności od konfiguracji sieci ICS należy rozważyć dodatkowe oddzielenie przyrządowych systemów bezpieczeństwa i systemów zabezpieczeń (np. fizyczne monitorowanie i kontrola dostępu, drzwi, bramy, kamery, VoIP, czytniki kart dostępu), które często są częścią sieci ICS lub korzystają z tej samej infrastruktury komunikacyjnej na potrzeby lokalizacji zdalnych. Tam, gdzie wymagana jest łączność z przedsiębiorstwem:

- Powinny istnieć udokumentowane i minimalne (pojedyncze, jeśli to możliwe) punkty dostępu między siecią ICS a siecią korporacyjną. Nadmiarowe (tj. zapasowe) punkty dostępu, jeśli występują, muszą być udokumentowane.
- Zapora sieciowa z inspekcją stanu pakietów (*stateful firewall*) pomiędzy siecią ICS a siecią korporacyjną powinna być skonfigurowana w taki sposób, aby uniemożliwiać wszelki ruch z wyjątkiem tego, który jest jednoznacznie autoryzowany.
- Reguły zapory powinny zapewniać co najmniej filtrowanie źródła i przeznaczenia (tzn. filtrowanie po adresie kontroli dostępu do nośnika [*MAC*]), a także filtrowanie portów TCP i User Datagram Protocol (*UDP*) oraz filtrowanie typu i kodu Internet Control Message Protocol (*ICMP*).

Dopuszczalnym podejściem do umożliwienia komunikacji między siecią ICS a siecią korporacyjną jest wdrożenie pośredniej sieci DMZ. Sieć DMZ powinna być połączona z zaporą sieciową w taki sposób, aby określona (ograniczona) komunikacja mogła odbywać się tylko między siecią korporacyjną a DMZ oraz między siecią ICS i DMZ. Sieć korporacyjna i sieć ICS nie powinny komunikować się ze sobą bezpośrednio. Takie podejście opisano w punktach 5.5.4 i 5.5.5. Dodatkowe zabezpieczenie można uzyskać

przez wdrożenie wirtualnej sieci prywatnej (*VPN*) między systemem ICS a sieciami zewnętrznymi.

5.5. Segregacja sieci

W celu zwiększenia cyberbezpieczeństwa, sieci ICS i sieci korporacyjne mogą być rozdzielone przy użyciu różnych architektur. W tej sekcji opisano kilka możliwych do zastosowania architektur oraz wyjaśniono zalety i wady każdej z nich. Należy pamiętać, że celem diagramów zaprezentowanych w sekcji 5.5 jest pokazanie rozmieszczenia zapór sieciowych w celu odseparowania sieci. Nie pokazano wszystkich urządzeń, które zazwyczaj znajdują się w sieci sterowania lub sieci korporacyjnej. Sekcja 5.6 zawiera wskazówki dotyczące zalecanej architektury "obrony w głąb".

5.5.1. Komputer typu dual-homed[14]/podwójna karta interfejsu sieciowego (Dual Network Interface Cards - NIC)

Komputery typu dual-homed mogą przekazywać ruch sieciowy z jednej sieci do drugiej. Komputer bez odpowiednich zabezpieczeń może stanowić dodatkowe zagrożenie. Aby temu zapobiec, nie należy konfigurować systemów innych niż zapory sieciowe jako komputerów typu dual-homed, które obejmowałyby zarówno sieć sterowania, jak i sieć korporacyjną. Wszystkie połączenia między siecią sterowania a siecią korporacyjną powinny być realizowane przez zaporę sieciową. Konfiguracja ta nie zapewnia żadnej poprawy bezpieczeństwa i nie powinna być stosowana do łączenia sieci (np. ICS i sieci korporacyjnych).

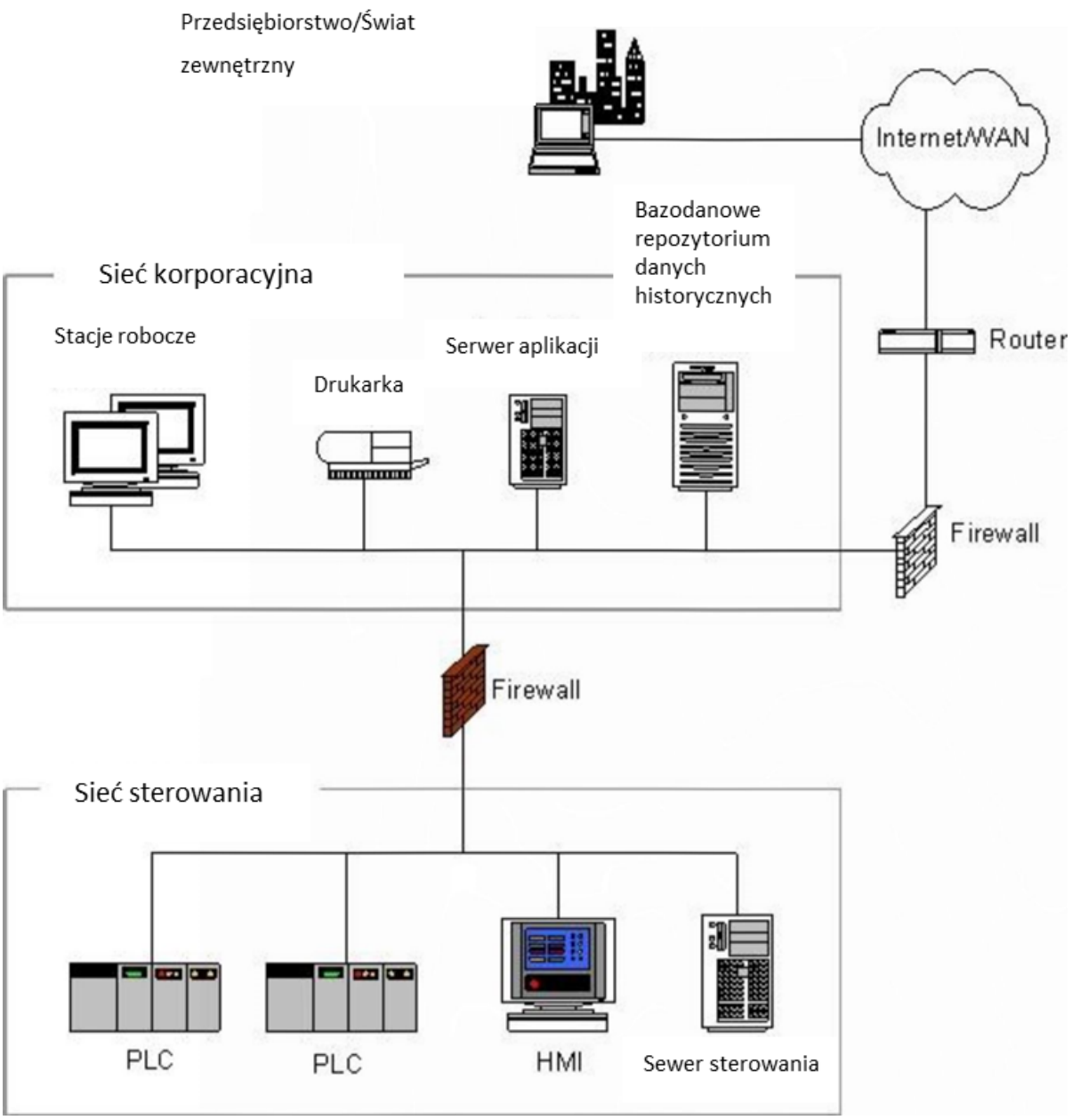
5.5.2. Zapora sieciowa pomiędzy siecią korporacyjną a siecią sterowania

Wprowadzając prostą, dwuportową zaporę sieciową pomiędzy siecią korporacyjną a siecią sterowania, jak pokazano na rysunku 5-1, można uzyskać znaczną poprawę bezpieczeństwa. Prawidłowo skonfigurowana zapora sieciowa znacznie zmniejsza szansę na przeprowadzenie udanego ataku zewnętrznego na sieć sterowania.

Niestety, w tym rozwiązaniu nadal pozostają dwa problemy. Po pierwsze, jeśli bazodanowe repozytorium danych historycznych (*ang. data historian*) znajduje się

[14] Host pracujący jednocześnie w dwóch (kilku) odrębnych sieciach.

w sieci korporacyjnej (*ang. corporate network*), zapora sieciowa (*ang. firewall*) musi umożliwić rejestratorowi danych komunikację z urządzeniami sterującymi w sieci sterowania (*ang. control network*). Pakiet pochodzący ze złośliwego lub nieprawidłowo skonfigurowanego hosta w sieci korporacyjnej (podającego się za rejestrator danych) byłby przekazywany do poszczególnych sterowników PLC/DCS.



Rysunek 5-1. Zapora sieciowa pomiędzy siecią korporacyjną a siecią sterowania.[15]

Jeżeli rejestrator danych znajduje się w sieci sterowania, musi istnieć reguła zapory sieciowej, która umożliwi wszystkim hostom w przedsiębiorstwie komunikację z tym rejestratorem. Zazwyczaj komunikacja ta odbywa się w warstwie aplikacji w postaci zapytań SQL (ang. *Structured Query Language*) lub HTTP (*ang. Hypertext Transfer*

[15] Polskie nazewnictwo angielskich nazw komponentów pokazanych na rysunkach znajduje się w treści publikacji.

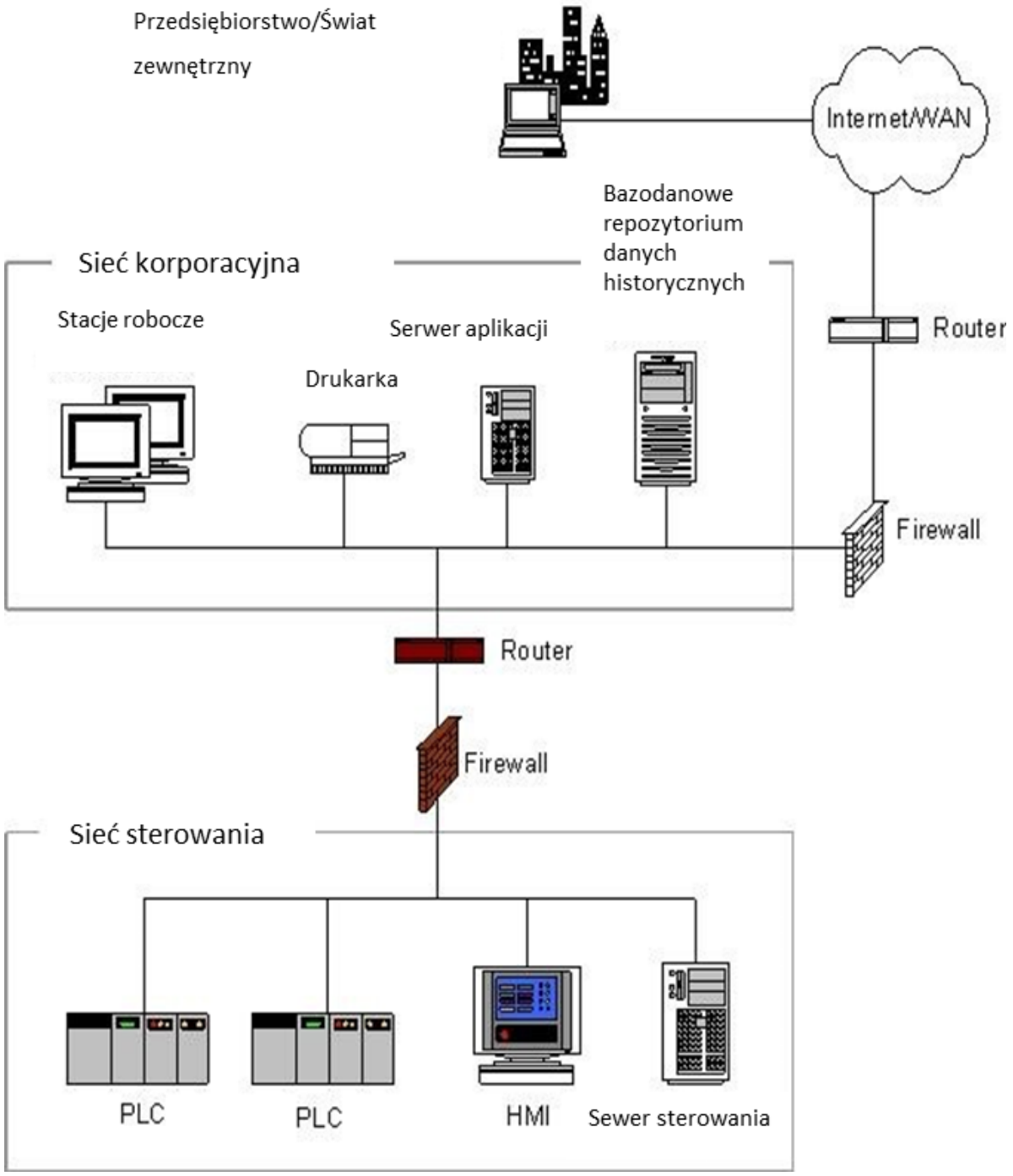
Protocol). Błędy w kodzie warstwy aplikacji bazodanowego repozytorium danych historycznych mogą skutkować jego kompromitacją. Gdy bazodanowe repozytorium danych historycznych jest skompromitowane, pozostałe węzły w sieci sterowania są podatne na rozprzestrzeniające się robaki lub interaktywny atak.

Innym problemem związanym z prostą zaporą sieciową jest możliwość konstruowania sfałszowanych pakietów, które mogą mieć wpływ na sieć sterowania, umożliwiając potencjalnie tunelowanie ukrytych danych w dozwolonych protokołach. Na przykład, jeśli pakiety HTTP są przepuszczane przez zaporę, to oprogramowanie konia trojańskiego przypadkowo wprowadzone do panelu operatorskiego lub laptopa w sieci sterowania, może być kontrolowane przez podmiot zdalny i przesyłać dane (takie jak przechwycone hasła) do tego podmiotu, ukryte jako legalny ruch.

Podsumowując, choć architektura ta stanowi znaczne ulepszenie w porównaniu z siecią niesegregowaną, wymaga stosowania reguł zapory sieciowej, które umożliwiają bezpośrednią komunikację między siecią korporacyjną a urządzeniami sieci sterującej. Może to skutkować potencjalnym naruszeniem bezpieczeństwa, jeśli nie jest bardzo starannie zaprojektowane i monitorowane [35].

5.5.3. Zapora sieciowa i router pomiędzy siecią korporacyjną a siecią sterowania

Nieco bardziej zaawansowane rozwiązanie, przedstawione na rysunku 5-2, wykorzystuje połączenie routera i zapory sieciowej. Router znajduje się przed zaporą sieciową i oferuje podstawowe usługi filtrowania pakietów, podczas gdy zapora sieciowa zajmuje się bardziej złożonymi problemami, wykonując inspekcję stanów lub stosując techniki proxy. Ten typ rozwiązania jest bardzo popularny w zaporach internetowych, ponieważ pozwala szybszemu routerowi obsłużyć większość przychodzących pakietów, zwłaszcza w przypadku ataków DoS, i zmniejszyć obciążenie zapory sieciowej. Zapewnia również lepszą obronę dogłębną, ponieważ istnieją dwa różne urządzenia, które przeciwnik musi ominąć [35].



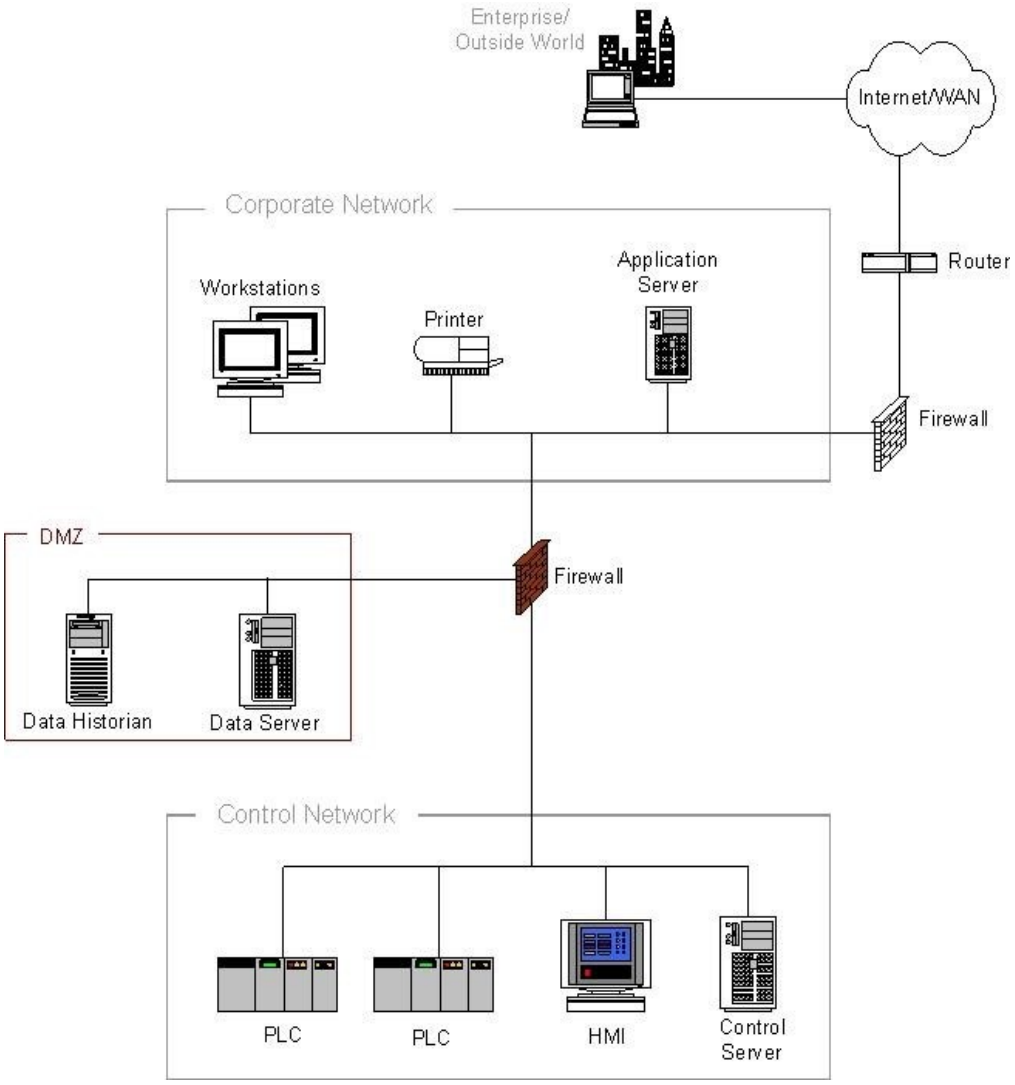
Rysunek 5-2. Zapora sieciowa i router pomiędzy siecią korporacyjną a siecią sterowania.

5.5.4. Zapora sieciowa z DMZ pomiędzy siecią korporacyjną a siecią sterowania

Znaczącym usprawnieniem jest zastosowanie zapór sieciowych z możliwością ustanowienia strefy DMZ pomiędzy siecią korporacyjną a siecią sterowania. Każdy

DMZ zawiera jeden lub więcej krytycznych komponentów, takich jak bazodanowe repozytorium danych historycznych, bezprzewodowy punkt dostępowy lub systemy zdalnego dostępu osób trzecich. W efekcie zastosowanie zapory sieciowej z możliwością tworzenia DMZ pozwala na stworzenie sieci pośredniej.

Utworzenie strefy DMZ wymaga, aby zapora sieciowa oferowała trzy lub więcej interfejsów, a nie typowe interfejsy: publiczny i prywatny. Jeden z tych interfejsów jest podłączony do sieci korporacyjnej, drugi do sieci sterowania, a pozostałe interfejsy do współdzielonych lub niezabezpieczonych urządzeń, takich jak bazodanowe repozytorium danych historycznych lub bezprzewodowe punkty dostępowe w sieci DMZ. Zalecane jest wdrożenie ciągłego monitorowania ruchu przychodzącego i wychodzącego w sieci DMZ. Ponadto zaleca się stosowanie zestawów reguł zapory sieciowej, które zezwalają na połączenia między siecią sterowania a DMZ tylko wtedy, gdy są inicjowane przez urządzenia sieci sterowania. Rysunek 5-3 przedstawia przykład takiej architektury.



Rysunek 5-3. Zapora sieciowa z DMZ pomiędzy siecią korporacyjną a siecią sterowania.

Umieszczenie komponentów dostępnych dla organizacji w strefie DMZ sprawia, że nie są wymagane bezpośrednie ścieżki komunikacyjne z sieci korporacyjnej do sieci sterowania; każda ścieżka w rzeczywistości kończy się w strefie DMZ. Większość zapór sieciowych umożliwia tworzenie wielu stref DMZ i może określać, jakiego rodzaju ruch może być przekazywany pomiędzy strefami. Jak widać na rysunku 5-3, firewall może blokować dowolne pakiety z sieci korporacyjnej przed wejściem do sieci sterującej, a także może regulować ruch z innych stref sieciowych, w tym z sieci sterującej. Dzięki dobrze zaplanowanym zestawom reguł można utrzymać jednoznaczny rozdział między

siecią sterującą a innymi sieciami, z niewielkim lub żadnym ruchem przechodzącym bezpośrednio między sieciami korporacyjnymi i sterującymi.

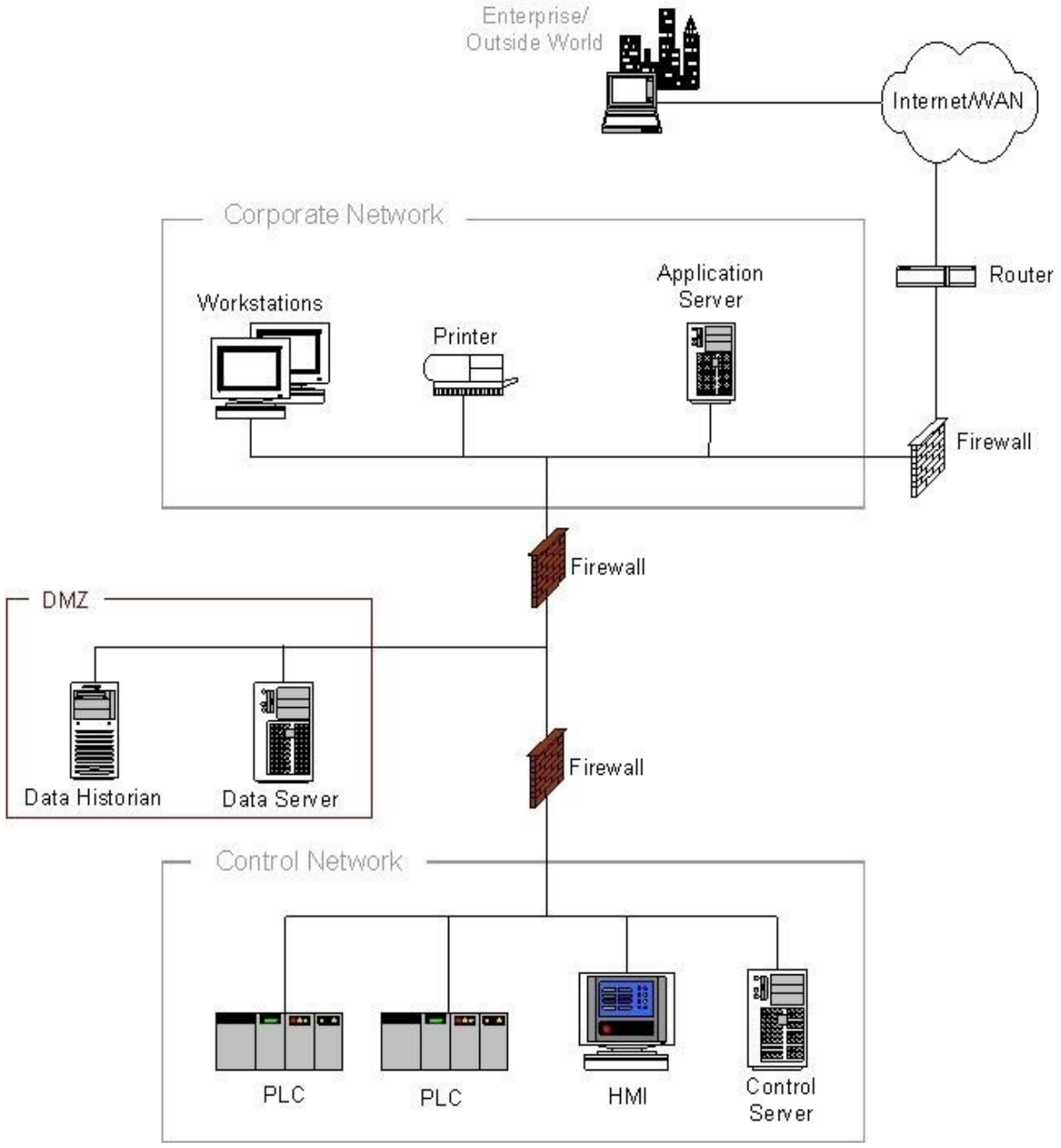
Jeśli w sieci sterowania ma być używany serwer zarządzania poprawkami (łatami), serwer antywirusowy lub inny serwer bezpieczeństwa, powinien on znajdować się bezpośrednio w strefie DMZ. Obie funkcje mogą znajdować się na jednym serwerze. Zarządzanie poprawkami i zarządzanie antywirusowe dedykowane dla sieci sterowania pozwala na kontrolowane i bezpieczne aktualizacje, które można dostosować do unikalnych potrzeb środowiska ICS. Pomocne może być również to, że produkt antywirusowy wybrany do ochrony ICS nie jest taki sam jak produkt antywirusowy używany w sieci firmowej. Na przykład, jeśli wystąpi incydent związany ze złośliwym oprogramowaniem i jeden produkt antywirusowy nie będzie w stanie wykryć lub zatrzymać złośliwego oprogramowania, jest dość prawdopodobne, że inny produkt może mieć taką możliwość.

Podstawowe zagrożenie bezpieczeństwa w tego typu architekturze polega na tym, że jeśli komputer w strefie DMZ zostanie zaatakowany, może zostać użyty do przeprowadzenia ataku na sieć sterowania za pośrednictwem dozwolonego ruchu aplikacji z DMZ do sieci sterowania. Ryzyko to można znacznie ograniczyć, jeśli podjęte zostaną wspólne wysiłki w celu utwardzenia i aktywnego łatania serwerów w DMZ oraz jeśli zestaw reguł zapory sieciowej będzie zezwalał tylko na połączenia między siecią sterowania a DMZ, które są inicjowane przez urządzenia sieci sterowania. Inne zastrzeżenia związane z tą architekturą to dodatkowa złożoność i potencjalnie wyższy koszt zapór sieciowych z wieloma portami. Jednak w przypadku bardziej krytycznych systemów poprawa bezpieczeństwa powinna z nawiązką zrekompensować te niedogodności [35].

5.5.5. Połączone zapory sieciowe pomiędzy siecią korporacyjną a siecią sterowania

Wariantem zapory sieciowej z DMZ jest zastosowanie pary zapór sieciowych umieszczonych między sieciami korporacyjną i ICS, jak pokazano na rysunku 5-4. Wspólne serwery, takie jak bazodanowe repozytorium danych historycznych, są umieszczone między zaporami w strefie sieciowej przypominającej DMZ, określanej czasem jako warstwa systemu produkcyjnego (*ang. Manufacturing Execution System -*

MES). Podobnie, jak w przypadku wcześniej opisanych architektur, pierwsza zapora blokuje dostęp dowolnych pakietów do sieci sterowania lub współdzielonych bazodanowych repozytoriów danych historycznych. Drugi firewall może zapobiegać przedostawaniu się niepożądanego ruchu ze skompromitowanego serwera do sieci sterowania oraz zapobiegać wpływowi ruchu w sieci sterowania na współdzielone serwery.



Rysunek 5-4. Połączone zapory sieciowe pomiędzy siecią korporacyjną a siecią sterowania.

Rozwiązanie to może być korzystne, jeśli używane są zapory dwóch różnych producentów. Umożliwia ono także wyraźne rozdzielenie odpowiedzialności za urządzenia między działem sterowania a działem informacyjnym, ponieważ każdy z nich może zarządzać zaporą samodzielnie, jeśli w organizacji zapadnie taka decyzja. Podstawową wadą architektury dwóch zapór sieciowych jest wzrost kosztów

i złożoność zarządzania. W przypadku środowisk o rygorystycznych wymaganiach w zakresie bezpieczeństwa lub konieczności wyraźnego rozdzielenia zarządzania, architektura ta ma pewne zdecydowane zalety.

5.5.6. Podsumowanie procesu segregacji sieci

Podsumowując:

- Komputery dual-homed na ogół nie zapewniają odpowiedniej izolacji pomiędzy sieciami sterowania a korporacyjnymi.
- Rozwiązania dwustrefowe (bez DMZ) nie są zalecane, ponieważ zapewniają jedynie słabą ochronę. Jeśli są stosowane, powinny być wdrażane tylko z najwyższą ostrożnością.
- Najbardziej bezpieczne, łatwe w zarządzaniu i skalowalne architektury segregacji sieci sterującej i korporacyjnej są zazwyczaj oparte na systemie z co najmniej trzema strefami, zawierającym jedną lub więcej stref DMZ.

5.6. Zalecana architektura „obrony w głąb”

Pojedynczy produkt, technologia lub rozwiązanie z zakresu bezpieczeństwa nie jest w stanie samodzielnie zapewnić odpowiedniej ochrony systemu ICS. Pożądana jest strategia wielowarstwowa obejmująca dwa (lub więcej) różne nakładające się mechanizmy zabezpieczeń, znana również jako "obrona w głąb" (*ang. defense-in-depth*), tak aby zminimalizować wpływ błędu w którymkolwiek z mechanizmów. Strategia architektury "defense-in-depth" obejmuje stosowanie zapór ogniowych, tworzenie stref zdemilitaryzowanych, wykrywanie włamań, a także skuteczną politykę bezpieczeństwa, programy szkoleniowe, mechanizmy reagowania na incydenty oraz zabezpieczenia fizyczne. Ponadto skuteczna strategia "defense-in-depth" wymaga dokładnego zrozumienia możliwych wektorów ataku na system ICS. Należą do nich:

- Tylne drzwi (*ang. backdors*) i „dziury” w obwodach sieci.
- Podatności w powszechnie stosowanych protokołach.
- Ataki na urządzenia obiektowe.
- Ataki na bazy danych.

- Ataki typu "man-in-the-middle" i "hijacking".
- Ataki typu spoofing.
- Ataki na konta uprzywilejowane i/lub współdzielone.

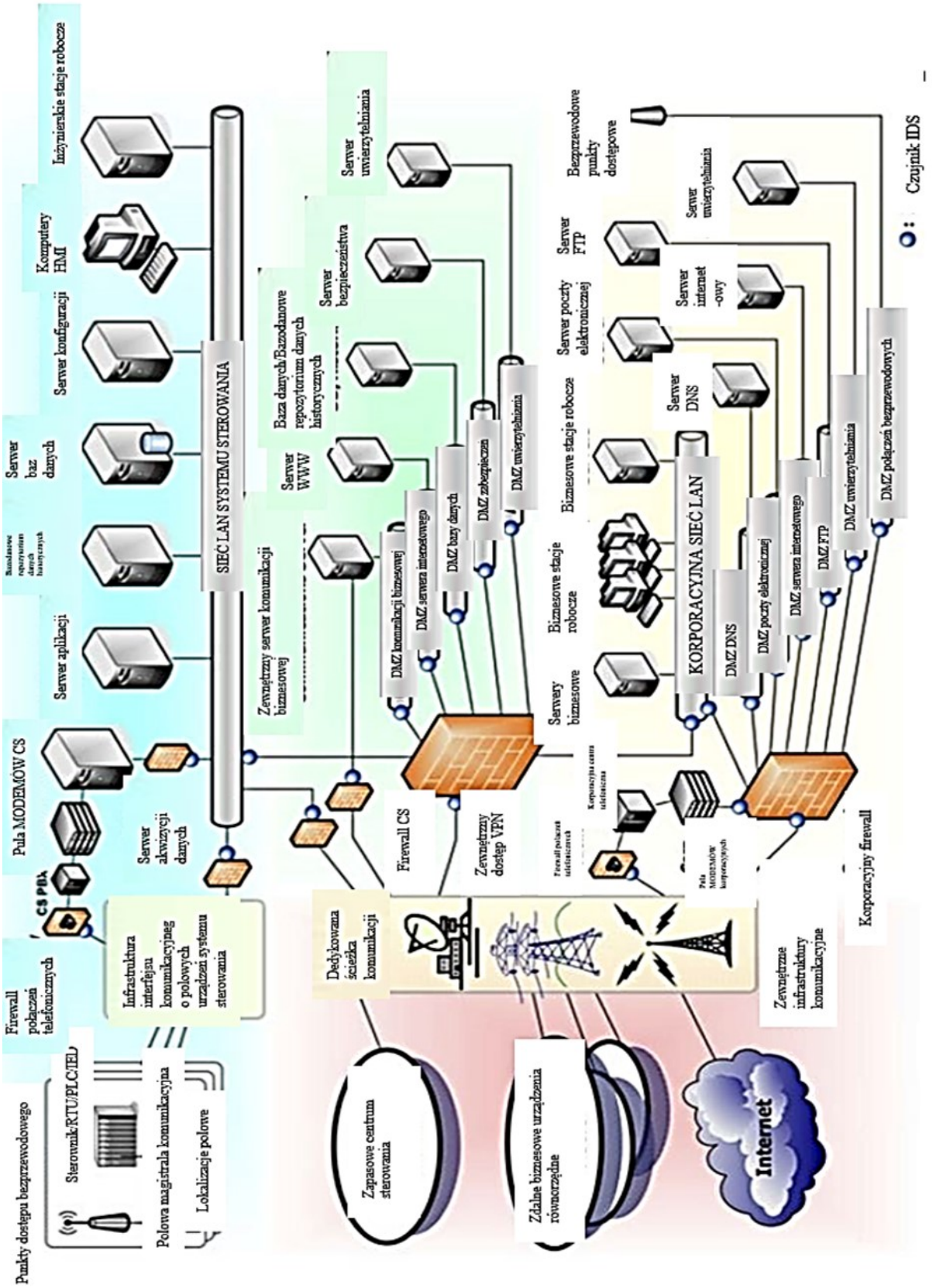
Rysunek 5-5 przedstawia strategię architektury obrony dogłębnej ICS, która została opracowana przez komitet DHS Control Systems Security Program (CSSP) NCCIC/ICS-CERT Recommended Practices, opisaną w dokumencie Control Systems Cyber Security: Defense in Depth Strategies[16] [36]. Na stronie internetowej zamieszczono również dodatkowe dokumenty uzupełniające, które dotyczą konkretnych zagadnień i związanych z nimi środków zaradczych.

Dokument Control Systems Cyber Security: Defense in Depth Strategies zawiera wytyczne i wskazówki dotyczące opracowywania strategii architektury "obrony w głąb" dla organizacji korzystających z sieci systemów sterowania przy zachowaniu wielowarstwowej architektury informacji, która wymaga:

- Utrzymania różnorodnych urządzeń terenowych, zbierania danych telemetrycznych i/lub systemów procesowych na poziomie produkcyjnym.
- Dostępu do obiektów za pośrednictwem zdalnego łącza danych lub modemu.
- Świadczenia usług publicznych dla odbiorców lub organizacji korporacyjnych.

Strategia ta obejmuje zapory sieciowe, stosowanie stref zdemilitaryzowanych oraz funkcje wykrywania włamań w całej architekturze ICS. Wykorzystanie kilku stref zdemilitaryzowanych (rysunek 5-5) zapewnia dodatkową możliwość oddzielenia funkcji i uprawnień dostępu, i sprawdza się bardzo dobrze w ochronie dużych architektur składających się z sieci o różnych zadaniach operacyjnych. W systemach wykrywania włamań stosuje się różne zestawy reguł i sygnatur, unikalne dla każdej monitorowanej domeny.

[16] Informacje o Zalecanych Praktykach CSSP znajdują się na stronie http://ics-cert.us-cert.gov/Recommended-Practices.



Rysunek 5-5. Zalecana architektura obrony w głąb w ramach CSSP.

5.7. Ogólne zasady stosowania zapory sieciowej w ICS

Po wprowadzeniu architektury " obrony w głąb" rozpoczyna się praca polegająca na określeniu, jaki dokładnie ruch sieciowy powinien być dopuszczany (absolutnie niezbędny dla organizacji) przez zapory. Konfigurowanie zapór sieciowych w taki sposób, aby odrzucały wszystko z wyjątkiem ruchu absolutnie niezbędnego dla potrzeb biznesowych, jest podstawowym założeniem każdej organizacji, ale rzeczywistość jest znacznie trudniejsza. Co dokładnie oznacza sformułowanie "absolutnie niezbędny dla działalności organizacji" i jaki wpływ na bezpieczeństwo ma dopuszczenie takiego ruchu? Na przykład wiele organizacji uważało, że dopuszczenie ruchu SQL przez zaporę sieciową jest niezbędne dla działalności biznesowej w przypadku wielu bazodanowe repozytoriów danych historycznych. Niestety, luka w SQL była również celem robaka Slammer [Tabela C-8 Przykładowe incydenty przeciwnika]. Wiele ważnych protokołów używanych w przemyśle, takich jak HTTP, FTP, OPC/DCOM, EtherNet/IP oraz Modbus/TCP, posiada istotne podatności dotyczące zabezpieczeń.

Materiały zawarte w tej sekcji podsumowują niektóre kluczowe punkty z dokumentu Centrum Ochrony Infrastruktury Narodowej (CPNI) Firewall Deployment for SCADA and Process Control Networks: Good Practice Guide [35].

W przypadku instalowania pojedynczej dwuportowej zapory bez strefy DMZ dla serwerów współdzielonych (jak np. W architekturze opisanej w punkcie 5.5.2) należy zwrócić szczególną uwagę na projekt reguł. Co najmniej wszystkie reguły powinny być regułami stanu (typu stateful), które są specyficzne zarówno dla adresu IP, jak i portu (aplikacji). Adresowa część reguł powinna ograniczać ruch przychodzący do bardzo małej grupy urządzeń współdzielonych (np. bazodanowe repozytorium danych historycznych) w sieci sterowania z kontrolowanej grupy adresów w sieci korporacyjnej. Nie zaleca się zezwalania dowolnym adresom IP w sieci korporacyjnej na dostęp do serwerów w sieci sterowania. Ponadto dozwolone porty należy starannie ograniczyć do stosunkowo bezpiecznych protokołów, takich jak Hypertext Transfer Protocol Secure (HTTPS). Zezwolenie na przejście przez zaporę sieciową protokołów HTTP, FTP lub innych niezabezpieczonych protokołów stanowi zagrożenie dla bezpieczeństwa ze względu na możliwość sniffowania i modyfikowania ruchu. Należy

dodać reguły uniemożliwiające hostom spoza sieci sterowania nawiązywanie połączeń z hostami w sieci sterowania. Reguły powinny zezwalać na nawiązywanie połączeń poza siecią tylko urządzeniom znajdującym się wewnątrz sieci sterowania.

Z drugiej strony, jeśli wykorzystywana jest architektura DMZ, możliwe jest skonfigurowanie systemu w taki sposób, aby żaden ruch nie przechodził bezpośrednio między siecią korporacyjną a siecią sterującą. Z kilkoma specjalnymi wyjątkami (opisanymi poniżej) cały ruch z obu stron może kończyć się na serwerach w strefie DMZ. Pozwala to na większą elastyczność w zakresie protokołów dopuszczanych przez zaporę. Na przykład protokół Modbus/TCP może być używany do komunikacji między sterownikami PLC a rejestratorem danych, natomiast protokół HTTP może być używany do komunikacji między rejestratorem a klientami przedsiębiorstwa. Oba protokoły są z natury niezabezpieczone, ale w tym przypadku można ich bezpiecznie używać, ponieważ żaden z nich nie przechodzi między dwoma sieciami. Rozszerzeniem tej koncepcji jest pomysł używania protokołów "rozłącznych" we wszystkich połączeniach między sieciami sterowania i sieciami korporacyjnymi. Oznacza to, że jeśli dany protokół jest dozwolony między siecią sterowania a DMZ, to nie jest on wyraźnie dozwolony między DMZ a siecią korporacyjną. Takie rozwiązanie znacznie zmniejsza szanse na przedostanie się robaka takiego jak Slammer do sieci sterowania, ponieważ musiałby on użyć dwóch różnych exploitów w dwóch różnych protokołach.

Jednym z obszarów, w którym występują znaczne różnice w praktyce, jest kontrola ruchu wychodzącego z sieci sterowania, który może stanowić poważne zagrożenie, jeśli nie jest zarządzany. Jednym z przykładów jest oprogramowanie typu koń trojański, które wykorzystuje tunelowanie HTTP w celu wykorzystania źle zdefiniowanych reguł ruchu wychodzącego. Dlatego ważne jest, aby reguły dotyczące ruchu wychodzącego były tak samo rygorystyczne jak reguły dotyczące ruchu przychodzącego.

Przykładowe reguły dla połączeń wychodzących obejmują:

- Ruch wychodzący przez zaporę sieciową sieci sterowania powinien być ograniczony tylko do niezbędnej komunikacji i do autoryzowanego ruchu pochodzącego z serwerów DMZ.

- Cały ruch wychodzący z sieci sterowania do sieci korporacyjnej powinien być ograniczony ze względu na źródło i miejsce docelowe za pomocą określonej usługi i określonego portu.

Dodatkowo do tych reguł, należy skonfigurować zaporę z funkcją filtrowania wychodzących pakietów, aby uniemożliwić sfałszowanym pakietom IP wyjście z sieci sterowania lub strefy DMZ. W praktyce odbywa się to przez sprawdzanie źródłowych adresów IP wychodzących pakietów z adresami odpowiednich interfejsów sieciowych zapory. Ma to na celu zapobieżenie sytuacji, w której sieć sterowania jest źródłem sfałszowanych pakietów, które są często wykorzystywane w atakach DoS. Dlatego zapory sieciowe powinny być skonfigurowane do przekazywania pakietów IP tylko wtedy, gdy pakiety te mają prawidłowy źródłowy adres IP sieci sterowania lub sieci DMZ. Ponadto należy zapobiegać dostępowi do Internetu przez urządzenia znajdujące się w sieci sterowania.

Podsumowując, poniższe zasady powinny być traktowane jako zalecane praktyki dla ogólnych zestawów reguł zapór sieciowych:

- Podstawowym zestawem reguł powinno być ustawienie opcji "odmowy wszystkim" (*ang. deny all*) i "nie zezwalaj nikomu" (*ang. permit none*).
- Porty i usługi pomiędzy środowiskiem sieci sterowania a siecią korporacyjną powinny być włączane, a uprawnienia przyznawane na podstawie indywidualnych przypadków. Powinno istnieć udokumentowane uzasadnienie biznesowe z analizą ryzyka oraz wyznaczona osoba odpowiedzialna za każdy dozwolony przychodzący lub wychodzący przepływ danych.
- Wszystkie reguły "zezwalania" powinny odnosić się zarówno do adresów IP, jak i portów TCP/UDP, a w razie potrzeby powinny być zgodne z regułami stanu.
- Wszystkie reguły powinny ograniczać ruch do określonego adresu IP lub zakresu adresów.
- Należy uniemożliwić bezpośrednie przechodzenie ruchu z sieci sterowania do sieci korporacyjnej. Cały ruch powinien być zakańczany w strefie DMZ.

- Każdy protokół dozwolony między siecią sterowania a DMZ powinien być jednoznacznie niedopuszczony między DMZ a siecią korporacyjną (i odwrotnie).
- Cały ruch wychodzący z sieci sterowania do sieci korporacyjnej powinien być ograniczony pod względem źródła i miejsca docelowego za pośrednictwem usługi i portu.
- Pakiety wychodzące z sieci sterowania lub DMZ powinny być dozwolone tylko wtedy, gdy pakiety te mają poprawny źródłowy adres IP, który jest przypisany do urządzeń sieci sterowania lub DMZ.
- Urządzenia sieci sterowania nie powinny mieć dostępu do Internetu.
- Sieci sterowania nie powinny być bezpośrednio połączone z Internetem, nawet jeśli są chronione przez zaporę sieciową.
- Cały ruch związany z zarządzaniem zaporą sieciową powinien odbywać się przez oddzielną, zabezpieczoną sieć zarządzania (np. poza pasmem) lub przez sieć szyfrowaną z uwierzytelnianiem wieloskładnikowym. Ruch powinien być również ograniczony przez adres IP do określonych stacji zarządzających.
- Wszystkie zasady dotyczące zapór sieciowych powinny być okresowo testowane.
- Kopie zapasowe konfiguracji wszystkich zapór sieciowych należy tworzyć bezpośrednio przed ich uruchomieniem.

Powyższe wytyczne należy traktować jedynie jako wskazówki. Przed wdrożeniem jakichkolwiek zestawów reguł zapory, należy dokładnie ocenić każde środowisko sterowania.

5.8. Zalecane reguły zapory sieciowej dla określonych usług

Oprócz opisanych powyżej ogólnych zasad, trudno jest przedstawić uniwersalne reguły dotyczące konkretnych protokołów. Potrzeby i zalecane praktyki różnią się znacznie w poszczególnych branżach dla każdego protokołu i powinny być analizowane indywidualnie przez każdą organizację. Stowarzyszenie Industrial Automation Open Networking Association (IAONA) oferuje szablon do przeprowadzenia takiej analizy [37], oceniając każdy z protokołów powszechnie występujących w środowiskach

przemysłowych pod względem funkcji, ryzyka bezpieczeństwa, najbardziej niekorzystnego wpływu oraz sugerowanych środków. Niektóre z kluczowych punktów dokumentu IAONA zostały podsumowane w tym rozdziale. Zaleca się, aby czytelnik zapoznał się z tym dokumentem bezpośrednio podczas opracowywania zestawów reguł.

5.8.1. System nazw domen (DNS)

System nazw domen (Domain Name System, DNS) służy przede wszystkim do konwersji nazw domen na adresy IP. Na przykład DNS może mapować nazwę domeny, taką jak control.com, na adres IP, taki jak 192.168.1.1. Większość usług internetowych w dużym stopniu korzysta z DNS, ale w chwili obecnej jego użycie w sieci sterowania jest stosunkowo rzadkie. W większości przypadków istnieje znikomy argument za tym, aby zezwalać na wysyłanie żądań DNS z sieci sterowania do sieci korporacyjnej i nie ma żadnego uzasadnienia, aby zezwalać na wysyłanie żądań DNS do sieci sterowania. Żądania DNS z sieci sterowania do DMZ powinny być rozpatrywane indywidualnie dla każdego przypadku. Zalecane jest stosowanie lokalnego DNS lub korzystanie z plików hostów.

5.8.2. Protokół przesyłania hipertekstu (HTTP)

HTTP (*ang. Hypertext Transfer Protocol*) to protokół, na którym opierają się usługi przeglądania stron WWW w Internecie. Podobnie jak DNS, ma on kluczowe znaczenie dla większości usług internetowych. Jest on coraz częściej wykorzystywany w halach produkcyjnych jako uniwersalne narzędzie zapytań. Niestety, nie jest on w pełni bezpieczny, a wiele aplikacji wykorzystujących protokół HTTP posiada podatności, które można wykorzystać. Protokół HTTP może być mechanizmem transportowym dla wielu ataków wykonywanych ręcznie i przez automatyczne robaki.

Ogólnie rzecz biorąc, nie należy zezwalać na przesyłanie plików HTTP z sieci publicznej/korporacyjnej do sieci sterowania.

Jeśli technologie internetowe są bezwzględnie wymagane, należy stosować następujące najlepsze praktyki:

- Kontrolowanie dostępu do usług internetowych na poziomie warstwy fizycznej lub sieciowej za pomocą białych list.
- Stosowanie kontroli dostępu zarówno do źródła, jak i do miejsca docelowego.
- Wdrażanie autoryzacji dostępu do usługi na poziomie warstwy aplikacji (zamiast kontroli na poziomie fizycznym lub sieciowym).
- Wdrażanie usługi przy użyciu tylko niezbędnych technologii (np. skrypty są używane tylko wtedy, gdy są wymagane).
- Sprawdzanie usługi zgodnie ze znanymi praktykami bezpieczeństwa aplikacji;
- Rejestrowanie wszystkich prób korzystania z usługi.
- Stosowanie protokołu HTTPS zamiast HTTP i tylko w przypadku określonych, autoryzowanych urządzeń.

5.8.3. Protokół transferu plików FTP i TFTP

Protokoły FTP (*File Transfer Protocol*) i TFTP (*Trivial File Transfer Protocol*) służą do przesyłania plików pomiędzy urządzeniami. Są one zaimplementowane na prawie każdej platformie, w tym wielu systemach SCADA, DCS, PLC i RTU, ponieważ są bardzo dobrze znane i zużywają minimalną moc obliczeniową. Niestety, żaden z tych protokołów nie został stworzony z myślą o bezpieczeństwie; w przypadku protokołu FTP hasło logowania nie jest szyfrowane, a w przypadku protokołu TFTP logowanie nie jest w ogóle wymagane. Co więcej, w niektórych implementacjach protokołu FTP występują podatności związane z przepełnieniem bufora. W rezultacie, cała komunikacja TFTP powinna być zablokowana, natomiast komunikacja FTP powinna być dozwolona tylko dla sesji wychodzących lub jeśli jest zabezpieczona dodatkowym uwierzytelnianiem wieloskładnikowym opartym na tokenach oraz szyfrowanym tunelem. W miarę możliwości należy stosować bezpieczniejsze protokoły, takie jak SFTP (*Secure FTP*) lub SCP (*Secure Copy*).

5.8.4. Telnet

Protokół telnet definiuje interaktywną, tekstową sesję komunikacyjną między klientem a hostem. Jest on używany głównie do zdalnego logowania i prostych usług sterowania

w systemach o ograniczonych zasobach lub systemach o ograniczonych potrzebach w zakresie bezpieczeństwa. Stanowi on poważne zagrożenie bezpieczeństwa, ponieważ cały ruch w protokole telnet, w tym hasła, jest niezaszyfrowany i może umożliwić osobie zdalnej uzyskanie znacznej kontroli nad urządzeniem. Do zdalnej administracji zaleca się używanie protokołu SSH (Secure Shell) [5.8.6]. Przychodzące sesje telnet z sieci korporacyjnej do sieci sterowania powinny być zabronione, chyba że są zabezpieczone wieloskładnikowym uwierzytelnianiem opartym na tokenach i szyfrowanym tunelem. Wychodzące sesje telnet powinny być dozwolone tylko przez szyfrowane tunele (np. VPN) do określonych, autoryzowanych urządzeń.

5.8.5. Protokół dynamicznego konfigurowania hostów (DHCP)

Protokół DHCP jest używany w sieciach IP do dynamicznej dystrybucji parametrów konfiguracyjnych sieci, takich jak adresy IP dla interfejsów i usług. Podstawowy DHCP nie zawiera mechanizmu uwierzytelniania serwerów i klientów. Nieuczciwe serwery DHCP mogą przekazywać klientom nieprawidłowe informacje. Nieautoryzowani klienci mogą uzyskać dostęp do serwera i spowodować wyczerpanie dostępnych zasobów (np. adresów IP). Aby temu zapobiec, zaleca się stosowanie konfiguracji statycznej zamiast dynamicznego przydzielania adresów, co powinno być typową konfiguracją dla urządzeń ICS. Jeśli konieczna jest dynamiczna alokacja, zaleca się włączenie funkcji snoopingu DHCP w celu obrony przed nieuczciwymi serwerami DHCP, protokołem rozpoznawania adresów (*ang. Address Resolution Protocol - ARP*) i spoofingiem IP[17]. Serwery DHCP powinny być umieszczone w tym samym segmencie sieci co konfigurowane urządzenia (np. na routerze). Nie zaleca się przekazywania ruchu DHCP.

5.8.6. Secure Shell (SSH)

SSH umożliwia zdalny dostęp do urządzenia. Zapewnia bezpieczne uwierzytelnianie i autoryzację w oparciu o kryptografię. Jeśli wymagany jest zdalny dostęp do sieci

[17] Termin określający fałszowanie źródłowego adresu IP w wysyłanym przez komputer pakiecie sieciowym. Takie działanie może służyć ukryciu tożsamości atakującego (np. W przypadku ataków DDoS), podszyciu się pod innego użytkownika sieci i ingerowanie w jego aktywność sieciową lub wykorzystaniu uprawnień posiadanych przez inny adres.

sterowania, SSH jest zalecany jako alternatywa dla telnet, rlogin, rsh, rcp i innych niezabezpieczonych narzędzi zdalnego dostępu.

5.8.7. Protokół prostego dostępu do obiektów (SOAP)

SOAP (*Simple Object Access Protocol*) jest opartym na XML formatem składni do wymiany wiadomości. Przepływy ruchu związane z usługami opartymi na SOAP powinny być kontrolowane na zaporze sieciowej między segmentami sieci korporacyjnej i ICS. Jeśli usługi te są niezbędne, należy zastosować głęboką inspekcję pakietów i/lub zapory warstwy aplikacji w celu ograniczenia zawartości komunikatów.

5.8.8. Protokół prostego przesyłania poczty (SMTP)

SMTP (*Simple Mail Transfer Protocol*)to podstawowy protokół przesyłania poczty elektronicznej w Internecie. Wiadomości e-mail często zawierają złośliwe oprogramowanie, dlatego nie należy zezwalać na przesyłanie przychodzących wiadomości e-mail do żadnego urządzenia sieci sterowania. Wiadomości wychodzące SMTP z sieci sterowania do sieci korporacyjnej są dopuszczalne w celu wysyłania komunikatów alarmowych.

5.8.9. Prosty protokół zarządzania siecią (SNMP)

SNMP(*Simple Network Management Protocol*) jest używany do świadczenia usług zarządzania siecią pomiędzy centralną konsolą zarządzającą a urządzeniami sieciowymi, takimi jak routery, drukarki i sterowniki PLC. Chociaż SNMP jest niezwykle przydatną usługą do obsługi sieci, jest bardzo niewydolny pod względem bezpieczeństwa. Wersje 1 i 2 SNMP używają niezaszyfrowanych haseł zarówno do odczytu, jak i konfiguracji urządzeń (w tym urządzeń takich jak sterowniki PLC), a w wielu przypadkach hasła są dobrze znane i nie można ich zmienić. Wersja 3 jest znacznie bezpieczniejsza, ale jej zastosowanie jest nadal ograniczone. Polecenia SNMP V1 i V2 wysyłane do i z sieci sterowania powinny być zabronione, chyba że są wysyłane przez oddzielną, zabezpieczoną sieć zarządzania, natomiast polecenia SNMP V3 mogą być wysyłane do ICS z wykorzystaniem zabezpieczeń właściwych dla V3.

5.8.10. Model obiektowy komponentu rozproszonego (DCOM)

DCOM (*Distributed Component Object Model*) jest protokołem bazowym dla OLE for Process Control (OPC)[18]. Wykorzystuje on usługę zdalnego wywoływania procedur (*Remote Procedure Call - RPC*) firmy Microsoft, która jeśli nie została załatana, posiada wiele podatności. Luki te były podstawą exploitów robaka Blaster[19]. Ponadto OPC, który wykorzystuje DCOM, dynamicznie otwiera szeroki zakres portów (od 1024 do 65535), które mogą być bardzo trudne do odfiltrowania przez zaporę sieciową. Protokół ten powinien być dozwolony tylko pomiędzy siecią sterowania a siecią DMZ i wprost zablokowany pomiędzy DMZ a siecią korporacyjną. Ponadto, zaleca się użytkownikom ograniczenie zakresów portów wykorzystywanych przez urządzenia korzystające z DCOM, poprzez modyfikację rejestru.

5.8.11. Protokoły SCADA i przemysłowe

Protokoły SCADA i przemysłowe, takie jak Modbus/TCP, EtherNet/IP, IEC 61850, ICCP i DNP3[20], są krytyczne dla komunikacji z większością urządzeń sterujących. Niestety, wiele z tych protokołów zostało zaprojektowanych bez wbudowanych zabezpieczeń i zazwyczaj nie wymagają żadnego uwierzytelnienia w celu zdalnego wykonania poleceń na urządzeniu sterującym. Protokoły te powinny być dozwolone tylko w obrębie sieci sterowania i nie powinny przedostawać się do sieci korporacyjnej.

[18] Otwarty standard komunikacyjny stosowany w automatyce przemysłowej i informacyjnych systemach wyższych warstw, a mianowicie biznesowej i zarządzania, przedsiębiorstw przemysłowych.

[19] http://en.wikipedia.org/wiki/Blaster_%28computer_worm%29

[20] IEEE 1815-2012, *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3),*) zawiera DNP3 Secure Authentication version 5 (DNP3-SAv5), który zapewnia silne uwierzytelnianie warstwy aplikacji ze zdalnym zarządzaniem poświadczeniami bezpieczeństwa.

Patrz: https://standards.ieee.org/findstds/standard/1815-2012.html

5.9. Translacja adresów sieciowych (NAT)

Translacja adresów sieciowych (*Network Address Translation - NAT*) to usługa, w ramach której adresy IP używane po jednej stronie urządzenia sieciowego mogą być mapowane na inny zestaw po drugiej stronie, w zależności od potrzeb. Pierwotnie została ona zaprojektowana w celu redukcji adresów IP, tak aby organizacja z dużą liczbą urządzeń, które od czasu do czasu potrzebują dostępu do Internetu, mogła sobie poradzić z mniejszym zestawem przypisanych adresów internetowych.

Aby to osiągnąć, większość implementacji NAT opiera się na założeniu, że nie każde urządzenie wewnętrzne komunikuje się aktywnie z hostami zewnętrznymi w danym momencie. Firewall jest skonfigurowany w taki sposób, że posiada ograniczoną liczbę widocznych na zewnątrz adresów IP. Kiedy wewnętrzny host chce się komunikować z zewnętrznym hostem, firewall dokonuje remapowania wewnętrznego adresu IP i portu na jeden z aktualnie nieużywanych, bardziej ograniczonych, publicznych adresów IP, efektywnie koncentrując ruch wychodzący na mniejszej liczbie adresów IP. Firewall musi śledzić stan każdego połączenia oraz to, w jaki sposób każdy prywatny wewnętrzny adres IP i port źródłowy został przemapowany na widoczną na zewnątrz parę adres IP/port. Kiedy ruch powracający dociera do zapory, mapowanie jest odwracane, a pakiety przekazywane do właściwego hosta wewnętrznego.

Na przykład, urządzenie sieci sterowania może potrzebować nawiązać połączenie z zewnętrznym, niekontrolowanym hostem sieci (na przykład, aby wysłać wiadomość e-mail z alarmem krytycznym). NAT pozwala na zastąpienie wewnętrznego adresu IP inicjującego hosta sieci sterowania przez zaporę sieciową; kolejne pakiety ruchu powrotnego są ponownie zamieniane na wewnętrzny adres IP i wysyłane do odpowiedniego urządzenia sieci sterowania. Mówiąc dokładniej, jeśli sieć sterowania ma przypisaną prywatną podsieć 192.168.1.xxx, a sieć internetowa oczekuje, że urządzenie będzie korzystać z adresów korporacyjnych z zakresu 192.6.yyy.zzz, wówczas zapora sieciowa NAT zastąpi (i będzie śledzić) adres źródłowy 192.6.yyy.zzz w każdym wychodzącym pakiecie IP generowanym przez urządzenie sieci sterowania.

Protokoły typu producent - konsument, takie jak EtherNet/IP i Foundation Fieldbus, są szczególnie kłopotliwe, ponieważ NAT nie obsługuje ruchu opartego na multicastach, którego te protokoły wymagają, aby oferować swoje pełne usługi.

Ogólnie rzecz biorąc, chociaż NAT oferuje pewne wyraźne korzyści, jego wpływ na rzeczywiste protokoły przemysłowe i konfigurację powinien być dokładnie oceniony przed jego wdrożeniem. Co więcej, niektóre protokoły są w szczególny sposób łamane przez NAT z powodu braku możliwości bezpośredniego adresowania. Na przykład, OPC wymaga specjalnego oprogramowania tunelującego firm trzecich do pracy z NAT.

5.10. Szczególne problemy związane z zaporą ICS

Oprócz omówionych już problemów z zaporami sieciowymi i ICS, istnieje kilka dodatkowych problemów, które należy zbadać bardziej szczegółowo. W dalszej części tej sekcji omówiono trzy konkretne obszary problemowe: rozmieszczenie bazodanowych repozytoriów danych historycznych, zdalny dostęp dla obsługi ICS oraz ruch multicastowy.

5.10.1. Bazodanowe repozytorium danych historycznych[21]

Istnienie współdzielonych serwerów sieci sterowania/korporacyjnej, takich jak bazodanowe repozytoria danych historycznych (*ang. data historian*) i serwery zarządzania aktywami, może mieć znaczący wpływ na projekt i konfigurację zapory sieciowej. W systemach trójstrefowych umieszczenie tych serwerów w strefie DMZ jest stosunkowo proste, ale w projektach dwustrefowych problemy stają się złożone. Umieszczenie historianów po korporacyjnej stronie zapory oznacza, że wiele niezabezpieczonych protokołów, takich jak Modbus/TCP czy DCOM, musi być przepuszczonych przez zaporę, a każde urządzenie sterujące raportujące do historiana jest wystawione na działanie korporacyjnej strony sieci. Z drugiej strony, umieszczenie repozytorium danych historycznych po stronie sieci sterowania oznacza, że inne równie problematyczne protokoły, takie jak HTTP lub SQL, muszą być przepuszczane

[21] W potocznym języku technicznym: *historian*.

przez zaporę, a w sieci sterowania znajduje się teraz serwer dostępny dla prawie wszystkich w organizacji.

Ogólnie rzecz biorąc, najlepszym rozwiązaniem jest unikanie systemów dwustrefowych (bez DMZ) i wykorzystanie projektu trójstrefowego, umieszczając kolektor danych w sieci sterowania, a komponent repozytorium danych historycznych w DMZ.

5.10.2. Zdalny dostęp pomocy technicznej

Kolejną kwestią przy projektowaniu zapory ICS jest zdalny dostęp użytkowników i/lub dostawców do sieci sterowania. Wszyscy użytkownicy uzyskujący dostęp do sieci sterowania z sieci zdalnych, powinni być zobowiązani do uwierzytelnienia przy użyciu odpowiednio silnego mechanizmu, takiego jak uwierzytelnianie oparte na tokenach. Chociaż możliwe jest, aby zespół sterowania skonfigurował własny system zdalnego dostępu z uwierzytelnianiem wieloskładnikowym w DMZ, w większości organizacji bardziej efektywne jest korzystanie z istniejących systemów skonfigurowanych przez dział IT. W takim przypadku konieczne jest połączenie przez zaporę z serwera zdalnego dostępu działu IT.

Aby połączyć się z ogólną siecią korporacyjną, pracownicy zdalnego wsparcia technicznego łączący się przez Internet lub modemy dial-up powinni korzystać z szyfrowanego protokołu, np. uruchamiając korporacyjnego klienta połączenia VPN, serwer aplikacji lub bezpieczny dostęp HTTP i uwierzytelniać się przy użyciu silnego mechanizmu, np. wieloskładnikowego schematu uwierzytelniania opartego na tokenie. Po uzyskaniu połączenia, aby uzyskać dostęp do sieci sterowania należy wymagać od nich drugiego uwierzytelnienia na zaporze sieci sterowania przy użyciu silnego mechanizmu, takiego jak schemat wieloskładnikowego uwierzytelniania oparty na tokenie. Dodatkowe możliwości zabezpieczenia dostępu zdalnego wsparcia technicznego mogą również zapewnić serwery proxy.

5.10.3. Ruch multicastowy

Większość przemysłowych protokołów typu producent-konsument (lub wydawca-użytkownik) działających w sieci Ethernet, takich jak EtherNet/IP i Foundation

Fieldbus HSE, bazuje na multicastingu[22] IP[23]. Pierwszą zaletą multicastingu IP jest wydajność sieci; dzięki temu, że nie powtarza się transmisji danych do wielu miejsc docelowych, można znacznie zmniejszyć obciążenie sieci. Drugą zaletą jest to, że host wysyłający nie musi znać wszystkich adresów IP każdego hosta docelowego, który nasłuchuje informacji o rozgłaszaniu. Trzecią i być może najważniejszą dla celów sterowania przemysłowego jest to, że pojedyncza wiadomość multicastowa oferuje znacznie lepsze możliwości synchronizacji czasu pomiędzy wieloma urządzeniami sterującymi niż wiele wiadomości unicastowych[24].

Jeśli źródło i miejsce docelowe pakietu multicast są połączone bez pośrednictwa routerów lub zapór sieciowych, transmisja multicast jest stosunkowo bezproblemowa. Jednakże, jeśli źródło i miejsce docelowe nie znajdują się w tej samej sieci LAN, przekazywanie wiadomości multicast do miejsca docelowego staje się bardziej skomplikowane. Aby rozwiązać problem routingu wiadomości multicast, hosty muszą dołączyć (lub opuścić) grupę, informując router multicastingu w swojej sieci o odpowiednim identyfikatorze grupy za pomocą protokołu IGMP (*Internet Group Management Protocol*). Routery multicastowe posiadają informacje na temat członków grup multicastowych w swojej sieci i mogą zdecydować, czy przekazać otrzymany komunikat multicastowy do swojej sieci. Wymagany jest również protokół routingu multicastów. Z punktu widzenia administracji zapory sieciowej monitorowanie i filtrowanie ruchu IGMP staje się kolejną serią zestawów reguł do zarządzania, co zwiększa złożoność zapory sieciowej.

Innym problemem związanym z multicastingiem jest użycie NAT. Zapora z funkcją NAT, która odbiera pakiet multicastingowy od zewnętrznego hosta, nie ma odwrotnego odwzorowania, który wewnętrzny identyfikator grupy powinien otrzymać dane. Jeśli obsługuje IGMP, może rozsyłać dane do wszystkich identyfikatorów grup,

[22] Multicast – sposób dystrybucji informacji, w którym dane są wysyłane przez jeden komputer do jednego bądź kilku komputerów w jednej chwili.

[23] IP Multicast to metoda przekazywania pakietów telekomunikacyjnych IP do grupy zainteresowanych odbiorców.

[24] Unicast - rodzaj transmisji, w której dokładnie jeden punkt wysyła pakiety do dokładnie jednego punktu - istnieje tylko jeden nadawca i tylko jeden odbiorca.

o których wie, ponieważ jeden z nich będzie prawidłowy, ale może to spowodować poważne problemy, jeśli niezamierzony pakiet sterujący zostanie rozesłany do krytycznego węzła. Najbezpieczniejszym działaniem podejmowanym przez firewall jest odrzucenie pakietu. Dlatego multicasting jest ogólnie uważany za nieprzyjazny dla NAT.

5.11. Bramki jednokierunkowe

Wymuszone sprzętowo bramki jednokierunkowe (np. diody danych) są coraz częściej stosowane na granicy między sieciami ICS i IT, a także między sieciami SIS (*ang. Safety Instrumented System*) i sieciami sterowania. Bramki jednokierunkowe są połączeniem sprzętu i oprogramowania. Sprzęt pozwala na przepływ danych z jednej sieci do drugiej, ale fizycznie nie jest w stanie przekazać żadnych informacji z powrotem do sieci źródłowej. Oprogramowanie replikuje bazy danych i emuluje serwery protokołów i urządzenia.

5.12. Pojedyncze punkty awarii

Pojedyncze punkty awarii mogą występować na każdym poziomie stosu ANSI/ISO. Przykładem jest sterowanie poprzez PLC blokadami bezpieczeństwa. Ponieważ zabezpieczenie jest zazwyczaj dodawane do środowiska ICS, należy przeprowadzić ocenę w celu zidentyfikowania potencjalnych punktów awarii oraz ocenę ryzyka w celu oszacowania narażenia każdego punktu. Następnie można zaproponować i ocenić metody zaradcze, określić stosunek ryzyka do korzyści oraz opracować i wdrożyć projekt.

5.13. Redundancja i tolerancja błędów

Składniki ICS lub sieci, które są sklasyfikowane jako krytyczne dla organizacji, mają wysokie wymagania dotyczące dostępności. Jedną z metod osiągnięcia wysokiej dostępności jest zastosowanie redundancji. Dodatkowo, w przypadku usterki komponentu, powinien on ulec awarii w sposób, który nie generuje niepotrzebnego ruchu w ICS lub nie powoduje innego problemu w innym miejscu, takiego jak zdarzenie kaskadowe.

System sterowania powinien posiadać zdolność do wykonania odpowiedniego procesu awaryjnego w przypadku utraty łączności z systemem ICS lub utraty samego systemu ICS. Organizacja powinna zdefiniować, co oznacza "utrata łączności" (np. 500 milisekund, 5 sekund, 5 minut, itd. bez łączności).). Organizacja powinna następnie, w oparciu o potencjalne konsekwencje, zdefiniować odpowiedni dla swojej branży proces zabezpieczający przed awarią.

Kopie zapasowe należy wykonywać zgodnie z podejściem „zaawansowanych kopii bezpieczeństwa" (*ang. "backup-in-depth"*), *z* warstwami kopii zapasowych (np. lokalną, obiektową, klęsk żywiołowych), które są uporządkowane czasowo w taki sposób, aby szybkie, aktualne lokalne kopie zapasowe były dostępne do natychmiastowego użytku, a bezpieczne kopie zapasowe były dostępne do odtworzenia po poważnym incydencie bezpieczeństwa. Należy stosować różne podejścia do tworzenia i odtwarzania kopii zapasowych oraz metody przechowywania, aby zapewnić rygorystyczne tworzenie kopii zapasowych, bezpieczne przechowywanie i odpowiedni dostęp do nich w celu odtworzenia.

5.14. Zapobieganie atakom typu „Man-in-the-Middle"

Atak typu „man-in-the-middle" wymaga znajomości protokołu, którym się manipuluje. Atak „man-in-the-middle" na protokół ARP (*Address Resolution Protocol*) jest popularną metodą uzyskiwania przez przeciwnika dostępu do sieciowego przepływu informacji w systemie docelowym. Odbywa się to poprzez atak na podręczne tablice sieciowe ARP (*ARP cache table*) sterownika i maszyn stacji roboczych. Używając skompromitowanego komputera w sieci sterowania, adwersarz „skaża" tablice ARP na każdym hoście i informuje je, że muszą kierować cały swój ruch przez określony adres IP i adres sprzętowy (tj. maszynę adwersarza). Manipulując tablicami ARP, adwersarz może umieścić swoją maszynę pomiędzy dwoma docelowymi maszynami i/lub urządzeniami.

Atak „man-in-the-middle" z użyciem ARP działa poprzez inicjowanie nieuzasadnionych poleceń ARP w celu zmylenia każdego hosta (tj. „skażenia" ARP). Te komendy ARP powodują, że każdy z dwóch hostów docelowych używa adresu MAC przeciwnika jako adresu drugiego hosta docelowego. Kiedy udany atak typu „man-in-the-middle" jest

wykonywany, hosty po każdej stronie ataku są nieświadome, że ich dane sieciowe ustanawiają trasę routingów przez komputer przeciwnika.

Po pomyślnym wprowadzeniu swojej maszyny do strumienia informacji, przeciwnik ma pełną kontrolę nad transmisją danych i może przeprowadzić różnego rodzaju ataki. Jedną z możliwych metod ataku jest atak powtórzeniowy. W najprostszej formie dane przechwycone z panelu sterowania (ang. Human-machine interface - HMI) są modyfikowane w celu wywołania aktywności po ich odebraniu przez sterownik urządzenia. Przechwycone dane odzwierciedlające normalne operacje w systemie ICS mogą być w razie potrzeby odtwarzane operatorowi. Dzięki temu interfejs HMI operatora będzie wyglądał na normalny, a atak pozostanie niezauważony. Podczas takiego ataku powtórzeniowego przeciwnik może nadal wysyłać polecenia do sterownika i/lub urządzeń obiektowych w celu wywołania niepożądanego zdarzenia, podczas gdy operator nie jest świadomy faktycznego stanu systemu.

Innym atakiem, który można przeprowadzić za pomocą ataku typu "man-in-the-middle", jest wysyłanie fałszywych komunikatów do operatora, które mogą mieć postać fałszywego negatywu lub fałszywego pozytywu. Może to spowodować, że operator podejmie działanie, np. przestawi wyłącznik, gdy nie jest to wymagane lub uzna, że wszystko jest w normie i nie podejmie żadnego działania, mimo że jest ono wymagane. Przeciwnik może wysyłać do konsoli operatora polecenia wskazujące na zmianę w systemie, a gdy operator postępuje zgodnie z odpowiednimi procedurami i próbuje naprawić problem, jego działanie może spowodować niepożądane zdarzenie. Istnieją różnego rodzaju sposoby modyfikacji i odtwarzania danych sterujących, które mogą wpływać na działanie systemu.

Manipulowanie protokołem oraz atak man-in-the-middle to jedne z najpopularniejszych sposobów manipulowania niezabezpieczonymi protokołami, takimi jak te występujące w systemach sterowania. Istnieją jednak odpowiednie techniki łagodzące [38], które można zastosować w celu zabezpieczenia systemów, np. blokowanie adresów MAC, tworzenie tablic statycznych, szyfrowanie, uwierzytelnianie i monitorowanie.

- **Blokowanie adresów MAC** - Atak typu „ARP man-in-the-middle" wymaga, aby przeciwnik był podłączony do sieci lokalnej lub miał kontrolę nad lokalnym komputerem w sieci. Bezpieczeństwo portów, zwane również blokowaniem adresów MAC, jest jedną z metod zabezpieczenia fizycznego połączenia na końcu każdego portu w przełączniku sieciowym. Wysokiej klasy przełączniki sieciowe klasy korporacyjnej zwykle posiadają opcję blokowania adresów MAC. Blokowanie adresów MAC jest bardzo skuteczne przeciwko nieuczciwym osobom, które chcą fizycznie podłączyć się do sieci wewnętrznej. Bez zabezpieczenia portu, każde otwarte gniazdo sieciowe na ścianie może zostać użyte jako droga do sieci korporacyjnej. Zabezpieczanie portów blokuje konkretny adres MAC do konkretnego portu w zarządzanym przełączniku. Jeśli adres MAC nie będzie zgodny, połączenie komunikacyjne zostanie zablokowane a intruz nie będzie mógł osiągnąć swojego celu. Niektóre bardziej zaawansowane przełączniki posiadają opcję automatycznego resetowania, która przywraca działanie zabezpieczenia, jeśli oryginalny adres MAC zostanie przywrócony do portu.

  Chociaż zabezpieczanie portów nie jest odporne na ataki, stanowi dodatkową warstwę bezpieczeństwa sieci fizycznej. Chroni również sieć lokalną przed pracownikami, którzy podłączają do chronionej sieci niezałatane i nieaktualizowane systemy. Zmniejsza to liczbę komputerów docelowych, do których może uzyskać dostęp zdalny napastnik. Te środki bezpieczeństwa nie tylko chronią przed atakami z sieci zewnętrznych, ale także zapewniają dodatkową ochronę fizyczną.

- **Tablice statyczne** - w sieci ICS, która jest stosunkowo statyczna, można wdrożyć statycznie kodowane tablice ARP. Większość systemów operacyjnych ma możliwość statycznego zakodowania wszystkich adresów MAC w tabeli ARP na każdym komputerze. Statyczne kodowanie tablic ARP na każdym komputerze uniemożliwia przeciwnikowi ich zmianę poprzez wysyłanie pakietów odpowiedzi ARP do komputera ofiary. Chociaż technika ta nie jest możliwa do zastosowania w dużej i/lub dynamicznej sieci korporacyjnej, ograniczona liczba hostów w sieci ICS może być skutecznie chroniona za pomocą tego rozwiązania.

- **Szyfrowanie** - jako rozwiązanie długoterminowe, systemy powinny być projektowane z uwzględnieniem szyfrowania między urządzeniami, co bardzo utrudnia odwrotną inżynierię protokołów i fałszowanie pakietów w sieciach systemów sterowania. Szyfrowanie komunikacji między urządzeniami sprawi, że przeprowadzenie takiego ataku będzie prawie niemożliwe. Protokoły zapewniające silne uwierzytelnianie są również odporne na ataki typu „man-in the-middle". Należy jednakże rozważyć wpływ szyfrowania na wydajność sieci i operacji.
- **Uwierzytelnianie -** protokoły z silnym uwierzytelnianiem są odporne na ataki typu man-in-the-middle.
- **Monitorowanie** - monitorowanie „skażenia" ARP stanowi dodatkową warstwę obrony. Dostępnych jest kilka programów (np. ARPwatch), które mogą monitorować zmiany adresów MAC przez pakiety ARP.

5.15. Uwierzytelnianie i autoryzacja

System ICS może zawierać dużą liczbę systemów, z których każdy musi być dostępny dla różnych użytkowników. Uwierzytelnianie i autoryzacja tych użytkowników stanowi wyzwanie dla systemu ICS. Zarządzanie kontami użytkowników może być problematyczne, ze względu na zmiany personalne i przydzielane role. Wraz ze wzrostem liczby systemów i użytkowników, proces zarządzania tymi kontami staje się coraz bardziej skomplikowany.

Uwierzytelnienie użytkownika lub systemu to proces weryfikacji deklarowanej tożsamości. Autoryzacja, jako proces przyznawania użytkownikowi praw dostępu, jest określana poprzez zastosowanie reguł polityki do uwierzytelnionej tożsamości i innych istotnych informacji[25]. Autoryzacja jest wymuszana przez określony mechanizm kontroli dostępu. Proces uwierzytelniania może być wykorzystywany do

[25] Ogólnie rzecz biorąc, autoryzacja do wykonania zestawu operacji jest określana poprzez ocenę atrybutów związanych z podmiotem, obiektem, żądanymi operacjami oraz, w niektórych przypadkach, warunkami środowiskowymi w odniesieniu do polityki, reguł lub relacji, które opisują dozwolone operacje dla danego zestawu atrybutów. Więcej informacji można znaleźć w publikacji specjalnej NIST SP 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, pod adresem:

Guide to Attribute Based Access Control (ABAC) Definition and Considerations (nist.gov)

kontrolowania dostępu zarówno do systemów (np. interfejsów HMI, urządzeń obiektowych, serwerów SCADA), jak i do sieci (np. sieci LAN zdalnych podstacji).

Uwierzytelnianie i autoryzacja mogą być wykonywane zarówno w podejściu rozproszonym jak i scentralizowanym. Przy rozproszonym uwierzytelnianiu i autoryzacji, każdy system wykonuje te kroki samodzielnie. Każdy system jest odpowiedzialny za przechowywanie swojego własnego zestawu kont użytkowników, poświadczeń i ról oraz za przeprowadzenie identyfikacji i uwierzytelnienia użytkownika. Takie podejście zazwyczaj nie wymaga żadnej dodatkowej infrastruktury. Podejście to jest jednak na tyle problematyczne, że nie skaluje się dobrze wraz ze wzrostem rozmiaru systemu. Na przykład, jeśli użytkownik opuszcza organizację, odpowiadające mu konto użytkownika musi zostać osobno usunięte z każdego systemu.

W przeciwieństwie do podejścia rozproszonego, scentralizowane systemy uwierzytelniania i autoryzacji są powszechnie stosowane do zarządzania większą liczbą użytkowników i kont. Podejście scentralizowane wykorzystuje centralny system uwierzytelniania (np. *Microsoft Active Directory*, *Lightweight Directory Access Protocol - LDAP*) do przechowywania wszystkich kont i zarządzania uwierzytelnianiem i autoryzacją wszystkich osób i systemów. Protokół uwierzytelniania (np. *Kerberos*, *RADIUS*, *TACACS+*) jest następnie wykorzystywany do przekazywania danych pomiędzy serwerem uwierzytelniania a systemem przeprowadzającym uwierzytelnianie.

Chociaż podejście scentralizowane zapewnia znacznie lepszą skalowalność, wiąże się ono również z wieloma dodatkowymi problemami, które mogą wpłynąć na jego zastosowanie w środowiskach ICS. Należy wziąć pod uwagę następujące kwestie:

- Serwery uwierzytelniające tworzą pojedynczy system, który jest odpowiedzialny za zarządzanie wszystkimi kontami systemowymi i muszą być bardzo dobrze zabezpieczone.
- System serwera uwierzytelniającego wymaga wysokiej dostępności, ponieważ jego awaria może uniemożliwić użytkownikom uwierzytelnienie się do systemu w sytuacjach awaryjnych. Może być wymagana jego redundancja.

- Niektórzy klienci mogą lokalnie buforować poświadczenia użytkownika, aby zapewnić, że użytkownicy mogą być nadal uwierzytelniani w przypadku braku dostępności serwera. Buforowanie może być dostępne tylko dla użytkowników, którzy niedawno się uwierzytelnili. Buforowanie wprowadza również komplikacje związane z unieważnianiem.
- Sieci wykorzystywane do obsługi protokołu uwierzytelniania muszą być niezawodne i bezpieczne, aby zapewnić, że próby uwierzytelniania nie będą utrudniane.

5.15.1. Uwagi dotyczące wdrożenia systemu ICS

Chociaż scentralizowane serwery uwierzytelniania i autoryzacji są powszechnie stosowane w środowisku IT, istnieje wiele wyzwań związanych z ich integracją z ICS. Podczas gdy serwery i protokoły uwierzytelniania integrują się z wieloma produktami IT (np. Microsoft Windows, Linux, Oracle), często ICS może wykorzystywać własne konta i mechanizmy uwierzytelniania specyficzne dla danej aplikacji, które nie zostały zaprojektowane do współpracy z serwerami i protokołami innych firm. Ogranicza to możliwość zaadoptowania takiego mechanizmu w środowisku ICS. Starsze urządzenia sieciowe i większość urządzeń obiektowych nie obsługuje żadnych mechanizmów integracji ze scentralizowanym systemem uwierzytelniania.

5.16. Monitorowanie, rejestrowanie i audytowanie

Architektura bezpieczeństwa ICS musi również obejmować mechanizmy monitorowania, rejestrowania i audytowania działań zachodzących w różnych systemach i sieciach. Monitorowanie, rejestrowanie i audytowanie działań są niezbędne do zrozumienia aktualnego stanu ICS, potwierdzenia, że system działa zgodnie z przeznaczeniem oraz, że żadne naruszenia polityki lub cyberincydenty nie utrudniają działania systemu. Monitorowanie bezpieczeństwa sieci jest cenne dla scharakteryzowania normalnego stanu ICS i może dostarczyć informacji o zagrożonych systemach, gdy zawiodą technologie oparte na sygnaturach. Ponadto ścisłe monitorowanie, rejestrowanie i audytowanie systemu są niezbędne do rozwiązywania

problemów i przeprowadzania wszelkich niezbędnych analiz kryminalistycznych systemu[26].

5.17. Wykrywanie incydentów, reagowanie i odzyskiwanie systemu

Incydenty są nie do uniknięcia, a plany wykrywania incydentów, reagowania na nie oraz odzyskiwania systemu są nieodzowne. Główną cechą prawidłowego programu bezpieczeństwa jest to, jak szybko po wystąpieniu incydentu można go wykryć i jak szybko można przywrócić system do stanu pierwotnego sprzed wystąpienia incydentu. Reagowanie na incydenty w systemach ICS jest ściśle powiązane z odzyskiwaniem danych po awarii, szczególnie w celu spełnienia rygorystycznych wymagań dotyczących czasu sprawności systemów ICS. Osoby reagujące na incydenty muszą być przeszkolone pod kątem scenariuszy specyficznych dla ICS, ponieważ normalne metody odzyskiwania systemów informacyjnych mogą nie mieć zastosowania w przypadku ICS.

[26] Więcej informacji można znaleźć w dokumencie NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems ,(IDPS)* [55].

6. STOSOWANIE ZABEZPIECZEŃ W SYSTEMACH ICS

Pojedynczy produkt lub technologia zabezpieczająca nie jest w stanie odpowiednio chronić systemu ICS. Zabezpieczenie ICS opiera się na połączeniu skutecznej polityki bezpieczeństwa i odpowiednio skonfigurowanego zestawu środków bezpieczeństwa. Wybór i wdrożenie środków bezpieczeństwa, które mają być zastosowane w systemie ICS, może mieć poważne konsekwencje dla operacji wykonywanych przez ICS, dlatego należy wziąć pod uwagę następujące kwestie:

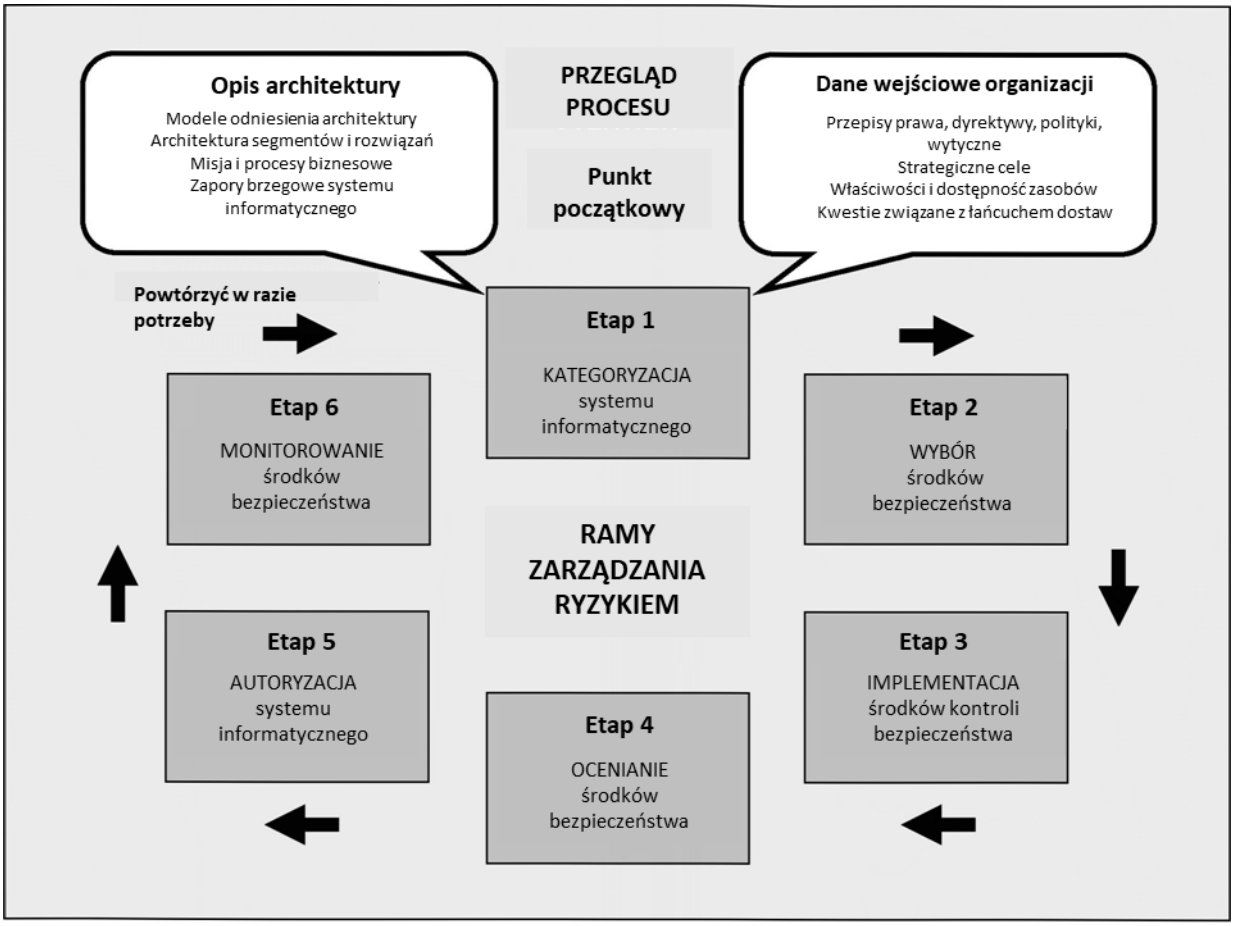
- Jakie zabezpieczenia są potrzebne, aby odpowiednio ograniczyć ryzyko do akceptowalnego poziomu, który wspiera misje organizacji i funkcje biznesowe?
- Czy wybrane zabezpieczenia zostały wdrożone lub czy istnieje realistyczny plan wdrożenia?
- Jaki jest wymagany poziom pewności, że wybrane zabezpieczenia są wdrożone prawidłowo, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty?

Jak wskazano w rozdziale 3, odpowiedzi na pytania powinny być udzielane w kontekście skutecznego, obejmującego całą organizację procesu zarządzania ryzykiem i strategii cyberbezpieczeństwa, w ramach których identyfikuje się, ogranicza (w razie potrzeby) i stale monitoruje ryzyko związane z danym systemem ICS. Skuteczna strategia cyberbezpieczeństwa ICS powinna wykorzystywać technikę "obrony w głąb", polegającą na tworzeniu warstw mechanizmów bezpieczeństwa w taki sposób, aby zminimalizować wpływ awarii jednego z mechanizmów. Stosowanie takiej strategii jest przedmiotem dyskusji na temat zabezpieczeń i ich zastosowania do ICS, które zostaną przedstawione poniżej.

6.1. Realizacja zadań ramowego systemu zarządzania ryzykiem w systemach sterowania przemysłowego

Poniżej opisano proces zastosowania Ramowego Systemu Zarządzania Ryzykiem (*ang. Risk Management Framework - RMF*) w ICS. Proces ten zawiera krótki opis każdej czynności oraz wskazuje dokumenty pomocnicze NIST/NSC. Poniższe kroki, choć

przedstawione w sposób sekwencyjny, mogą być realizowane w innej kolejności, aby zachować spójność z ustalonymi procesami zarządzania w cyklu życia systemu [21].



Rysunek 6-1. Zadania w ramach zarządzania ryzykiem.

6.1.1. Krok 1: Kategoryzacja systemu informacyjnego

Pierwszą czynnością w RMF jest kategoryzacja informacji i systemów informacyjnych pod względem potencjalnych skutków ich ewentualnego utracenia. Dla każdego typu informacji i systemu informacyjnego, trzy podstawowe atrybuty bezpieczeństwa - poufność, integralność i dostępność - są powiązane z jednym z trzech poziomów wpływów na system w przypadku naruszenia bezpieczeństwa. Należy pamiętać, że w przypadku ICS największym problemem jest dostępność.

Rekomendacje dotyczące procesu kategoryzacji można znaleźć odpowiednio w standardach NSC 199 (bazującym na publikacji FIPS 199 [15]) i NSC 800-60 (bazującym na publikacji NIST SP 800-60 [25]).

Poniższy przykład systemu ICS pochodzi z dokumentu NSC 199 (FIPS 199 [15]):

Zalecenia i wytyczne dotyczące ICS

Elektrownia posiada system kontroli nadzorczej i pozyskiwania danych SCADA kontrolujący rozdział energii elektrycznej w dużej instalacji wojskowej. System SCADA przetwarza zarówno dane czasu rzeczywistego z czujników, jak i informacje administracyjne. Kierownictwo w elektrowni ustala, że: (I) w przypadku danych z czujników pozyskiwanych przez system SCADA nie występuje potencjalny wpływ utraty poufności, natomiast potencjalny wpływ utraty integralności i dostępności jest wysoki; oraz (II) w przypadku informacji administracyjnych przetwarzanych przez system występuje niewielki potencjalny wpływ utraty poufności, niski potencjalny wpływ utraty integralności oraz niski potencjalny wpływ utraty dostępności. Wynikowe kategorie bezpieczeństwa (KB) tych rodzajów informacji wyrażane są jako:

KB[27] danych z czujników = {(**poufność**, NIE DOTYCZY), (**integralność**, WYSOKI), (**dostępność**, WYSOKI)},

oraz

KB informacji administracyjnej = {(**poufność**, NISKI), (**integralność**, NISKI), (**dostępność**, NISKI)}.

Wynikowa kategoria bezpieczeństwa systemu informacyjnego wyrażona jest jako:

KB systemu SCADA = {(**poufność**, NISKI), (**integralność**, WYSOKI), (**dostępność**, WYSOKI)},

przedstawiając najwyższy wpływ lub potencjalnie maksymalne wartości wpływu poszczególnych atrybutów bezpieczeństwa dla rodzajów informacji przetwarzanych

[27] Kategoria bezpieczeństwa (KB) rodzaju informacji = {(**poufność**, wpływ), (**integralność**, wpływ), (**dostępność**, wpływ)}, gdzie dopuszczalne wartości potencjalnego wpływu to NISKI, UMIARKOWANY, WYSOKI, oraz NIE DOTYCZY. Patrz: NSC 199.

w systemie SCADA. Zarząd elektrowni wybiera podniesienie potencjalnego wpływu utraty poufności z niskiego do umiarkowanego w celu odzwierciedlenia bardziej realistycznego obrazu potencjalnego wpływu na system informacyjny w sytuacji, w której wystąpiłoby naruszenie bezpieczeństwa związane z nieuprawnionym ujawnieniem informacji na poziomie systemu lub funkcji przetwarzania. Ostateczna kategoria bezpieczeństwa systemu informacyjnego wyrażana jest, jako:

KB systemu SCADA = {(poufność, UMIARKOWANY), (integralność, WYSOKI), (dostępność, WYSOKI)}.

Publikacja NSC 199 definiuje trzy poziomy potencjalnego wpływu na organizacje i osoby fizyczne w przypadkach wystąpienia naruszenia bezpieczeństwa (tj. utraty poufności, integralności lub dostępności).

W tabeli 6-1 przedstawiono przykładowe definicje niskich, umiarkowanych i wysokich poziomów wpływu na ICS, biorąc pod uwagę standard ISA99.

Tabela 6-1. Możliwe definicje poziomów wpływu ICS na podstawie ISA99 (przykład).

Kategoria wpływu	Niskie oddziaływanie	Umiarkowane oddziaływanie	Wysokie oddziaływanie
Obrażenia	Skaleczenia, stłuczenia wymagające pierwszej pomocy	Wymaga hospitalizacji	Utrata życia lub kończyny
Strata finansowa	5 000 zł	500 000 zł	> 1 000 000 zł
Ochrona środowiskowa	Szkody tymczasowe	Trwałe uszkodzenie	Trwałe szkody, szkody poza terenem organizacji
Przerwa w produkcji	Godziny	Dni	Tygodnie
Obraz publiczny	Szkody tymczasowe	Trwałe uszkodzenie	Trwałe uszkodzenie

W tabeli 6-2 przedstawiono przykładowe identyfikacje poziomów wpływu systemu ICS w zależności od wytwarzanego produktu, branży i wymogów bezpieczeństwa.

Tabela 6-2. Przykładowe identyfikacje poziomów wpływu systemu ICS w zależności od wytwarzanego produktu, branży i kwestii bezpieczeństwa.

Kategoria wpływu	Niskie oddziaływanie	Umiarkowane oddziaływanie	Wysokie oddziaływanie
Wytwarzany produkt	• Materiały lub produkty inne niż niebezpieczne • Produkty konsumenckie, które nie uległy rozpadowi.	• Niektóre niebezpieczne produkty lub procesy produkcyjne • Znaczna liczba informacji prawnie zastrzeżonych	• Infrastruktura krytyczna (np. energia elektryczna) • Materiały niebezpieczne • Produkty spożywcze
Przykłady branżowe	• Formowanie wtryskowe tworzyw sztucznych • Magazynowanie	• Motoryzacyjny przemysł metalowy • Celuloza i papier • Półprzewodniki	• Usługi komunalne • Przemysł petrochemiczny • Przemysł spożywczy • Przemysł farmaceutyczny
Kwestie bezpieczeństwa	• Ochrona przed drobnymi urazami • Zagwarantowanie czasu pracy	• Ochrona przed umiarkowanymi obrażeniami • Zagwarantowanie czasu pracy • Inwestycje kapitałowe	• Ochrona przed poważnymi obrażeniami/utratą życia • Zagwarantowanie czasu sprawności • Inwestycja kapitałowa • Tajemnice handlowe • Zapewnienie podstawowych usług społecznych • Przestrzeganie przepisów prawnych

6.1.2. Krok 2: Wybór zabezpieczeń

To działanie ramowe obejmuje wstępny wybór minimalnych zabezpieczeń planowanych lub stosowanych w celu ochrony systemu informacyjnego w oparciu o zestaw wymagań. Standard NSC 200 wer. 2[28] dokumentuje zestaw minimalnych

[28] NSC 200 wer. 2 odnosi się do publikacji NSC 800-53 wer. 2 oraz NSC 800-53B.

wymagań w zakresie bezpieczeństwa obejmujących 20 obszarów związanych z bezpieczeństwem[29], odnoszących się do zapewnienia poufności, integralności i dostępności systemów informacyjnych podmiotów publicznych oraz informacji przetwarzanych, przechowywanych i przekazywanych przez te systemy [16]. Dodatkowe informacje na temat każdej z 20 rodzin zabezpieczeń znajdują się w sekcji 6.2.

Zabezpieczenia bazowe stanowią punkt wyjścia dla procesu wyboru zabezpieczeń i są ustanawiane w oparciu o kategorię bezpieczeństwa i powiązany z nią poziom wpływu na systemy informacyjne określony w kroku 1.

W celu zaspokojenia potrzeby opracowania ogólnych i specjalistycznych zestawów zabezpieczeń dla systemów informacyjnych i organizacji, wprowadzono koncepcję ***nakładek. Nakładka*** jest w pełni określonym zestawem zabezpieczeń, zabezpieczeń rozszerzonych oraz powiązanych, powstałych w wyniku zastosowania wskazówek dostosowawczych do zabezpieczeń bazowych opisanych w publikacji NSC 800-53 oraz NSC 800-53B.

Ogólnie rzecz biorąc, nakładki mają na celu zmniejszenie potrzeby doraźnego dostosowywania zabezpieczeń bazowych przez organizacje i wybór zestawu zabezpieczeń i zabezpieczeń rozszerzonych, które bardziej odpowiadają danym okolicznościom, sytuacjom i/lub warunkom. Jednakże, wykorzystanie nakładek w żaden sposób nie zwalnia organizacji z dalszego dostosowywania zabezpieczeń (tj. nakładki mogą być również przedmiotem dostosowywania) w celu odzwierciedlenia specyficznych dla organizacji potrzeb, założeń lub ograniczeń. Więcej informacji na temat dostosowywania nakładek można znaleźć w publikacjach NSC 800-53, oraz NSC 800-53B.

Załącznik G- zawiera specyficzną dla ICS nakładkę obowiązujących zabezpieczeń NSC 800-53 oraz NSC 800-53B, które zapewniają dostosowanie zabezpieczeń bazowych do ICS o niskim, umiarkowanym i wysokim poziomie wpływu. Te dostosowane

[29] NSC 200 wer. 1 odnosi się do 18 kategorii bezpieczeństwa przedstawionych w publikacji NSC 800-53 wer. 1.

zabezpieczenia bazowe mogą być wykorzystane jako specyfikacje wyjściowe i zalecenia, które mogą być stosowane przez personel w konkretnych ICS. Jak omówiono we wcześniejszych sekcjach, użycie nakładki w żaden sposób nie zabrania organizacji możliwości przeprowadzania dalszego dostosowywania w celu dodania lub usunięcia zabezpieczeń i zabezpieczeń rozszerzonych (tj. nakładki mogą również podlegać dostosowywaniu), aby odzwierciedlić specyficzne dla organizacji potrzeby, założenia lub ograniczenia.

Dodatkowo, właściciele ICS mogą skorzystać z możliwości dostosowania wstępnych zabezpieczeń bazowych przedstawionych w Załączniku G - Nakładki ICS - gdy nie jest możliwe lub wykonalne wdrożenie określonych środków bezpieczeństwa zawartych w zabezpieczeniach bazowych. Jednakże wszystkie działania dostosowawcze powinny, jako swój główny cel, koncentrować na spełnieniu intencji zabezpieczeń pierwotnych, gdy tylko jest to możliwe lub wykonalne. Na przykład w sytuacjach, w których ICS nie może obsługiwać lub organizacja stwierdza, że nie jest wskazane wdrożenie określonych zabezpieczeń lub ich rozszerzeń w ICS (np. niekorzystny wpływ na wydajność, bezpieczeństwo lub niezawodność), organizacja przedstawia pełne i przekonujące uzasadnienie tego, w jaki sposób wybrane zabezpieczenia kompensacyjne zapewniają równoważną zdolność bezpieczeństwa lub poziom ochrony ICS oraz dlaczego nie można było zastosować odpowiednich zabezpieczeń bazowych. Jeżeli ICS nie może wspierać użycia mechanizmów automatycznych, organizacja stosuje niezautomatyzowane mechanizmy lub procedury jako zabezpieczenia kompensacyjne zgodnie z ogólnymi wskazówkami dotyczącymi dostosowania zawartymi w NSC 800-53 oraz NSC 800-53B. Zabezpieczenia kompensacyjne nie są wyjątkami, ani odstępstwami od zabezpieczeń bazowych; są to alternatywne zabezpieczenia i środki zaradcze stosowane w ICS, które realizują intencje pierwotnych środków bezpieczeństwa, które nie mogły być skutecznie zastosowane. Decyzje organizacyjne dotyczące stosowania zabezpieczeń kompensacyjnych są udokumentowane w planie bezpieczeństwa ICS.

6.1.3. Krok 3: Implementacja zabezpieczeń

Działanie to obejmuje wdrażanie zabezpieczeń w nowych lub starszych systemach informacyjnych. Proces wyboru środków bezpieczeństwa opisany w tej sekcji może być stosowany do ICS z dwóch różnych perspektyw: (I) nowych instalacji; oraz (II) dziedziczonych istniejących rozwiązań.

W przypadku nowych systemów proces wyboru zabezpieczeń jest stosowany z perspektywy definicji wymagań, ponieważ systemy te jeszcze nie istnieją, a organizacje przeprowadzają wstępną kategoryzację zabezpieczeń. Zabezpieczenia zawarte w planach bezpieczeństwa systemów informacyjnych służą jako specyfikacja bezpieczeństwa i oczekuje się, że zostaną włączone do systemów podczas faz rozwoju i wdrażania życia systemu.

Z kolei, w przypadku starszych systemów informacyjnych proces wyboru zabezpieczeń jest stosowany z perspektywy analizy podatności, gdy organizacje przewidują znaczące zmiany w systemach (np. podczas dużych uaktualnień, modyfikacji lub outsourcingu). Ponieważ systemy informacyjne już istnieją, organizacje najprawdopodobniej zakończyły procesy kategoryzacji bezpieczeństwa i wyboru zabezpieczeń, co skutkuje ustanowieniem wcześniej uzgodnionych zabezpieczeń w odpowiednich planach ochrony oraz wdrożeniem tych zabezpieczeń w systemach informacyjnych.

6.1.4. Krok 4: Ocenianie zabezpieczeń

Czynność ta określa, w jakim stopniu zabezpieczenia w systemie informacyjnym są skuteczne w swoim zastosowaniu. NSC 800-53A zawiera wytyczne dotyczące oceniania zabezpieczeń wstępnie wybranych z NSC 800-53 oraz NSC 800-53B w celu zapewnienia, że są one prawidłowo wdrożone, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty w odniesieniu do spełnienia wymagań bezpieczeństwa systemu. Aby to osiągnąć, NSC 800-53A zawiera założenia oparte na wymaganiach bezpieczeństwa zdefiniowanych w NSC 800-53 i NSC 800-53B w celu scharakteryzowania oczekiwań związanych z oceną bezpieczeństwa według poziomu wpływu przedstawionego w NSC 199.

6.1.5. Krok 5: Autoryzacja systemu informacyjnego

Działanie to skutkuje podjęciem przez kierownictwo decyzji i zezwoleniu na eksploatację systemu informacyjnego i wyraźnym zaakceptowaniu ryzyka dla działań organizacji, jej majątku lub osób fizycznych w oparciu o wdrożenie uzgodnionego zestawu zabezpieczeń.

6.1.6. Krok 6: Monitorowanie zabezpieczeń

Czynność ta polega na ciągłym śledzeniu zmian w systemie informacyjnym, które mogą mieć wpływ na zabezpieczenia, oraz na ocenie ich skuteczności. Publikacja specjalna NIST SP 800-137 zawiera wytyczne dotyczące ciągłości monitorowania bezpieczeństwa informacji [21].

6.2. Wytyczne dotyczące stosowania zabezpieczeń w systemach ICS

Ponieważ dzisiejsze ICS są często połączeniem starszych systemów, często o planowanym okresie eksploatacji wynoszącym od dwudziestu do trzydziestu lat, lub hybrydą starszych systemów uzupełnionych nowszym sprzętem i oprogramowaniem, które są połączone z innymi systemami, stosowanie niektórych zabezpieczeń zawartych w NSC 800-53 i NSC 800-53B jest często trudne lub niewykonalne. Chociaż wiele zabezpieczeń zawartych NSC 800-53 i NSC 800-53B ma zastosowanie do ICS w wersji takiej, jak zostały opisane, niektóre zabezpieczenia wymagają specyficznej dla ICS interpretacji i/lub uzupełnienia. W publikacji NSC 800-53B zawarty jest przykładowy opis szablonu nakładki oraz dodatkowe informacje na temat każdej sekcji nakładki.

Zabezpieczenia zawarte w NSC 800-53 wer. 2 są podzielone na 20 kategorii. Każda kategoria zawiera zabezpieczenia związane z ogólnym tematem bezpieczeństwa dla danego obszaru. Zabezpieczenia mogą dotyczyć aspektów polityki, nadzoru (w tym nadzoru nad procesami manualnymi), działań podejmowanych przez poszczególne osoby lub zautomatyzowanych mechanizmów wdrażanych w systemach/urządzeniach informacyjnych.

Kategorie związane z bezpieczeństwem, omówione w poniższych sekcjach, to:

- **Kontrola dostępu** (*ang. Access Control - AC*): proces przyznawania lub odrzucania określonych wniosków i uzyskanie i wykorzystanie informacji oraz związanych z nimi usług przetwarzania informacji w celu uzyskania fizycznego dostępu do obszarów w środowisku systemu informacyjnego.
- **Uświadamianie i szkolenia** (*ang. Awareness and Training - AT*): polityki i procedury zapewniające wszystkim użytkownikom systemu informacyjnego odpowiednie przeszkolenie w zakresie bezpieczeństwa, związane z korzystaniem z systemu oraz prowadzenie szczegółowej dokumentacji szkoleniowej.
- **Audyt i rozliczalność** (*ang. Audit and Accountability - AU*): niezależny przegląd i badanie zapisów i działań w celu oceny adekwatności zabezpieczeń systemu, zapewnienia zgodności z ustalonymi politykami i procedurami operacyjnymi oraz zalecenia niezbędnych zmian w zabezpieczeniach, politykach lub procedurach.
- **Ocena, autoryzacja i monitorowanie** (*ang. Certification, Accreditation, and Security Assessments – CA*): zapewnienie, że określone zabezpieczenia zostały wdrożone prawidłowo, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty.
- **Zarządzanie konfiguracją** (*ang. Configuration Management - CM*): zasady i procedury kontroli modyfikacji sprzętu, oprogramowania, firmware'u i dokumentacji, w celu zapewnienia ochrony systemu informacyjnego przed niewłaściwymi modyfikacjami przed, w trakcie i po wdrożeniu systemu do eksploatacji.
- **Planowanie awaryjne / ciągłość działania** (*ang. Contingency Planning - CP*): zasady i procedury mające na celu utrzymanie lub przywrócenie operacji biznesowych, w tym operacji w systemach informacyjnych, w miarę możliwości w alternatywnej lokalizacji, w przypadku sytuacji awaryjnych, awarii systemu lub katastrofy.
- **Identyfikacja i uwierzytelnianie** (*ang. Identification and Authentication - IA*): proces weryfikacji tożsamości użytkownika, procesu lub urządzenia poprzez wykorzystanie określonych danych uwierzytelniających (np. haseł, tokenów, danych biometrycznych), jako warunek wstępny przyznania dostępu do zasobów w systemie informacyjnym.

- **Reagowanie na incydenty** (*ang. Incident Response - IR*): polityki i procedury dotyczące szkoleń, testowania, obsługi, monitorowania, raportowania i usług pomocniczych w zakresie reagowania na incydenty.
- **Utrzymanie i wsparcie** (*ang. Maintenance - MA*): polityki i procedury zarządzania wszystkimi aspektami utrzymania i wsparcia systemu informacyjnego.
- **Ochrona nośników danych** (*ang. Media Protection - MP*): polityki i procedury zapewniające bezpieczną obsługę nośników danych. Zabezpieczenia obejmują dostęp, etykietowanie, przechowywanie, transport, sanityzację, niszczenie i utylizację.
- **Ochrona fizyczna i środowiskowa** (*ang. Physical and Environmental Protection* - PE): zasady i procedury dotyczące kontroli dostępu do danych fizycznych, transmisji i wyświetlaczy, jak również kontroli środowiska w zakresie utrzymania stosownych parametrów (np. temperatury, wilgotności) oraz przepisów dotyczących sytuacji awaryjnych (np. wyłączanie, zasilanie, oświetlenie, ochrona przeciwpożarowa).
- **Planowanie** (*ang. Planning - PL*): opracowywanie i utrzymywanie planu ochrony systemu informacyjnego poprzez przeprowadzanie ocen, określanie i wdrażanie zabezpieczeń, przypisywanie poziomów ochrony oraz reagowanie na incydenty.
- **Programy zarządzania** (*ang. Program Management – PM*): zapewnianie zabezpieczeń na poziomie organizacyjnym a nie na poziomie systemu informacyjnego.
- **Bezpieczeństwo osobowe** (*ang. Personnel Security - PS*): polityki i procedury dotyczące kategoryzacji stanowisk pracy, sprawdzania, przenoszenia, karania i rozwiązywania umów; dotyczy również bezpieczeństwa osobowego personelu stron trzecich.
- **Przejrzystość przetwarzanie danych osobowych** *(ang. Personally Identifiable Information Processing and Transparency - PT*): operacja lub zestaw operacji przeprowadzanych na informacjach umożliwiających identyfikację osób, które obejmują między innymi gromadzenie, przechowywanie, rejestrowanie, generowanie, przekształcanie, wykorzystywanie, upublicznianie, przekazywanie i usuwanie informacji umożliwiających identyfikację osób.

- **Szacowanie ryzyka** (*ang. Risk Assessment - RA*): proces identyfikacji ryzyka dla operacji, aktywów lub osób poprzez określenie prawdopodobieństwa jego wystąpienia, wynikającego z niego wpływu oraz dodatkowych zabezpieczeń, które mogłyby złagodzić ten wpływ.
- **Nabywanie systemu i usług** (*ang. System and Services Acquisition - SA*): alokacja zasobów na rzecz bezpieczeństwa systemów informacyjnych, które mają być utrzymywane przez cały cykl życia systemów oraz opracowanie polityki nabywania w oparciu o wyniki szacowania ryzyka, w tym wymagania, kryteria projektowe, procedury testowe i związaną z nimi dokumentację.
- **Ochrona systemów i sieci telekomunikacyjnych** (*ang. System and Communications Protection - SC*): mechanizmy ochrony zarówno systemu, jak i elementów służących do transmisji danych.
- **Integralność systemu i informacji** (*ang. System and Information Integrity - SI*): polityki i procedury mające na celu ochronę systemów informacyjnych i ich danych przed wadami projektowymi i modyfikacją danych za pomocą weryfikacji funkcjonalności, sprawdzania integralności danych, wykrywania włamań, wykrywania złośliwego kodu oraz kontroli alarmów i udzielania porad w zakresie bezpieczeństwa.
- **Zarządzanie ryzykiem w łańcuchu dostaw** (*ang. Supply Chain Risk Management - SR*): proces identyfikacji, oceny i ograniczania ryzyka związanego z globalnym i rozproszonym charakterem łańcuchów dostaw produktów i usług z dziedziny technologii informacyjnych i telekomunikacyjnych.

6.2.1. Kontrola dostępu - AC

Zabezpieczenia należące do kategorii Kontrola dostępu – AC, zapewniają polityki i procedury określające korzystanie z zasobów systemu jedynie przez uprawnionych użytkowników, programy, procesy lub inne systemy. Ta grupa określa zabezpieczenia w zakresie zarządzania kontami w systemie informacyjnym, w tym zakładanie, aktywowanie, modyfikowanie, przeglądanie, wyłączanie i usuwanie kont. Obejmuje kwestie egzekwowania dostępu i przepływu, takie jak rozdzielenie obowiązków, zasady minimalnych uprawnień, nieudane próby logowania, powiadamianie o użyciu systemu,

powiadamianie o poprzednim logowaniu, kontrola sesji współbieżnych, blokowanie sesji i kończenie sesji. Istnieją również zabezpieczenia dotyczące korzystania z urządzeń przenośnych i zdalnych oraz systemów informacyjnych będących własnością osobistą używanych w celu uzyskania dostępu do systemu informacyjnego, jak również korzystania z możliwości zdalnego dostępu i wdrażania technologii bezprzewodowych. Dostęp może przybierać różne formy, w tym przeglądania, wykorzystywania i zmieniania określonych danych lub funkcji urządzenia.

Uzupełniające rekomendacje dotyczące zabezpieczeń z kategorii AC można znaleźć w następujących publikacjach:

- NIST SP 800-63, zawierającej wytyczne dotyczące zdalnego uwierzytelniania elektronicznego [53].
- NIST SP 800-48, zawierającej wytyczne dotyczące bezpieczeństwa sieci bezprzewodowych ze szczególnym uwzględnieniem standardów IEEE 802.11b i Bluetooth 0.
- NIST SP 800-97, zawierającej wytyczne dotyczące bezpieczeństwa sieci bezprzewodowych IEEE 802.11i [64].
- Standard FIPS 201, określającej wymagania dotyczące weryfikacji tożsamości personelu organizacji publicznych i kontrahentów [65].
- NIST SP 800-96, zawierającej wytyczne dotyczące interoperacyjności karty PIV z czytnikiem [66].
- NIST SP 800-73, zawierającej wytyczne dotyczące interfejsów wykorzystywanych do weryfikacji tożsamości osobistej [49].
- NIST SP 800-76, zawierającej wytyczne dotyczące biometrii do weryfikacji tożsamości osób [50].
- NIST SP 800-78, zawierającej wytyczne dotyczące algorytmów kryptograficznych i długości kluczy do weryfikacji tożsamości osób [67].

Jeżeli jako token identyfikacyjny wykorzystywany jest nowy system weryfikacji tożsamości osobistej ang. (*Personal Identity Verification - PIV*), system kontroli dostępu

powinien spełniać wymagania norm FIPS 201 i NIST SP 800-73 oraz wykorzystywać weryfikację kryptograficzną lub biometryczną. Jeżeli w ramach kontroli dostępu opartej na tokenach stosowana jest weryfikacja kryptograficzna, system kontroli dostępu powinien być zgodny z wymaganiami określonymi w normie NIST SP 800-78. Jeżeli w ramach kontroli dostępu opartej na tokenach stosowana jest weryfikacja biometryczna, system kontroli dostępu powinien być zgodny z wymaganiami NIST SP 800-76.

Technologie kontroli dostępu to technologie filtrujące i blokujące, których zadaniem jest kierowanie i regulowanie przepływu informacji między urządzeniami lub systemami, po uprzednim określeniu uprawnień. W kolejnych rozdziałach przedstawiono kilka technologii kontroli dostępu i ich zastosowanie w ICS.

6.2.1.1. Kontrola dostępu oparta na rolach (RBAC)

RBAC jest technologią, która ma potencjał do zmniejszenia złożoności i kosztów administrowania bezpieczeństwem w sieciach z dużą liczbą inteligentnych urządzeń. W ramach RBAC, administracja bezpieczeństwem jest uproszczona poprzez wykorzystanie ról, hierarchii i ograniczeń umożliwiających organizację poziomów dostępu użytkowników.. RBAC redukuje koszty w organizacji, ponieważ akceptuje fakt, że pracownicy zmieniają role częściej niż obowiązki w ramach ról.

Zalecenia i wytyczne dotyczące ICS

RBAC może być stosowany do zapewnienia jednolitego sposobu zarządzania dostępem do urządzeń ICS przy jednoczesnym obniżeniu kosztów utrzymywania indywidualnych poziomów dostępu do urządzeń i minimalizacji błędów. RBAC powinien być stosowany do ograniczania uprawnień użytkowników ICS tylko do tych, które są wymagane do wykonywania pracy każdej osoby (tj. konfigurowanie każdej roli w oparciu o zasadę minimalnych uprawnień). Poziom dostępu może przybierać różne formy, w tym przeglądania, używania i zmieniania określonych danych ICS lub funkcji urządzeń.

Narzędzia RBAC mogą ustanawiać, modyfikować lub usuwać uprawnienia w aplikacjach, ale nie zastępują mechanizmu autoryzacji; nie sprawdzają i nie uwierzytelniają użytkowników za każdym razem, gdy użytkownik chce uzyskać dostęp

do aplikacji. Narzędzia RBAC oferują interfejsy do mechanizmów autoryzacji dla większości aktualnych platform w branży IT. Jednak starsze systemy ICS lub specjalistyczny sprzęt ICS mogą wymagać opracowania dedykowanego oprogramowania interfejsowego. Kwestia ta stanowi poważny problem w przypadku systemów ICS, które korzystają z wielu zastrzeżonych systemów operacyjnych lub niestandardowych implementacji systemów operacyjnych i interfejsów.

6.2.1.2. Serwery internetowe

Technologie oparte na sieciach Web i Internecie są dodawane do wielu różnych systemów ICS, ponieważ ułatwiają one dostęp do informacji, a produkty są bardziej przyjazne dla użytkownika i łatwiejsze do zdalnego konfigurowania. Mogą one jednak również zwiększać cyberzagrożenia i tworzyć nowe podatności, które wymagają wyeliminowania.

Zalecenia i wytyczne dotyczące ICS

Producenci oprogramowania SCADA i bazodanowych repozytorium danych historycznych (historianów) zazwyczaj oferują serwery WWW jako opcję produktu, dzięki czemu użytkownicy znajdujący się poza sterownią mogą uzyskać dostęp do informacji o ICS. W wielu przypadkach komponenty oprogramowania, takie jak zabezpieczenia ActiveX lub aplety Java, muszą być zainstalowane lub załadowane na każdy komputer kliencki uzyskujący dostęp do serwera WWW. Niektóre produkty, takie jak sterowniki PLC i inne urządzenia sterujące, są dostępne z wbudowanymi serwerami WWW, FTP i poczty elektronicznej, co ułatwia ich zdalną konfigurację i pozwala na generowanie powiadomień i raportów pocztą elektroniczną w przypadku wystąpienia określonych warunków. Jeśli to możliwe, należy używać protokołu HTTPS zamiast HTTP, SFTP lub SCP zamiast FTP, blokować przychodzący ruch FTP oraz poczty elektronicznej itp. Na rynku pojawiają się urządzenia zabezpieczające (lub bramy) wyposażone w aplikacje proxy, które są w stanie badać ruch internetowy, FTP i poczty elektronicznej w celu blokowania ataków i zapobiegania pobieraniu zabezpieczeń ActiveX® lub apletów Java®.

Jeżeli podłączenie systemów ICS do Internetu nie przyniesie istotnych korzyści, najlepiej nie podłączać ich do tego rodzaju sieci.

6.2.1.3. Wirtualna sieć lokalna (VLAN)

VLAN-y dzielą sieci fizyczne na mniejsze sieci logiczne w celu zwiększenia wydajności, poprawy zarządzania i uproszczenia projektowania sieci. VLAN-y są osiągane poprzez stosowną konfigurację przełączników ethernetowych. Każda sieć VLAN składa się z pojedynczej domeny rozgłoszeniowej, która izoluje ruch od innych sieci VLAN. Podobnie jak zastąpienie koncentratorów przełącznikami redukuje kolizje, użycie sieci VLAN ogranicza ruch rozgłoszeniowy, a także pozwala logicznym podsieciom obejmować wiele fizycznych lokalizacji. Istnieją dwie kategorie sieci VLAN:

- Statyczne, często określane jako port-based, gdzie porty przełącznika są przypisane do sieci VLAN tak, że jest to przezroczyste dla użytkownika końcowego.
- Dynamiczne, gdzie urządzenie końcowe negocjuje charakterystykę VLAN z przełącznikiem lub określa VLAN na podstawie adresów IP lub sprzętowych.

Chociaż w tej samej sieci VLAN może współistnieć więcej niż jedna podsieć IP, ogólnym zaleceniem jest stosowanie relacji jeden do jednego między podsieciami a sieciami VLAN. Praktyka ta wymaga użycia routera lub przełącznika wielowarstwowego w celu połączenia wielu sieci VLAN. Wiele routerów i zapór sieciowych obsługuje ramki oznaczone (tagowane), dzięki czemu pojedynczy interfejs fizyczny może być wykorzystywany do trasowania między wieloma sieciami logicznymi.

Sieci VLAN nie są zazwyczaj wdrażane w celu wyeliminowania podatności w zabezpieczeniach hostów lub sieci w sposób, w jaki wdrażane są zapory sieciowe lub systemy IDS (*ang. Intrusion detection system*). Jednak prawidłowo skonfigurowane sieci VLAN pozwalają przełącznikom na egzekwowanie zasad bezpieczeństwa i segregację ruchu w warstwie Ethernet. Prawidłowo posegmentowane sieci mogą również ograniczyć ryzyko „szumu rozgłoszeniowego, który może wynikać ze skanowania portów lub aktywności robaków.

Przełączniki są podatne na ataki takie jak spoofing MAC, przepełnienie tablicy oraz ataki na protokoły drzewa rozpinającego (*ang. spanning tree protocol*), w zależności od urządzenia i jego konfiguracji. Skokowe przełączanie VLAN (*ang. VLAN hopping*), czyli możliwość wstrzykiwania ramek do nieautoryzowanych portów, została zademonstrowana przy użyciu spoofingu przełącznika lub podwójnie enkapsulowanych ramek. Ataki te nie mogą być przeprowadzane zdalnie i wymagają lokalnego, fizycznego dostępu do przełącznika. W zależności od urządzenia i sposobu wdrożenia można zastosować różne funkcje, takie jak filtrowanie adresów MAC, uwierzytelnianie oparte na portach przy użyciu standardu IEEE 802.1x oraz specjalne praktyki rekomendowane przez producenta mające na celu złagodzenie tych ataków.

Zalecenia i wytyczne dotyczące ICS

Sieci VLAN zostały skutecznie wdrożone w sieciach ICS, gdzie każda komórka automatyki jest przypisana do pojedynczej sieci VLAN w celu ograniczenia zbędnego ruchu w sieci i umożliwienia urządzeniom sieciowym korzystania z tej samej sieci VLAN przez wiele przełączników. [34

6.2.1.4. Modemy Dial-up

Systemy ICS podlegają rygorystycznym wymogom dotyczącym niezawodności i dostępności. Zasoby techniczne mogą nie znajdować się fizycznie w pomieszczeniach lub obiektach dyspozytorni, gdy zaistnieje potrzeba rozwiązania problemów i dokonania napraw. Dlatego w systemach ICS często stosuje się modemy, które umożliwiają sprzedawcom, integratorom systemów lub inżynierom zajmującym się kontrolą systemu nawiązanie połączenia sieciowego w celu zdiagnozowania, naprawy, skonfigurowania i przeprowadzenia konserwacji sieci lub komponentu. Pozwala to na łatwy dostęp upoważnionemu personelowi, ale jeśli modemy dial-up nie są odpowiednio zabezpieczone, mogą również stanowić "tylne wejścia" dla osób nieupoważnionych.

Modemy dial-up często wykorzystują oprogramowanie do zdalnego sterowania, które daje użytkownikowi zdalnemu zaawansowany dostęp (administracyjny lub jako root)

do systemu docelowego. Takie oprogramowanie zazwyczaj posiada opcje bezpieczeństwa, które należy dokładnie sprawdzić i skonfigurować.

Zalecenia i wskazówki dotyczące ICS

- Po zainstalowaniu w ICS modemów dial-up należy rozważyć zastosowanie systemów oddzwaniania (ang. callback). Gwarantuje to, że osoba dzwoniąca jest autoryzowanym użytkownikiem, ponieważ modem nawiązuje połączenie robocze na podstawie danych osoby dzwoniącej i numeru zwrotnego zapisanego na liście autoryzowanych użytkowników zatwierdzonych przez system ICS.
- Należy upewnić się, że domyślne hasła są zmieniane i każdemu modemowi przydzielane są silne hasła.
- Należy fizycznie zidentyfikować modemy używane przez operatorów centrum sterowania.
- Należy skonfigurować oprogramowanie do zdalnego sterowania tak, aby używało unikalnych nazw użytkowników i bezpiecznych haseł, silnego uwierzytelniania, szyfrowania, jeśli uznano to za stosowne, oraz rejestrów zdarzeń (logów). Korzystanie z tego oprogramowania przez użytkowników zdalnych powinno być monitorowane w czasie zbliżonym do rzeczywistego.
- Jeśli to możliwe, należy odłączać nieużywane modemy lub rozważyć zautomatyzowanie procesu ich odłączania, tak, aby modemy były odłączane po upływie określonego czasu. Należy zauważyć, że czasami podłączenie modemu jest częścią umowy z dostawcą usług wsparcia (np. wsparcie 24x7 z 15-minutowym czasem reakcji). Personel powinien być świadomy, że odłączenie/usunięcie modemów może wymagać renegocjacji umów.

6.2.1.5. Sieci bezprzewodowe

Wykorzystanie sieci bezprzewodowej w systemie ICS jest decyzją opartą na ryzyku, która musi być podjęta przez organizację. Ogólnie rzecz biorąc, bezprzewodowe sieci LAN powinny być wdrażane tylko tam, gdzie implikacje zdrowotne, bezpieczeństwa,

środowiskowe i finansowe są niewielkie. Publikacje specjalne NIST SP 800-48 i NIST SP 800-97 zawierają wskazówki dotyczące bezpieczeństwa sieci bezprzewodowych.

Zalecenia i wytyczne dotyczące ICS

Bezprzewodowe sieci LAN

- Przed instalacją należy przeprowadzić inspekcję sieci bezprzewodowej w celu określenia lokalizacji i mocy anteny, która pozwoli zminimalizować narażenie sieci bezprzewodowej. Badanie powinno uwzględniać fakt, że napastnicy mogą używać czułych anten kierunkowych, które zwiększają efektywny zasięg bezprzewodowej sieci LAN poza oczekiwany zasięg standardowy. Dostępne są obudowy Faradaya i inne metody minimalizujące narażenie sieci bezprzewodowej poza wyznaczonymi obszarami.
- Dostęp użytkowników bezprzewodowych powinien opierać się na uwierzytelnianiu IEEE 802.1x z wykorzystaniem bezpiecznego protokołu uwierzytelniania (np. Extensible Authentication Protocol [EAP] with TLS [EAP-TLS]), który uwierzytelnia użytkowników za pomocą certyfikatów użytkownika lub serwera RADIUS (Remote Authentication Dial In User Service).
- Punkty dostępu bezprzewodowego i serwery danych obsługujące bezprzewodowe urządzenia robocze powinny znajdować się w odizolowanej sieci z udokumentowanymi i minimalnymi (pojedynczymi, jeśli to możliwe) połączeniami z siecią ICS.
- Punkty dostępu bezprzewodowego powinny być skonfigurowane tak, aby miały unikalny identyfikator zestawu usług (SSID), wyłączone rozgłaszanie SSID i włączone filtrowanie MAC, jako minimum.
- Urządzenia bezprzewodowe, jeśli są używane w sieci ICS z systemem Microsoft Windows, powinny być skonfigurowane jako osobna jednostka organizacyjna w domenie Windows.
- Komunikacja za pomocą urządzeń bezprzewodowych powinna być szyfrowana i zabezpieczona przed utratą integralności. Szyfrowanie nie może pogarszać wydajności operacyjnej urządzenia końcowego. Należy rozważyć szyfrowanie

w warstwie 2 OSI a nie w warstwie 3, aby zmniejszyć opóźnienia w szyfrowaniu. Należy również rozważyć wykorzystanie akceleratorów sprzętowych do wykonywania funkcji kryptograficznych.

W przypadku sieci kratowych należy rozważyć zastosowanie zarządzania kluczem rozgłoszeniowym zamiast zarządzania kluczem publicznym w warstwie 2 OSI, co pozwoli zmaksymalizować wydajność. Do wykonywania funkcji administracyjnych należy stosować kryptografię asymetryczną, a do zabezpieczania każdego strumienia danych oraz ruchu sterującego siecią należy stosować szyfrowanie symetryczne. Jeśli urządzenia mają być wykorzystywane do komunikacji bezprzewodowej, należy rozważyć zastosowanie adaptacyjnego protokołu routingu. Czas konwergencji sieci powinien być jak najkrótszy, aby umożliwić szybkie odtworzenie sieci w przypadku awarii lub zaniku zasilania. Wykorzystanie sieci kratowej może zapewnić odporność na awarie poprzez wybór alternatywnej trasy i wyprzedzające przełączanie sieci w przypadku awarii.

Bezprzewodowe sieci obiektowe

Komitet ISA100[30] pracuje nad wprowadzeniem standardów, zalecanych praktyk, raportów technicznych i powiązanych informacji, które określą procedury wdrażania systemów bezprzewodowych w środowisku automatyki i sterowania, ze szczególnym uwzględnieniem ich zastosowania w terenie (np. IEEE 802.15.4). Wytyczne są skierowane do osób odpowiedzialnych za cały cykl życia, w tym za projektowanie, wdrażanie, bieżące utrzymanie, skalowalność lub zarządzanie systemami automatyki przemysłowej i sterowania, i dotyczą użytkowników, integratorów systemów, specjalistów oraz producentów i sprzedawców systemów sterowania.

6.2.2. Uświadamianie i szkolenia

Zabezpieczenia, które należą do kategorii Uświadamianie i szkolenia – AT, określają polityki i procedury zapewniające wszystkim użytkownikom systemu informacyjnego

[30] Dodatkowe informacje o ISA100 można znaleźć na stronie: http://www.isa.org/isa100

odpowiednie przeszkolenie w zakresie bezpieczeństwa, związane z korzystaniem z systemu oraz prowadzenie szczegółowej dokumentacji szkoleniowej.

Uzupełniające rekomendacje dotyczące kategorii AT można znaleźć w następujących publikacjach:

- NIST SP 800-50, zawierającej wytyczne dotyczące szkolenia w zakresie świadomości bezpieczeństwa [61].
- NIST SP 800-100, zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].

Zalecenia i wytyczne dotyczące ICS

W przypadku środowiska ICS, należy uwzględnić świadomość bezpieczeństwa informacji specyficzną dla danego systemu sterowania oraz szkolenie w zakresie konkretnych aplikacji ICS. Ponadto, organizacja powinna zidentyfikować, udokumentować i przeszkolić cały personel pełniący kluczowe role i obowiązki w zakresie ICS. Świadomość i szkolenie muszą obejmować zarówno zabezpieczany proces fizyczny, jak i dany system ICS.

Świadomość bezpieczeństwa jest krytycznym elementem zapobiegania incydentom związanym z ICS, szczególnie jeśli chodzi o zagrożenia socjotechniczne. Inżynieria socjalna to technika stosowana w celu zmanipulowania osób, tak, aby podały prywatne informacje, takie jak hasła. Informacje te mogą być następnie wykorzystane do złamania zabezpieczeń systemów.

Wdrożenie programu bezpieczeństwa ICS może spowodować zmiany w sposobie dostępu personelu do programów komputerowych, aplikacji i samego pulpitu komputerowego. Organizacje powinny opracować skuteczne programy szkoleniowe i środki komunikacji, aby pomóc pracownikom zrozumieć, dlaczego wymagane są nowe metody dostępu i kontroli, jakie pomysły mogą wykorzystać do zmniejszenia ryzyka oraz jaki wpływ na organizację będzie miało niewdrożenie odpowiednich metod zabezpieczeń. Programy szkoleniowe pokazują również zaangażowanie kierownictwa w program cyberbezpieczeństwa oraz jego wartość. Informacje zwrotne od personelu,

który uczestniczył w tego typu szkoleniach, mogą być cennym źródłem informacji do udoskonalania założeń i zakresu programu bezpieczeństwa.

6.2.3. Audyt i rozliczalność

Audyt jest niezależnym przeglądem i badaniem zapisów i działań mającym na celu ocenę adekwatności zabezpieczenia systemu, zapewnienia zgodności z ustalonymi politykami i procedurami operacyjnymi oraz zalecenia niezbędnych zmian w zabezpieczeniach, politykach lub procedurach. Środki bezpieczeństwa, które należą do kategorii Audyt i rozliczalność - AU, określają zasady i procedury generowania zapisów audytowych, ich zawartość, pojemność i wymagania dotyczące przechowywania. Zabezpieczenia te zapewniają również środki bezpieczeństwa umożliwiające reagowanie na problemy, takie jak usterki procesów audytu lub wyczerpanie pojemności dziennika audytu. Dane audytowe powinny być chronione przed modyfikacją i być zaprojektowane w sposób zapewniający ich niezaprzeczalność.

Dodatkowe wytyczne dotyczące zabezpieczeń kategorii AU można znaleźć w następujących publikacjach:

- NSC 800-61, zawierający rekomendacje dotyczące obsługi incydentów bezpieczeństwa komputerowego i retencji dzienników audytowych.
- NIST SP 800-92, zawierającej wytyczne dotyczące zarządzania logami (w tym logami audytowymi) [68].
- NIST SP 800-100, zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].

Zalecenia i wytyczne dotyczące ICS

Niezbędne jest ustalenie, czy system działa zgodnie z założeniami. Należy przeprowadzać okresowe audyty ICS w celu potwierdzenia następujących elementów:

- Sprawdzenia czy zabezpieczenia zastosowane podczas testów walidacji systemu (np. fabryczne testy akceptacyjne i testy akceptacyjne w miejscu instalacji) są nadal zainstalowane i działają poprawnie w systemie produkcyjnym.

- Sprawdzenia czy system produkcyjny nie został skompromitowany pod względem bezpieczeństwa i w miarę możliwości dostarcza informacji o naturze i zakresie naruszeń zasad ochrony, w przypadku ich wystąpienia.
- Sprawdzenia czy program zarządzania zmianami jest rygorystycznie przestrzegany a wszystkie zmiany są weryfikowane i zatwierdzane w drodze audytu.

Wyniki każdego okresowego audytu powinny być przedstawiane w formie wyników uzyskanych z uwzględnieniem zestawu uprzednio zdefiniowanych i odpowiednich metryk obrazujących działanie systemu bezpieczeństwa i tendencje w tym zakresie. Metryki wyników w zakresie bezpieczeństwa powinny być przesyłane do odpowiednich interesariuszy wraz z przeglądem trendów w zakresie bezpieczeństwa.

Tradycyjnie, podstawowym elementem audytu systemów informacyjnych jest prowadzenie dokumentacji. Użycie odpowiednich narzędzi w środowisku ICS wymaga od specjalisty IT obszernej wiedzy na temat ICS, krytycznych parametrów produkcji i implikacji dla bezpieczeństwa danego obiektu. Wiele z urządzeń sterujących procesem technologicznym, które są zintegrowane z ICS, jest zainstalowanych od wielu lat i nie ma możliwości dostarczania zapisów audytowych opisanych w tym rozdziale. Dlatego możliwość zastosowania tych nowocześniejszych narzędzi do audytu aktywności systemu i sieci zależy od możliwości komponentów w systemie ICS.

Kluczowe zadania w zarządzaniu siecią w środowisku ICS to zapewnienie niezawodności i dostępności w celu wspierania bezpiecznej i wydajnej pracy. W branżach podlegających regulacjom prawnym zachowanie zgodności z przepisami może dodatkowo komplikować zarządzanie bezpieczeństwem i uwierzytelnianiem, zarządzanie integralnością rejestru i instalacji oraz wszystkie funkcje, które mogą wspomagać proces kwalifikacji instalacyjnej i operacyjnej. Rzetelne korzystanie z narzędzi do audytu i zarządzania dziennikami może stanowić cenną pomoc w utrzymaniu i udowodnieniu integralności ICS od momentu instalacji przez cały cykl życia systemu. Wartość tych narzędzi w tym środowisku można obliczyć na podstawie nakładu pracy potrzebnego do ponownej kwalifikacji lub innych ponownych badań ICS, w przypadku, gdy integralność spowodowana atakiem, wypadkiem lub błędem jest

kwestionowana. System powinien zapewniać niezawodne, zsynchronizowane znaczniki czasu na potrzeby narzędzi audytu.

Monitorowanie czujników, rejestrów, systemów wykrywania włamań (*ang. Intrusion Detection Systems - IDS*), oprogramowania antywirusowego, zarządzania poprawkami, zarządzania politykami i innych mechanizmów bezpieczeństwa powinno odbywać się w czasie rzeczywistym, jeśli jest to możliwe. Usługa monitorowania wstępnego powinna rejestrować alarmy, szybko określać problem i podejmować odpowiednie działania, aby powiadomić personel obiektu o konieczności interwencji.

Do nowych i istniejących projektów ICS należy włączyć narzędzia do audytu systemu. Przed wdrożeniem w operacyjnym systemie ICS, narzędzia te powinny zostać przetestowane (np. W trybie off-line na porównywalnym systemie ICS). Narzędzia te mogą zapewnić namacalne zapisy dowodów i integralności systemu. Ponadto narzędzia do aktywnego zarządzania dziennikami mogą faktycznie sygnalizować trwający atak lub zdarzenie oraz zapewniać informacje o lokalizacji i pochodzeniu w celu ułatwienia reakcji na incydent [34].

Powinna istnieć metoda śledzenia wszystkich działań wykonywanych na konsoli przez użytkownika, zarówno wykonywanych ręcznie (np. logowanie w dyspozytorni), jak i automatycznie (np. logowanie w warstwie aplikacji i/lub systemu operacyjnego). Należy opracować zasady i procedury dotyczące tego, co jest rejestrowane, w jaki sposób dzienniki są przechowywane (lub drukowane), jak są chronione, kto ma dostęp do dzienników oraz jak i kiedy są one przeglądane. Te zasady i procedury będą się różnić w zależności od aplikacji i platformy ICS. Starsze systemy zazwyczaj wykorzystują rejestratory wydruku, które są przeglądane przez pracowników administracyjnych, operacyjnych i pracowników ochrony. Dzienniki utrzymywane przez aplikację ICS mogą być przechowywane w różnych miejscach i mogą, ale nie muszą, być szyfrowane.

6.2.4. Ocena, autoryzacja i monitorowanie

Zabezpieczenia należące do kategorii Ocena, autoryzacja i monitorowanie - CA, stanowią podstawę do przeprowadzania okresowych ocen i certyfikacji środków

bezpieczeństwa wdrożonych w systemie informacyjnym w celu określenia, czy zabezpieczenia są wdrożone prawidłowo, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty pozwalające spełnić wymagania bezpieczeństwa systemu. Za akceptację ryzyka szczątkowego i wydanie zezwolenia na użytkowanie systemu odpowiedzialny jest wyższy pracownik organizacji. Działania te stanowią akredytację. Ponadto wszystkie środki bezpieczeństwa powinny być na bieżąco monitorowane. Działania monitorujące obejmują zarządzanie konfiguracją i kontrolę komponentów systemu informacyjnego, analizę wpływu zmian w systemie na bezpieczeństwo, bieżącą ocenę środków bezpieczeństwa oraz raportowanie stanu.

Uzupełniające rekomendacje dotyczące zabezpieczeń z kategorii CA można znaleźć w następujących publikacjach:

- NSC 800-53A, zawierający rekomendacje dotyczące procesu oceniania środków bezpieczeństwa (bazuje na publikacji specjalnej NIST SP 800-53A [23]).
- NSC 800-37, zawierający rekomendacje określające granicę systemu informacyjnego oraz certyfikację i akredytację bezpieczeństwa systemu informacyjnego (bazuje na publikacji specjalnej NIST SP 800-37 [21]).
- NIST SP 800-100, zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].

6.2.5. Zarządzanie konfiguracją

Polityka i procedury zarządzania konfiguracją są stosowane do kontroli modyfikacji sprzętu, firmware'u, oprogramowania i dokumentacji, w celu zapewnienia, że system informacyjny jest chroniony przed niewłaściwymi modyfikacjami zarówno przed, w trakcie, jak i po jego wdrożeniu. Środki bezpieczeństwa wchodzące w skład kategorii Zarządzanie konfiguracją - CM, określają reguły i procedury ustanawiania bazowych zabezpieczeń do zastosowania w systemach informacyjnych. Określone są również zabezpieczenia dotyczące utrzymywania, monitorowania i dokumentowania zmian w konfiguracji. Dostęp do ustawień konfiguracyjnych powinien być ograniczony, a ustawienia zabezpieczeń produktów informacyjnych powinny być przełączone na najbardziej restrykcyjny tryb zgodny z wymaganiami operacyjnymi ICS.

Uzupełniające rekomendacje dotyczące zabezpieczeń CM można znaleźć w następujących publikacjach:

- NIST SP 800-70, zawierającej wytyczne dotyczące ustawień konfiguracyjnych produktów IT [26].
- NIST SP 800-100, zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].
- NIST SP 800-128, zawierającej wytyczne dotyczące wdrożenia programu zarządzania konfiguracją bezpieczeństwa [80].

Zalecenia i wytyczne dotyczące ICS

Należy ustanowić formalny program zarządzania zmianami i stosować procedury zapewniające, że wszelkie modyfikacje sieci ICS spełniają te same wymagania w zakresie bezpieczeństwa, co oryginalne komponenty zidentyfikowane w ocenie aktywów oraz związanej z nimi ocenie ryzyka i planach ograniczania ryzyka. Ocenę ryzyka należy przeprowadzać w odniesieniu do wszystkich zmian w sieci ICS, które mogą mieć wpływ na bezpieczeństwo, w tym zmian konfiguracji, dodawania komponentów sieciowych i instalowania oprogramowania. Wymagane mogą być także zmiany w politykach i procedurach. Zawsze należy znać i dokumentować aktualną konfigurację sieci ICS oraz konfiguracje urządzeń.

6.2.6. Planowanie awaryjne / ciągłość działania

Plany awaryjne mają na celu utrzymanie lub przywrócenie operacji biznesowych, w tym operacji komputerowych, w miarę możliwości w alternatywnej lokalizacji, w przypadku wystąpienia sytuacji awaryjnych, zakłóceń systemu lub katastrofy. Zabezpieczenia kategorii Planowanie awaryjne / ciągłość działania - CP, określają zasady i procedury wdrażania planu awaryjnego poprzez określenie ról i obowiązków oraz przydzielenie personelu i działań związanych z przywróceniem systemu informacyjnego po wystąpieniu zakłócenia lub awarii. Oprócz planowania istnieją również środki bezpieczeństwa odnoszące się do szkoleń, testowania i aktualizacji planów awaryjnych oraz zapasowych miejsc przetwarzania i przechowywania informacji.

Uzupełniające rekomendacje dotyczące planowania awaryjnego można znaleźć w następujących publikacjach:

- NSC 800-34, zawierający rekomendacje w zakresie planowania awaryjnego (bazuje na publikacji specjalnej NIST SP 800-34 [52]).
- NIST SP 800-100, zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].

Zalecenia i wytyczne dotyczące ICS

Plany awaryjne powinny obejmować wszystkie rodzaje awarii lub problemów, które mogą być spowodowane cyberincydentami. Plany awaryjne powinny zawierać procedury przywracania systemów ze znanych, aktualnych kopii zapasowych, odseparowania systemów od wszelkich niepożądanych zakłóceń i połączeń, które mogłyby umożliwić włamania naruszające cyberbezpieczeństwo, oraz alternatywne rozwiązania umożliwiające uzyskanie niezbędnych interfejsów i koordynacji. Personel powinien być przeszkolony i zaznajomiony z treścią planów awaryjnych. Plany awaryjne powinny być okresowo przeglądane przy udziale personelu odpowiedzialnego za przywrócenie ICS i testowane w celu zapewnienia, że nadal spełniają one założone cele. Organizacje opracowują również plany ciągłości działania (ang. business continuity plans – BCP) i plany odtwarzania po katastrofie (ang. disaster recovery plans - DRP), które są ściśle związane z planami awaryjnymi. Ponieważ plany ciągłości działania i odtwarzania po awarii są szczególnie istotne z punktu widzenia ICS, zostały one opisane bardziej szczegółowo w kolejnych sekcjach.

6.2.6.1. Planowanie ciągłości działania

Planowanie ciągłości działania dotyczy ogólnej kwestii utrzymania lub przywrócenia produkcji w przypadku wystąpienia zakłóceń. Przerwy te mogą przybrać formę klęski żywiołowej (np. huraganu, orkanu, trzęsienia ziemi, powodzi), niezamierzonego zdarzenia spowodowanego przez człowieka (np. przypadkowego uszkodzenia sprzętu, pożaru lub wybuchu, błędu operatora), zamierzonego zdarzenia spowodowanego przez człowieka (np. ataku bombowego, z użyciem broni palnej, wandalizmu, lub wirusa) albo samoistnej awarii sprzętu. Z perspektywy potencjalnego przestoju może to oznaczać

dni, tygodnie lub miesiące niezbędne do przywrócenia sprawności po klęsce żywiołowej, lub minuty czy godziny na odzyskanie sprawności po infekcji złośliwym oprogramowaniem lub uszkodzeniu mechanicznym/elektrycznym. Ponieważ często istnieje odrębny dział zajmujący się niezawodnością oraz utrzymaniem elektrycznym/mechanicznym, niektóre organizacje decydują się na zdefiniowanie ciągłości działania w sposób wykluczający te źródła awarii. Ponieważ ciągłość działania dotyczy w szczególności długoterminowych skutków przerw w produkcji, niektóre organizacje decydują się również na określenie minimalnego limitu przerw w działalności w odniesieniu do rozważanych zagrożeń. Dla celów cyberbezpieczeństwa ICS zaleca się nie wprowadzać żadnego z tych ograniczeń. Powinny być brane pod uwagę zarówno długoterminowe przerwy w pracy (odtwarzanie po awarii) jak i krótkoterminowe (odtwarzanie operacyjne). Ponieważ niektóre z tych potencjalnych zakłóceń dotyczą zdarzeń spowodowanych przez człowieka, ważna jest również współpraca z komórką organizacyjną zajmującą się bezpieczeństwem fizycznym, w celu zrozumienia względnego ryzyka tych zdarzeń oraz środków zaradczych bezpieczeństwa fizycznego, które są stosowane w celu zapobiegania im. Ważne jest również, aby komórka organizacyjna zajmująca się bezpieczeństwem fizycznym wiedziała, w których strefach produkcji znajdują się systemy pozyskiwania danych i sterowania, które mogą być obarczone wyższym poziomem ryzyka.

Przed stworzeniem planu ciągłości działania (BCP) na wypadek potencjalnych przestojów, ważne jest określenie celów odzyskiwania danych dla różnych systemów i podsystemów w oparciu o typowe potrzeby biznesowe. Istnieją dwa odrębne rodzaje celów: odzyskiwanie systemu i odzyskiwanie danych. Odzyskiwanie systemu obejmuje odzyskiwanie łączy telekomunikacyjnych i możliwości przetwarzania i jest zwykle określane w kategoriach czasu odzyskiwania (*ang. Recovery Time Objective - RTO*). Jest on definiowany jako czas wymagany do odzyskania wymaganych łączy telekomunikacyjnych i możliwości przetwarzania. Odzyskiwanie danych polega na przywracaniu danych opisujących warunki produkcji lub produktu w przeszłości i jest zwykle określane w kontekście punktu odtworzenia danych (*ang. Recovery Point*

Objective - RPO). Jest on definiowany jako najdłuższy okres czasu, przez jaki można zaakceptować utratę danych.

Po określeniu celów przywracania należy stworzyć listę potencjalnych zakłóceń, a następnie opracować i opisać procedurę przywracania. W przypadku większości zakłóceń o mniejszej skali, działania polegające na naprawie i wymianie w oparciu o zapas krytycznych części zamiennych będą wystarczające do osiągnięcia celów odbudowy. Jeśli tak się nie stanie, należy opracować plany awaryjne. Ze względu na potencjalne koszty i znaczenie planów awaryjnych, powinny one zostać zweryfikowane z menedżerami odpowiedzialnymi za planowanie ciągłości działania w celu sprawdzenia, czy są one uzasadnione. Po udokumentowaniu procedur odzyskiwania danych należy opracować harmonogram testowania części lub całości tych procedur. Szczególną uwagę należy zwrócić na weryfikację kopii zapasowych danych dotyczących konfiguracji systemu oraz danych dotyczących produktu lub produkcji. Przykłady danych konfiguracyjnych systemu obejmują kopie zapasowe konfiguracji komputera, kopie zapasowe konfiguracji aplikacji, operacyjne limity sterowania, zakresy sterowania i wartości zadane dla działania przed zdarzeniem dla wszystkich programowalnych urządzeń ICS. Konieczne jest nie tylko testowanie tych danych po ich wytworzeniu, ale także okresowe sprawdzanie procedur ich przechowywania w celu sprawdzenia, czy kopie zapasowe są przechowywane w warunkach środowiskowych, które nie spowodują, że staną się bezużyteczne, oraz czy są przechowywane w bezpiecznym miejscu, tak aby w razie potrzeby mogły być szybko pozyskane przez upoważnione osoby.

6.2.6.2. Planowanie odtworzenia po katastrofie

Plan odtworzenia po katastrofie (*ang. Disaster Recovery Planning - DRP*) jest udokumentowanym procesem lub zestawem procedur służących do odzyskiwania i ochrony infrastruktury IT w przypadku katastrofy. DRP, zwykle udokumentowany w formie pisemnej, określa procedury, które organizacja ma stosować w przypadku katastrofy. Jest to kompleksowa deklaracja spójnych działań, które należy podjąć przed, w trakcie i po wystąpieniu katastrofy. Katastrofa może być naturalna,

środowiskowa lub spowodowana przez człowieka. Katastrofy spowodowane przez człowieka mogą być zamierzone lub niezamierzone.

Zalecenia i wytyczne dotyczące ICS

DRP jest niezbędny dla zapewnienia ciągłej dostępności ICS. DRP powinien zawierać następujące elementy:

- Wymagane reakcje na zdarzenia lub warunki trwające przez różny czas i charakteryzujące się różnym stopniem nasilenia, które spowodują uruchomienie planu odtwarzania.
- Procedury obsługi systemu ICS w trybie ręcznym z przerwanymi wszystkimi zewnętrznymi połączeniami elektronicznymi do czasu przywrócenia bezpiecznych warunków.
- Role i obowiązki osób uczestniczących w działaniach.
- Procesy i procedury tworzenia kopii zapasowych i bezpiecznego przechowywania informacji.
- Kompletny i aktualny schemat logiczny sieci.
- Listę osób upoważnionych do fizycznego i wirtualnego dostępu do ICS.
- Procedurę komunikacyjną i listę osób, z którymi należy się kontaktować w przypadku awarii, w tym dostawców ICS, administratorów sieci, personelu obsługi ICS itp.
- Aktualne informacje o konfiguracji wszystkich komponentów.
- Harmonogram ćwiczeń procedur DRP.

Plan DRP powinien również określać wymagania dotyczące terminowej wymiany komponentów w przypadku zaistnienia sytuacji awaryjnej. Jeśli to możliwe, zamienniki trudno dostępnych komponentów krytycznych powinny być przechowywane w magazynie.

Plan bezpieczeństwa powinien określać kompleksową politykę tworzenia i odtwarzania kopii zapasowych. Przy formułowaniu tej polityki należy wziąć pod uwagę następujące kwestie:

- Szybkość, z jaką dane lub system muszą zostać przywrócone. Wymaganie to może uzasadniać potrzebę posiadania systemu redundantnego, zapasowego komputera znajdującego się w trybie offline lub aktualnych kopii zapasowych systemu plików.
- Częstotliwość, z jaką zmieniają się krytyczne dane i konfiguracje. Będzie to dyktować częstotliwość i kompleksowość wykonywania kopii zapasowych.
- Bezpieczne przechowywanie pełnych i przyrostowych kopii zapasowych w siedzibie firmy i poza nią.
- Bezpieczne przechowywanie nośników instalacyjnych, kluczy licencyjnych i informacji o konfiguracji.
- Wskazanie osób odpowiedzialnych za wykonywanie, testowanie, przechowywanie i przywracanie kopii zapasowych.

6.2.7. Identyfikacja i uwierzytelnianie

Uwierzytelnianie opisuje proces pozytywnej identyfikacji potencjalnych użytkowników sieci, hostów, aplikacji, usług i zasobów przy użyciu kombinacji czynników identyfikacyjnych lub poświadczeń. Wynik procesu uwierzytelniania staje się podstawą do zezwolenia lub odmowy dalszych działań (np. gdy automat weryfikujący prosi o podanie kodu PIN). W oparciu o ustalenia dotyczące uwierzytelniania, system może zezwolić lub nie zezwolić potencjalnemu użytkownikowi na dostęp do jego zasobów.

Autoryzacja jest procesem określania, kto i co powinno mieć dostęp do danego zasobu; kontrola dostępu jest mechanizmem egzekwowania autoryzacji. Kontrola dostępu została opisana w punkcie 6.2.1.

Istnieje kilka możliwych czynników określenia autentyczności osoby, urządzenia lub systemu, w tym coś co wiesz, coś co posiadasz lub coś kim jesteś. Na przykład uwierzytelnianie może opierać się na czymś znanym (np. numer PIN lub hasło), czymś posiadanym (np. klucz, klucz sprzętowy, karta inteligentna), kim się jest, np. określanym

przez cechę biologiczną (np. odcisk palca, skan siatkówki), lokalizacją (np. dostęp do lokalizacji w ramach globalnego systemu pozycjonowania [GPS]), czasem złożenia wniosku lub kombinacją tych atrybutów. Ogólnie rzecz biorąc, im więcej czynników jest wykorzystywanych w procesie uwierzytelniania, tym bardziej niezawodny będzie ten proces. W przypadku stosowania dwóch lub więcej czynników, proces ten jest ogólnie znany jako *uwierzytelnianie wieloczynnikowe (ang. multifactor - MFA).*

Zabezpieczenia należące do kategorii Identyfikacja i uwierzytelnianie – IA, określają politykę i wytyczne dotyczące identyfikacji i uwierzytelniania użytkowników i urządzeń w systemie informacyjnym. Obejmują one zabezpieczenia w zakresie zarządzania identyfikatorami i urządzeniami uwierzytelniającymi w ramach każdej stosowanej technologii (np. tokeny, certyfikaty, biometria, hasła, karty kluczowe).

Uzupełniające rekomendacje dotyczące zabezpieczeń i oceny skutków można znaleźć w następujących publikacjach:

- NIST SP 800-63, zawierającej wytyczne dotyczące zdalnego uwierzytelniania elektronicznego [53].
- NIST SP 800-73, zawierającej wytyczne dotyczące interfejsów weryfikacji tożsamości osobistej [49].
- NIST SP 800-76, zawierającej wytyczne dotyczące biometrii do weryfikacji tożsamości osób [50].
- NIST SP 800-100, zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].

Zalecenia i wytyczne dotyczące ICS

Systemy komputerowe w środowiskach ICS zazwyczaj opierają się na tradycyjnych hasłach uwierzytelniających. Dostawcy systemów sterowania często dostarczają systemy z hasłami domyślnymi. Hasła te są ustawiane fabrycznie i często są łatwe do odgadnięcia lub są rzadko zmieniane, co stwarza dodatkowe zagrożenia bezpieczeństwa. Ponadto protokoły stosowane obecnie w środowiskach ICS zazwyczaj nie zapewniają lub oferują nieodpowiednie uwierzytelnianie usług sieciowych. Oprócz tradycyjnych technik haseł stosowanych w ICS, dostępnych jest obecnie kilka form

uwierzytelniania. Niektóre z nich, w tym uwierzytelnianie za pomocą hasła, zostały przedstawione w kolejnych rozdziałach wraz z omówieniem ich zastosowania w ICS.

6.2.7.1. Uwierzytelnianie za pomocą hasła

Technologie uwierzytelniania za pomocą hasła określają autentyczność na podstawie testowania czegoś, co urządzenie lub człowiek żądający dostępu powinien znać, np. numeru PIN lub hasła. Schematy uwierzytelniania za pomocą haseł są uważane za najprostsze i najbardziej powszechne formy uwierzytelniania.

Podatności związane z wykorzystaniem haseł można zmniejszyć, stosując aktywny mechanizm sprawdzania haseł, który zabrania stosowania słabych, niedawno używanych lub często używanych haseł. Innym słabym punktem haseł jest łatwość podsłuchiwania przez osoby trzecie. Hasła wpisywane na klawiaturze są łatwo obserwowane lub nagrywane, szczególnie w miejscach, gdzie przeciwnicy mogliby umieścić małe bezprzewodowe kamery lub rejestratory naciśnięć klawiszy. Przy uwierzytelnianiu usług sieciowych hasła są często przesyłane w postaci jawnej (niezaszyfrowanej), co umożliwia ujawnienie haseł przez dowolne narzędzie do przechwytywania danych w sieci.

Zalecenia i wytyczne dotyczące ICS

Jednym z problemów z hasłami charakterystycznym dla środowiska ICS jest to, że na zdolność użytkownika do przypomnienia sobie i wprowadzenia poprawnego hasła może wpłynąć stres związany z daną chwilą. Podczas poważnej sytuacji kryzysowej, gdy do sterowania procesem krytycznie niezbędna jest interwencja człowieka, operator może wpaść w panikę i mieć trudności z przypomnieniem sobie lub wprowadzeniem hasła i albo zostać całkowicie zablokowany, albo opóźnić reakcję na zdarzenie. Jeżeli hasło zostało wprowadzone błędnie a system ma limit dozwolonych błędnych haseł, operator może zostać zablokowany na stałe, dopóki upoważniona osoba nie zresetuje konta. Identyfikatory biometryczne mogą mieć podobne wady. Organizacje powinny dokładnie rozważyć potrzeby bezpieczeństwa i potencjalne konsekwencje stosowania mechanizmów uwierzytelniania w tych krytycznych systemach.

W sytuacjach, gdy system ICS nie jest w stanie lub organizacja stwierdza, że nie jest wskazane (np. niekorzystnie wpływa to na wydajność, bezpieczeństwo lub niezawodność) wdrożenie mechanizmów uwierzytelniania w systemie ICS, organizacja stosuje zabezpieczenia kompensacyjne, takie jak rygorystyczne kontrole bezpieczeństwa fizycznego (np. dostęp upoważnionych użytkowników za pomocą kart-kluczy do centrum sterowania), aby zapewnić równoważną zdolność bezpieczeństwa lub poziom ochrony systemu ICS. Niniejsze rekomendacje dotyczą także stosowania blokady sesji i zakończenia sesji w systemie ICS.

Szczególną uwagę należy zwrócić przy wprowadzaniu w środowisku ICS zasad opartych na uwierzytelnianiu logowania za pomocą hasła. Bez listy wykluczeń opartej na identyfikacji maszyny (ID) logowanie osób niebędących operatorami może skutkować wprowadzeniem zasad, takich jak czas automatycznego wylogowania i wymiana hasła administratora, co może mieć negatywny wpływ na działanie systemu.

Niektóre systemy operacyjne ICS utrudniają ustanawianie bezpiecznych haseł, ponieważ długość hasła jest bardzo mała a system dopuszcza tylko hasła grupowe na każdym poziomie dostępu, a nie hasła indywidualne. Niektóre protokoły przemysłowe (oraz internetowe) przesyłają hasła w postaci jawnego tekstu, co czyni je podatnymi na przechwycenie. W przypadkach, gdy nie można uniknąć takiej praktyki, ważne jest, aby użytkownicy mieli różne (i niepowiązane) hasła do protokołów szyfrowanych i nieszyfrowanych.

Poniżej przedstawiono ogólne zalecenia i uwagi dotyczące stosowania haseł.

- Długość, siła i złożoność haseł powinny zapewniać równowagę między bezpieczeństwem a łatwością dostępu w ramach możliwości oprogramowania i systemu operacyjnego, na którym są oparte.
- Hasła powinny mieć odpowiednią długość i złożoność w stosunku do wymaganego poziomu bezpieczeństwa. W szczególności nie powinny być możliwe do znalezienia w słowniku, ani zawierać przewidywalnych ciągów cyfr lub liter.
- Hasła powinny być ostrożnie stosowane w urządzeniach interfejsu operatora, takich jak konsole sterujące w procesach krytycznych. Stosowanie haseł na tych konsolach

może powodować potencjalne problemy z bezpieczeństwem, jeśli operatorzy zostaną zablokowani lub będą mieli opóźniony dostęp podczas zdarzeń krytycznych. W przypadku gdy ochrona hasłem jest niemożliwa, konsole sterownicze operatorów należy uzupełnić o zabezpieczenia fizyczne.

- Posiadaczem haseł głównych powinien być zaufany pracownik, dostępny w sytuacjach awaryjnych. Wszelkie kopie haseł wzorcowych muszą być przechowywane w bardzo bezpiecznym miejscu z ograniczonym dostępem.
- Hasła użytkowników uprzywilejowanych (takich jak technicy sieciowi, technicy elektrycy i elektronicy oraz kadra kierownicza, projektanci i operatorzy sieci) powinny być najbezpieczniejsze i często zmieniane. Uprawnienia do zmiany haseł głównych powinny być ograniczone do zaufanych pracowników. Rejestr audytu haseł, zwłaszcza haseł głównych, powinien być odseparowany od systemu sterowania.
- W środowiskach o wysokim ryzyku przechwycenia lub włamania (takich jak zdalne interfejsy operatora w obiekcie, w którym brakuje lokalnych fizycznych zabezpieczeń dostępu), organizacje powinny rozważyć uzupełnienie uwierzytelniania opartego na hasłach innymi formami uwierzytelniania, takimi jak uwierzytelnianie wieloczynnikowe z użyciem tokenów biometrycznych lub fizycznych.
- Do celów uwierzytelniania użytkowników, hasło jest powszechnie stosowane i ogólnie akceptowalne w przypadku użytkowników logujących się bezpośrednio do lokalnego urządzenia lub komputera. Hasła nie powinny być przesyłane przez sieć, chyba że są chronione za pomocą zatwierdzonej przez stosowną władzę bezpieczeństwa formy szyfrowania lub soli skrótu kryptograficznego, zaprojektowanego specjalnie w celu zapobiegania atakom powtórzenia. Zakłada się, że urządzenie używane do wprowadzania hasła jest podłączone do sieci w bezpieczny sposób.
- Do celów uwierzytelniania usług sieciowych nie należy przekazywać haseł w postaci zwykłego tekstu. Istnieją bezpieczniejsze alternatywy, takie jak uwierzytelnianie

metodą „wezwanie/odpowiedź (*ang. challenge/response*) lub uwierzytelnianie z użyciem klucza publicznego.

6.2.7.2. Uwierzytelnianie typu „wezwanie/odpowiedź”

Uwierzytelnianie na zasadzie „wezwania/odpowiedzi” (*ang. challenge/response authentication*) wymaga, aby zarówno żądający usługi, jak i usługodawca znali wcześniej "tajny" kod[31]. Po zażądaniu wykonania usługi, usługodawca wysyła losową liczbę lub ciąg znaków jako wezwanie do wykonania usługi. Żądający usługi używa tajnego kodu do wygenerowania unikalnej odpowiedzi dla usługodawcy. Jeśli odpowiedź jest zgodna z oczekiwaniami, dowodzi to, że żądający usługi ma dostęp do "sekretu " bez ujawniania go w sieci.

Przy tradycyjnym przesyłaniu haseł (zaszyfrowanych lub jawnych) przez sieć, przekazywana jest również część rzeczywistego "sekretu", który jest przekazywany zdalnemu urządzeniu przeprowadzającemu uwierzytelnianie. Z tego powodu tradycyjna wymiana haseł zawsze jest narażona na ryzyko odkrycia lub powtórzenia. Ponieważ w systemach typu "wezwanie/odpowiedź", "sekret" jest znany z góry i nigdy nie jest przesyłany, ryzyko jego odkrycia jest wyeliminowane. Jeżeli usługodawca nigdy nie może wysłać dwa razy tego samego wezwania, a odbiorca może wykryć wszystkie duplikaty, ryzyko przechwycenia w sieci i ataków powtórkowych jest wyeliminowane.

Zalecenia i wytyczne dotyczące ICS

W przypadku uwierzytelniania użytkowników bezpośrednie zastosowanie uwierzytelniania typu "wezwanie/odpowiedź" może być niewykonalne dla systemu sterowania ze względu na możliwe opóźnienia, które mogą być wprowadzone w niezbędnej szybkiej dynamice wymaganej do uzyskania dostępu do systemu sterowania lub sieci przemysłowej. W przypadku uwierzytelniania usług sieciowych, stosowanie uwierzytelniania typu "wezwanie/odpowiedź" jest korzystniejsze od tradycyjnych schematów uwierzytelniania za pomocą hasła lub tożsamości źródłowej.

[31] Znany również jako „sekret”.

Uwierzytelnianie typu "wezwanie/odpowiedź" zapewnia większe bezpieczeństwo niż szyfrowane hasła do uwierzytelniania użytkowników w sieci. Zarządzanie głównymi algorytmami szyfrowania i hasłami głównymi staje się coraz bardziej złożone, gdy w procesach zabezpieczeń bierze udział więcej stron, i stanowi ważny czynnik wpływający na odporność systemu zabezpieczeń.

6.2.7.3. Uwierzytelnianie za pomocą tokena fizycznego

Uwierzytelnianie fizyczne lub uwierzytelnianie przy użyciu tokenów jest podobne do uwierzytelniania przy użyciu haseł, z tą różnicą, że te technologie określają autentyczność poprzez testowanie tajnego kodu lub klucza wytwarzanego przez urządzenie lub token, który osoba żądająca dostępu ma w swoim posiadaniu. Coraz częściej klucze prywatne są osadzane w urządzeniach fizycznych, takich jak klucze USB. Niektóre tokeny obsługują tylko uwierzytelnianie jednoskładnikowe, a więc samo posiadanie tokena wystarcza do uwierzytelnienia. Inne obsługują uwierzytelnianie wieloczynnikowe, które wymaga znajomości kodu PIN lub hasła oprócz posiadania tokena.

Podstawową słabością systemu uwierzytelniania, którą eliminuje uwierzytelnianie przy użyciu tokena, jest łatwe powielanie tajnego kodu lub udostępnianie go innym osobom. Eliminowany jest zbyt często spotykany scenariusz, w którym hasło do "bezpiecznego" systemu zostaje pozostawione na ścianie obok komputera lub stanowiska operatora. Token zabezpieczający nie może zostać powielony bez specjalnego dostępu do urządzenia i wyposażenia.

Drugą zaletą jest to, że sekret w tokenie fizycznym może być bardzo rozbudowany, bezpieczny fizycznie i generowany losowo. Ponieważ jest on osadzony w przedmiocie materialnym, nie wiąże się z nim takie samo ryzyko, jak w przypadku haseł wprowadzanych ręcznie. W przypadku zgubienia lub kradzieży tokena bezpieczeństwa uprawniony użytkownik traci dostęp, w przeciwieństwie do tradycyjnych haseł, które mogą zostać zgubione lub skradzione bez zauważenia tego.

Popularne formy uwierzytelniania fizycznego/tokenowego obejmują:

- Tradycyjny fizyczny zamek i klucze.

- Karty bezpieczeństwa (np. magnetyczne, chipowe, z kodem optycznym).
- Urządzenia radiowe (*ang. Radio frequency devices - RFID*) w postaci kart, breloczków lub identyfikatorów.
- Klucze sprzętowe z bezpiecznymi kluczami szyfrującymi, które podłącza się do portów USB, szeregowych lub równoległych komputerów.
- Generatory kodów jednorazowego uwierzytelniania.

W przypadku uwierzytelniania jednoskładnikowego największą słabością jest to, że fizyczne posiadanie tokena oznacza przyznanie dostępu (np. każdy, kto znajdzie zestaw zgubionych kluczy, ma teraz dostęp do wszystkiego, co otwiera takie zabezpieczenie). Uwierzytelnianie fizyczne/tokenowe jest bezpieczniejsze, gdy jest połączone z drugą formą uwierzytelniania, taką jak kod PIN używany razem z tokenem.

Zalecenia i wytyczne dotyczące ICS

Uwierzytelnianie wieloczynnikowe jest przyjętą dobrą praktyką w zakresie dostępu do aplikacji ICS z zewnątrz zapory ICS.

Uwierzytelnianie fizyczne/tokenowe może potencjalnie odgrywać ważną rolę w środowiskach ICS. Karta dostępu lub inny token może być skuteczną formą uwierzytelniania przy dostępie do komputera, o ile komputer znajduje się w bezpiecznym miejscu (np. po uzyskaniu przez operatora dostępu do pomieszczenia z odpowiednim uwierzytelnieniem wtórnym, sama karta może być użyta do umożliwienia działań sterujących).

6.2.7.4. Uwierzytelnianie za pomocą kart inteligentnych

Karty inteligentne są podobne do tokenów uwierzytelniających, jednakże mogą zapewniać dodatkowe funkcje. Karty inteligentne można skonfigurować w taki sposób, aby obsługiwały wiele pokładowych aplikacji umożliwiających dostęp do budynku, dwu- lub trójskładnikowe uwierzytelnianie komputerowe oraz sprzedaż bezgotówkową na jednej karcie, a jednocześnie pełniły funkcję firmowego identyfikatora ze zdjęciem.

Zazwyczaj karty inteligentne mają format karty kredytowej, która może być zadrukowana, wytłoczona i indywidualnie spersonalizowana. Karty inteligentne mogą być dostosowane do potrzeb klienta, zindywidualizowane i wydawane we własnym zakresie lub zlecane usługodawcom, którzy zazwyczaj wydają setki tysięcy kart dziennie.

Karty inteligentne rozszerzają rozwiązania oparte wyłącznie na oprogramowaniu, takie jak uwierzytelnianie za pomocą hasła, oferując dodatkowy czynnik uwierzytelniający i eliminując element ludzki związany z zapamiętywaniem złożonych sekretów. Ponadto:

- Odseparowują operacje o kluczowym znaczeniu dla bezpieczeństwa, obejmujące uwierzytelnianie, podpisy cyfrowe i wymianę kluczy, od innych obszarów systemu, które nie powinny być znane.
- Umożliwiają przenoszenie danych uwierzytelniających i innych prywatnych informacji między wieloma systemami komputerowymi.
- Zapewniają odporne na manipulacje przechowywanie kluczy prywatnych i innych rodzajów informacji osobistych.

Większość trudności stanowią kwestie logistyczne związane z wydawaniem kart, zwłaszcza z wymianą zgubionych lub skradzionych kart.

Zalecenia i wytyczne dotyczące ICS

Chociaż karty inteligentne są stosunkowo niedrogie i oferują przydatne funkcje w kontekście systemu sterowania przemysłowego, ich wdrożenie musi odbywać się w ramach ogólnego kontekstu bezpieczeństwa organizacji. Niezbędna identyfikacja osób, wydawanie kart, ich unieważnianie w przypadku podejrzenia kompromitacji oraz przypisywanie uprawnień do uwierzytelnionych tożsamości stanowi poważne początkowe i ciągłe wyzwanie. W niektórych przypadkach mogą być dostępne korporacyjne zasoby informacyjne lub inne, które pomogą we wdrożeniu infrastruktury opartej na kartach inteligentnych i kluczach publicznych.

Jeśli karty inteligentne są wdrażane w środowisku sterowania przemysłowego, należy uwzględnić zarządzanie zagubionymi lub uszkodzonymi kartami, a także koszty

włączenia odpowiedniego systemu kontroli dostępu i zapewnienia procesu zarządzania dystrybucją i odzyskiwaniem kart.

6.2.7.5. Uwierzytelnianie biometryczne

Technologie uwierzytelniania biometrycznego określają autentyczność poprzez ustalenie przypuszczalnie unikatowych cech biologicznych człowieka żądającego dostępu. Użyteczne cechy biometryczne obejmują odciski palców, geometrię twarzy, sygnatury siatkówki i tęczówki, wzorce głosu, wzorce pisma i geometrię dłoni.

Podobnie jak tokeny fizyczne i karty inteligentne, uwierzytelnianie biometryczne usprawnia rozwiązania oparte wyłącznie na oprogramowaniu, takie jak uwierzytelnianie za pomocą hasła, oferując dodatkowy czynnik uwierzytelniający i eliminując zapamiętywanie złożonych sekretów. Ponadto, ponieważ cechy biometryczne są unikatowe dla danej osoby, uwierzytelnianie biometryczne rozwiązuje problem zagubionych lub skradzionych fizycznych tokenów i kart inteligentnych.

Do podstawowych problemów związanych z uwierzytelnianiem biometrycznym należą:

- Odróżnianie prawdziwego obiektu od fałszywego (np. jak odróżnić prawdziwy ludzki palec od jego silikonowo-gumowego odlewu lub prawdziwy ludzki głos od nagranego).
- Generowanie błędów typu I i typu II (odpowiednio prawdopodobieństwo odrzucenia prawidłowego obrazu biometrycznego oraz prawdopodobieństwo zaakceptowania nieprawidłowego obrazu biometrycznego). Biometryczne urządzenia uwierzytelniające powinny być skonfigurowane w taki sposób, aby uzyskać najniższą wartość krzyżową pomiędzy tymi dwoma prawdopodobieństwami, zwaną również poziomem błędu krzyżowego.
- Obsługa czynników środowiskowych, takich jak temperatura i wilgotność, na które wrażliwe są niektóre urządzenia biometryczne.
- Zastosowanie w warunkach przemysłowych, gdzie pracownicy używają okularów i/lub rękawic ochronnych, a chemikalia przemysłowe mogą mieć wpływ na skanery biometryczne.

- Ponowne uczenie skanerów cech biometrycznych, które "dryfują" z upływem czasu. Cechy biometryczne człowieka mogą zmieniać się w czasie, co wymaga okresowego uczenia skanerów.
- Wymóg bezpośredniego wsparcia technicznego i weryfikacji w przypadku szkoleń z obsługi urządzeń, w przeciwieństwie do hasła, które można podać przez telefon lub karty dostępu, którą może przekazać osobie trzeciej.
- Odmowa dostępu do systemu sterowania z powodu tymczasowej niezdolności urządzenia wykrywającego do rozpoznania prawowitego użytkownika.
- Akceptacja społeczna. Użytkownicy uważają niektóre biometryczne urządzenia uwierzytelniające za bardziej akceptowalne niż inne. Na przykład skanery siatkówki mogą być uważane za bardzo słabo akceptowalne, podczas gdy skanery odcisków palców mogą być uważane za powszechnie akceptowalne. Organizacje wdrażające biometryczne urządzenia uwierzytelniające będą musiały wziąć pod uwagę akceptację społeczną dla swojej grupy docelowej przy wyborze różnych technologii uwierzytelniania biometrycznego.

Zalecenia i wytyczne dotyczące ICS

Urządzenia biometryczne stanowią użyteczne dodatkowe zabezpieczenie obok innych form uwierzytelniania, które mogą zostać zgubione lub zapomniane. Zastosowanie uwierzytelniania biometrycznego w połączeniu z kontrolą dostępu opartą na tokenach lub zegarami czasu pracy obsługiwanymi przez identyfikatory zwiększa poziom bezpieczeństwa. Możliwe jest zastosowanie tego rozwiązania w sterowni, która jest zabezpieczona fizycznie i kontrolowana pod względem środowiskowym [34].

Biometria może stanowić wartościowy mechanizm uwierzytelniania, ale musi być starannie oceniona w zastosowaniach przemysłowych, ponieważ kwestie fizyczne i środowiskowe w środowisku instalacji mogą wymagać zmiany struktury w celu zapewnienia niezawodnego autoryzowanego uwierzytelniania. Szczegółowe warunki fizyczne i środowiskowe instalacji powinny być uzgodnione z dostawcą lub producentem systemu.

6.2.8. Reagowanie na incydenty

Plan reagowania na incydenty to udokumentowany, wcześniej ustalony zestaw instrukcji lub procedur służących do wykrywania, reagowania i ograniczania skutków incydentów związanych z systemami informacyjnymi organizacji. Sposób reagowania powinien być mierzony przede wszystkim w odniesieniu do "świadczonej usługi", a nie tylko do systemu, który został naruszony. W przypadku wykrycia incydentu należy przeprowadzić szybkie oszacowanie ryzyka, aby ocenić skutki zarówno ataku, jak i możliwości reakcji. Na przykład, jedną z możliwych reakcji jest fizyczne odizolowanie zaatakowanego systemu. Może to jednak mieć tak poważny wpływ na usługi, że zostanie odrzucone jako nierealne.

Zabezpieczenia należące do kategorii Reagowanie na incydenty – IR, określają polityki i procedury monitorowania, obsługi i raportowania reakcji na incydenty. Obsługa incydentu bezpieczeństwa obejmuje przygotowanie, wykrywanie i analizę, ograniczanie, eliminowanie i odzyskiwanie. Zabezpieczenia obejmują również szkolenia personelu w zakresie reagowania na incydenty oraz testowanie zdolności reagowania na incydenty systemu informacyjnego.

Uzupełniające rekomendacje dotyczące zabezpieczeń IR można znaleźć w następujących publikacjach:

- NSC 800-61, zawierający rekomendacje dotyczące obsługi i zgłaszania incydentów [59].
- NIST SP 800-83, zawierającej wytyczne dotyczące zapobiegania i obsługi incydentów związanych ze złośliwym oprogramowaniem [60].
- NIST SP 800-100 zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].

Zalecenia i wytyczne dotyczące ICS

Niezależnie od podjętych kroków zmierzających do ochrony systemu ICS, zawsze istnieje prawdopodobieństwo jego naruszenia w wyniku celowego lub niezamierzonego incydentu. Przedstawione poniżej symptomy mogą wynikać z normalnych problemów z siecią, jednak jeżeli zaczyna pojawiać się kilka zjawisk, określony wzorzec może wskazywać, że system ICS jest atakowany i powinien zostać poddany szczegółowej analizie. Jeśli atakujący jest odpowiednio doświadczony, wykrycie ataku może nie być łatwe.

Objawy incydentu mogą dotyczyć jednej z poniższych sytuacji:

- Nietypowo duży ruch w sieci.
- Brak miejsca na dysku lub znaczne zmniejszenie ilości wolnego miejsca na dysku.
- Nietypowo wysokie użycie procesora.
- Zakładanie nowych kont użytkowników.
- Próby lub faktyczne korzystanie z kont na poziomie administratora.
- Zablokowane konta.
- Używanie konta w godzinach pozasłużbowych.
- Wyczyszczone pliki rejestru logów.
- Przepełnione pliki rejestru zawierające nietypową liczbę zdarzeń.
- Alerty systemów antywirusowych lub IDS.
- Wyłączone oprogramowanie antywirusowe i inne środki bezpieczeństwa.
- Nieoczekiwane zmiany w ustawieniach poprawek.
- Połączenia maszyn z zewnętrznymi adresami IP.
- Prośby o informacje o systemie (próby socjotechniczne).
- Nieoczekiwane zmiany w ustawieniach konfiguracyjnych.
- Nieoczekiwane wyłączenie systemu.

W celu zminimalizowania skutków takich incydentów konieczne jest odpowiednie zaplanowanie reakcji. Planowanie reakcji na incydent określa procedury, które należy wykonać po jego wystąpieniu. Publikacja NSC 800-61 (bazująca na publikacji specjalnej NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide [59]), zawiera rekomendacje w zakresie planowania reakcji na incydent, które mogą obejmować następujące elementy:

- **Klasyfikacja incydentów**. Różne rodzaje incydentów ICS powinny być identyfikowane i klasyfikowane pod względem potencjalnego wpływu, tak aby dla każdego potencjalnego incydentu można było sformułować właściwą reakcję.
- **Reakcje na incydenty**. W przypadku wystąpienia incydentu możliwe jest podjęcie szeregu działań. Zakres tych reakcji rozciąga się od niepodejmowania żadnych działań do pełnego wyłączenia systemu (choć całkowite wyłączenie systemu ICS jest bardzo mało prawdopodobną reakcją). Podjęta reakcja będzie zależała od rodzaju zdarzenia i jego wpływu na system ICS oraz kontrolowany proces fizyczny. Należy przygotować pisemny plan dokumentujący rodzaje incydentów i sposób reagowania na każdy z nich. Pozwoli to na uzyskanie wskazówek w czasie, gdy może dojść do dezorientacji lub stresu związanego z incydentem. Plan ten powinien obejmować działania krok po kroku podejmowane przez różne organizacje. Należy uwzględnić wymagania dotyczące raportowania, a także wskazać punkt kontaktowy, w którym należy dokonać powiadomienia, aby uniknąć zamieszania związanego z dokonywanymi zgłoszeniami.
- **Działania odtworzeniowe**. Skutki incydentu mogą być znikome, ale mogą też spowodować wiele problemów w systemie ICS. Należy przeprowadzić szacowanie ryzyka w celu określenia wrażliwości kontrolowanego systemu fizycznego na wystąpienie awarii w systemie ICS. W każdym przypadku należy udokumentować krok po kroku działania naprawcze, tak aby system mógł jak najszybciej i najbezpieczniej powrócić do stanu normalnego funkcjonowania. Działania naprawcze w przypadku wystąpienia incydentu, który ma wpływ na działanie ICS, będą ściśle powiązane z planem odtwarzania po katastrofie i powinny uwzględniać ustanowione wcześniej procedury planowania i koordynacji.

Podczas przygotowywania planu reagowania na incydenty należy wziąć pod uwagę informacje pozyskane od różnych zainteresowanych stron, w tym od personelu operacyjnego, inżynieryjnego, informatyków, dostawców wsparcia systemowego, kierownictwa, zorganizowanych grup pracowniczych, prawników i służb bezpieczeństwa. Interesariusze ci powinni także dokonać przeglądu i zatwierdzenia planu.

6.2.9. Utrzymanie i wsparcie

Zabezpieczenia należące do kategorii Utrzymanie i wsparcie – MA, określają politykę i procedury wykonywania rutynowego i zapobiegawczego utrzymania i wsparcia (konserwacji) komponentów systemu informacyjnego. Obejmuje to wykorzystanie narzędzi konserwacyjnych (zarówno lokalnych jak i zdalnych) oraz zarządzanie personelem utrzymaniowym.

Uzupełniające rekomendacje dotyczące zabezpieczeń MA można znaleźć w następujących publikacjach:

- NIST SP 800-63, zawierającej wytyczne dotyczące elektronicznego uwierzytelniania na potrzeby zdalnego utrzymania i wsparcia [53].
- NIST SP 800-100, zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].

6.2.10. Ochrona nośników danych

Zabezpieczenia, które wchodzą w skład kategorii Ochrona nośników danych – MP, określają polityki i procedury ograniczające dostęp do nośników danych przez autoryzowanych użytkowników. Istnieją również zabezpieczenia dotyczące etykietowania nośników pod kątem wymogów dystrybucji i obsługi, a także przechowywania, transportu, sanityzacji (usuwania informacji z nośników cyfrowych), niszczenia i utylizacji nośników.

Uzupełniające rekomendacje dotyczące zabezpieczeń MP można znaleźć w następujących publikacjach:

- NIST SP 800-88, zawierającej wytyczne dotyczące właściwych technik i procedur sanityzacji sprzętu [78].
- NIST SP 800-100, zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].

Zalecenia i wytyczne dotyczące ICS

Zasoby nośnikowe obejmują przenośne nośniki i urządzenia, takie jak dyskietki, płyty CD, DVD i pamięci USB, a także drukowane raporty i dokumenty. Zabezpieczenia fizyczne nośników danych powinny obejmować szczegółowe wymagania dotyczące bezpiecznego przechowywania tych zasobów oraz zawierać precyzyjne wytyczne dotyczące transportu, obsługi, kasowania i niszczenia tych zasobów. Wymagania dotyczące bezpieczeństwa mogą obejmować ochronę przed utratą, pożarem, kradzieżą, niezamierzonym rozpowszechnieniem lub uszkodzeniem środowiskowym.

Jeżeli przeciwnik uzyska dostęp do nośników kopii zapasowych dotyczących systemu ICS, mogą one stanowić cenne źródło danych umożliwiających przeprowadzenie ataku. Odzyskanie z kopii zapasowych pliku zawierającego dane uwierzytelniające może umożliwić napastnikowi uruchomienie narzędzi do łamania haseł i wydobycie z nich haseł użytkowych. Ponadto kopie zapasowe zazwyczaj zawierają nazwy urządzeń, adresy IP, numery wersji oprogramowania, nazwy użytkowników i inne dane przydatne przy planowaniu ataku.

Nie należy zezwalać na korzystanie z nieautoryzowanych płyt CD, DVD, dyskietek, pamięci USB i innych podobnych nośników wymiennych w żadnym węźle, który jest częścią ICS lub jest do niego podłączony. Pozwala to zapobiec wprowadzeniu złośliwego oprogramowania oraz nieumyślnej utracie lub kradzieży danych. Jeśli składniki systemu korzystają z niezmodyfikowanych standardowych protokołów przemysłowych, do egzekwowania zasad ochrony danych można użyć automatycznego oprogramowania zarządzającego politykami.

6.2.11. Ochrona fizyczna i środowiskowa

Środki bezpieczeństwa należące do kategorii Ochrona fizyczna i środowiskowa – PE, określają politykę i procedury dotyczące wszelkiego fizycznego dostępu do systemu

informacyjnego, w tym wyznaczonych punktów wejścia/wyjścia, mediów transmisyjnych i urządzeń obrazujących. Obejmują one zabezpieczenia dostępu fizycznego, utrzymywania rejestrów wejść i obsługi gości. Do tej kategorii należą również zabezpieczenia służące do wdrażania i zarządzania środkami bezpieczeństwa w sytuacjach awaryjnych, takimi jak awaryjne wyłączanie systemu informacyjnego, zasilanie i oświetlenie awaryjne, kontrola temperatury i wilgotności oraz ochrona przed pożarem i zalaniem.

Uzupełniające rekomendacje dotyczące zabezpieczeń PE można znaleźć w następujących publikacjach:

- NSC 800-46, zawierającym wytyczne dotyczące telepracy i bezpieczeństwa komunikacji szerokopasmowej (bazującym na publikacji specjalnej NIST SP 800-46 [51]).
- NIST SP 800-100, zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].

Środki bezpieczeństwa fizycznego mają na celu zmniejszenie ryzyka przypadkowej lub celowej utraty lub uszkodzenia majątku organizacji i otaczającego ją środowiska. Zabezpieczane zasoby mogą być zasobami fizycznymi, takimi jak sprzęt i wyposażenie organizacji, środowisko, otaczająca społeczność, a także własność intelektualna, w tym dane stanowiące tajemnicę, takie jak ustawienia procesów i informacje o klientach. Wdrażanie zabezpieczeń fizycznych często podlega wymogom środowiskowym, bezpieczeństwa, regulacyjnym, prawnym i innym, które muszą być określone i uwzględnione w danym środowisku. Temat wdrażania środków bezpieczeństwa fizycznego jest obszerny i musi być dostosowany do rodzaju wymaganej ochrony.

Zalecenia i wytyczne dotyczące ICS

Fizyczna ochrona komponentów sprzętowych i programowych oraz danych związanych z ICS musi być uwzględniona jako część ogólnego bezpieczeństwa instalacji organizacyjnych. Bezpieczeństwo w wielu obiektach ICS jest ściśle związane z bezpieczeństwem instalacji. Podstawowym celem jest zabezpieczenie ludzi przed niebezpiecznymi sytuacjami, tak aby nie przeszkadzało im to w wykonywaniu pracy lub

przeprowadzaniu procedur awaryjnych. Środki bezpieczeństwa fizycznego to wszelkie środki fizyczne, zarówno aktywne, jak i pasywne, które ograniczają fizyczny dostęp do wszelkich zasobów informacyjnych w środowisku ICS. Środki te są stosowane w celu zapobiegania wielu rodzajom niepożądanych efektów, w tym:

- Nieuprawnionego dostępu fizycznego do miejsc o szczególnym znaczeniu.
- Fizycznej modyfikacji, manipulacji, kradzieży lub innego rodzaju usunięcia albo zniszczenia istniejących systemów, infrastruktury, interfejsów komunikacyjnych, personelu lub lokalizacji fizycznych.
- Nieuprawnionej inwigilacji wrażliwych zasobów informacyjnych na drodze obserwacji wzrokowej, robienia notatek, zdjęć lub za pomocą innych środków.
- Nieuprawnionego wprowadzania nowych systemów, infrastruktury, interfejsów komunikacyjnych lub innego sprzętu.
- Nieuprawnionemu wprowadzaniu urządzeń celowo zaprojektowanych do manipulowania sprzętem, podsłuchiwania komunikacji lub wywierania innego szkodliwego wpływu.

Uzyskaniu fizycznego dostępu do pomieszczenia sterowania lub elementów systemu sterowania. Często oznacza to uzyskanie również logicznego dostępu do systemu sterowania procesem. Podobnie, logiczny dostęp do systemów, takich jak serwery główne i komputery w sterowni, umożliwia przeciwnikowi sprawowanie kontroli nad procesem fizycznym.

Jeżeli komputery są łatwo dostępne i wyposażone w napędy wymienne (np. dyskietki, płyty kompaktowe, zewnętrzne dyski twarde) lub porty USB, napędy te można zablokować lub wyjąć z komputerów, a porty USB zablokować. W zależności od potrzeb i ryzyka związanego z bezpieczeństwem, rozsądnym rozwiązaniem może być również zablokowanie lub fizyczna ochrona przycisków zasilania, aby zapobiec ich nieuprawnionemu użyciu. W celu zapewnienia maksymalnego bezpieczeństwa serwery powinny być umieszczone w zamkniętych pomieszczeniach, a mechanizmy uwierzytelniania (takie jak klucze) odpowiednio zabezpieczone. Ponadto, urządzenia sieciowe wykorzystywane w sieci ICS, w tym przełączniki, routery, gniazda sieciowe,

serwery, stacje robocze i kontrolery, powinny znajdować się w zabezpieczonym obszarze, do którego dostęp ma tylko upoważniony personel. Zabezpieczony obszar powinien być także zgodny z wymaganiami środowiskowymi stawianymi przez urządzenia.

Rozwiązanie z zakresu bezpieczeństwa fizycznego typu "obrona w głąb" powinno obejmować następujące elementy:

- **Fizyczna ochrona lokalizacji**. W klasycznych rozwiązaniach z zakresu bezpieczeństwa fizycznego zazwyczaj mówi się o architekturze warstwowej. Wokół budynków, obiektów, pomieszczeń, sprzętu i innych zasobów informacyjnych tworzy się kilka barier fizycznych, zarówno aktywnych, jak i pasywnych, które wyznaczają granice bezpieczeństwa fizycznego. Środki bezpieczeństwa fizycznego, które mają chronić fizyczne lokalizacje, obejmują ogrodzenia, rowy ochronne przeciw pojazdom, kopce ziemne, mury, wzmocnione barykady, bramy i inne środki. Większość organizacji stosuje ten model warstwowy, uniemożliwiając dostęp do obiektu poprzez zastosowanie w pierwszej kolejności ogrodzeń, budek strażniczych, bram i zamykanych drzwi.
- **Kontrola dostępu**. Systemy kontroli dostępu powinny umożliwiać dostęp do kontrolowanych obszarów tylko upoważnionym osobom. System kontroli dostępu powinien być elastyczny. Potrzeba dostępu może zależeć od czasu (zmiana dzienna lub nocna), poziomu wyszkolenia, statusu zatrudnienia, przydziału pracy, statusu obiektu i wielu innych czynników. System musi być w stanie zweryfikować, czy osoby, którym przyznaje się dostęp, są tymi, za które się podają (zazwyczaj przy użyciu posiadanych przez daną osobę przedmiotów, takich jak karta dostępu lub klucz; posiadanych środków, takich jak osobisty numer identyfikacyjny (PIN); lub posiadanych przedmiotów, takich jak urządzenie biometryczne). Kontrola dostępu powinna być wysoce niezawodna, a jednocześnie nie powinna przeszkadzać w wykonywaniu rutynowych lub awaryjnych obowiązków przez personel obiektu. Integracja kontroli dostępu z systemem przetwarzania umożliwia wgląd nie tylko w zabezpieczenia dostępu, ale także w fizyczne i personalne śledzenie zasobów, co znacznie przyspiesza czas reakcji w sytuacjach awaryjnych, pomaga w kierowaniu

osób do bezpiecznych miejsc i poprawia ogólną wydajność. W danym obszarze dostęp do szafek instalacyjnych powinien być ograniczony tylko do niezbędnego personelu, takiego jak technicy i inżynierowie sieciowi lub pracownicy zajmujący się konserwacją komputerów. Szafy na sprzęt powinny być zamykane na klucz, a okablowanie powinno być uporządkowane i umieszczone w szafach. Należy rozważyć umieszczenie wszystkich komputerów w zabezpieczonych szafach i wykorzystanie technologii ekstenderów peryferyjnych w celu podłączenia interfejsów człowiek-maszyna do komputerów w szafach.

- **Systemy monitorowania dostępu**. Systemy monitorowania dostępu obejmują kamery fotograficzne i wideo, czujniki oraz różnego rodzaju systemy identyfikacji. Przykładem takich systemów są kamery monitorujące parkingi, sklepy lub terminale linii lotniczych. Urządzenia te nie uniemożliwiają dostępu do danego miejsca, ale rejestrują fizyczną obecność lub brak fizycznej obecności osób, pojazdów, zwierząt i innych obiektów. W zależności od rodzaju zainstalowanego urządzenia monitorującego dostęp, należy zapewnić odpowiednie oświetlenie monitorowanego miejsca.
- **Systemy ograniczające dostęp**. Systemy ograniczające dostęp mogą wykorzystywać kombinację urządzeń do fizycznej kontroli lub zapobiegania dostępowi do chronionych zasobów. Systemy ograniczające dostęp obejmują zarówno aktywne, jak i pasywne urządzenia zabezpieczające, takie jak ogrodzenia, drzwi, sejfy, bramy i osłony. Często są one połączone z systemami identyfikacji i monitorowania, aby zapewnić dostęp do zasobów w oparciu o role przypisane określonym osobom lub grupie osób.
- **Lokalizacja osób i mienia**. Lokalizowanie osób i pojazdów w dużych instalacjach jest ważne ze względów ochronnych, a coraz ważniejsze staje się także ze względów bezpieczeństwa. Technologie lokalizacji zasobów można wykorzystać do śledzenia ruchu osób i pojazdów na terenie obiektu, w celu upewnienia się, że przebywają one w dozwolonych obszarach; identyfikacji personelu wymagającego pomocy; oraz wspierania działań w sytuacjach awaryjnych.

- **Czynniki środowiskowe**. Przy uwzględnianiu potrzeb związanych z bezpieczeństwem systemu i danych ważne jest, aby wziąć pod uwagę czynniki środowiskowe. Na przykład, jeśli w danym miejscu panuje duże zapylenie, systemy powinny być umieszczone w pomieszczeniach posiadających filtry. Jest to szczególnie ważne, jeżeli pył może być przewodnikiem lub magnesem, jak w przypadku zakładów przetwarzających węgiel lub żelazo. Jeżeli problemem mogą być wibracje, systemy należy montować na gumowych tulejach, aby zapobiec awariom dysków i problemom z połączeniami przewodowymi. Ponadto środowiska, w których znajdują się systemy i nośniki (np. taśmy zapasowe, dyskietki), powinny mieć stabilną temperaturę i wilgotność. W przypadku przekroczenia parametrów środowiskowych, takich jak temperatura i wilgotność, powinien być uruchamiany alarm w systemie sterowania procesem.
- **Systemy kontroli środowiska**. Systemy ogrzewania, wentylacji i klimatyzacji (ang. Heating, ventilation, and air conditioning - HVAC) pomieszczeń sterowniczych muszą wspomagać personel obsługujący obiekty podczas normalnej pracy i w sytuacjach awaryjnych, które mogą obejmować emisję substancji toksycznych. Systemy przeciwpożarowe powinny być zaprojektowane tak, aby nie powodować więcej szkód niż pożytku (np. aby uniknąć mieszania wody z nieodpowiednimi substancjami). Systemy HVAC i przeciwpożarowe znacząco zwiększyły swoją rolę w zakresie bezpieczeństwa, co wynika z wzajemnej zależności między sterowaniem procesami a bezpieczeństwem. Na przykład, systemy przeciwpożarowe i HVAC, które wspierają przemysłowe komputery sterujące, muszą być chronione przed cyberincydentami.
- **Zasilanie**. Niezbędne jest zagwarantowanie niezawodnego zasilania systemu ICS, dlatego należy zainstalować zasilacz bezprzerwowy (UPS). Jeżeli w obiekcie znajduje się agregat prądotwórczy, wystarczający czas pracy baterii UPS może wynosić tylko kilka sekund do kilku minut; jeżeli jednak obiekt jest uzależniony od zasilania zewnętrznego, czas pracy na bateriach UPS może wynosić wiele godzin. Zasilacz UPS powinien mieć co najmniej taką pojemność, która pozwoli na bezpieczne wyłączenie systemu.

6.2.11.1. Centrum sterowania/dyspozytornia

Zalecenia i wytyczne dotyczące ICS

Zapewnienie bezpieczeństwa fizycznego w centrum sterowania/dyspozytorni jest niezbędne do ograniczenia możliwości wystąpienia wielu zagrożeń. W centrach sterowania/dyspozytorniach często znajdują się konsole stale zalogowane do głównego serwera sterującego, gdzie szybkość reakcji i ciągły podgląd instalacji ma ogromne znaczenie. W tych obszarach często znajdują się same serwery, inne krytyczne węzły komputerowe, a czasem także sterowniki instalacji. Istotne jest, aby dostęp do tych obszarów był ograniczony tylko do uprawnionych użytkowników, przy użyciu metod uwierzytelniania, takich jak inteligentne lub magnetyczne karty identyfikacyjne lub urządzenia biometryczne. W skrajnych przypadkach może być konieczne wykonanie centrum sterowania/dyspozytorni w sposób odporny na eksplozje lub zapewnienie awaryjnego centrum sterowania/dyspozytorni poza stałą lokalizacją, tak, aby można było utrzymywać sterowanie, jeśli główne centrum sterowania/dyspozytornia staje się bezużyteczne.

6.2.11.2. Urządzenia przenośne

Zalecenia i wytyczne dotyczące ICS

Komputery i urządzenia komputerowe wykorzystywane do wykonywania funkcji systemu ICS (takich jak programowanie sterowników PLC) nie powinny nigdy być przenoszone poza obszar systemu ICS. Laptopy, przenośne inżynierskie stacje robocze i urządzenia podręczne (np. komunikator polowy HART 375) powinny być odpowiednio zabezpieczone i nigdy nie powinny być używane poza siecią ICS. Programy antywirusowe i zarządzania poprawkami powinny być na bieżąco aktualizowane.

6.2.11.3. Okablowanie

Zalecenia i wytyczne dotyczące ICS

W celu zapewnienia ochrony przed wilgocią, pyłem i wibracjami należy stosować przemysłowe złącza RJ-45. W przypadku sieci sterowania często lepszym wyborem okablowania sieciowego jest kabel światłowodowy i kabel koncentryczny, ponieważ są

one odporne na wiele typowych warunków środowiskowych, w tym zakłócenia elektryczne i radiowe występujące w środowisku sterowania przemysłowego. Kable i złącza powinny być oznaczone kolorami i etykietami, aby sieci ICS i IT były wyraźnie rozgraniczone oraz aby zmniejszyć możliwość niezamierzonego połączenia krzyżowego. Ciągi kablowe powinny być zainstalowane w taki sposób, aby dostęp do nich był ograniczony do minimum (tzn. tylko dla upoważnionego personelu), a sprzęt powinien być zainstalowany w zamkniętych szafach z odpowiednią wentylacją i filtracją powietrza.

6.2.12. Planowanie

Plan bezpieczeństwa jest formalnym dokumentem, który przedstawia przegląd wymagań bezpieczeństwa dla systemu informacyjnego oraz opisuje istniejące lub planowane zabezpieczenia, mające na celu spełnienie tych wymagań. Zabezpieczenia, które należą do kategorii Planowanie – PL, stanowią podstawę do opracowania planu ochrony. Zabezpieczenia te dotyczą również kwestii utrzymaniowych, czyli okresowej aktualizacji planu bezpieczeństwa. Zbiór zasad opisuje obowiązki użytkownika i oczekiwane zachowanie w odniesieniu do korzystania z systemu informacyjnego, przy czym przed udzieleniem dostępu do systemu informacyjnego użytkownicy muszą podpisać oświadczenie, że przeczytali, zrozumieli i zgadzają się przestrzegać zasad postępowania.

Uzupełniające rekomendacje dotyczące zabezpieczeń PL można znaleźć w następujących publikacjach:

- NSC SP 800-18, zawierającym wskazówki dotyczące przygotowania reguł zachowania (bazującym na publikacji specjalnej NIST SP 800-18 [19]).
- NIST SP 800-100 ,zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].

Zalecenia i wytyczne dotyczące ICS

Plan bezpieczeństwa systemu ICS powinien opierać się na odpowiednich istniejących doświadczeniach, programach i praktykach w zakresie bezpieczeństwa IT. Jednak krytyczne różnice pomiędzy IT a ICS omówione w sekcji 2.4, będą miały wpływ na to,

w jaki sposób zabezpieczenia będą stosowane w ICS. Plan perspektywiczny jest niezbędny, aby zapewnić metodę ciągłego usprawniania bezpieczeństwa. W każdej fazie projektowania i instalowania nowego systemu, konieczne jest poświęcenie czasu na uwzględnienie kwestii bezpieczeństwa w całym cyklu życia systemu, od architektury, poprzez zamówienia, instalację, konserwację, aż po wycofanie z eksploatacji. Bezpieczeństwo ICS to szybko rozwijająca się dziedzina, która wymaga, aby w procesie planowania bezpieczeństwa stale badać pojawiające się możliwości w zakresie bezpieczeństwa ICS oraz nowe zagrożenia identyfikowane przez organizacje takie jak ICS-CERT.

6.2.13. Bezpieczeństwo osobowe

Zabezpieczenia należące do kategorii Bezpieczeństwo osobowe – PS, określają zasady i procedury mające na celu zmniejszenie ryzyka wystąpienia błędu ludzkiego, kradzieży, oszustwa lub innego zamierzonego lub niezamierzonego niewłaściwego wykorzystania systemów informacyjnych.

Uzupełniające rekomendacje dotyczące zabezpieczeń PS można znaleźć w następujących publikacjach:

- NIST SP 800-35, zawierającej wytyczne dotyczące usług bezpieczeństwa technologii informacyjnych [44].
- NIST SP 800-73, zawierającej wytyczne dotyczące interfejsów do weryfikacji tożsamości osobistej [49].
- NIST SP 800-76, zawierającej wytyczne dotyczące biometrii do weryfikacji tożsamości osób [50].
- NIST SP 800-100, zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].

Środki bezpieczeństwa odnoszące się do personelu mają na celu zmniejszenie ryzyka wystąpienia błędu ludzkiego, kradzieży, oszustwa lub innego zamierzonego lub niezamierzonego niewłaściwego wykorzystania zasobów informacyjnych.

Istnieją trzy główne aspekty bezpieczeństwa personelu:

- **Zasady zatrudniania.** Obejmują one postępowanie sprawdzające przed zatrudnieniem, takie jak sprawdzanie przeszłości, rozmowę kwalifikacyjną, określenie warunków zatrudnienia, pełny opis stanowiska pracy i wyszczególnienie obowiązków, warunków zatrudnienia oraz praw i obowiązków pracowników i wykonawców.
- **Polityki i praktyki organizacji.** Obejmują one politykę bezpieczeństwa, klasyfikację informacji, politykę utrzymania i obsługi dokumentów i nośników, szkolenia użytkowników, politykę akceptowalnego użytkowania zasobów organizacji, okresowe oceny wydajności pracowników, odpowiednie sprawdzanie przeszłości oraz wszelkie inne polityki i działania, które szczegółowo opisują oczekiwane i wymagane zachowania pracowników organizacji, wykonawców i gości. Polityka organizacji, która ma być egzekwowana, powinna być opisana i łatwo dostępna dla wszystkich pracowników w formie podręcznika pracowniczego, rozpowszechniane jako powiadomienia pocztą elektroniczną, umieszczone w scentralizowanym obszarze zasobów lub wywieszone bezpośrednio w miejscu, za które pracownik jest odpowiedzialny.
- **Zasady i warunki zatrudnienia.** Kategoria ta obejmuje obowiązki związane z pracą i stanowiskiem, informowanie pracowników o naruszeniach dających podstawę do rozwiązania stosunku pracy, działania dyscyplinarne i kary oraz okresowe oceny wyników pracy pracowników.

Zalecenia i wytyczne dotyczące ICS

Stanowiska powinny być podzielone na kategorie ze wskazaniem ryzyka i kryteriów weryfikacji, a osoby obsadzone na danym stanowisku powinny być sprawdzone pod kątem tych kryteriów. Przed uzyskaniem dostępu do systemu informacyjnego należy również zawrzeć umowę o dostępie. Personel powinien być sprawdzany pod kątem możliwości zajmowania krytycznych stanowisk związanych z nadzorowaniem i utrzymaniem systemu ICS.

Ponadto należy starannie opracować programy szkoleniowe, aby upewnić się, że każdy pracownik przeszedł szkolenie istotne i niezbędne do wykonywania swoich zadań.

Dodatkowo należy upewnić się, że pracownicy wykazują się kompetencjami w zakresie wykonywanych przez siebie zadań.

6.2.14. Szacowanie ryzyka

Zabezpieczenia wchodzące w skład kategorii Szacowanie ryzyka – RA, określają zasady i procedury opracowywania, rozpowszechniania i utrzymywania udokumentowanej polityki szacowania ryzyka, która opisuje cel, zakres, role, obowiązki i zgodność, a także procedury wdrażania polityki. System informacyjny i związane z nim dane są kategoryzowane w oparciu o atrybuty bezpieczeństwa i zakres poziomów ryzyka. Szacowanie ryzyka przeprowadza się w celu określenia zagrożeń i skali szkód, jakie mogą wyniknąć z nieuprawnionego dostępu, wykorzystania, ujawnienia, zakłócenia, modyfikacji lub zniszczenia systemu informacyjnego i danych. Zabezpieczenia te obejmują również mechanizmy utrzymywania aktualnych szacowań ryzyka oraz przeprowadzania okresowych testów i ocen podatności.

Uzupełniające rekomendacje dotyczące zabezpieczeń RA można znaleźć w następujących publikacjach:

- NSC 800-30, zawierającym wskazówki dotyczące przeprowadzania szacowania ryzyka i aktualizacji.
- NSC 800-39, zawierającym wskazówki dotyczące zarządzania ryzykiem na wszystkich poziomach organizacyjnych.
- NIST SP 800-40, zawierającej wytyczne dotyczące obsługi poprawek bezpieczeństwa [40].
- NIST SP 800-115, zawierającej wytyczne dotyczące testowania bezpieczeństwa sieci [41].
- NSC SP 800-60, zawierającym wskazówki dotyczące określania kategorii bezpieczeństwa dla danych typów informacji [25].
- NIST SP 800-100, zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].

Zalecenia i wytyczne dotyczące ICS

Organizacje muszą brać pod uwagę potencjalne konsekwencje wynikające z incydentu w systemie ICS. Dobrze zdefiniowane polityki i procedury umożliwiają zastosowanie technik ograniczania skutków, które mają na celu udaremnienie incydentów i zarządzanie ryzykiem w celu wyeliminowania lub zminimalizowania ich konsekwencji. Potencjalne pogorszenie stanu fizycznego obiektu, statusu ekonomicznego lub zaufania interesariuszy/kraju może uzasadniać zastosowanie środków zaradczych.

W przypadku ICS, bardzo ważnym aspektem szacowania ryzyka jest określenie wartości danych, które przepływają z sieci sterowania do sieci korporacyjnej. W przypadkach, gdy na podstawie tych danych podejmowane są decyzje finansowe, dane te mogą mieć bardzo istotną wartość. Uzasadnienie fiskalne dla łagodzenia skutków musi być wyprowadzone poprzez porównanie kosztów łagodzenia skutków do konsekwencji skutków. Nie jest jednak możliwe zdefiniowanie jednego uniwersalnego zestawu wymogów bezpieczeństwa. Bardzo wysoki poziom bezpieczeństwa może być osiągalny, ale w wielu sytuacjach niepożądany ze względu na utratę funkcjonalności i inne związane z tym koszty. Dobrze przemyślane wdrożenie bezpieczeństwa jest równowagą pomiędzy ryzykiem a kosztami. W niektórych sytuacjach ryzyko może być związane z bezpieczeństwem, zdrowiem lub środowiskiem, a nie mieć charakter czysto ekonomiczny. Ryzyko może spowodować nieodwracalne skutki, a nie tymczasowe niepowodzenie finansowe.

6.2.15. Nabywanie systemu i usług

Zabezpieczenia wchodzące w skład kategorii nabywanie systemu i usług – SA, stanowią podstawę do opracowania polityki i procedur nabywania zasobów niezbędnych do właściwej ochrony systemu informacyjnego. Zakupy te opierają się na wymaganiach bezpieczeństwa i specyfikacjach bezpieczeństwa. W ramach procedur akwizycji, system informacyjny jest zarządzany z wykorzystaniem metodologii cyklu życia systemu, która uwzględnia kwestie bezpieczeństwa informacji. W ramach nabywania należy prowadzić odpowiednią dokumentację dotyczącą systemu informacyjnego i jego elementów składowych.

Kategoria SA dotyczy również systemów zlecanych na zewnątrz oraz włączenia przez sprzedawców odpowiednich zabezpieczeń określonych przez wspieraną organizację. Sprzedawcy są również odpowiedzialni za zarządzanie konfiguracją i testowanie bezpieczeństwa tych zleconych na zewnątrz systemów informacyjnych.

Wytyczne uzupełniające dotyczące zabezpieczeń SA można znaleźć w następujących publikacjach:

- NIST SP 800-23, zawierającej wytyczne dotyczące pozyskiwania i wykorzystywania przetestowanych/ocenionych produktów technologii informacyjnej [42].
- NIST SP 800-27, zawierającej wytyczne dotyczące zasad inżynierii bezpieczeństwa systemów informacyjnych [43].
- NIST SP 800-35, zawierającej wytyczne dotyczące usług bezpieczeństwa technologii informacyjnych [44].
- NIST SP 800-36, zawierającej wytyczne dotyczące wyboru produktów bezpieczeństwa informacji [45].
- NIST SP 800-64, zawierającej wytyczne dotyczące rozważań nad bezpieczeństwem w cyklu życia systemu [46].
- NIST SP 800-65, zawierającej wytyczne dotyczące włączania bezpieczeństwa do procesu planowania kapitałowego i kontroli inwestycji [47].
- NIST SP 800-70, zawierającej wytyczne dotyczące ustawień konfiguracyjnych dla produktów technologii informacyjnych [26].
- NIST SP 800-100, zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].

Zalecenia i wytyczne dotyczące ICS

Wymagania dotyczące bezpieczeństwa organizacji zlecającej na zewnątrz zarządzanie i kontrolę wszystkich lub niektórych swoich systemów informacyjnych, sieci i środowisk komputerowych powinny być określone w umowie uzgodnionej między stronami. Dostawcy zewnętrzni, którzy mają wpływ na bezpieczeństwo organizacji, muszą być objęci tymi samymi politykami i procedurami bezpieczeństwa, aby utrzymać

ogólny poziom bezpieczeństwa ICS. Polityki i procedury bezpieczeństwa dostawców drugiego i trzeciego szczebla powinny być również zgodne z korporacyjnymi politykami i procedurami cyberbezpieczeństwa w przypadku, gdy mają one wpływ na bezpieczeństwo ICS.

Przykładowy dokument służący do określania wymogów bezpieczeństwa przy zamawianiu nowych systemów lub utrzymania istniejących, przedstawiono w Załączniku F, Referencje, w pozycji [48].

6.2.16. Ochrona systemów i sieci telekomunikacyjnych

Zabezpieczenia należące do kategorii Ochrona systemów i sieci telekomunikacyjnych - SC, określają politykę i procedury ochrony systemów i komponentów telekomunikacyjnych.

Wytyczne uzupełniające dotyczące zabezpieczeń SC można znaleźć w następujących publikacjach:

- NIST SP 800-28, zawierającej wytyczne dotyczące aktywnego kontentu i kodu mobilnego [69].
- NIST SP 800-52, zawierającej wytyczne dotyczące implementacji Transport Layer Security (TLS) [70].
- NIST SP 800-56, zawierającej wytyczne dotyczące generowania kluczy kryptograficznych [71].
- NIST SP 800-57, zawierającej wytyczne dotyczące zarządzania kluczami kryptograficznymi [72].
- NIST SP 800-58, zawierającej wytyczne dotyczące rozważań nad bezpieczeństwem technologii VoIP [73].
- NIST SP 800-63, zawierającej wytyczne dotyczące zdalnego uwierzytelniania elektronicznego [53].
- NIST SP 800-77, zawierającej wytyczne dotyczące sieci VPN IPsec [74].

6.2.16.1. Szyfrowanie

Szyfrowanie jest kryptograficznym przekształceniem danych (zwanych tekstem jawnym) w formę, zwaną szyfrogramem, która ukrywa oryginalne znaczenie danych, aby uniemożliwić ich poznanie lub wykorzystanie. Jeśli transformacja jest odwracalna, odpowiadający jej proces odwracania nazywany jest deszyfrowaniem, czyli transformacją, która przywraca zaszyfrowane dane do ich pierwotnego stanu [75].

Zalecenia i wytyczne dotyczące ICS

Przed wdrożeniem szyfrowania należy najpierw ustalić, czy szyfrowanie jest odpowiednim rozwiązaniem dla konkretnego zastosowania ICS, ponieważ uwierzytelnianie i integralność są na ogół kluczowymi kwestiami bezpieczeństwa w zastosowaniach ICS. Należy również rozważyć inne rozwiązania kryptograficzne, takie jak hasze kryptograficzne.

Stosowanie szyfrowania w środowisku ICS może powodować opóźnienia w komunikacji ze względu na dodatkowy czas i zasoby obliczeniowe wymagane do zaszyfrowania, odszyfrowania i uwierzytelnienia każdego komunikatu. W przypadku ICS wszelkie opóźnienia wynikające z zastosowania szyfrowania lub jakiejkolwiek innej techniki zabezpieczeń nie mogą obniżać wydajności operacyjnej urządzenia lub systemu końcowego. Przed wdrożeniem szyfrowania w środowisku ICS, planowane do wdrożenia rozwiązania powinny zostać poddane szczegółowym testom wydajności. Należy rozważyć szyfrowanie w warstwie 2 OSI, a nie w warstwie 3, aby zmniejszyć opóźnienia w szyfrowaniu.

Ponadto zaszyfrowane wiadomości są często obszerniejsze niż wiadomości niezaszyfrowane, z powodu wystąpienia co najmniej jednego z poniższych czynników:

- Dodatkowe sumy kontrolne zmniejszające liczby błędów.
- Protokoły kontrolujące kryptografię.
- Wypełnianie (w przypadku szyfrów blokowych).
- Procedury uwierzytelniania.
- Inne wymagane procesy kryptograficzne.

Kryptografia wprowadza również zagadnienia związane z zarządzaniem kluczami. Rozsądna polityka bezpieczeństwa wymaga okresowych zmian kluczy. Proces ten staje się coraz trudniejszy wraz ze wzrostem geograficznego rozmiaru ICS, czego najbardziej dotkliwym przykładem są rozległe systemy SCADA. Ponieważ wizyty na miejscu w celu zmiany kluczy mogą być kosztowne i powolne, przydatna jest możliwość zdalnej zmiany kluczy. Jeśli wybrano kryptografię, najskuteczniejszym zabezpieczeniem jest stosowanie kompletnego systemu kryptograficznego zatwierdzonego przez stosowną krajową władzę bezpieczeństwa. W ramach tego programu utrzymywane są standardy zapewniające, że systemy kryptograficzne zostały dokładnie zbadane pod kątem słabych punktów przez szerokie grono ekspertów, a nie zostały opracowane przez kilku inżynierów z jednej organizacji. Certyfikacja pozwala co najmniej uprawdopodobnić, że:

- Zostanie zastosowana metoda (np. tryb licznika) w celu zapewnienia, że ten sam komunikat nie będzie generował za każdym razem tej samej wartości.
- Komunikaty ICS są zabezpieczone przed powtórzeniem i fałszowaniem.
- Zarządzanie kluczami jest bezpieczne przez cały cykl życia klucza.
- System korzysta z efektywnego generatora liczb losowych.
- Cały system został wdrożony w bezpieczny sposób.

Nawet w takim przypadku technologia jest skuteczna tylko wtedy, gdy stanowi integralną część skutecznie wdrożonej polityki bezpieczeństwa informacji. Raport 12-1 [5] Amerykańskiego Stowarzyszenia Gazowniczego (AGA) zawiera przykład takiej polityki bezpieczeństwa. Chociaż jest on skierowany do systemu SCADA gazu ziemnego, wiele z jego zaleceń można zastosować do dowolnego ICS.

W przypadku ICS szyfrowanie można wdrożyć jako część kompleksowej, wymuszonej polityki bezpieczeństwa. Organizacje powinny wybrać ochronę kryptograficzną na podstawie oceny ryzyka i zidentyfikowanej wartości chronionych informacji oraz ograniczeń operacyjnych ICS. W szczególności klucz kryptograficzny powinien być na tyle długi, aby jego odgadnięcie lub określenie w drodze analizy wymagało więcej wysiłku, czasu i kosztów niż wartość chronionego zasobu.

Sprzęt szyfrujący powinien być zabezpieczony przed fizyczną ingerencją i niekontrolowanymi połączeniami elektronicznymi. Zakładając, że kryptografia jest odpowiednim rozwiązaniem, organizacje powinny wybrać ochronę kryptograficzną ze zdalnym zarządzaniem kluczami, jeśli chronione jednostki są tak liczne lub rozproszone geograficznie, że zmiana kluczy jest trudna lub kosztowna.

Należy używać oddzielnych portów tekstu jawnego i szyfrującego, chyba że sieć bezwzględnie wymaga ograniczenia do przepuszczania zarówno tekstu jawnego, jak i szyfrującego przez każdy port.

Należy używać wyłącznie modułów, które mogą uzyskać certyfikat zgodności, np. ze standardem, takim jak FIPS 140-2 [90], w ramach programu walidacji modułów kryptograficznych (*ang. Cryptographic Module Validation Program - CMVP*).

6.2.16.2. Wirtualna sieć prywatna (VPN)

Jedną z metod szyfrowania danych telekomunikacyjnych jest VPN, czyli sieć prywatna, która działa jako nakładka na infrastrukturę publiczną, dzięki czemu sieć prywatna może funkcjonować w sieci publicznej. Najpopularniejsze rodzaje technologii VPN stosowane obecnie to:

- **Bezpieczny protokół internetowy (*ang. Internet Protocol Security - IPsec*).**[32] IPsec to zestaw standardów zdefiniowanych przez IETF (*Internet Engineering Task Force*) w celu regulowania bezpiecznej komunikacji danych w sieciach publicznych w warstwie IP. IPsec jest integralną częścią wielu obecnych systemów operacyjnych. Intencją standardów jest zagwarantowanie interoperacyjności między platformami producentów; w rzeczywistości jednak określenie interoperacyjności implementacji wielu producentów zależy od konkretnych testów wdrożeniowych przeprowadzonych przez organizację użytkownika końcowego. IPsec obsługuje dwa tryby szyfrowania: transportowy i tunelowy. Tryb transportowy szyfruje tylko część danych (payload) każdego pakietu, pozostawiając niezmieniony nagłówek. Bardziej bezpieczny tryb tunelowy dodaje nowy nagłówek do każdego pakietu i szyfruje

[32] NIST SP 800-77 zawiera wytyczne dotyczące IPsec VPN [74].

zarówno oryginalny nagłówek, jak i zawartość. Po stronie odbiorczej urządzenie zgodne z protokołem IPsec odszyfrowuje każdy pakiet. Protokół ten jest stale udoskonalany w celu spełnienia specyficznych wymagań, takich jak rozszerzenia protokołu dotyczące uwierzytelniania poszczególnych użytkowników oraz przechodzenia przez urządzenia NAT. Rozszerzenia te są zwykle specyficzne dla producenta i mogą prowadzić do problemów z interoperacyjnością, głównie w środowiskach hosta bramy bezpieczeństwa.

- **Secure Sockets Layer (SSL).**[33] SSL zapewnia bezpieczny kanał pomiędzy dwoma urządzeniami, który szyfruje zawartość każdego pakietu. IETF wprowadził niewielkie modyfikacje do protokołu SSL w wersji 3 i stworzył nowy protokół o nazwie Transport Layer Security (TLS). Terminy "SSL" i "TLS" są często używane zamiennie, a w tej publikacji ogólnie używana jest terminologia SSL. SSL jest najczęściej znany z zabezpieczania ruchu HTTP; ta implementacja protokołu jest znana jako HTTP Secure (HTTPS). SSL nie jest jednak ograniczony do ruchu HTTP; może być wykorzystywany do zabezpieczania wielu różnych programów warstwy aplikacji. Produkty VPN oparte na protokole SSL zyskały akceptację dzięki rynkowi "bezklientowych" produktów VPN. Produkty te wykorzystują jako klientów standardowe przeglądarki internetowe, które mają wbudowaną obsługę SSL. Termin "bezklientowy" oznacza, że nie ma potrzeby instalowania lub konfigurowania oprogramowania "klienckiego" VPN firm trzecich na systemach użytkowników.
- **Secure Shell (SSH).** SSH jest interfejsem poleceń i protokołem służącym do bezpiecznego uzyskiwania dostępu do zdalnego komputera. Jest on powszechnie używany przez administratorów sieci do zdalnego kontrolowania serwerów WWW i innych typów serwerów. Najnowsza wersja, SSH2, jest proponowanym przez IETF zestawem standardów. Zazwyczaj SSH jest wdrażany jako bezpieczna alternatywa dla aplikacji telnet. SSH jest dołączany do większości dystrybucji UNIX-a, a na innych platformach jest zazwyczaj dodawany poprzez pakiety firm trzecich.

[33] NIST SP 800-52 zawiera wytyczne dotyczące konfiguracji SSL [70].

Zalecenia i wytyczne dotyczące ICS

Sieci VPN są najczęściej używane w środowisku ICS w celu zapewnienia bezpiecznego dostępu z niezaufanej sieci do sieci sterowania ICS. Niezaufane sieci mogą obejmować zarówno Internet, jak i firmową sieć LAN. Odpowiednio skonfigurowane sieci VPN mogą znacznie ograniczyć dostęp do/z komputerów głównych i kontrolerów systemu sterowania, zwiększając w ten sposób bezpieczeństwo. Mogą także potencjalnie poprawić szybkość reakcji sieci sterowania poprzez usunięcie z sieci pośredniczącej nieautoryzowanego ruchu, który nie jest niezbędny.

Inne możliwe wdrożenia obejmują wykorzystanie bramek bezpieczeństwa opartych na hoście lub mini samodzielnych bramek bezpieczeństwa, umieszczonych przed poszczególnymi urządzeniami sterującymi lub działających na nich. Ta technika wdrażania sieci VPN na bazie pojedynczych urządzeń może wiązać się ze znacznymi kosztami administracyjnymi.

Urządzenia VPN używane do ochrony systemów sterowania powinny być dokładnie przetestowane w celu sprawdzenia, czy technologia VPN jest zgodna z daną aplikacją i czy wdrożenie urządzeń VPN nie wpływa w niedopuszczalny sposób na charakterystykę ruchu sieciowego.

6.2.17. Integralność systemu i informacji

Utrzymanie integralności systemu i informacji zapewnia, że dane wrażliwe nie zostały zmodyfikowane lub usunięte w sposób nieuprawniony i niewykryty. Zabezpieczenia należące do kategorii Integralność systemu i informacji – SI, określają zasady i procedury identyfikowania, raportowania i korygowania wad systemu informacyjnego. Istnieją zabezpieczenia pozwalające na wykrywanie złośliwych kodów, ochrony przed spamem i oprogramowaniem szpiegującym oraz wykrywania włamań, chociaż mogą one nie być odpowiednie dla wszystkich aplikacji ICS. Uwzględniono również środki bezpieczeństwa służące do otrzymywania alertów i ostrzeżeń dotyczących bezpieczeństwa oraz do weryfikacji funkcji bezpieczeństwa w systemie informacyjnym. Ponadto w tej grupie zabezpieczeń znajdują się środki bezpieczeństwa mające na celu wykrywanie i ochronę przed nieuprawnionymi zmianami

oprogramowania i danych, ograniczenia dotyczące wprowadzania i wyprowadzania danych oraz sprawdzania dokładności, kompletności i ważności danych, a także obsługi stanów awaryjnych. Środki te mogą jednak nie być odpowiednie dla wszystkich aplikacji ICS.

Uzupełniające rekomendacje dotyczące zabezpieczeń SI można znaleźć w następujących publikacjach:

- NIST SP 800-40, zawierającej wytyczne dotyczące instalacji poprawek bezpieczeństwa [40].
- NIST SP 800-94, zawierającej wytyczne dotyczące systemów wykrywania i zapobiegania włamaniom (*Intrusion Detection and Prevention - IDP*) [55].
- NIST SP 800-100, zawierającej wytyczne dotyczące zarządzania i planowania bezpieczeństwa informacji [27].

Zalecenia i wytyczne dotyczące ICS

Dostępne są zabezpieczenia służące do wykrywania złośliwego kodu, ochrony przed spamem i oprogramowaniem szpiegującym oraz wykrywania włamań, chociaż mogą one nie być odpowiednie dla wszystkich aplikacji ICS.

6.2.17.1. Wykrywanie wirusów i złośliwego kodu

Produkty antywirusowe i wykrywania złośliwego kodu porównują pliki zapisane na urządzeniach pamięci masowej komputera z wykazem znanych sygnatur plików złośliwego oprogramowania. Jeśli któryś z plików na komputerze odpowiada profilowi znanego wirusa, jest on usuwany w procesie „dezynfekcji” (np. kwarantanna, usuwanie), aby nie mógł zainfekować innych plików lokalnych lub komunikować się przez sieć w celu zainfekowania innych plików. Oprogramowanie antywirusowe może być wdrażane na stacjach roboczych, serwerach, zaporach sieciowych i urządzeniach przenośnych.

Zalecenia i wytyczne dotyczące ICS

Narzędzia antywirusowe działają skutecznie wyłącznie wtedy, gdy są zainstalowane, skonfigurowane, działają w pełnym wymiarze godzin i są odpowiednio aktualizowane

na podstawie znanych metod ataków i środków ataku. Chociaż narzędzia antywirusowe są powszechnie stosowane w systemach informacyjnych, ich użycie w systemach ICS może wymagać przyjęcia specjalnych praktyk, obejmujących sprawdzanie kompatybilności, kwestie zarządzania zmianami oraz pomiary wpływu na wydajność. Te specjalne praktyki powinny być stosowane za każdym razem, gdy instalowane są nowe sygnatury lub nowe wersje oprogramowania antywirusowego.

Główni producenci systemów ICS zalecają, a nawet wspierają stosowanie określonych narzędzi antywirusowych. W niektórych przypadkach producenci systemów sterowania mogą przeprowadzać testy regresji dla całej linii swoich produktów pod kątem obsługiwanych wersji danego narzędzia antywirusowego, a także dostarczać związaną z nim dokumentację instalacyjną i konfiguracyjną. Podejmowane są również wysiłki w celu opracowania ogólnego zestawu wskazówek i procedur testowych koncentrujących się na wpływie na wydajność systemów ICS, aby wypełnić luki tam, gdzie nie są dostępne wytyczne dostawców systemów ICS i antywirusów [56].

Ogólnie:

- Systemy Windows, Unix, Linux itp. używane jako konsole, inżynierskie stacje robocze, historiany, HMI oraz serwery SCADA i serwery zapasowe ogólnego przeznaczenia można zabezpieczyć tak samo, jak komercyjny sprzęt IT: zainstalować oprogramowanie antywirusowe i zarządzające poprawkami w sposób automatyczny lub „push”, z aktualizacjami rozprowadzanymi za pośrednictwem serwera antywirusowego i serwera zarządzającego poprawkami znajdującego się wewnątrz sieci sterowania procesami i autoaktualizowanego z sieci IT.
- Należy postępować zgodnie z zaleceniami producenta w przypadku wszystkich innych serwerów i komputerów (DCS, PLC, przyrządy), które mają kod zależny od czasu, zmodyfikowany lub rozszerzony system operacyjny lub jakiekolwiek inne zmiany, które odróżniają je od standardowych komputerów PC. Należy oczekiwać, że dostawca będzie okresowo wydawał wersje aktualizujące zawierające poprawki bezpieczeństwa.

6.2.17.2. Wykrywanie i zapobieganie włamaniom

Systemy wykrywania włamań (IDS) monitorują zdarzenia w sieci, takie jak wzorce ruchu lub w systemie, takie jak wpisy w dzienniku lub dostęp do plików, dzięki czemu mogą zidentyfikować intruza włamującego się lub próbującego włamać się do systemu [57]. Systemy IDS zapewniają, że nietypowe działania, takie jak nowe otwarte porty, nietypowe wzorce ruchu lub zmiany w krytycznych plikach systemu operacyjnego są zgłaszane odpowiednim pracownikom ochrony. Dwa najczęściej stosowane typy IDS to:

- **Sieciowe systemy IDS.** Systemy te monitorują ruch sieciowy i generują alarmy w przypadku zidentyfikowania ruchu, który uznają za atak.
- **Systemy IDS na hoście (*ang. -Based IDS*).** Oprogramowanie to monitoruje jeden lub więcej rodzajów charakterystyk systemu, takich jak wpisy w plikach dziennika aplikacji, zmiany konfiguracji systemu oraz dostęp do wrażliwych danych w systemie i reaguje alarmem lub środkiem zaradczym w przypadku próby naruszenia bezpieczeństwa przez użytkownika.

Zalecenia i wytyczne dotyczące ICS

Skuteczne wdrażanie systemów IDS zazwyczaj obejmuje zarówno systemy IDS oparte na hoście, jak i na sieci. W obecnym środowisku ICS systemy IDS oparte na sieci są najczęściej rozmieszczane między siecią sterowania a siecią korporacyjną w połączeniu z zaporą sieciową; systemy IDS oparte na hoście są najczęściej rozmieszczane na komputerach korzystających z systemów operacyjnych ogólnego przeznaczenia lub aplikacji, takich jak panele operatorskie, serwery SCADA i inżynierskie stacje robocze. Odpowiednio skonfigurowany system IDS może znacznie zwiększyć zdolność zespołu zarządzającego bezpieczeństwem do wykrywania ataków wchodzących do systemu lub wychodzących z niego, a tym samym poprawić bezpieczeństwo. Mogą również potencjalnie poprawić wydajność sieci sterowania, wykrywając ruch w sieci, który nie jest niezbędny. Jednak nawet po wdrożeniu systemów IDS, to przede wszystkim pracownicy ochrony mogą rozpoznawać pojedyncze ataki, a nie już znane wzorce ataków. Monitorowanie bezpieczeństwa sieci i zrozumienie normalnego stanu sieci ICS

może pomóc w odróżnieniu ataków od stanów przejściowych, a także w wyzwalaniu i dostarczaniu informacji o zdarzeniach, które wykraczają poza normalny stan.

Obecne produkty IDS i IPS są skuteczne w wykrywaniu i zapobieganiu dobrze znanych ataków internetowych, ale do niedawna nie zajmowały się atakami na protokoły ICS. Producenci systemów IDS i IPS zaczynają opracowywać i wprowadzać sygnatury ataków dla różnych protokołów ICS, takich jak Modbus, DNP3 i ICCP [58].

6.2.17.3. Zarządzanie poprawkami

Poprawki[34] to dodatkowe fragmenty kodu, które zostały opracowane w celu rozwiązania konkretnych problemów lub błędów w istniejącym oprogramowaniu. Podatności to błędy, które mogą zostać wykorzystane, umożliwiając nieautoryzowany dostęp do systemów informacyjnych lub umożliwiając użytkownikom uzyskanie większych uprawnień niż te, do których zostali upoważnieni.

Systematyczne podejście do zarządzania i używania poprawek oprogramowania może pomóc organizacjom w poprawie ogólnego bezpieczeństwa ich systemów IT w sposób efektywny kosztowo. Organizacje, które aktywnie zarządzają i używają poprawek oprogramowania, mogą zmniejszyć szanse na wykorzystanie podatności w swoich systemach informacyjnych; ponadto, mogą zaoszczędzić czas i pieniądze, które musiałyby zostać wydane na reagowanie na incydenty związane z podatnościami.

Publikacja specjalna NIST SP 800-40 [40] zawiera wytyczne dla organizacyjnych menedżerów bezpieczeństwa, którzy są odpowiedzialni za projektowanie i wdrażanie programów zarządzania poprawkami bezpieczeństwa i podatnościami oraz za testowanie skuteczności tych programów w celach redukcji podatności. Wskazówki te są również przydatne dla administratorów systemów i personelu operacyjnego, który jest odpowiedzialny za stosowanie i testowanie poprawek oraz za wdrażanie mechanizmów rozwiązywania problemów związanych z podatnościami.

[34] W potocznym języku technicznym – *łaty*.

Zalecenia i wytyczne dotyczące ICS

Stosowanie poprawek do składników systemu operacyjnego to kolejna sytuacja, w której w środowisku ICS należy zachować szczególną ostrożność. Poprawki powinny być odpowiednio przetestowane (np. W trybie off-line na porównywalnym funkcjonalnie systemie ICS) w celu określenia dopuszczalności efektów ubocznych. Zalecane jest przeprowadzenie testów regresji. Nierzadko zdarza się, że poprawki mają niekorzystny wpływ na inne oprogramowanie. Łata może usunąć lukę, ale może też wprowadzić większe ryzyko z punktu widzenia produkcji lub bezpieczeństwa. Łata może również zmienić sposób współpracy systemu operacyjnego lub aplikacji z aplikacjami sterującymi, powodując utratę części funkcjonalności aplikacji sterujących. Innym problemem jest to, że wiele systemów ICS wykorzystuje starsze wersje systemów operacyjnych, które nie są już wspierane przez producenta. W związku z tym, dostępne poprawki mogą nie mieć zastosowania. Organizacje powinny wdrożyć systematyczny, odpowiedzialny i udokumentowany proces zarządzania poprawkami systemów ICS w celu zarządzania narażeniem na podatności.

Po podjęciu decyzji o wdrożeniu poprawki, istnieją inne narzędzia, które automatyzują ten proces ze scentralizowanego serwera i z potwierdzają, że poprawka została wdrożona poprawnie. Należy rozważyć oddzielenie zautomatyzowanego procesu zarządzania poprawkami w ICS od zautomatyzowanego procesu zarządzania aplikacjami nie związanymi z ICS. Wprowadzanie poprawek powinno być zaplanowane w czasie planowanych przestojów w systemach ICS.

6.2.18. Programy zarządzania

Zabezpieczenia zgrupowane w kategorii Programy zarządzania – PM, koncentrują się na wymaganiach dotyczących bezpieczeństwa informacji w całej organizacji, które są niezależne od konkretnego systemu informacyjnego i są niezbędne do zarządzania programami bezpieczeństwa informacji.

Organizacje dokumentują zabezpieczenia dotyczące programów zarządzania w planie programu bezpieczeństwa informacji. Ogólnoorganizacyjny plan programu bezpieczeństwa informacji uzupełnia indywidualne plany bezpieczeństwa opracowane

dla każdego systemu informacyjnego organizacji. Poza dokumentowaniem zabezpieczeń dotyczących zarządzania programem bezpieczeństwa informacji, plan programu bezpieczeństwa zapewnia organizacji, w centralnym repozytorium, narzędzie do dokumentowania wszystkich zabezpieczeń, które zostały określone jako zabezpieczenia wspólne (tj. zabezpieczenia dziedziczone przez organizacyjne systemy informacyjne).

6.2.19. Ochrona prywatności

Ochrona prywatności informacji umożliwiających identyfikację osób (*ang. personally identifiable information - PII*) gromadzonych, wykorzystywanych, przechowywanych, udostępnianych i usuwanych przez programy i systemy informacyjne ma zasadnicze znaczenie ze względu na postęp w technologiach informacyjnych i zastosowaniach tych technologii. Skuteczna ochrona prywatności osób fizycznych zależy od zabezpieczeń stosowanych w ramach organizacyjnych systemów informacyjnych, które przetwarzają, przechowują i przekazują PII. Organizacje nie mogą zapewnić skutecznej ochrony prywatności bez stworzenia fundamentów w postaci bezpieczeństwa informacji. Prywatność jest jednak czymś więcej niż tylko bezpieczeństwem i obejmuje na przykład zasady przejrzystości, powiadamiania i wyboru.

Zabezpieczenia w zakresie ochrony prywatności koncentrują się na prywatności informacji jako wartości odrębnej od bezpieczeństwa informacji, ale silnie z nim powiązanej. Zabezpieczenia w zakresie ochrony prywatności opierają się na zasadach określonych przez Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. W sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz towarzyszących aktach prawnych i pomagają organizacjom w unikaniu kosztów materialnych i szkód niematerialnych wynikających z incydentów związanych z ochroną prywatności.

Zabezpieczenia w zakresie prywatności to zabezpieczenia administracyjne, techniczne i fizyczne stosowane w organizacjach w celu ochrony i zapewnienia właściwego postępowania z danymi osobowymi. Istnieje osiem rodzin mechanizmów zabezpieczeń

w zakresie prywatności. Zabezpieczenia w zakresie ochrony prywatności mogą być wdrażane na poziomie organizacji, departamentu, komponentu, biura, programu lub systemu informacyjnego. Zabezpieczenia te mają strukturę podobną do zabezpieczeń systemu informacyjnego zawartych w publikacji NSC 800-53 i NSC 800-53B.

Katalog ochrony prywatności zawiera uporządkowany zestaw zabezpieczeń w zakresie prywatności, oparty na międzynarodowych standardach i najlepszych praktykach, który ma pomóc organizacjom w egzekwowaniu wymagań wynikających z ustawodawstwa, polityk, regulacji, dyrektyw, standardów i wytycznych dotyczących ochrony prywatności. Dodatkowo, ustanawia on powiązania i relacje pomiędzy zabezpieczeniami w zakresie ochrony prywatności i bezpieczeństwa w celu egzekwowania odpowiednich wymogów prywatności i bezpieczeństwa.

Zabezpieczenia te ułatwiają organizacji spełnianie wymagań dotyczących ochrony prywatności, które mają wpływ na programy i/lub systemy gromadzące, wykorzystujące, utrzymujące, udostępniające lub usuwające dane osobowe. Promuje to bliższą współpracę pomiędzy personelem odpowiedzialnym za ochronę prywatności i personelem odpowiedzialnym za bezpieczeństwo w organizacji, co pomaga w osiągnięciu celów, jakie stawiają sobie liderzy/kierownicy wyższego szczebla w zakresie egzekwowania wymogów zawartych w ustawodawstwie, polityce, przepisach, dyrektywach, standardach i wytycznych dotyczących ochrony prywatności.

Zabezpieczenia prywatności obejmują:

- Uprawnienia i cel (ang. Authority and Purpose - AP).
- Odpowiedzialność, audyt i zarządzanie ryzykiem (ang. Accountability, Audit, and Risk Management - AR).
- Jakość i integralność danych (ang. Data Quality and Integrity - DI).
- Minimalizacja i retencja danych (ang. Data Minimization and Retention - DM).
- Indywidualne uczestnictwo i środki odwoławcze (*ang. Individual Participation and Redress - IP*).
- Bezpieczeństwo (*ang. Security - SE*).

- Przejrzystość (ang. Transparency - TR).
- Ograniczenie wykorzystania (*ang. Use Limitation - UL*).

ZAŁĄCZNIK A - AKRONIMY

PATRZ: NSC 7298, *SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA*

ZAŁĄCZNIK B - SŁOWNIK

PATRZ: NSC 7298, *SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA*

ZAŁĄCZNIK C - ŹRÓDŁA ZAGROŻEŃ, PODATNOŚCI I INCYDENTY

Do opisania wzajemnie powiązanych pojęć takich jak: zagrożenie, źródło zagrożenia, zdarzenie zagrożenia oraz incydent, używanych jest szereg terminów[35]. Zagrożenia mają pewien zamiar lub metodę, która może wykorzystać podatność (lukę w zabezpieczeniach) w sposób zamierzony lub niezamierzony; zamiar ten lub metoda określane są jako źródło zagrożenia. W przypadku wystąpienia zdarzenia powodującego zagrożenie, staje się ono incydentem, który faktycznie lub potencjalnie zagraża poufności, integralności lub dostępności systemu informacyjnego lub przetwarzanych, przechowywanych lub przesyłanych przez ten system informacji lub który stanowi naruszenie lub bezpośrednie zagrożenie naruszenia zasad bezpieczeństwa, procedur bezpieczeństwa lub zasad dopuszczalnego użytkowania. W tej części omówione zostaną źródła zagrożeń, podatności i incydenty charakterystyczne dla ICS.

Źródła zagrożeń

Zagrożenia dla systemów ICS mogą pochodzić z wielu źródeł, które można sklasyfikować jako agresywne, przypadkowe, infrastrukturalne i środowiskowe. W tabeli C-1 wymieniono i zdefiniowano znane źródła zagrożeń występujących w ICS. Konieczne jest stworzenie strategii zarządzania ryzykiem w ICS, która chroni system przed tymi możliwymi źródłami zagrożeń. Źródło zagrożenia musi być dobrze zrozumiane, aby można było zdefiniować i wdrożyć odpowiednią ochronę. Zdarzenia środowiskowe (np. powodzie, pożary) są dobrze rozumiane, ale mogą różnić się pod względem wielkości, częstotliwości i zdolności do potęgowania innych powiązanych ze sobą zdarzeń. Z kolei zagrożenia agresywne zależą od zasobów posiadanych przez przeciwnika oraz od pojawienia się nieznanych wcześniej podatności lub sposobów ataków.

Tabela C-1. Zagrożenia dla systemów ICS.

[35] Patrz: NSC 7298, Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.

Źródło zagrożeń	Opis	Charakterystyka
AGRESYWNE ✓ Osoba fizyczna ✓ Podmiot wewnętrzny ✓ Podmiot zewnętrzny ✓ Zaufany podmiot wewnętrzny ✓ Uprzywilejowany podmiot wewnętrzny ✓ Grupa ✓ Podmiot ad hoc ✓ Ustanowione w celu ataku ✓ Organizacja ✓ Konkurent ✓ Dostawca ✓ Partner ✓ Klient ✓ Społeczeństwo - państwo	Osoby, grupy, organizacje lub państwa, które próbują wykorzystać zależność organizacji od zasobów cyfrowych (np. informacji w formie elektronicznej, technologii informacyjnych i telekomunikacyjnych oraz możliwości komunikacji i przetwarzania informacji zapewnianych przez te technologie).	Zdolność, zamiar, przeznaczenie
PRZYPADKOWE ✓ Użytkownik ✓ Użytkownik uprzywilejowany/Administrator	Błędne działania podejmowane przez osoby w trakcie wykonywania codziennych obowiązków.	Zakres skutków
INFRASTRUKTURALNE ✓ Technologia informacyjna (IT) ✓ Sprzęt ✓ Pamięć masowa ✓ Przetwarzanie ✓ Komunikacja ✓ Wyświetlacz ✓ Czujnik ✓ Sterownik ✓ Zabezpieczenia środowiskowe ✓ Regulatory temperatury i wilgotności ✓ Zasilanie elektryczne	Awarie sprzętu, zabezpieczeń środowiskowych lub oprogramowania, spowodowane starzeniem się, wyczerpaniem zasobów lub innymi okolicznościami, które wykraczają poza zakładane kryteria eksploatacyjne.	Zakres skutków

Źródło zagrożeń	Opis	Charakterystyka
✓ Oprogramowanie ✓ System operacyjny ✓ Topologia sieci ✓ Aplikacje ogólnego zastosowania ✓ Aplikacje dedykowane		
ŚRODOWISKOWE ✓ Klęska żywiołowa lub katastrofa spowodowana przez człowieka ✓ Pożar ✓ Powódź ✓ Wichura ✓ Huragan ✓ Trzęsienie ziemi ✓ Działania dywersyjne/wojenne ✓ Przeciążenie ✓ Nietypowe zdarzenie naturalne (np. plamy słoneczne) ✓ Awaria/wyłączenie infrastruktury ✓ Telekomunikacja ✓ Zasilanie elektryczne	Klęski żywiołowe i awarie infrastruktury krytycznej, od której organizacja jest zależna, ale na którą nie ma wpływu. *Uwaga: Klęski żywiołowe i katastrofy spowodowane przez człowieka można również scharakteryzować pod względem ich dotkliwości i/lub czasu trwania. Ponieważ jednak źródło zagrożenia i zdarzenie powodujące zagrożenie są ściśle określone, powaga i czas trwania mogą zostać włączone do opisu zdarzenia powodującego zagrożenie.*	Zakres efektów

Podatności i warunki predysponujące

W tym rozdziale omówiono podatności i warunki predysponujące, które mogą występować w typowych systemach ICS. Podatności to słabe punkty w systemach informacyjnych, procedurach systemowych, zabezpieczeniach lub wdrożonych rozwiązaniach, które mogą być wykorzystane przez źródło zagrożenia. Warunki predysponujące to właściwości organizacji, misji/procesu biznesowego, architektury lub systemów informacyjnych, które przyczyniają się do zwiększenia prawdopodobieństwa wystąpienia zagrożenia. Kolejność podawanych podatności i warunków predysponujących nie stanowi priorytetu pod względem

prawdopodobieństwa wystąpienia lub dotkliwości wpływu. Ponadto, podatności i warunki predysponujące zidentyfikowane w tym rozdziale nie powinny być uważane za kompletną listę; nie należy również zakładać, że problemy te występują w każdym ICS.

Podatności i warunki predysponujące są grupowane w zależności od miejsca ich występowania - np. W polityce i procedurach organizacji lub niedoskonałości mechanizmów bezpieczeństwa zaimplementowanych w sprzęcie, oprogramowaniu układowym i aplikacjach. Pierwsze z nich są określane jako występujące w organizacji, a drugie jako występujące w systemie. Zrozumienie źródła podatności i warunków predysponujących może pomóc w określeniu optymalnych strategii ich łagodzenia. Grupy podatności użyte w tym załączniku to:

- Polityka i procedury.
- Architektura i projektowanie.
- Konfiguracja i utrzymanie.
- Sprzęt.
- Rozwój oprogramowania.
- Komunikacja i sieć.

Głębsza analiza może wykazać, że przyczyny i zauważone symptomy mogą nie być ze sobą powiązane; to znaczy, niektóre przyczyny mogą wywoływać wiele symptomów, a niektóre objawy mogą wynikać z więcej niż jednej przyczyny. Dokument NSC 800-53 zawiera taksonomię środków bezpieczeństwa, czyli środków zaradczych, służących do ograniczania podatności i warunków predysponujących. Są one podzielone na kategorie, gdzie każda z nich zawiera środki bezpieczeństwa odnoszące się do głównego obszaru bezpieczeństwa w danej kategorii. Ponieważ poszczególne kategorie i zabezpieczenia opisane w dokumencie NSC 800-53 stanowią bardziej kompleksowy przegląd potencjalnych podatności i warunków predysponujących związanych z systemem ICS, w niniejszym rozdziale dokonano krótkiego przeglądu problemów, które są powszechnie spotykane w ICS.

Każdy system ICS będzie zazwyczaj charakteryzował się podzbiorem zidentyfikowanych podatności, ale może także zawierać dodatkowe podatności i warunki predysponujące unikalne dla danego wdrożenia ICS, które nie zostały wymienione w tym załączniku. Specyficzne, aktualne informacje na temat podatności ICS można znaleźć na stronie internetowej Zespołu Reagowania na Incydenty Komputerowe w Systemach Sterowania Przemysłowego (ICS-CERT)[36].

Niektóre podatności i warunki predysponujące mogą być ograniczane; inne można jedynie zaakceptować i kontrolować za pomocą odpowiednich środków zaradczych, jednakże będą one powodować pewne ryzyko szczątkowe dla systemów ICS. Na przykład, niektóre istniejące polityki i procedury mogą być zmienione przy zaangażowaniu nakładów, które organizacja uzna za akceptowalne; z innymi można skuteczniej sobie poradzić, wprowadzając dodatkowe polityki i procedury.

Podatność produktów i usług nabywanych z zewnątrz rzadko znajduje się pod bezpośrednią kontrolą organizacji. Na zmiany mogą wpływać mechanizmy rynkowe, ale jest to podejście powolne i pośrednie. Zamiast tego organizacja może zmienić warunki predysponujące tak, aby zmniejszyć prawdopodobieństwo wykorzystania systemowej podatności.

Podatności polityk i procedur oraz warunki predysponujące

Podatności i warunki predysponujące są często stwarzane w ICS z powodu niepełnej, niewłaściwej lub nieistniejącej polityki bezpieczeństwa, w tym dokumentacji, wytycznych dotyczących wdrażania (np. procedur) i jej egzekwowania. Wsparcie zarządzania polityką i procedurami bezpieczeństwa jest fundamentem każdego programu bezpieczeństwa. Polityka bezpieczeństwa organizacji może zmniejszyć podatność na zagrożenia poprzez nakazanie i egzekwowanie właściwego postępowania. Pisemna polityka i procedury są mechanizmami informowania pracowników i interesariuszy i decyzjach dotyczących właściwych zachowań, korzystnych z punktu widzenia organizacji. z tej perspektywy, polityka jest edukacyjnym i instruktażowym sposobem redukcji podatności. Wprowadzanie zasad

[36] http://ics-cert.us-cert.gov

w życie to działanie wspierające, zachęcające personel do robienia tego, co "właściwe". Konsekwencją nieprzestrzegania zasad i procedur przez pracowników jest podejmowanie różnego rodzaju działań naprawczych. Polityka powinna jasno określać konsekwencje wobec osób lub organizacji, które nie stosują się do niej.

Zazwyczaj mamy do czynienia z kompleksową polityką i procedurami, na które składają się przepisy prawne, wzajemnie nakładające się jurysdykcje i strefy wpływów, ekonomia, tradycje i uwarunkowania historyczne. Duże przedsiębiorstwo jest często podzielone na jednostki organizacyjne, które powinny ze sobą współpracować w celu zmniejszenia podatności na zagrożenia. W celu uzyskania maksymalnej efektywności należy zarządzać zakresem i hierarchicznymi relacjami między politykami i procedurami.

Niektóre zabezpieczenia zawarte w NSC 800-53 i w Załączniku G niniejszej publikacji, określają odpowiedzialność i wymagania stawiane organizacji, podczas gdy inne koncentrują się na możliwościach i działaniu poszczególnych systemów w organizacji. Na przykład, zabezpieczenie AC-6, Zasada wiedzy koniecznej, określa, że "Organizacja stosuje zasadę wiedzy koniecznej (jak najmniejszych uprawnień), zezwalając tylko na autoryzowane dostępy użytkownikom (lub procesom działającym w ich imieniu), które są niezbędne do realizacji przydzielonych zadań organizacyjnych". Organizacja musi podejmować decyzje, które zostają ustalone w polityce i procedurach. Niektóre z powstałych artefaktów, takie jak opisy stanowisk pracy zawierające role, obowiązki i uprawnienia, pozostają w formie odpowiedniej dla ludzi, podczas gdy inne artefakty, takie jak atrybuty, uprawnienia i reguły kontroli dostępu, są wdrażane w technologii informacyjnej.

Należy zauważyć, że nakładka na ICS jest zgodna z rekomendacjami NSC 800-53, ponieważ określa termin "organizacja" w sposób bardzo elastyczny, tak, że jej wskazówki mogą być stosowane przez organizacje każdej wielkości, zarówno na wyższych, jak i niższych szczeblach struktury organizacyjnej. Należy zidentyfikować konkretne organizacje, zaczynając od organizacji odpowiedzialnej za wydawanie i utrzymywanie polityki lub procedury.

Tabela C-2 przedstawia przykłady zaobserwowanych przypadków podatności polityk i procedur dotyczących ICS.

Tabela C-2. Podatności polityk i procedur oraz warunki predysponujące.

Podatność	Opis
Niewłaściwa polityka bezpieczeństwa systemu ICS	Podatności są często wprowadzane do ICS z powodu nieodpowiedniej polityki lub braku polityki dotyczącej bezpieczeństwa systemów sterowania. Każdy środek zaradczy powinien być identyfikowalny z polityką. Zapewnia to jednolitość i rozliczalność. Polityka musi obejmować urządzenia przenośne i mobilne używane w systemach ICS.
Brak formalnego programu szkoleń i podnoszenia świadomości w zakresie bezpieczeństwa ICS	Udokumentowana formalna polityka i program szkoleń w zakresie uświadamiania bezpieczeństwa mają na celu aktualizowanie wiedzy personelu na temat organizacyjnych polityk i procedur bezpieczeństwa, a także zagrożeń, branżowych standardów cyberbezpieczeństwa i zalecanych praktyk. Nie można oczekiwać, że bez przeszkolenia w zakresie szczegółowych zasad i procedur dotyczących ICS, personel będzie w stanie utrzymać bezpieczne środowisko ICS.
Brak lub niewystarczające wytyczne dotyczące wdrażania wyposażenia ICS	Wytyczne dotyczące wdrażania wyposażenia powinny być aktualizowane i powszechnie dostępne. Wytyczne te stanowią integralną część procedur bezpieczeństwa w przypadku awarii ICS.
Brak mechanizmów administracyjnych do egzekwowania polityki bezpieczeństwa	Personel odpowiedzialny za egzekwowanie bezpieczeństwa powinien być rozliczany ze stosowania opracowanych polityk i procedur bezpieczeństwa.
Niewłaściwy przegląd skuteczności środków bezpieczeństwa IC	Powinny istnieć procedury i harmonogramy pozwalające określić zakres, w jakim program bezpieczeństwa i jego elementy zabezpieczające są poprawnie wdrożone, funkcjonują zgodnie z założeniami i przynoszą pożądane rezultaty w zakresie spełniania wymogów bezpieczeństwa ICS. Badanie to jest nazywane " audytem", " oceną" lub "szacowaniem". Polityka powinna określać etap cyklu życia, cel, wiedzę techniczną, metodykę i poziom niezależności.

Podatność	Opis
Brak planu awaryjnego dotyczącego ICS.	Należy przygotować, przetestować i udostępnić plan awaryjny na wypadek wystąpienia istotnej awarii sprzętu lub oprogramowania, albo zniszczenia obiektów. Brak szczegółowego planu dotyczącego ICS może prowadzić do wydłużenia czasu przestojów i strat w produkcji.
Brak polityki zarządzania konfiguracją	Brak polityki i procedur zarządzania zmianami w konfiguracji ICS może prowadzić do powstania niezarządzanych i bardzo podatnych na ataki zasobów sprzętowych, oprogramowania układowego i aplikacji.
Brak odpowiedniej polityki kontroli dostępu	Egzekwowanie kontroli dostępu zależy od polityki, która prawidłowo modeluje role, odpowiedzialności i uprawnienia. Model polityki powinien uwzględniać sposób funkcjonowania organizacji.
Brak właściwej polityki uwierzytelniania	Zasady uwierzytelniania są niezbędne, aby określić, kiedy należy stosować mechanizmy uwierzytelniania (np. hasła, karty inteligentne), jak silne muszą one być i jak należy je utrzymywać. Bez stosownej polityki systemy mogą nie być wyposażone w odpowiednie mechanizmy uwierzytelniania, co zwiększa prawdopodobieństwo nieuprawnionego dostępu do nich. Zasady uwierzytelniania powinny być opracowywane jako część ogólnego programu bezpieczeństwa ICS z uwzględnieniem możliwości ICS i jego personelu w zakresie obsługi zaawansowanych haseł i innych mechanizmów.
Niewłaściwy plan i procedury wykrywania i reagowania na incydenty	Plany, procedury i metody rozpoznawania i reagowania na incydenty są niezbędne do szybkiego wykrywania incydentów, minimalizowania strat i zniszczeń, zachowywania dowodów do późniejszych ekspertyz śledczych, łagodzenia wykorzystanych słabości oraz przywracania usług ICS. Ustanowienie skutecznej zdolności reagowania na incydenty obejmuje ciągłe monitorowanie anomalii, określanie priorytetów obsługi incydentów oraz wdrażanie skutecznych metod gromadzenia, analizowania i zgłaszania danych.
Brak redundancji komponentów krytycznych	Brak redundancji kluczowych komponentów może spowodować awarię pojedynczego punktu.

Podatność systemu i warunki predysponujące

Środki bezpieczeństwa powinny jednoznacznie określać systemy, do których mają zastosowanie. Systemy są bardzo zróżnicowane pod względem wielkości, zakresu

i funkcjonalności. Systemem może być pojedynczy produkt lub usługa, będąca sprzętem lub oprogramowaniem. Z drugiej strony spektrum znajdują się duże, złożone systemy, zestawy systemów (*ang. systems-of-systems – SoS*)[37] i sieci, z których wszystkie zawierają architekturę sprzętową i strukturę oprogramowania (w tym struktury aplikacji), a ich połączenie wspomaga działanie ICS.

Podatności systemu mogą dotyczyć sprzętu, oprogramowania układowego i aplikacji wykorzystanych do budowy ICS. Źródła podatności obejmują błędy projektowe, błędy rozwojowe, błędną konfigurację, niewłaściwe utrzymanie, niewłaściwą administrację oraz powiązania z innymi systemami i sieciami. Wiele zabezpieczeń zawartych w NSC 800-53 i nakładkach ICS zawartych w Załączniku G określa, co system musi zapewnić, aby złagodzić te podatności.

Potencjalne podatności i warunki predysponujące powszechnie występujące w systemach ICS zostały skategoryzowane w poniższych tabelach:

- Tabela C-3. Podatności i warunki predysponujące w zakresie architektury i projektowania ICS.
- Tabela C-4. Podatności i warunki predysponujące w zakresie konfiguracji i utrzymania ICS.
- Tabela C-5. Fizyczne podatności i warunki predysponujące ICS.
- Tabela C-6. Podatności i warunki predysponujące w zakresie rozwoju oprogramowania.
- Tabela C-7. Podatności i warunki predysponujące w zakresie komunikacji i konfiguracji sieci.

Tabela C-3. Podatności i warunki predysponujące w zakresie architektury i projektowania ICS.

[37] Zbiór systemów, z których każdy może działać niezależnie, ale które współdziałają ze sobą w celu osiągnięcia dodatkowych pożądanych możliwości.

Podatność	Opis
Niewłaściwe uwzględnienie kwestii bezpieczeństwa w ramach architektury i projektowania.	Włączenie kwestii bezpieczeństwa do architektury ICS, jak również projektowania, musi się rozpocząć na etapie ustalania budżetu i harmonogramu ICS. Architektura bezpieczeństwa jest częścią architektury korporacyjnej. Architektura ta musi obejmować identyfikację i autoryzację użytkowników, mechanizmy kontroli dostępu, topologie sieci oraz mechanizmy konfiguracji i integralności systemu.
Pozwolenie na powstanie niezabezpieczonej architektury.	Środowisko infrastruktury sieciowej w ramach ICS było często rozwijane i modyfikowane w oparciu o wymagania biznesowe i operacyjne, przy czym w niewielkim stopniu uwzględniano potencjalny wpływ tych zmian na bezpieczeństwo. Z czasem, w wyniku nieumyślnego wprowadzenia zmian w poszczególnych częściach infrastruktury, mogły powstać luki w zabezpieczeniach. Jeśli nie zostały one usunięte, mogą stanowić "tylne drzwi" (*ang. backdoors*) do ICS.
Brak zdefiniowanych obwodów bezpieczeństwa.	Jeśli system ICS nie ma jasno zdefiniowanego obwodu bezpieczeństwa, nie można zapewnić, że niezbędne środki bezpieczeństwa są rozmieszczone i skonfigurowane w sposób prawidłowy. Może to prowadzić do nieautoryzowanego dostępu do systemów i danych, a także do powstawania innych problemów.
Systemy bezpieczeństwa wykorzystywane do obsługi transmisji niewymagającej zabezpieczania.	Przepływ danych sterujących i innych danych wiąże się z różnymi wymaganiami, takimi jak dokładność i wiarygodność, dlatego obecność obu rodzajów ruchu w jednej sieci utrudnia jej skonfigurowanie w taki sposób, aby spełniała wymagania ruchu sterującego. Na przykład, ruch niesłużący celom sterowania może powodować niezamierzone zużycie zasobów, które są niezbędne do obsługi ruchu wykorzystywanego na potrzeby sterowania, powodując zakłócenia w funkcjonowaniu ICS.
Realizacja usług sterowania poza siecią kontrolowaną.	Jeśli w sieciach sterowania wykorzystywane są usługi informacyjne, takie jak system nazw domen (DNS) i protokół dynamicznego konfigurowania hostów (DHCP), są one często wdrażane w sieci informacyjnej, co powoduje uzależnienie sieci ICS od sieci informacyjnej, która może nie spełniać wymagań dotyczących niezawodności i dostępności, jakie są wymagane w ICS.

Podatność	Opis
Niewłaściwe zbieranie historii zdarzeń.	Warunkiem przeprowadzenia analiz jest zebranie i przechowywanie wystarczającej ilości danych. Bez właściwego i dokładnego gromadzenia danych określenie przyczyny wystąpienia incydentu bezpieczeństwa może być niemożliwe. Incydenty mogą pozostać niezauważone, co prowadzi do dodatkowych szkód i/lub zakłóceń. Regularne monitorowanie bezpieczeństwa jest również niezbędne do identyfikowania problemów związanych z bezpieczeństwem, takich jak błędne konfiguracje i awarie.

Tabela C-4. Podatności i warunki predysponujące w zakresie konfiguracji i utrzymania ICS.

Podatność	Opis
Sprzęt, oprogramowanie układowe i aplikacje nieobjęte zarządzaniem konfiguracją.	Organizacja nie dysponuje wiedzą o tym, co posiada, gdzie to jest zlokalizowane, jakimi wersjami dysponuje, ani jaki jest status wprowadzanych poprawek, co skutkuje niespójną i nieefektywną postawą obronną. Należy wdrożyć proces kontrolowania wprowadzania sprzętu, oprogramowania układowego, aplikacji i dokumentacji, aby zapewnić ochronę ICS przed nieodpowiednimi lub niewłaściwymi modyfikacjami dokonywanymi przed, w trakcie i po wdrożeniu systemu. Brak procedur zarządzania zmianami konfiguracji może prowadzić do niedopatrzeń w zakresie bezpieczeństwa, powstawania zagrożeń i ryzyka. W celu właściwego zabezpieczenia systemu ICS powinna istnieć dokładna lista zasobów znajdujących się w systemie oraz ich aktualna konfiguracja. Procedury te mają krytyczne znaczenie dla realizacji planów ciągłości działania i odtwarzania po katastrofie.
Wprowadzanie poprawek do systemu operacyjnego i oprogramowania producenta odbywa się niekiedy dopiero po wykryciu luk w zabezpieczeniach.	Ze względu na ścisłe powiązanie oprogramowania ICS z danym ICS, zmiany muszą być poddawane kosztownym i czasochłonnym kompleksowym testom korekcyjnym. Czas, jaki upływa od przeprowadzenia takich testów do dystrybucji zaktualizowanego oprogramowania, stwarza możliwości wykorzystania obszarów podatnych na ataki.

Podatność	Opis
Poprawki bezpieczeństwa systemu operacyjnego i aplikacji nie są wprowadzane lub sprzedawca odmawia „łatania" podatności.	Nieaktualne systemy operacyjne i aplikacje mogą zawierać nowo wykryte podatności, które mogą zostać wykorzystane. Należy opracować udokumentowane procedury dotyczące sposobu wprowadzania poprawek bezpieczeństwa. Wsparcie w postaci poprawek bezpieczeństwa może nie być dostępne dla systemów ICS, które korzystają z nieaktualnych systemów operacyjnych, dlatego procedury powinny zawierać plany awaryjne służące do ograniczania podatności również w przypadku, gdy poprawki nie będą dostępne.
Niewłaściwe testowanie zmian w zabezpieczeniach.	Modyfikacje sprzętu, oprogramowania układowego i aplikacji wprowadzone bez przeprowadzenia testów, mogą zagrażać normalnemu funkcjonowaniu systemu ICS. Należy opracować udokumentowane procedury testowania wszystkich zmian pod kątem wpływu na bezpieczeństwo. Do testowania nigdy nie należy wykorzystywać działających systemów działających operacyjnie. Testowanie modyfikacji systemu może wymagać koordynacji ze sprzedawcami i integratorami systemu.
Niedostateczna kontrola zdalnego dostępu.	Istnieje wiele powodów, dla których system ICS może wymagać zdalnego dostępu. Obejmuje to dostawców i integratorów systemów wykonujących funkcje utrzymaniowe systemu, a także inżynierów systemów ICS uzyskujących dostęp do geograficznie odległych komponentów systemu. Funkcje zdalnego dostępu muszą być odpowiednio kontrolowane, aby zapobiec uzyskaniu dostępu do ICS przez osoby nieupoważnione.
Stosowanie niewłaściwych konfiguracji.	Nieprawidłowo skonfigurowane systemy mogą udostępniać włączone niewykorzystywane porty i protokoły, a te zbędne funkcje mogą zawierać podatności, które zwiększają ogólne ryzyko ponoszone przez system. Używanie domyślnych konfiguracji często naraża system na wykrycie podatności i udostępnienie usług, które można wykorzystać. Dlatego należy przeanalizować wszystkie ustawienia konfiguracyjne.
Nie są przechowywane, ani tworzone kopie zapasowe krytycznych konfiguracji.	Powinny być dostępne procedury przywracania ustawień konfiguracyjnych ICS w przypadku przypadkowych lub zainicjowanych przez przeciwników zmian konfiguracji, co pozwoli utrzymać dostępność systemu i zapobiec utracie danych. Należy opracować udokumentowane procedury utrzymywania ustawień konfiguracyjnych ICS.

Podatność	Opis
Niezabezpieczone dane na urządzeniu przenośnym.	Jeśli dane wrażliwe (np. hasła, numery telefonów) są przechowywane w sposób niezabezpieczony na urządzeniach przenośnych, takich jak laptopy i urządzenia mobilne, a urządzenia te zostaną zgubione lub skradzione, bezpieczeństwo systemu może być narażone na kompromitację. Konieczne jest opracowanie i wprowadzenie w życie stosownych zasad, procedur i mechanizmów ochrony.
Niezgodne z wprowadzonymi regułami generowanie, stosowanie i ochrona haseł.	Istnieje duży zbiór rozwiązań w zakresie stosowania haseł w IT, które można zastosować w ICS. Polityka i procedury dotyczące stosowania haseł muszą być przestrzegane, aby były skuteczne. Naruszenie zasad i procedur dotyczących haseł może drastycznie zwiększyć podatność ICS na ataki.
Niewłaściwe prowadzenie kontroli dostępu.	Kontrole dostępu muszą być dopasowane do metod przydzielania odpowiedzialności i uprawnień personelowi organizacji. Niewłaściwie ustalone zasady kontroli dostępu mogą skutkować nadaniem użytkownikowi systemu ICS zbyt dużych lub zbyt ograniczonych uprawnień. Poniżej przedstawiono przykłady poszczególnych przypadków: • System skonfigurowany z domyślnymi ustawieniami kontroli dostępu daje operatorowi uprawnienia administracyjne. • Nieprawidłowo skonfigurowany system powoduje, że operator nie jest w stanie podjąć działań naprawczych w sytuacji awaryjnej.
Niewłaściwe powiązanie danych.	Systemy przechowywania danych ICS mogą być połączone ze źródłami danych spoza ICS. Przykładem tego są łącza do baz danych, które umożliwiają automatyczną replikację danych z jednej bazy danych do innych. Powiązanie danych może stanowić zagrożenie, jeśli nie jest odpowiednio skonfigurowane, i może umożliwić nieuprawniony dostęp do danych lub manipulację nimi.
Niezainstalowana lub niezaktualizowana ochrona przed złośliwym oprogramowaniem.	Instalowanie złośliwego oprogramowania (tzw. malware) jest powszechnie spotykanym atakiem. Oprogramowanie chroniące przed złośliwym oprogramowaniem, takie jak oprogramowanie antywirusowe, musi być na bieżąco aktualizowane w bardzo dynamicznym środowisku. Nieaktualne oprogramowanie i definicje chroniące przed złośliwym oprogramowaniem sprawiają, że system jest otwarty na nowe zagrożenia.

Podatność	Opis
Wdrożenie ochrony przed złośliwym oprogramowaniem bez przeprowadzenia odpowiednich testów.	Oprogramowanie chroniące przed złośliwym oprogramowaniem wdrożone bez wystarczających testów może wpłynąć na normalne funkcjonowanie ICS i zablokować system.
Odmowa świadczenia usługi (DoS)	Oprogramowanie ICS może być podatne na ataki DoS, których skutkiem jest uniemożliwienie autoryzowanego dostępu do zasobów systemu lub opóźnienie operacji i funkcji systemu.
Brak zainstalowanego oprogramowania do wykrywania i zapobiegania włamaniom.	Incydenty mogą powodować utratę dostępności i integralności systemu; przechwytywanie, modyfikowanie i usuwanie danych; oraz nieprawidłowe wykonywanie poleceń sterujących. Oprogramowanie IDS/IPS może powstrzymywać lub zapobiegać różnego rodzaju atakom, w tym atakom DoS, a także identyfikować zaatakowane hosty wewnętrzne, np. zainfekowane robakami. Oprogramowanie IDS/IPS[38] musi zostać przetestowane przed wdrożeniem, aby upewnić się, że nie zagraża ono normalnej pracy systemu ICS.
Brak prowadzenia rejestrów zdarzeń (dzienników logów).	Z powodu braku odpowiednich i dokładnych dzienników logów ustalenie przyczyny wystąpienia zdarzenia związanego z bezpieczeństwem może być niemożliwe.

Tabela C-5. Fizyczne podatności i warunki predysponujące ICS.

[38] IDS, IPS (*ang. Intrusion Detection System, Intrusion Prevention System*) – systemy wykrywania i zapobiegania włamaniom.

Podatność	Opis
Fizyczny dostęp do sprzętu przez nieupoważniony personel.	Fizyczny dostęp do urządzeń ICS powinien być ograniczony tylko do niezbędnego personelu, z uwzględnieniem wymogów bezpieczeństwa, takich jak awaryjne wyłączanie lub ponowne uruchamianie. Niewłaściwy dostęp do sprzętu ICS może prowadzić do: • Fizycznej kradzieży danych i sprzętu. • Fizycznego uszkodzenia lub zniszczenia danych i sprzętu. • Nieuprawnionych zmian w środowisku funkcjonalnym (np. połączenie danych, nieuprawnione użycie nośników wymiennych, dodanie/usunięcie zasobów). • Rozłączenia fizycznego łączy danych. • Przechwytywania danych w sposób niewykrywalny (rejestrowanie naciśnięć klawiszy i innych wprowadzanych danych).
Częstotliwości radiowe, impulsy elektromagnetyczne (EMP), wyładowania statyczne, wyładowania łukowe i skoki napięcia, itp.	Sprzęt używany w systemach sterowania jest podatny na oddziaływanie częstotliwości radiowych i impulsów elektromagnetycznych (EMP), wyładowań elektrostatycznych, wyładowań łukowych i skoków napięcia. Skutki mogą być różne - od chwilowego zakłócenia sterowania i kontroli po trwałe uszkodzenie płytek drukowanych. Zalecane jest odpowiednie ekranowanie, uziemienie, filtrowanie zasilania i/lub tłumienie przepięć.
Niedostępność zasilania awaryjnego.	Jeśli kluczowe zasoby nie posiadają zasilania awaryjnego, utrata zasilania spowoduje wyłączenie systemu ICS i może doprowadzić do niebezpiecznej sytuacji. Utrata zasilania może również spowodować, że ustawienia domyślne oprogramowania zostaną przywrócone w sposób niezgodny z zasadami bezpieczeństwa.
Utrata zabezpieczeń środowiskowych.	Utrata zabezpieczeń środowiskowych (np. W odniesieniu do temperatury, wilgotności) może doprowadzić do uszkodzenia sprzętu, np. przegrzania procesorów. Niektóre procesory wyłączą się w celu ochrony własnej; inne mogą nadal działać, ale w minimalnym zakresie i mogą generować sporadyczne błędy, ciągle się restartować lub trwale utracić funkcjonalność.
Niezabezpieczone porty fizyczne.	Niezabezpieczone porty uniwersalnej magistrali szeregowej (USB) i PS/2 mogą umożliwiać nieuprawnione podłączanie dysków twardych, rejestratorów naciśnięć klawiszy itp.

Tabela C-6. Podatności i warunki predysponujące w zakresie rozwoju oprogramowania.

Podatność	Opis
Nieprawidłowa weryfikacja danych.	Oprogramowanie ICS może nie weryfikować poprawności wprowadzanych przez użytkownika lub otrzymywanych danych. Nieprawidłowe dane mogą powodować liczne podatności, w tym przepełnienie bufora, wstrzykiwanie poleceń, cross-site scripting[39] i path traversals[40].
Niewłączone domyślnie zainstalowane funkcje bezpieczeństwa.	Zainstalowane funkcje zabezpieczeń są bezużyteczne, jeśli nie są włączone lub przynajmniej zidentyfikowane jako wyłączone.
Niewystarczające uwierzytelnianie, uprawnienia i kontrola dostępu przy korzystaniu z oprogramowania.	Nieuprawniony dostęp do narzędzi konfiguracyjnych i programujących może doprowadzić do uszkodzenia urządzenia.

Tabela C-7. Podatności i warunki predysponujące w zakresie komunikacji i konfiguracji sieci.

Podatność	Opis
Brak kontroli przepływu danych.	Mechanizmy kontroli przepływu danych, oparte na charakterystyce danych, są potrzebne do ograniczenia liczby informacji, które mogą być przekazywane między systemami. Zabezpieczenia te mogą zapobiegać eksfiltracji informacji i nielegalnym operacjom.
Brak lub niewłaściwa konfiguracja zapór sieciowych.	Brak prawidłowo skonfigurowanych zapór sieciowych może umożliwiać przesyłanie niepożądanych danych między sieciami, takimi jak sieci sterowania i sieci korporacyjne; pozwalać na rozprzestrzenianie się ataków i złośliwego oprogramowania między sieciami; sprawiać, że dane wrażliwe będą podatne na monitorowanie/podsłuchiwanie, a osoby nieupoważnione będą miały dostęp do systemów.

[39] Sposób ataku na serwis WWW, polegający na osadzeniu w treści atakowanej strony kodu (zazwyczaj JavaScript), który wyświetlony innym użytkownikom może doprowadzić do wykonania przez nich niepożądanych akcji.

[40] Atak, za pomocą którego osoba atakująca może spowodować, że aplikacja internetowa odczyta, a następnie ujawni zawartość plików znajdujących się poza katalogiem głównym aplikacji lub serwera WWW. Ina nazwa: Directory Traversal.

Podatność	Opis
Niewłaściwe prowadzenie zapisów logów zapory sieciowej i routera.	Bez odpowiednich i dokładnych logów może być niemożliwe ustalenie, co było przyczyną wystąpienia incydentu bezpieczeństwa.
Wykorzystywanie w postaci tekstu jawnego standardowych, ściśle udokumentowanych protokołów komunikacyjnych.	Przeciwnicy, którzy mogą monitorować aktywność sieci ICS, mogą używać analizatora protokołów lub innych narzędzi do dekodowania danych przesyłanych przez protokoły takie jak telnet, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) i Network File System (NFS). Wykorzystanie takich protokołów ułatwia również przeciwnikom przeprowadzanie ataków na ICS i manipulowanie aktywnością sieciową ICS.
Brak lub niespełniające standardów uwierzytelnianie użytkowników, danych lub urządzeń.	W wielu protokołach ICS nie stosuje się uwierzytelniania na żadnym poziome dostępu. Brak uwierzytelniania umożliwia odtwarzanie, modyfikowanie i fałszowanie danych lub podrabianie urządzeń, takich jak czujniki i identyfikatory użytkowników.
Stosowanie niezabezpieczonych, protokołów ICS.	Protokoły ICS często mają ograniczone lub nie posiadają żadnych funkcji bezpieczeństwa, takich jak uwierzytelnianie i szyfrowanie, które chroniłyby dane przed nieuprawnionym dostępem lub manipulacją. Ponadto nieprawidłowe wdrożenie protokołów może prowadzić do powstania dodatkowych podatności.
Brak kontroli integralności komunikacji.	W większości protokołów sterowania przemysłowego nie ma wbudowanej kontroli integralności; przeciwnicy mogą manipulować komunikacją w sposób niewykryty. W tej sytuacji, w celu zapewnienia integralności system ICS może korzystać z protokołów niższej warstwy (np. IPsec), które oferują ochronę integralności danych.
Niewystarczające uwierzytelnianie między klientami sieci bezprzewodowej a punktami dostępowymi.	Wzajemne (dwustronne) uwierzytelnianie pomiędzy klientami sieci bezprzewodowej a punktami dostępowymi jest konieczne, aby klienci nie łączyli się z nielegalnie działającymi punktami dostępowymi rozmieszczonymi przez przeciwnika, a także aby przeciwnicy nie mogli łączyć się z żadną z sieci bezprzewodowych należących do ICS.
Niewystarczająca ochrona danych przekazywanych między klientami sieci bezprzewodowej a punktami dostępowymi.	Wrażliwe dane przekazywane pomiędzy klientami sieci bezprzewodowymi a punktami dostępowymi powinny być chronione za pomocą silnego szyfrowania, aby zapewnić, że przeciwnicy nie będą mogli uzyskać nieautoryzowanego dostępu do niezaszyfrowanych danych.

Incydenty

Zdarzenie zagrożenia to zdarzenie lub sytuacja, która może potencjalnie spowodować niepożądane skutki lub wpływ na ICS, a która pochodzi z dowolnego źródła zagrożenia. W załączniku E publikacji NSC SP 800-30 określono ogólny zestaw zagrożeń, które mogą potencjalnie wpływać na systemy informacyjne. Właściwości ICS mogą również stwarzać unikalne zagrożenia, szczególnie w odniesieniu do sposobu, w jaki zagrożenia mogą wpływać na procesy zachodzące w ICS i powodować uszkodzenia fizyczne. Tabela C-8 zawiera przegląd potencjalnych zdarzeń zagrażających systemowi ICS.

Tabela C-8. Przykładowe wrogie incydenty.

Zdarzenie zagrażające	Opis
Odmowa świadczenia usługi.	Zakłócanie działania systemów sterowania poprzez opóźnianie lub blokowanie przepływu informacji, a tym samym uniemożliwianie dostępu do sieci operatorom systemów sterowania lub powodowanie ograniczeń w przesyłaniu informacji lub odmowy świadczenia usług przez usługi rezydujące w systemie IT (np. DNS).
Przeprogramowane urządzenia sterujące.	Nieautoryzowane zmiany zaprogramowanych instrukcji w sterownikach PLC, RTU, DCS lub SCADA, zmiana progów alarmowych lub nieautoryzowane polecenia wydawane urządzeniom sterującym, które mogą potencjalnie prowadzić do uszkodzenia urządzeń (jeśli przekroczone są dopuszczalne tolerancje), przedwczesnych wyłączeń procesów (np. przedwczesnego wyłączenia linii przesyłowych), mogą spowodować incydenty środowiskowe, a nawet uniemożliwić działanie urządzeń sterujących.
Sfałszowane informacje o stanie systemu.	Fałszywe informacje wysyłane do operatorów systemu sterowania w celu ukrycia nieautoryzowanych zmian lub w celu zainicjowania niewłaściwych działań operatorów systemu.
Manipulacja logiką sterowania.	Zmodyfikowanie oprogramowania lub ustawień konfiguracyjnych systemu sterowania, którego skutkiem są nieprzewidywalne wyniki działania systemu.
Zmodyfikowane systemy bezpieczeństwa.	Działanie systemów bezpieczeństwa jest manipulowane w taki sposób, aby: (1) nie zadziałały w razie konieczności lub (2) wykonywały nieprawidłowe działania zabezpieczające, które mogą wyrządzić szkody w ICS.
Złośliwe oprogramowanie w systemach sterowania.	Złośliwe oprogramowanie (np. wirus, robak, koń trojański) wprowadzone do systemu.

Ponadto w systemach sterowania, które obejmują rozległy obszar geograficzny, zdalne lokalizacje często nie są obsadzone przez personel i mogą nie być fizycznie monitorowane. Jeśli takie systemy zdalne zostaną fizycznie naruszone, przeciwnicy mogą uzyskać dostęp do sieci sterowania.

Źródła incydentów

Trudno jest określić dokładną liczbę cyberincydentów dotyczących systemów sterowania. Jednak osoby z branży, które koncentrują się na tym zagadnieniu, dostrzegają podobne tendencje wzrostowe pomiędzy podatnościami ujawnionymi w tradycyjnych systemach IT, a tymi, które są wykrywane w systemach sterowania.

Organizacje powinny współpracować i na bieżąco dzielić się informacjami o potencjalnych incydentach[41].

Odnotowano wiele incydentów związanych z ICS, które pokazują, w jaki sposób źródła zagrożeń mogą negatywnie wpływać na ICS. Zdarzenia te pomagają wykazać dotkliwość źródeł zagrożeń, podatności i skutków w obszarze ICS. Jak przedstawiono w tabeli C-1, cztery główne kategorie źródeł zagrożeń to zagrożenia agresywne, przypadkowe, infrastrukturalne i środowiskowe. Często incydent może być wynikiem działania wielu źródeł zagrożeń (np. zdarzenie środowiskowe powoduje awarię systemu, na którą operator reaguje nieprawidłowo, co prowadzi do zdarzenia przypadkowego). Do zgłoszonych incydentów z tych kategorii należą:

Zdarzenia agresywne

- **Usługi telekomunikacyjne w Worcester Air Traffic**[42]. W marcu 1997 r. nastolatek z Worcester w stanie Massachusetts zablokował część publicznej komutowanej sieci telefonicznej za pomocą modemu dial-up podłączonego do systemu. Spowodowało to przerwanie połączeń telefonicznych z wieżą kontrolną, ochroną lotniska, strażą pożarną, służbami meteorologicznymi i przewoźnikami korzystającymi z lotniska. Wyłączony został również główny nadajnik radiowy wieży oraz inny nadajnik

[41] Patrz: NSC 800-61.

[42] Dodatkowe informacje na temat incydentu w Worcester Air Traffic Communications można znaleźć na stronie: http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html

uruchamiający oświetlenie pasa startowego, a także drukarka, której kontrolerzy używają do monitorowania postępu lotów. Atak spowodował również przerwę w dostawie usług telefonicznych do 600 domów i firm w pobliskim mieście Rutland.

- **Wyciek ścieków w Maroochy Shire**[43]. Wiosną 2000 r. były pracownik australijskiej organizacji zajmującej się tworzeniem oprogramowania przemysłowego starał się o pracę w samorządzie lokalnym, ale jego podanie o pracę zostało odrzucone. W ciągu dwóch miesięcy ten niezadowolony, niezatrudniony pracownik użył podobno aż 46 razy nadajnika radiowego, aby zdalnie włamać się do systemu sterowania oczyszczalni ścieków. Zmienił dane elektroniczne poszczególnych przepompowni ścieków i spowodował zakłócenia w ich pracy, co ostatecznie doprowadziło do wypuszczenia około 1 mld litrów nieoczyszczonych ścieków do pobliskich rzek i parków.
- **Davis-Besse**[44]. W sierpniu 2003 r. Nuclear Regulatory Commission potwierdziła, że w styczniu 2003 r. robak Microsoft SQL Server, znany jako Slammer, zainfekował prywatną sieć komputerową w nieczynnej elektrowni atomowej Davis-Besse w Oak Harbor w stanie Ohio, wyłączając na prawie pięć godzin system monitorowania bezpieczeństwa. Ponadto awarii uległ komputer obsługujący proces technologiczny w elektrowni, a jego ponowne uruchomienie zajęło około sześciu godzin. Slammer wpłynął także na komunikację w sieciach sterowania co najmniej pięciu innych zakładów, rozprzestrzeniając się tak szybko, że zablokował komunikację w systemach sterowania.

[43] Dodatkowe informacje na temat incydentu z wyciekiem ścieków w Maroochy Shire można znaleźć na stronie:

http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/[każdy dostęp 4/16/15]

[44] Dodatkowe informacje na temat incydentu Davis-Besse można znaleźć na stronie:

http://www.securityfocus.com/news/6767 [dostęp: 4/16/15].

- **Robak Zotob**[45]. W sierpniu 2005 r. seria infekcji robakami internetowymi spowodowała, że 13 zakładów samochodowych Daimler Chrysler przestało działać na prawie godzinę, pozbawiając pracowników pracy, ponieważ zainfekowane systemy Microsoft Windows musiały zostać "załatane". Robak zaatakował przede wszystkim systemy Windows 2000, ale także niektóre wcześniejsze wersje Windows XP. Objawy obejmowały wielokrotne wyłączanie i ponowne uruchamiani komputerów.

  Zotob i jego odmiany spowodowały awarie komputerów także w firmach Caterpillar Inc. produkującej ciężki sprzęt, Boeing produkującej samoloty oraz w kilku dużych amerykańskich organizacjach informacyjnych.

- **Robak Stuxnet**[46]. Stuxnet to odkryty w lipcu 2010 r. robak komputerowy działający w systemie Microsoft Windows, którego celem było oprogramowanie i sprzęt przemysłowy. Robak początkowo rozprzestrzeniał się masowo, ale zawierał wysoce wyspecjalizowane złośliwe oprogramowanie, które zostało zaprojektowane tak, aby atakować tylko określone systemy SCADA, które były skonfigurowane do sterowania i monitorowania określonych procesów przemysłowych.

- **Ataki typu brute force na systemy sterowania z dostępem do Internetu**[47]. W dniu 22 lutego 2013 roku ICS-CERT otrzymał zgłoszenie od właściciela tłoczni gazu o wzroście liczby prób ataków typu brute force[48] na sieć sterowania procesami. Materiał dowodowy zawierał 10 odrębnych adresów IP oraz dodatkowe zgłoszenia o podobnym charakterze od innych właścicieli gazociągów, co dało 39 dodatkowych adresów IP budzących niepokój. Po przeprowadzeniu analizy logów stwierdzono, że

[45] Dodatkowe informacje na temat incydentu Zotob Worm można znaleźć na stronie: http://www.eweek.com/c/a/Security/Zotob-PnP-Worms Slam-13-DaimlerChrysler-Plants[dostęp 4/16/15].

[46] Dodatkowe informacje na temat robaka Stuxnet można znaleźć na stronie: http://en.wikipedia.org/wiki/Stuxnet [dostęp 4/16/15].

[47] Dodatkowe informacje na temat zgłoszonych incydentów ICS-CERT można znaleźć na stronie: https://ics-cert.us-cert.gov/Information-Products [dostęp 4/16/15].

[48] Technika łamania haseł lub kluczy kryptograficznych polegająca na sprawdzeniu wszystkich możliwych kombinacji.

zdarzenia miały miejsce od 16 stycznia 2013 r., ale od 8 marca 2013 r. nie było zarejestrowanych żadnych raportów.

- **Shamoon**[49]. Saudi Aramco, ósma co do wielkości rafineria ropy naftowej na świecie, doświadczyła ataku złośliwego oprogramowania, które zaatakowało ich rafinerie i nadpisało główny rekord rozruchowy (ang. Master Boot Records - MBR), tablice partycji i inne losowe pliki danych zaatakowanego systemu. W wyniku tego zaatakowane systemy stały się bezużyteczne.
- **Atak na niemiecką walcownię stali**[50]. W 2014 r. hakerzy zmanipulowali i zakłócili działanie systemów sterowania do tego stopnia, że nie można było prawidłowo wyłączyć wielkiego pieca, co spowodowało "ogromne - choć nieokreślone - szkody".

Zdarzenia infrastrukturalne

- **System sygnalizacji kolejowej CSX**[51]. W sierpniu 2003 r. wirus komputerowy Sobig został uznany za przyczynę wyłączenia systemów sygnalizacji kolejowej na całym wschodnim wybrzeżu USA. Wirus zainfekował system komputerowy w siedzibie CSX Corp. W Jacksonville na Florydzie, wyłączając sygnalizację, dyspozytornię i inne systemy. Według rzecznika firmy Amtrak, w godzinach porannych odnotowano nieprawidłowości w kursowaniu dziesięciu pociągów Amtrak. Pociągi między Pittsburghiem a Florence w Południowej Karolinie zostały wstrzymane z powodu braku sygnalizacji, a jeden regionalny pociąg Amtrak z Richmond w Wirginii do Waszyngtonu i Nowego Jorku był opóźniony o ponad dwie godziny. Pociągi dalekobieżne były również opóźnione od czterech do sześciu godzin.

[49] Dodatkowe informacje na temat Shamoon można znaleźć na stronie:

http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2012.pdf [dostęp 4/16/15].

[50] Dodatkowe informacje na temat incydentu w niemieckiej hucie można znaleźć na stronie: http://www.wired.com/2015/01/german-steel-mill-hack-destruction/ [accessed 4/16/15].

[51] Dodatkowe informacje na temat incydentu w systemie sygnalizacji kolejowej CSX można znaleźć na stronie:

http://www.cbsnews.com/stories/2003/08/21/tech/main569418.shtml

http://www.informationweek.com/story/showArticle.jhtml?articleID=13100807 [każdy dostęp 4/16/15].

- **Przerwa w dostawie energii elektrycznej**[52]. W sierpniu 2003 r. awaria procesora alarmowego w systemie SCADA firmy First Energy uniemożliwiła operatorom dyspozytorni uzyskanie odpowiedniej świadomości sytuacyjnej w zakresie krytycznych zmian operacyjnych w sieci elektrycznej. Ponadto skuteczny nadzór nad niezawodnością został uniemożliwiony, gdy estymator stanu u Midwest Independent System Operator uległ awarii z powodu niekompletnych informacji o zmianach topologii, co uniemożliwiło przeprowadzenie analizy awarii. Kilka kluczowych linii przesyłowych 345 kV w północnym Ohio uległo uszkodzeniu w wyniku styczności z drzewami. Zapoczątkowało to kaskadowe przeciążenia dodatkowych linii 345 kV i 138 kV, co doprowadziło do niekontrolowanej kaskadowej awarii sieci. W wyniku awarii 508 jednostek wytwórczych w 265 elektrowniach utraciło łącznie 61 800 MW mocy.
- **Awaria zapory wodnej Taum Sauk** [53]. W grudniu 2005 roku zapora wodna Taum Sauk uległa katastrofie, uwalniając miliardy litrów wody. Awaria zbiornika nastąpiła w trakcie jego napełniania, lub też mogło dojść do jego przepełnienia. Według obecnej teorii zbiornik został przepełniony, gdy rutynowa nocna operacja pompowania nie zakończyła się po napełnieniu zbiornika. Według przedsiębiorstwa energetycznego, wskazania mierników na zaporze różniły się od wskazań mierników w zakładzie Osage w Lake of the Ozarks, który zdalnie monitoruje i obsługuje zakład Taum Sauk. Stacje są połączone ze sobą za pomocą sieci radiowych, a w Taum Sauk brak jest personelu obsługującego.
- **Awaria rurociągu paliwowego w Bellingham w stanie Waszyngton**[54]. W czerwcu 1999 r. z rurociągu o średnicy 40,64 cm wyciekło 900 tys. litrów benzyny, która

[52] Dodatkowe informacje na temat incydentu Northeast Power Blackout można znaleźć na stronie: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinalImplementationReport%282%29.pdf [dostęp 4/16/15]; Department of Energy

[53] Dodatkowe informacje na temat awarii zapory Taum Sauk Water Storage Dam można znaleźć na stronie: http://www.ferc.gov/industries/hydropower/safety/projects/taum-sauk/ipoc-rpt/full-rpt.pdf [dostęp 4/16/15].

[54] Dodatkowe informacje na temat incydentu Bellingham, Washington Gasoline Pipeline Failure można znaleźć na stronach: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Bellingham_Case_Study_report%2020Sep071.pdf

zapaliła się 1,5 godziny później, powodując 3 ofiary śmiertelne, 8 osób zostało rannych i spowodowała rozległe szkody materialne. Awarię rurociągu pogłębił system sterowania, który nie był w stanie realizować funkcji sterowania i monitorowania. "Bezpośrednio przed i w trakcie zdarzenia system SCADA wykazywał niską wydajność, która uniemożliwiała kontrolerom rurociągu wykrycie i zareagowanie na rozwój nietypowej pracy rurociągu". Kluczowym zaleceniem raportu NTSB wydanego w październiku 2002 r. było wykorzystanie systemu opracowywania i testowania off-line do wdrażania i testowania zmian w bazie danych SCADA.

- **Awaria sterownika PLC w elektrowni Browns Ferry-3** [55]. W sierpniu 2006 roku firma TVA została zmuszona do ręcznego wyłączenia jednego z dwóch reaktorów elektrowni po tym, jak niereagujące na problemy sterowniki PLC spowodowały awarię dwóch pomp wodnych, co zagroziło stabilności samej elektrowni. Mimo, że istniały dwa redundantne sterowniki PLC, były one podłączone do tej samej sieci Ethernet. Późniejsze testy uszkodzonych urządzeń wykazały, że ulegały one zawieszeniu po wystąpieniu zwiększonego ruchu w sieci.

Zdarzenia środowiskowe

- **Katastrofa nuklearna w Fukushimie Daiichi**[56]. W dniu 11 marca 2011 r. u wybrzeży Japonii wystąpiło potężne trzęsienie ziemi, które spowodowało uderzenie potężnej fali tsunami w głąb lądu, kierując się w stronę elektrowni jądrowej. Tsunami naruszyło falochron elektrowni, zalewając znaczną część obiektu, w tym miejsce, w którym znajdowały się generatory awaryjne. Zasilanie awaryjne miało kluczowe znaczenie dla funkcjonowania dyspozytorni, a także dla zapewnienia wody chłodzącej reaktory. Utrata chłodziwa spowodowała przegrzanie rdzeni reaktorów

http://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf [każdy dostęp 4/16/15].

[55] Dodatkowe informacje na temat incydentu Browns Ferry -3 PLC Failure można znaleźć na stronie: http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2007/in200715.pdf [dostęp 4/16/15].

[56] Dodatkowe informacje można znaleźć na stronach:

EBO (iaea.org) oraz http://pbadupws.nrc.gov/docs/ML1414/ML14140A185.pdf [każdy dostęp 4/16/15].

do tego stopnia, że cyrkonowa powłoka paliwa weszła w reakcję z wodą, uwalniając wodór i wywołując potężne eksplozje w trzech z czterech budynków reaktorów. Spowodowało to wyciek promieniowania na dużą skalę, który wywarł wpływ na pracowników elektrowni, okolicznych mieszkańców i lokalne środowisko. Analiza po zdarzeniu wykazała, że centrum reagowania kryzysowego elektrowni nie miało wystarczających bezpiecznych linii komunikacyjnych, aby przekazywać do innych rejonów elektrowni informacje o kluczowych urządzeniach zabezpieczających.

Zdarzenia przypadkowe

- **Incydenty związane ze skanerem podatności**[57]. Podczas przeprowadzania testu pingowania (*ang. ping sweep*[58]) w aktywnej sieci SCADA, która kontrolowała 3-metrowe ramiona robotów, zauważono, że jedno z ramion uaktywniło się i obróciło o 180 stopni. Kontroler tego ramienia był w trybie gotowości przed zainicjowaniem operacji ping sweep. W innym przypadku, w sieci ICS przeprowadzono test pingowy, aby zidentyfikować w celach inwentaryzacyjnych wszystkie hosty podłączone do sieci. Spowodowało to zawieszenie się systemu kontrolującego tworzenie układów scalonych w zakładzie produkcyjnym. W wyniku tego testu zniszczeniu uległy płytki półprzewodnikowe o wartości 50 tys. dolarów.
- **Incydent związany z testami penetracyjnymi**[59]. Zakład gazowniczy do przeprowadzenia testów penetracyjnych swojej sieci informacyjnej zatrudnił firmę konsultingową zajmującą się bezpieczeństwem IT. Organizacja konsultingowa nieświadomie "włamała" się do części sieci, która była bezpośrednio podłączona do systemu SCADA. Test penetracyjny spowodował zablokowanie systemu SCADA, co

[57] Dodatkowe informacje na temat incydentów związanych ze skanerem podatności można znaleźć na stronie:

http://www-pub.iaea.org/MTCD/meetings/PDFplus/2011/cn200/documentation/cn200_Final-Fukushima-Mission_Report.pdf

http://pbadupws.nrc.gov/docs/ML1414/ML14140A185.pdf [dostęp: 4/16/15].

[58] Technika wykorzystywana w celu identyfikacji podłączonych urządzeń. *Ping sweep* polega na wysyłaniu pakietów ICMP w celu identyfikacji aktywnych hostów.

[59] Dodatkowe informacje na temat incydentów związanych z testami penetracyjnymi można znaleźć na stronie: http://energy.sandia.gov/wp/wp-content/gallery/uploads/sand_2005_2846p.pdf [dostęp: 4/16/15].

uniemożliwiło przedsiębiorstwu przesyłanie gazu rurociągami przez cztery godziny. Skutkiem tego była utrata przez odbiorców usług w okresie wspomnianych czterech godzin.

ZAŁĄCZNIK D - BIEŻĄCE DZIAŁANIA W ZAKRESIE BEZPIECZEŃSTWA SYSTEMÓW STEROWANIA PRZEMYSŁOWEGO

Niniejszy załącznik zawiera streszczenia niektórych z wielu działań, które są podejmowane w zakresie cyberbezpieczeństwa ICS. Należy pamiętać, że opisy organizacji i powiązane informacje zawarte w tym Załączniku zostały zaczerpnięte głównie ze stron internetowych wymienionych organizacji oraz innych wiarygodnych źródeł publicznych, ale nie zostały zweryfikowane. Czytelnicy są zachęcani do bezpośredniego kontaktu z tymi organizacjami w celu uzyskania najbardziej aktualnych i kompletnych informacji.

Norma 12 Amerykańskiego Stowarzyszenia Gazownictwa (AGA), "Ochrona kryptograficzna komunikacji SCADA".

Amerykańskie Stowarzyszenie Gazownictwa: http://www.aga.org/

Amerykańskie Stowarzyszenie Gazownictwa (*American Gas Association – AGA*), reprezentuje 195 lokalnych organizacji użyteczności publicznej, które dostarczają gaz ziemny do ponad 56 milionów domów, firm i zakładów przemysłowych w całych Stanach Zjednoczonych, broni interesów swoich członków i ich klientów, a także dostarcza informacji i usług. Seria dokumentów AGA 12 rekomenduje praktyki mające na celu ochronę komunikacji SCADA przed cyberincydentami. Zalecane praktyki koncentrują się na zapewnieniu poufności komunikacji SCADA.

Celem serii AGA 12 jest zaoszczędzenie czasu i wysiłku właścicielom systemów SCADA poprzez rekomendowanie kompleksowego systemu wykorzystującego kryptografię, zaprojektowanego specjalnie do ochrony komunikacji SCADA. Seria AGA 12 może być stosowana w systemach dystrybucji wody, ścieków i energii elektrycznej opartych na SCADA ze względu na ich podobieństwa do systemów gazu ziemnego, jednak wymagania czasowe mogą być inne. Zalecenia zawarte w dokumentach serii 12 mogą być również stosowane w innych ICS. Dodatkowe tematy planowane w przyszłych uzupełnieniach tej serii obejmują zarządzanie kluczami, ochronę danych w stanie spoczynku oraz polityki bezpieczeństwa.

Norma 1164 Amerykańskiego Instytutu Naftowego (API), "Bezpieczeństwo rurociągów SCADA".

Amerykański Instytut Naftowy: http://www.api.org/

Amerykański Instytut Naftowy (*American Petroleum Institute – API*) reprezentuje ponad 400 członków zajmujących się wszystkimi aspektami przemysłu naftowego i gazowego. Standard API 1164 zawiera wytyczne dla operatorów systemów rurociągów naftowych i gazowych dotyczące zarządzania integralnością i bezpieczeństwem systemu SCADA. Wytyczne te zostały opracowane specjalnie po to, aby dostarczyć operatorom opis praktyk branżowych w zakresie bezpieczeństwa systemów SCADA oraz zapewnić ramy niezbędne do opracowania prawidłowych praktyk bezpieczeństwa w poszczególnych organizacjach operatorów. Podkreślają one znaczenie zrozumienia przez operatorów podatności systemu na zagrożenia i ryzyka, podczas dokonywania przeglądu systemu SCADA w celu jego ewentualnego ulepszenia. API 1164 zapewnia środki do poprawy bezpieczeństwa eksploatacji rurociągów SCADA poprzez:

- Określenie procesów stosowanych w celu identyfikacji i analizy podatności systemu SCADA na incydenty.
- Udostępnienie kompleksowej listy praktyk mających na celu utwardzenie (*ang. hardening*) podstawowej architektury.
- Przedstawienie przykładów rekomendowanych przez branżę praktyk.

Wytyczne są skierowane do małych i średnich operatorów rurociągów o ograniczonych zasobach w zakresie bezpieczeństwa IT. Wytyczne mają zastosowanie do niemal wszystkich systemów SCADA, a nie tylko do systemów SCADA związanych z ropą naftową i gazem ziemnym. W załącznikach do dokumentu znajduje się lista kontrolna do oceny systemu SCADA oraz przykład planu bezpieczeństwa systemu sterowania SCADA.

Instytut Badawczy Energii Elektrycznej (Electric Power Research Institute - EPRI)

http://www.epri.com/Our-Work/Pages/Cyber-Security.aspx

http://smartgrid.epri.com/NESCOR.aspx

Instytut Badawczy Energii Elektrycznej (EPRI) jest ośrodkiem non-profit zajmującym się w interesie publicznym badaniem źródeł energii i ochrony środowiska. Instytut EPRI zrzesza organizacje członkowskie, naukowców i inżynierów Instytutu oraz innych czołowych ekspertów, którzy wspólnie pracują nad rozwiązaniami problemów związanych z energią elektryczną. Rozwiązania te obejmują niemal wszystkie dziedziny wytwarzania, dostarczania i użytkowania energii, w tym ochronę zdrowia, bezpieczeństwo i środowisko. Członkowie EPRI dostarczają ponad 90% energii elektrycznej wytwarzanej w Stanach Zjednoczonych.

Zespół reagowania na incydenty związane z systemami sterowania przemysłowego (Industrial Control Systems Cyber Emergency Response Team - ICS-CERT)

ICS-CERT) https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team

ICS-CERT działa w ramach Krajowego Centrum Integracji Cyberbezpieczeństwa i Komunikacji (National Cybersecurity and Communications Integration Center - NCCIC), oddziału Biura Cyberbezpieczeństwa i Komunikacji Departamentu Bezpieczeństwa Wewnętrznego (Department of Homeland Security's Office of Cybersecurity and Communications - DHS CS&C). NCCIC/ICS-CERT jest kluczowym elementem Strategii Bezpieczeństwa Systemów Sterowania DHS (DHS Strategy for Securing Control Systems). Głównym celem Strategii jest stworzenie długoterminowej wspólnej wizji, w której skuteczne zarządzanie ryzykiem w zakresie bezpieczeństwa systemów sterowania może być realizowane poprzez skuteczną koordynację działań. ICS-CERT koncentruje się na bezpieczeństwie systemów sterowania we współpracy z US-CERT w celu:

- Reagowania i analizowania incydentów związanych z systemami sterowania.
- Przeprowadzania analizy podatności i złośliwego oprogramowania.

- Zapewnienia wsparcia w miejscu zdarzenia podczas reagowania na incydenty i prowadzonej analizie kryminalistycznej.
- Zapewnienia świadomości sytuacyjnej w formie użytecznych informacji analitycznych.
- Koordynacji odpowiedzialnego informowania o podatnościach/wyzwaniach.
- Udostępniania i koordynowania wymiany informacji o podatnościach i analizach zagrożeń za pośrednictwem materiałów informacyjnych i ostrzeżeń.

ICS-CERT koordynuje działania związane z bezpieczeństwem systemów sterowania oraz wymianę informacji z agencjami i organizacjami rządowymi, regionalnymi i lokalnymi, społecznością analityczną oraz podmiotami sektora prywatnego, w tym sprzedawcami, właścicielami i operatorami oraz międzynarodowymi i prywatnymi zespołami CERT. Nacisk na zagadnienia cyberbezpieczeństwa systemów sterowania umożliwia bezpośrednią koordynację działań pomiędzy wszystkimi członkami społeczności infrastruktury krytycznej.

Jako funkcjonalny komponent NCCIC, ICS-CERT zapewnia skoncentrowane możliwości operacyjne w zakresie obrony środowisk systemów sterowania przed pojawiającymi się cyberzagrożeniami.

ICS-CERT zapewnia sprawną koordynację incydentów bezpieczeństwa związanych z systemami sterowania oraz wymianę informacji z instytucjami i organizacjami rządowymi, regionalnymi i lokalnymi, społecznością analityczną, podmiotami sektora prywatnego, w tym sprzedawcami, właścicielami i operatorami oraz międzynarodowymi i prywatnymi zespołami reagowania na incydenty bezpieczeństwa komputerowego (CSIRT). Skupienie się na kwestiach cyberbezpieczeństwa systemów sterowania zapewnia bezpośrednią ścieżkę koordynacji działań dla wszystkich członków społeczności zainteresowanych stron.

Narzędzie do oceny cyberbezpieczeństwa (CSET®)

http://ics-cert.us-cert.gov/Assessments

Narzędzie oceny cyberbezpieczeństwa (CSET®) jest produktem DHS, który wspomaga organizacje w ochronie ich kluczowych krajowych cyberaktywów. Zostało ono opracowane pod kierownictwem DHS ICS-CERT przez ekspertów ds. cyberbezpieczeństwa przy wsparciu NIST. Narzędzie to zapewnia użytkownikom systematyczne i powtarzalne podejście do oceny stanu bezpieczeństwa ich cybersystemów i cybersieci. Zawiera ono zarówno wysokopoziomowe, jak i szczegółowe kwestie dotyczące wszystkich systemów sterowania przemysłowego i systemów informacyjnych.

CSET jest desktopową aplikacją, która prowadzi użytkowników krok po kroku przez proces oceny ich systemów sterowania i praktyk bezpieczeństwa sieci informacyjnych pod kątem zgodności z uznanymi standardami branżowymi. Wynikiem działania CSET jest lista priorytetowych zaleceń mających na celu poprawę stanu cyberbezpieczeństwa przedsiębiorstwa oraz systemów sterowania przemysłowego. Narzędzie czerpie rekomendacje z biblioteki standardów, wytycznych i praktyk z zakresu cyberbezpieczeństwa. Każde zalecenie jest powiązane z zestawem działań, które mogą być zastosowane w celu poprawy cyberzabezpieczeń.

CSET został zaprojektowany tak, aby można go było łatwo zainstalować i używać na samodzielnym laptopie lub stacji roboczej. Uwzględnia on szereg dostępnych standardów pochodzących z organizacji takich jak NIST, NERC, Transportation Security Administration (TSA), Departament Obrony USA (DoD) i innych. Po wybraniu przez użytkownika narzędzia określonego standardu lub standardów, CSET otworzy zestaw pytań, na które należy odpowiedzieć. Odpowiedzi na te pytania zostaną porównane z wybranym poziomem zapewnienia bezpieczeństwa, a następnie zostanie wygenerowany szczegółowy raport wskazujący obszary wymagające potencjalnej poprawy. CSET stanowi dobry sposób na przeprowadzenie samooceny stanu bezpieczeństwa środowiska systemu sterowania.

Zalecane praktyki ICS-CERT

https://ics-cert.us-cert.gov/Introduction-Recommended-Practices

ICS-CERT współpracuje ze społecznością zajmującą się systemami sterowania w celu zweryfikowania zalecanych praktyk, udostępnianych przez ekspertów branżowych, przed ich publicznym udostępnieniem.

Zalecane praktyki są opracowywane z myślą o zmniejszeniu narażenia i podatności użytkowników na cyberataki. Zalecenia te opierają się na zrozumieniu cyberzagrożeń, podatności systemów sterowania i ścieżek ataków oraz na projektowaniu bezpiecznej architektury.

Grupa robocza ds. zalecanych praktyk wybiera tematy, które mają być wdrożone w części poświęconej zalecanym praktykom. Grupa robocza opracowuje i weryfikuje pod kątem poprawności dodatkowe dokumenty zawierające szczegóły dotyczące szerokiego zakresu zagadnień związanych z systemami sterowania, cyberpodatności i sposobów ich łagodzenia. Dokumenty te są uaktualniane, a kolejne tematy są dodawane w celu uwzględnienia dodatkowych treści i pojawiających się problemów.

Instytut Inżynierów Elektryków i Elektroników (*Institute of Electrical and Electronics Engineers, Inc. - IEEE*)

http://www.ieee.org

IEEE 1686-2007 - Standard for Substation IED Cybersecurity Capabilities.

W niniejszym standardzie zdefiniowano funkcje i cechy podstacji inteligentnych urządzeń elektronicznych (ang. intelligent electronic devices - IEDs), w celu realizacji programów ochrony infrastruktury krytycznej. Standard ten dotyczy bezpieczeństwa w zakresie dostępu, działania, konfiguracji, aktualizacji oprogramowania układowego oraz pobierania danych z urządzenia IED. W standardzie nie uwzględniono kwestii łączności na potrzeby ochrony systemu elektroenergetycznego (teleochrony). Szyfrowanie zapewniające bezpieczną transmisję danych zarówno w podstacji jak i poza nią, w tym kontrola nadzorcza i pozyskiwanie danych, nie jest przedmiotem niniejszego standardu, jako że zagadnienia te są przedmiotem innych prac.

IEEE P1711 - Standard for a Cryptographic Protocol for Cybersecurity of Substation Serial Links.

Standard ten definiuje protokół kryptograficzny zapewniający integralność i opcjonalnie poufność dotyczącą cyberbezpieczeństwa łączy szeregowych. Nie dotyczy on konkretnych aplikacji lub implementacji sprzętowych i jest niezależny od podstawowego protokołu komunikacyjnego.

IEEE 1815-2012 - Standard for Electric Power System Communications-Distributed Network Protocol (DNP3).

Standard ten opisuje protokół DNP3 SCADA, włączając w to wersję piątą procedury uwierzytelniania warstwy aplikacji zwanej DNP3 Secure Authentication (DNP3-SAv5). DNP3-SAv5 wykorzystuje proces HMAC do weryfikacji, czy dane i polecenia są odbierane (bez manipulowania) od autoryzowanych indywidualnych użytkowników lub urządzeń, przy jednoczesnym ograniczeniu obciążenia obliczeniowego i komunikacyjnego.

SAv5 obsługuje zdalną aktualizację (dodawanie/zmianę/odwoływanie) danych uwierzytelniających użytkownika przy użyciu technik symetrycznych lub PKI. SAv5 uwierzytelnia, ale nie szyfruje wiadomości, dlatego nie zapewnia poufności. SAv5 może być stosowana razem z technikami szyfrowania, takimi jak TLS lub IEEE 1711, gdy wymagane jest zapewnienie poufności.

Instytut Ochrony Infrastruktury Informatycznej (*Institute for Information Infrastructure Protection - I3P*)

http://www.thei3p.org/

Instytut I3P jest konsorcjum wiodących krajowych (USA) instytucji zajmujących się cyberbezpieczeństwem, w tym akademickich ośrodków badawczych, laboratoriów rządowych i organizacji non-profit. Został on założony we wrześniu 2001 roku, aby pomóc w zaspokojeniu powszechnie znanych potrzeb w zakresie badań i rozwoju (R&D), mających na celu ochronę krajowej infrastruktury informacyjnej przed katastrofalnymi awariami. Główną rolą Instytutu jest koordynacja krajowego programu badawczo-rozwojowego w zakresie cyberbezpieczeństwa oraz pomoc w budowaniu

powiązań między środowiskiem akademickim, przemysłem i rządem. Instytut I3P kontynuuje prace nad identyfikacją i rozwiązywaniem krytycznych problemów badawczych w zakresie ochrony infrastruktury informacyjnej oraz otwieraniem kanałów informacyjnych pomiędzy naukowcami, decydentami i operatorami infrastruktury. Obecnie I3P realizuje następujące zadania:

- Wspieranie współpracy między środowiskiem akademickim, przemysłem i rządem w zakresie istotnych problemów związanych z cyberbezpieczeństwem.
- Opracowywanie, zarządzanie i wspieranie projektów badawczych na skalę krajową.
- Zapewnienie naukowcom ubiegającym się o stopień doktora, wykładowcom i naukowcom badawczym możliwości uzyskania stypendium badawczego.
- Organizowanie warsztatów, spotkań i konferencji poświęconych cyberbezpieczeństwu i ochronie infrastruktury informacyjnej.
- Tworzenie i wspieranie bazy wiedzy, jako internetowego narzędzia wymiany i dystrybucji informacji wśród członków I3P i innych osób pracujących nad wyzwaniami związanymi z bezpieczeństwem informacji.

Komitety Techniczne 65 i 57 Międzynarodowej Komisji Elektrotechnicznej (*International Electrotechnical Commission - IEC*)

http://www.iec.ch/

IEC jest organizacją standaryzacyjną, która przygotowuje i publikuje międzynarodowe standardy dla wszystkich technologii elektrycznych, elektronicznych i pokrewnych. Standardy te służą za podstawę do tworzenia narodowych standardów oraz jako punkty odniesienia przy opracowywaniu międzynarodowych przetargów i kontraktów. Członkami IEC są producenci, dostawcy, dystrybutorzy, sprzedawcy, konsumenci i użytkownicy, agencje rządowe wszystkich szczebli, stowarzyszenia zawodowe, stowarzyszenia handlowe oraz podmioty opracowujące standardy z ponad 60 krajów.

W 2004 roku Podkomitet Techniczny IEC 65C ds. Sieci Przemysłowych, poprzez swoją grupę roboczą WG13 ds. cyberbezpieczeństwa, rozpoczął prace nad zagadnieniami bezpieczeństwa - w ramach normy IEC 61784 - dotyczącymi fieldbusów i innych

przemysłowych sieci komunikacyjnych. Wyniki tych prac zostały przedstawione w części 4, zatytułowanej "Cyfrowa transmisja danych do pomiaru i sterowania - Profile bezpiecznej komunikacji w sieciach przemysłowych."

TC65 WG10 pracuje nad rozszerzeniem zakresu tej komunikacji na poziomie obiektowym, aby uwzględnić standardy bezpieczeństwa w typowych scenariuszach sieci automatyki. Norma będąca wynikiem tych prac to IEC 62443, zatytułowana "Bezpieczeństwo pomiarów i sterowania procesami przemysłowymi - Bezpieczeństwo sieci i systemu". Jest ona oparta na modułowej architekturze bezpieczeństwa składającej się z zestawów wymagań. Moduły te są mapowane na komponenty ICS i architekturę sieci. Wynikające z tego wymagania mogą być następnie wykorzystywane jako wzór do składania zapytań ofertowych (*ang. Requests for Proposals - RFP*) dotyczących standardów teleinformacyjnych oraz do przeprowadzania audytów bezpieczeństwa.

TC 57 koncentruje się na zarządzaniu systemami zasilania i związanej z tym wymianie informacji i jest podzielona na szereg grup roboczych. Każda grupa robocza składa się z członków krajowych komitetów standaryzacyjnych z krajów, które uczestniczą w IEC. Każda grupa robocza jest odpowiedzialna za rozwój standardów w ramach swojej dziedziny. Obecnie działające grupy robocze to:

- WG 3: Protokoły telekontroli.
- WG 9: Automatyzacja dystrybucji z wykorzystaniem systemów linii dystrybucyjnych.
- WG 10: Komunikacja IED systemu elektroenergetycznego i powiązane modele danych.
- WG 13: Interfejs aplikacji systemu zarządzania energią (*Energy management system application program interface - EMS-API*).
- WG 14: Interfejsy systemowe do zarządzania dystrybucją (*System interfaces for distribution management - SIDM*).
- WG 15: Bezpieczeństwo danych i komunikacji.

- WG 16: Komunikacja na zderegulowanym rynku energii.
- WG 17: Systemy komunikacji dla rozproszonych zasobów energetycznych (*Distributed Energy Resources - DER*).
- WG 18: Elektrownie wodne – Komunikacja w zakresie monitorowania i sterowania.
- WG 19: Interoperacyjność w ramach TC 57 w perspektywie długoterminowej.
- WG 20: Planowanie (jednopasmowych) systemów linii elektroenergetycznych (IEC 60495); Planowanie (jednopasmowych) systemów linii elektroenergetycznych (IEC 60663).
- WG 21: Interfejsy i profile protokołów istotne dla systemów podłączonych do sieci elektrycznej.

ISA99, Standardy bezpieczeństwa systemów automatyki przemysłowej i sterowania

http://www.isa.org/isa99

Komitet opracowywania standardów ISA99 skupia ekspertów z całego świata zajmujących się cyberbezpieczeństwem przemysłowym, w celu opracowania standardów ISA[60] dotyczących bezpieczeństwa automatyki przemysłowej i systemów sterowania (IACS). Prace prowadzone przez ISA99 są standaryzowane przez IEC w ramach serii norm IEC 62443. Komitet koncentruje się na poprawie poufności, integralności i dostępności komponentów lub systemów wykorzystywanych w automatyce i sterowaniu oraz zapewnia kryteria zamawiania i wdrażania bezpiecznych systemów sterowania. Zgodność z wytycznymi komitetu wpłynie na poprawę bezpieczeństwa elektronicznego systemów automatyki przemysłowej i sterowania, pomoże w identyfikacji podatności i ich eliminacji, zmniejszając tym samym ryzyko narażenia poufnych informacji bądź spowodowania degradacji lub awarii systemu sterowania automatyki przemysłowej.

Wszystkie standardy i raporty techniczne ISA-62443 są podzielone na cztery kategorie: informacje ogólne, polityki i procedury, system oraz komponenty.

[60] International Society of Automation

- Kategoria Informacje ogólne obejmuje informacje powszechne lub źródłowe, takie jak koncepcje, modele i terminologia. Obejmuje również produkty opisujące metryki bezpieczeństwa i cykle życia zabezpieczeń dla IACS.
- Produkty z kategorii Polityki i Procedury są przeznaczone dla właścicieli aktywów. Dotyczą one różnych aspektów tworzenia i utrzymywania efektywnego programu bezpieczeństwa IACS.
- Kategoria System obejmuje produkty robocze, które opisują wytyczne i wymagania dotyczące projektowania systemu w celu bezpiecznej integracji systemów sterowania. Kluczowym elementem jest model projektowy stref i przepustów.
- Kategoria Komponenty obejmuje produkty robocze, które opisują rozwój konkretnych wyrobów i wymagania techniczne dotyczące produktów systemu sterowania. Są one przeznaczone przede wszystkim dla dostawców produktów sterowania, ale mogą być również wykorzystywane przez integratorów i właścicieli zasobów w celu pomocy w zamawianiu bezpiecznych produktów.

Aktualny status dokumentów ISA-62443 jest dostępny na stronie ISA99 Wiki pod adresem: http://isa99.isa.org/ISA99 Wiki/

Informacje ogólne

- **ISA-62443-1-1 (IEC/TS 62443-1-1)** (wcześniej określana jako „ISA-99 Część 1”) została pierwotnie opublikowana jako norma ISA ANSI/ISA-99.00.01-2007, jak również specyfikacja techniczna IEC/TS 62443-1-1.
- **ISA-TR62443-1-2 (IEC 62443-1-2)** jest głównym glosariuszem terminów, używanych przez komitet ISA99. Dokument ten jest szkicem roboczym.
- **ISA-62443-1-3 (IEC 62443-1-3)** określa zbiór wskaźników zgodności dla bezpieczeństwa IACS.
- **ISA-TR62443-1-4 (IEC/TS 62443-1-4)** definiuje cykl życia zabezpieczeń IACS i przypadek użycia.

Polityki i Procedury

- **ISA-62443-2-1** (**IEC 62443-2-1)** (poprzednio określana jako "ANSI/ISA 99.02.01-2009 lub ISA-99 Part 2") dotyczy sposobu ustanowienia programu bezpieczeństwa IACS. Norma ta jest zatwierdzona i opublikowana przez IEC jako IEC 62443-2-1. Po poddaniu rewizji, umożliwia ściślejsze dostosowanie do serii norm ISO 27000.
- **ISA-TR62443-2-2 (IEC 62443-2-2)** dotyczy sposobu obsługi programu bezpieczeństwa IACS.
- **ISA-TR62443-2-3 (IEC/TR 62443-2-3)** jest raportem technicznym na temat zarządzania poprawkami w środowiskach IACS.
- **ISA-62443-2-4 (IEC 62443-2-4)** koncentruje się na certyfikacji polityk i praktyk bezpieczeństwa dostawców IACS. Dokument ten został opracowany przez organizację WIB i jest obecnie produktem roboczym komitetu IEC TC65/WG10. Proponowana wersja ISA będzie krajową publikacją normy IEC w Stanach Zjednoczonych.

System

- **ISA-TR62443-3-1** (**IEC/TR 62443-3-1**) jest raportem technicznym na temat odpowiednich technologii dla bezpieczeństwa IACS. Raport ten został zatwierdzony i opublikowany jako ANSI/ISA-TR99.00.01-2007, a obecnie jest w trakcie rewizji.
- **ISA-62443-3-2 (IEC 62443-3-2)** dotyczy sposobu definiowania poziomów zapewnienia bezpieczeństwa z wykorzystaniem koncepcji stref i łączy.
- **ISA-62443-3-3 (IEC 62443-3-3)** definiuje szczegółowe wymagania techniczne w zakresie bezpieczeństwa IACS. Norma ta została opublikowana jako ANSI/ISA-62443-3-3 (99.03.03)-2013. Wcześniej była oznaczona numerem ISA-99.03.03.

Komponent

- Norma **ISA-62443-4-1 (IEC 62443-4-1)** dotyczy wymagań dla rozwoju bezpiecznych produktów i rozwiązań IACS. Norma ta jest obecnie w trakcie opracowywania.

- Seria **ISA-62443-4-2 (IEC 62443-4-2)** dotyczy szczegółowych wymagań technicznych dla poziomu komponentów IACS. Norma ta jest obecnie w trakcie opracowywania.

ISA100, Systemy bezprzewodowe stosowane w automatyce

http://www.isa.org/isa100

Komitet ISA100 ustanawia standardy, zalecane praktyki, raporty techniczne i powiązane informacje, które określają procedury wdrażania systemów bezprzewodowych w środowisku automatyki i sterowania, ze szczególnym uwzględnieniem poziomu lokalnego. Wytyczne są skierowane do osób odpowiedzialnych za cały cykl życia, w tym za projektowanie, wdrażanie, bieżącą obsługę, skalowalność lub zarządzanie systemami automatyki przemysłowej i sterowania. Dotyczą one użytkowników, integratorów systemów, specjalistów oraz producentów i sprzedawców systemów sterowania.

ISO 27001

http://www.iso.org/

http://www.27000.org

Norma ISO 27001 określa model ustanawiania, wdrażania, obsługi, monitorowania, przeglądu, utrzymywania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji. Celem samej normy jest "dostarczenie wymagań do ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji (Information Security Management System - ISMS)". Przyjęcie tej normy powinno być decyzją strategiczną. Ponadto, "na projekt i wdrożenie systemu zarządzania bezpieczeństwem informacji w organizacji mają wpływ potrzeby i cele organizacji, wymagania dotyczące bezpieczeństwa, stosowane procesy organizacyjne oraz wielkość i struktura organizacji." Sekcje merytoryczne normy obejmują:

- Kontekst organizacji.
- Kierowanie bezpieczeństwem informacji.
- Planowanie ISMS.

- Wsparcie.
- Funkcjonowanie.
- Ocenę działania.
- Doskonalenie.
- Załącznik a - Lista zabezpieczeń i celów ich stosowania.

Wersja normy z 2005 roku w dużym stopniu wykorzystywała model Plan-Do-Check-Act[61] do strukturyzacji procesów i odzwierciedlała zasady określone w wytycznych OECG[62] (zob. http://www.oecd.org). W najnowszej wersji z 2013 r. położono jednak większy nacisk na pomiar i ocenę skuteczności systemu ISMS organizacji.

ISO 27002

http://www.iso.org/, http://www.27000.org

Norma ISO 27002 "ustanawia wytyczne i ogólne zasady dotyczące inicjowania, wdrażania, utrzymywania i doskonalenia zarządzania bezpieczeństwem informacji w organizacji". Poszczególne środki bezpieczeństwa wymienione w normie mają na celu spełnienie specyficznych wymagań zidentyfikowanych w drodze formalnego oszacowania ryzyka. Norma ma również stanowić przewodnik w przygotowaniu "organizacyjnych standardów bezpieczeństwa i skutecznych praktyk zarządzania bezpieczeństwem oraz wspierać budowanie zaufania do działań międzyorganizacyjnych." [63]

W 2013 r. opublikowano aktualną wersję normy ISO 27002:2013. Zawiera 114 zabezpieczeń, czyli mniej niż poprzednie 133 zabezpieczenia przedstawione w wersji

[61] Cykl Deminga (określany też jako cykl P-D-S-A z ang. *Plan-Do-Study-Act* lub koło Deminga) – schemat ilustrujący podstawową zasadę ciągłego ulepszania (ciągłego doskonalenia, kaizen), stworzoną przez Williama Edwardsa Deminga, amerykańskiego specjalistę statystyka pracującego w Japonii.

[62] Organizacja Współpracy Gospodarczej i Rozwoju (*ang. Organisation for Economic Co-operation and Development*).

[63] http://www.27000.org/iso-27002.htm

z 2005 roku. Jednak w celu zapewnienia dodatkowej przejrzystości, zabezpieczenia te zostały przedstawione w 14, a nie jak pierwotnie w 11 kategoriach:

- Polityka bezpieczeństwa.
- Organizacja bezpieczeństwa informacji.
- Bezpieczeństwo zasobów ludzkich.
- Zarządzanie aktywami.
- Kontrola dostępu.
- Kryptografia.
- Bezpieczeństwo fizyczne i środowiskowe.
- Bezpieczeństwo operacji.
- Bezpieczeństwo łączności.
- Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych.
- Relacje z dostawcami.
- Zarządzanie incydentami związanymi z bezpieczeństwem informacji.
- Aspekty bezpieczeństwem informacji związane z ciągłością działania.
- Zgodność.

Międzynarodowy Komitet Wielkich Sieci Elektrycznych (*fr. Conseil International des Grands Réseaux Électriques - CIGRE*)[64]

http://www.cigre.org/

CIGRE jest międzynarodowym stowarzyszeniem typu non-profit z siedzibą we Francji. Stowarzyszenie powołało kilka komitetów badawczych w celu promowania rekomendowanych praktyk i opracowywanie zaleceń oraz wspierania międzynarodowej wymiany wiedzy w branży elektrycznej. Trzy z komitetów badawczych skupiają się na systemach sterowania:

[64] ang. International Council on Large Electric Systems.

- Komitet B3 ds. Podstacji zajmuje się wdrażaniem zaawansowanych rozwiązań technologicznych w urządzeniach i systemach w celu zwiększenia ich niezawodności i dostępności.
- Komitet C2 ds. Eksploatacji i Sterowania Systemami koncentruje się na możliwościach technicznych niezbędnych do bezpiecznej i ekonomicznej eksploatacji istniejących systemów elektroenergetycznych, w tym centrów sterowania i operatorów.
- Komitet D2 ds. Systemów Informatycznych i Telekomunikacji w Systemach Elektroenergetycznych monitoruje technologie pojawiające się w branży i ocenia ich ewentualny potencjał. Ponadto koncentruje się na wymaganiach dotyczących bezpieczeństwa systemów informacyjnych i usług związanych z systemami sterowania.

LOGIIC – Powiązanie przemysłu naftowego i gazowego w celu poprawy cyberbezpieczeństwa

http://www.dhs.gov/csd-logiic

Program LOGIIC został stworzony w 2004 roku w celu ułatwienia współpracy w zakresie badań, rozwoju, testowania i oceny procedur mających na celu poprawę cyberbezpieczeństwa w cyfrowych systemach sterowania przemysłu naftowego. W ramach programu realizowane są wspólne projekty badawczo-rozwojowe mające na celu poprawę poziomu cyberbezpieczeństwa w krytycznych systemach będących przedmiotem zainteresowania sektora ropy naftowej i gazu ziemnego. Celem programu jest promowanie interesów sektora przy jednoczesnym zachowaniu bezstronności, niezależności uczestników i neutralności wobec dostawców. Po udanym pierwszym projekcie, utworzono oficjalnie konsorcjum LOGIIC, w skład którego wchodzą: DHS, Automation Federation oraz pięć największych firm naftowych i gazowych. W ramach programu LOGIIC zrealizowano kilka projektów badawczo-rozwojowych, jednocześnie planowane i rozpoczynane są kolejne projekty.

Narodowy program testów systemów SCADA (NSTB SCADA)

http://energy.sandia.gov/infrastructure-security/cyber/scada-systems/testbeds/national-scada-testbed/

Narodowy Program Testów Systemów Kontroli Nadzoru i Akwizycji Danych (*National Supervisory Control and Data Acquisition Test Bed - NTSB SCADA*) to sponsorowane przez Biuro ds. Dostaw Energii i Niezawodności Systemów Energetycznych Departamentu Energii (*DOE Office of Electricity Delivery and Energy Reliability - OE*) źródło pomocy w zabezpieczaniu krajowych systemów sterowania energią. Łączy ono najnowocześniejsze urządzenia do testowania systemów operacyjnych z badaniami, rozwojem i szkoleniami w celu odkrycia i wyeliminowania krytycznych podatności i zagrożeń bezpieczeństwa w sektorze energetycznym.

We współpracy z sektorem energetycznym, NSTB SCADA ma na celu:

- Identyfikację i łagodzenie istniejących podatności na zagrożenia.
- Ułatwianie rozwoju standardów bezpieczeństwa.
- Pełnienie roli niezależnej jednostki testującej systemy SCADA i powiązane technologie systemów sterowania.
- Identyfikowanie i promowanie najlepszych praktyk w zakresie cyberbezpieczeństwa.
- Zwiększanie świadomości w zakresie bezpieczeństwa systemów sterowania w sektorze energetycznym.
- Rozwój zaawansowanych architektur i technologii systemów sterowania, które są bezpieczniejsze i solidniejsze.

Partnerami NSTB są Idaho National Laboratory, Sandia National Laboratories, Argonne National Laboratory, Pacific Northwest National Laboratory oraz National Institute of Standards and Technology.

Specjalne publikacje NIST SP serii 800 - Rekomendacje w zakresie bezpieczeństwa

http://csrc.nist.gov/publications/nistpubs/index.html

Seria dokumentów NIST Special Publication 800 dotyczących technologii informacyjnej zawiera informacje na temat badań, wsparcia i pomocy udzielanej przez Laboratorium Technologii Informatycznych NIST (International Information Technology Laboratory - ITL) w zakresie bezpieczeństwa komputerowego oraz działań podejmowanych we współpracy z przemysłem, instytucjami rządowymi i organizacjami akademickimi. Obszary zainteresowania obejmują technologie i zastosowania kryptograficzne, zaawansowane uwierzytelnianie, infrastrukturę klucza publicznego, bezpieczeństwo sieci internetowych, kryteria i zapewnienie bezpieczeństwa oraz zarządzanie bezpieczeństwem i wsparcie. W uzupełnieniu do NIST SP 800-82, poniżej znajduje się lista kilku dodatkowych dokumentów serii 800, które mają istotne znaczenie dla społeczności związanej z bezpieczeństwem ICS. Dokumenty te, jak również wiele innych, są dostępne pod adresem URL podanym powyżej.

- NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems [19].
- NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments [79].
- NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations. a System Life Cycle Approach for Security and Privacy [21].
- NSC 800-39, Managing Information Security Risk: Organization, Mission, and Information System View [20].
- NIST SP 800-40 Revision 3, Guide to Enterprise Patch Management Technologies [40].
- NIST SP 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy [85].
- NIST SP 800-48 Revision 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks 0.
- NIST SP 800-50, Building an Information Technology Security Awareness and Training Program [61].

- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations [22].
- NIST SP 800-53A Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans [23]. NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide [59].
- NIST SP 800-63-2, Electronic Authentication Guideline [53].
- NIST SP 800-64 Revision 2, Security Considerations in the Information System Development Life Cycle [46].
- NIST SP 800-70 Revision 2, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers [26].
- NIST SP 800-77, Przewodnik po IPsec VPNs [74].
- NIST SP 800-83 Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops [60].
- NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response [93].
- NIST SP 800-88 Revision 1, Guidelines for Media Sanitization [78].
- NIST SP 800-92, Guide to Computer Security Log Management [68].
- NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) [55].
- NIST SP 800-97, Establishing Robust Security Networks: a Guide to IEEE 802.11i [64].
- NIST SP 800-100, Podręcznik bezpieczeństwa informacji: a Guide for Managers [27].
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices [94]. NIST SP 800-115, Przewodnik techniczny do testowania i oceny bezpieczeństwa informacji [41]
- NIST SP 800-123, Guide to General Server Security [95].
- NIST SP 800-127, Guide to Securing WiMAX Wireless Communications [96].

- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems [97].
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations [81]

Projekt NIST dotyczący bezpieczeństwa systemów sterowania przemysłowego (*NIST Industrial Control System Security Project*)

http://csrc.nist.gov/groups/SMA/fisma/ics/

W ramach ciągłych wysiłków zmierzających do opracowania efektywnych standardów bezpieczeństwa i wytycznych dla agencji federalnych i ich wykonawców w ramach ustawy o zarządzaniu bezpieczeństwem informacji federalnych (Federal Information Security Management Act) oraz w celu ochrony infrastruktury krytycznej kraju, NIST kontynuuje współpracę z podmiotami sektora publicznego i prywatnego w zakresie zagadnień bezpieczeństwa specyficznych dla danego sektora. Systemy sterowania przemysłowego i procesowego stanowią integralną część amerykańskiej infrastruktury krytycznej, a ochrona tych systemów jest priorytetem dla rządu federalnego. Projekt ten ma na celu oparcie się na obecnych standardach bezpieczeństwa FISMA i zapewnienie ukierunkowanego rozszerzenia i/lub interpretacji tych standardów w stosunku do systemów sterowania przemysłowego i procesowego tam, gdzie jest to wymagane. Ponieważ wiele systemów sterowania procesami przemysłowymi i technologicznymi wspiera organizacje sektora prywatnego, NIST będzie prowadzić ciągłą współpracę z organizacjami zajmującymi się normami dotyczącymi tych specyficznych typów systemów.

Projekt NIST dotyczący cyberbezpieczeństwa systemów produkcyjnych (*NIST Cybersecurity for Manufacturing Systems Project*)

http://www.nist.gov/el/isd/cs/csms.cfm

Inteligentne systemy produkcyjne muszą być skutecznie zabezpieczane przed podatnościami, które mogą powstać w wyniku rosnącej powszechności ich podłączania, korzystania z sieci bezprzewodowych i czujników oraz powszechnego stosowania

technologii informacyjnych. Producenci niechętnie stosują popularne technologie zabezpieczeń, takie jak szyfrowanie i uwierzytelnianie urządzeń, ze względu na obawy o potencjalne negatywne skutki dla wydajności ich systemów. Sytuację pogarsza jeszcze środowisko zagrożeń, które zmieniło się diametralnie wraz z pojawieniem się zaawansowanych, uporczywych ataków, takich jak Stuxnet, ukierunkowanych na systemy przemysłowe. W ramach tego projektu zostaną opracowane ramy zarządzania ryzykiem w zakresie cyberbezpieczeństwa oraz wytyczne, metody, mierniki i narzędzia, które umożliwią producentom, dostawcom technologii i rozwiązań ocenę i zapewnienie cyberbezpieczeństwa inteligentnych systemów produkcyjnych. Ramy i metodologia zarządzania ryzykiem w zakresie cyberbezpieczeństwa będą stymulować wdrażanie przez producentów i umożliwią efektywne wykorzystanie technologii bezpieczeństwa, co prowadzi do powstania inteligentnych systemów produkcyjnych oferujących bezpieczeństwo, niezawodność, odporność i ciągłość działania w obliczu zakłóceń i znaczących incydentów.

Projekt NIST dotyczący cyberbezpieczeństwa inteligentnych systemów sieci energetycznych (*NIST Cybersecurity for Smart Grid Systems*)

http://www.nist.gov/el/smartgrid/cybersg.cfm

Cyberbezpieczeństwo inteligentnych sieci energetycznych powinno uwzględniać nie tylko ataki celowe, takie jak ataki niezadowolonych pracowników, szpiegostwo przemysłowe i terroryzm, ale także nieumyślne naruszenia infrastruktury informacyjnej spowodowane błędami użytkowników, usterkami sprzętu i klęskami żywiołowymi. Smart Grid Interoperability Panel (SGIP) Cybersecurity Committee (SGCC), który jest prowadzony i zarządzany przez NIST Information Technology Laboratory (ITL), Computer Security Division, w roku budżetowym 2014 prowadził działania mające na celu zaspokojenie krytycznych potrzeb w zakresie cyberbezpieczeństwa w obszarach zaawansowanych wymogów bezpieczeństwa infrastruktury pomiarowej (Advanced Metering Infrastructure - AMI), przetwarzania w chmurze, łańcucha dostaw oraz zaleceń dotyczących ochrony prywatności związanych z opracowywanymi standardami. W ramach tego projektu planowane jest opracowanie podstawowych wytycznych w zakresie cyberbezpieczeństwa, przegląd

standardów i wymagań dotyczących cyberbezpieczeństwa, prowadzenie działań informacyjnych oraz promowanie współpracy w zakresie szeroko pojętego cyberbezpieczeństwa inteligentnych sieci energetycznych.

Projekt NIST dotyczący infrastruktury testów systemu inteligentnych sieci energetycznych (*NIST Smart Grid System Testbed Facility*)

http://www.nist.gov/el/smartgrid/sgtf.cfm

Zgodnie z Energy Independence and Security Act (*EISA*) z 2007 r., NIST ma za zadanie ułatwić opracowanie standardów interoperacyjności, które umożliwią pomyślne wdrożenie rozwijającego się cyberfizycznego systemu krajowej sieci energetycznej, znanego jako inteligentna sieć energetyczna (*Smart Grid - SG*). Smart Grid Testbed Facility stworzy unikalny zestaw połączonych i wzajemnie oddziałujących na siebie laboratoriów w kilku kluczowych obszarach pomiarowych - zlokalizowanych bezpośrednio na terenie NIST Gaithersburg - które przyspieszą rozwój standardów interoperacyjności SG poprzez zapewnienie połączonej platformy testowej do przeprowadzania badań systemów, charakterystyki protokołów inteligentnych sieci oraz walidacji standardów SG, ze szczególnym uwzględnieniem mikrosieci[65]. Pomiary obejmą osiem obszarów: kondycjonowanie poboru mocy, metrologię synchrofazorów, cyberbezpieczeństwo, precyzyjną synchronizację czasu, pomiary energii elektrycznej, modelowanie/ocenę komunikacji w ramach SG, interfejsy czujników oraz magazynowanie energii. Stanowisko badawcze będzie służyło jako główny obiekt badawczy programu Smart Grid, aby zaspokoić potrzeby pomiarowe rozwijającego się środowiska przemysłowego SG, w tym kwestie pomiarów i walidacji.

[65] Mikrosieć definiuje się jako podzbiór sieci, który może być szybko odłączony od większej sieci i funkcjonować niezależnie od niej.

Północnoamerykański Komitet ds. Niezawodności Energetycznej (*North American Electric Reliability Corporation - NERC*)

http://www.nerc.com/

Misją NERC jest poprawa niezawodności i bezpieczeństwa hurtowego systemu elektroenergetycznego w Ameryce Północnej. W tym celu NERC opracowuje i egzekwuje standardy niezawodnościowe, monitoruje system elektroenergetyczny, ocenia jego przyszłą przydatność, przeprowadza audyty przygotowania do działania właścicieli, operatorów i użytkowników, a także kształci i szkoli pracowników branży. NERC jest organizacją samoregulującą, która opiera się na różnorodnej i zbiorowej wiedzy fachowej uczestników sektora. Jako Organizacja Niezawodności Energetycznej (*Electric Reliability Organization*), NERC podlega kontroli Federalnej Komisji Regulacji Energetyki w USA oraz władzom rządowym w Kanadzie.

NERC wydała zestaw standardów z zakresu cyberbezpieczeństwa w celu zmniejszenia ryzyka zagrożenia zasobów wytwarzania energii elektrycznej oraz systemów przesyłowych wysokiego napięcia powyżej 100 kV, zwanych również systemami hurtowego przesyłu energii elektrycznej (ang. bulk electric systems). Masowe systemy elektryczne obejmują organy bilansujące, koordynatorów niezawodności, organy wymiany międzysystemowej, dostawców usług przesyłowych, właścicieli sieci przesyłowych, operatorów sieci przesyłowych, właścicieli źródeł wytwórczych, operatorów sieci przesyłowych oraz podmioty obsługujące odbiorców. Standardy cyberbezpieczeństwa obejmują środki audytu i wartości dopuszczalnych poziomów niezgodności, które mogą być powiązane z karami.

Zestaw standardów cyberbezpieczeństwa NERC obejmuje następujące dokumenty:

- CIP-002, Cyberbezpieczeństwo – Identyfikacja krytycznych aktywów związanych z cyberbezpieczeństwem (*Cyber Security - Critical Cyber Asset Identification*).
- CIP-003, Cyberbezpieczeństwo – Środki zarządzania bezpieczeństwem (*Cyber Security - Security Management Controls*).
- CIP-004, Cyberbezpieczeństwo – Personel i szkolenia (*Cyber Security - Personnel & Training*).

- CIP-005, Cyberbezpieczeństwo – Elektroniczne granice bezpieczeństwa (*Cyber Security - Electronic Security Perimeter(s)*).
- CIP-006, Cyberbezpieczeństwo – Fizyczne bezpieczeństwo krytycznych cyberaktywów (*Cyber Security - Physical Security of Critical Cyber Assets*).
- CIP-007, Cyberbezpieczeństwo – Zarządzanie bezpieczeństwem systemów (*Cyber Security - Systems Security Management*).
- CIP-008, Cyberbezpieczeństwo – Zgłaszanie incydentów i planowanie odpowiedzi (*Cyber Security - Incident Reporting and Response Planning*).
- CIP-009, Cyberbezpieczeństwo – Plany odtworzenia krytycznych cyberaktywów (*Cyber Security - Recovery Plans for Critical Cyber Assets*).

Prowadzone przez Instytut SANS kursy w zakresie bezpieczeństwa systemów sterowania

http://ics.sans.org/

Program szkoleń z zakresu bezpieczeństwa systemów sterowania obejmuje praktyczne kursy koncentrujące się na atakowaniu i obronie środowisk systemów sterowania (*Attacking and Defending ICS environments*). Kursy te dostarczają zarówno specjalistom ds. bezpieczeństwa, jak i inżynierom systemów sterowania wiedzę i umiejętności niezbędne do ochrony infrastruktury krytycznej.

Global Industrial Cyber Security Professional (GICSP) jest najnowszym certyfikatem w serii *Global Information Assurance Certification* (GIAC) i koncentruje się na podstawowej wiedzy z zakresu zabezpieczania zasobów infrastruktury krytycznej. GICSP łączy IT, inżynierię i cyberbezpieczeństwo w celu zapewnienia bezpieczeństwa systemów sterowania przemysłowego od momentu ich zaprojektowania do wycofania z eksploatacji.

Panel ds. interoperacyjności inteligentnych sieci (*Smart Grid Interoperability Panel - SGIP*) Grupa robocza ds. cyberbezpieczeństwa (*Cyber Security Working Group - CSWG*)

http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG

Głównym celem grupy roboczej jest opracowanie ogólnej strategii cyberbezpieczeństwa dla inteligentnych sieci (Smart Grid), która obejmuje strategię ograniczania ryzyka w celu zapewnienia interoperacyjności rozwiązań w różnych domenach/komponentach infrastruktury. Strategia cyberbezpieczeństwa powinna obejmować zapobieganie, wykrywanie, reagowanie i odzyskiwanie danych. Wdrożenie strategii cyberbezpieczeństwa wymaga zdefiniowania i wdrożenia ogólnego procesu szacowania ryzyka związanego z cyberbezpieczeństwem sieci Smart Grid.

Prace grupy roboczej zostały udokumentowane w dokumencie NIST Interagency Report (NISTIR) 7628 Revision 1, Guidelines for Smart Grid Cybersecurity [98].

ZAŁĄCZNIK E - FUNKCJE I NARZĘDZIA BEZPIECZEŃSTWA STOSOWANE W ICS

W tej części przedstawiono przegląd funkcji bezpieczeństwa, które są dostępne dla społeczności ICS lub są opracowywane na jej potrzeby. Istnieje szereg produktów zabezpieczających, które są wprowadzane na rynek specjalnie z myślą o ICS, podczas gdy inne rozwiązania są ogólnymi produktami zabezpieczającymi IT, które znajdują zastosowanie w ICS. Wiele z dostępnych produktów oferuje "rozwiązania jednopunktowe" (*ang. "single point solutions"*), w których pojedynczy produkt zabezpieczający oferuje wiele poziomów ochrony. Dodatkowo, oprócz informacji o dostępnych produktach, w tej części przedstawiono również prace badawczo-rozwojowe nad nowymi produktami i technologiami. Podejmowanie decyzji, o zastosowaniu możliwości i narzędzi bezpieczeństwa wymienionych w tym załączniku, każda organizacja powinna oprzeć na analizie ryzyka.

Dioda danych

Dioda danych (zwana również jednokierunkową bramą, deterministycznym jednokierunkowym urządzeniem brzegowym lub siecią jednokierunkową) to osprzęt sieciowy lub urządzenie pozwalające na przesyłanie danych tylko w jednym kierunku, stosowane w celu zapewnienia bezpieczeństwa informacji lub ochrony krytycznych systemów cyfrowych, takich jak systemy sterowania przemysłowego, przed zagrażającymi im cyberatakami. Chociaż urządzenia te są powszechnie stosowane w środowiskach o wysokim poziomie bezpieczeństwa, takich jak systemy obronne, gdzie służą jako połączenia między dwiema lub większą liczbą sieci o różnych klasyfikacjach bezpieczeństwa, technologia ta jest również wykorzystywana do wymuszania jednokierunkowej komunikacji pomiędzy krytycznymi systemami cyfrowymi a niezaufanymi sieciami.

Szyfrowanie

Szyfrowanie chroni poufność danych, kodując je w taki sposób, aby tylko odbiorca, dla którego są przeznaczone, mógł je odkodować. Na rynku dostępne są produkty szyfrujące zaprojektowane specjalnie do zastosowań w systemach ICS, a także

uniwersalne produkty szyfrujące, które obsługują klasyczną komunikację szeregową i Ethernet.

Zapory sieciowe

Zapory sieciowe (*ang. firewalls*) są powszechnie stosowane do rozdzielania sieci w celu ochrony i izolowania systemów ICS. W tych implementacjach wykorzystuje się dostępne na rynku zapory sieciowe, które są skoncentrowane na protokołach internetowych i korporacyjnych protokołach warstwy aplikacji oraz nie są przystosowane do obsługi protokołów ICS. W 2003 r. jeden z producentów zabezpieczeń IT przeprowadził badania mające na celu opracowanie zapory sieciowej opartej na protokole Modbus, która umożliwia podejmowanie decyzji operacyjnych na podstawie wartości nagłówka Modbus/TCP, podczas gdy tradycyjne zapory sieciowe filtrują na podstawie portów TCP/UDP i adresów IP [76]. Obecnie dostępnych jest kilka zapór sieciowych przeznaczonych dla ICS.

Wykrywanie i zapobieganie włamaniom

Sieciowe rozwiązania IDS monitorują ruch sieciowy i stosują różne metody wykrywania, między innymi porównują fragmenty ruchu z sygnaturami znanych ataków. Z kolei wykrywanie włamań na hoście wykorzystuje oprogramowanie (często z sygnaturami ataków), zainstalowane na komputerze-hoście do monitorowania bieżących zdarzeń i danych w systemie komputerowym pod kątem możliwych do wykorzystania exploitów[66]. Produkty IPS rozszerzają wykrywanie włamań o kolejny krok - automatycznie reagują na wykryte exploity, próbując je powstrzymać [57].

Obowiązek ciągłego monitorowania, oceny i szybkiego reagowania na zdarzenia związane z wykrywaniem włamań, spoczywający na zespole bezpieczeństwa, jest czasami zlecany zewnętrznemu dostawcy zarządzanych usług bezpieczeństwa (*ang. managed security service provider - MSSP*). MSSP dysponują silnikami korelacyjnymi i analitycznymi, które przetwarzają i ograniczają ogromną liczbę zdarzeń rejestrowanych w ciągu dnia do niewielkiego podzbioru, który musi być oceniony

[66] Exploit – program mający na celu wykorzystanie istniejących błędów w oprogramowaniu.

indywidualnie. Istnieją również silniki korelacji i analizy dostępne dla dużych organizacji, które chcą wykonywać tę funkcję we własnym zakresie. Produkty bezpieczeństwa i zarządzania zdarzeniami (*ang. security information and event management - SIEM*) są wykorzystywane w niektórych organizacjach do monitorowania, analizowania i korelowania zdarzeń z rejestrów logów systemów IDS i IPS, a także dzienników audytów z innych systemów komputerowych, aplikacji, urządzeń infrastruktury oraz innego sprzętu i oprogramowania, co pozwala na wyszukiwanie prób włamań.

Producenci systemów IDS i IPS opracowują i wdrażają sygnatury ataków dotyczące różnych protokołów ICS, takich jak Modbus, DNP3 i ICCP [58]. Reguły Snort zostały opracowane dla Modbus TCP, DNP3 oraz ICCP. Snort jest systemem wykrywania i zapobiegania włamaniom do sieci typu open source, wykorzystującym język reguł do wykonywania inspekcji opartych na sygnaturach, protokołach i anomaliach. Do platformy Bro IDS dodano również reguły obsługujące protokoły DNP3 i Modbus.

Podobnie jak w przypadku każdego oprogramowania dodawanego do komponentu systemu ICS, wprowadzenie oprogramowania hosta IDS lub IPS może wpłynąć na wydajność systemu. Systemy IPS są powszechnie stosowane we współczesnym sektorze bezpieczeństwa informacji, ale mogą być bardzo zasobochłonne. Systemy te mają zdolność do automatycznej rekonfiguracji systemów w przypadku wykrycia próby włamania. Ta zautomatyzowana i szybka reakcja ma na celu zapobieganie wykorzystaniu exploitów, jednak takie zautomatyzowane narzędzie może zostać wykorzystane przez przeciwnika do wywarcia negatywnego wpływu na działanie systemu ICS poprzez wyłączenie segmentów sieci lub serwera. Fałszywe wyniki mogą również utrudniać działanie systemu ICS.

Oprogramowanie antywirusowe

Oprogramowanie służące do wykrywania i usuwania złośliwego oprogramowania jest tradycyjnie nazywane "oprogramowaniem antywirusowym", mimo, że może ono wykrywać wiele rodzajów złośliwego oprogramowania. Oprogramowanie antywirusowe jest wykorzystywane do przeciwdziałania zagrożeniom związanym ze złośliwym oprogramowaniem poprzez porównywanie plików znajdujących się

w urządzeniach pamięci masowej komputera (niektóre narzędzia wykrywają również złośliwe oprogramowanie w czasie rzeczywistym na obwodzie sieci i/lub na stacji roboczej użytkownika) z wykazem plików zawierających sygnatury złośliwego oprogramowania. Jeśli któryś z plików na komputerze pasuje do profilu znanego złośliwego oprogramowania, jest ono usuwane w procesie od infekowania, dzięki czemu nie może zainfekować innych plików lokalnych, ani przenosić się przez sieć w celu zainfekowania innych plików na innych komputerach. Dostępne są również techniki umożliwiające identyfikację nieznanego złośliwego oprogramowania "na żywo", gdy plik sygnatur nie jest jeszcze dostępny.

Wielu użytkowników końcowych i dostawców systemów ICS zaleca stosowanie w swoich systemach oprogramowania antywirusowego COTS. Opracowali oni nawet wskazówki dotyczące instalacji i konfiguracji w oparciu o własne testy laboratoryjne. Niektórzy producenci systemów ICS zalecają stosowanie oprogramowania antywirusowego w swoich produktach, ale nie oferują żadnych wytycznych w tym zakresie. Niektórzy użytkownicy końcowi i sprzedawcy niechętnie korzystają z oprogramowania antywirusowego, obawiając się, że jego użycie spowoduje problemy z wydajnością ICS lub nawet awarię. NIST i Sandia National Laboratories (SNL) przeprowadziły badania i opracowały raport, który ma pomóc właścicielom/ operatorom ICS we wdrożeniu oprogramowania antywirusowego oraz zminimalizowaniu i ocenie wpływu na wydajność produktów antywirusowych przeznaczonych dla stacji roboczych i serwerów. Badanie to stanowi podsumowanie wiedzy na temat antywirusów stosowanych w systemach ICS i służy jako punkt wyjścia lub źródło pomocnicze podczas instalowania, konfigurowania, uruchamiania i utrzymywania oprogramowania antywirusowego w systemie ICS [56]. W wielu przypadkach wpływ na wydajność można ograniczyć za pomocą ustawień konfiguracyjnych oraz harmonogramu skanowania i obsługi antywirusowej wykraczającego poza praktyki dotyczące oprogramowania antywirusowego zalecane dla typowych systemów informacyjnych.

Podsumowując, oprogramowanie antywirusowe COTS może być z powodzeniem stosowane w większości komponentów systemów ICS. Jednak podczas wyboru, instalacji, konfiguracji, eksploatacji i utrzymania należy wziąć pod uwagę szczególne uwarunkowania związane z ICS. Użytkownicy końcowi ICS powinni konsultować się z dostawcami ICS w sprawie stosowania oprogramowania antywirusowego.

Narzędzia do oceny podatności

Istnieje wiele dostępnych narzędzi do przeprowadzania oceny podatności na zagrożenia typowych sieci informacyjnych; należy jednak dokładnie rozważyć wpływ, jaki narzędzia te mogą wywierać na działanie ICS [77]. Dodatkowy ruch i exploity wykorzystywane podczas aktywnych testów podatności i testów penetracyjnych, w połączeniu z ograniczonymi zasobami wielu ICS, mogą powodować nieprawidłowe działanie ICS. Jako wytyczne w tej dziedzinie, Sandia National Laboratories opracowało preferowaną listę technik testowania podatności i technik penetracyjnych stosowanych w ICS [77]. Są to mniej inwazyjne metody pasywne, a nie aktywne, pozwalające na zebranie większości informacji, których często wyszukują zautomatyzowane narzędzia do przeprowadzania testów podatności i testów penetracyjnych. Metody te mają na celu umożliwienie zebrania niezbędnych informacji o podatnościach bez ryzyka spowodowania usterki podczas testowania.

Sophia jest zgłoszonym do opatentowania, pasywnym, działającym w czasie rzeczywistym narzędziem diagnostycznym i zabezpieczającym, zaprojektowanym i zbudowanym specjalnie dla profesjonalistów z dziedziny systemów sterowania. Sophia tworzy i obsługuje sieciowy odcisk (*ang. network fingerprint*) systemu ICS i stale monitoruje działalność w tym systemie, z możliwością tworzenia białych, szarych i czarnych list, ostrzegając menedżerów o każdej nietypowej aktywności wymagającej dalszego badania, monitorowania i/lub działania. Testy Beta przeprowadzone przez Battelle Energy Alliance (BEA) w Idaho National Laboratories (INL) z udziałem ponad 30 uczestników, w tym dużych przedsiębiorstw użyteczności publicznej i dostawców systemów sterowania, zostały niedawno zakończone. Uczestnicy testów Beta zgłosili bezpośrednie korzyści z procesu tworzenia odcisków sieci oraz długoterminowe korzyści z monitorowania, zabezpieczania i wprowadzania bieżących modyfikacji

w konfiguracjach ICS podczas okresu testów Beta. Uczestnicy Beta, jak również podmioty nie uczestniczące, które śledziły rozwój Sophii prowadzonej przez BEA/INL, od dawna wyrażały zainteresowanie uzyskaniem komercyjnej wersji oprogramowania, usług i wsparcia Sophia. Testy Beta dowiodły, że ten zestaw narzędzi oferuje unikalne możliwości, w tym wizualizację aktywności i raportowanie dostosowane do potrzeb klienta.

Shodan[67] to wyszukiwarka umożliwiająca znajdowanie w Internecie określonych typów komputerów (routerów, serwerów itp.) przy użyciu różnych filtrów. Niektórzy opisują ją również jako wyszukiwarkę banerów usług, czyli metadanych, które serwer wysyła z powrotem do klienta. Mogą to być informacje o oprogramowaniu serwera, opcjach obsługiwanych przez usługę, wiadomość powitalna lub cokolwiek innego, czego klient może się dowiedzieć przed nawiązaniem interakcji z serwerem. Użytkownicy Shodan są w stanie znaleźć takie systemy, jak sygnalizacja świetlna, kamery bezpieczeństwa, systemy ogrzewania domów oraz systemy sterowania. Użytkownicy mogą korzystać z Shodan, aby ustalić, czy któreś z urządzeń w ich systemie ICS jest dostępne z Internetu.

Narzędzie oceny cyberbezpieczeństwa (*ang. Cyber Security Evaluation Tool - CSET*) jest produktem Departamentu Bezpieczeństwa Wewnętrznego USA (ang. Department of Homeland Security - DHS), który pomaga organizacjom w ochronie ich kluczowych krajowych cyberzasobów. Zostało ono opracowane pod kierownictwem Zespołu Reagowania na Incydenty Cyberbezpieczeństwa Systemów Sterowania Przemysłowego DHS (ang. DHS Industrial Control System Cyber Emergency Response Team - ICS-CERT) przez ekspertów ds. cyberbezpieczeństwa i przy wsparciu NIST. Narzędzie to zapewnia użytkownikom systematyczne i powtarzalne podejście do oceny stanu bezpieczeństwa ich cybersystemów i cybersieci. Zawiera ono zarówno szczegółowe, jak i wysokopoziomowe pytania dotyczące wszystkich systemów sterowania przemysłowego i systemów informacyjnych. CSET jest narzędziem programowym, które prowadzi użytkowników krok po kroku przez proces oceny ich

[67] Więcej informacji ina temat Shodan znajduje się pod linkiem https://www.shodan.io/

praktyk w zakresie bezpieczeństwa systemów sterowania i sieci informacyjnych w odniesieniu do uznanych standardów branżowych.

Wynikiem działania CSET jest lista priorytetowych zaleceń mających na celu poprawę stanu cyberbezpieczeństwa przedsiębiorstwa oraz cyberbezpieczeństwa systemów sterowania przemysłowego. Narzędzie czerpie rekomendacje z bazy danych standardów, wytycznych i praktyk z zakresu cyberbezpieczeństwa. Każde zalecenie jest powiązane z zestawem działań, które mogą być podjęte w celu poprawy cyberbezpieczeństwa. CSET został zaprojektowany tak, aby można go było łatwo zainstalować i używać na samodzielnym laptopie lub stacji roboczej. Uwzględnia on szereg dostępnych standardów opracowanych przez takie organizacje, jak NIST, NERC, TSA, DoD i inne. Po wybraniu przez użytkownika narzędzia określonego standardu lub standardów, CSET otworzy zestaw pytań, na które należy odpowiedzieć. Odpowiedzi na te pytania zostaną porównane z wybranym poziomem zapewnienia bezpieczeństwa, a następnie zostanie wygenerowany szczegółowy raport wskazujący obszary wymagające potencjalnej poprawy. CSET stanowi doskonały sposób na przeprowadzenie samooceny stanu bezpieczeństwa środowiska systemu sterowania.

SamuraiSTFU to opracowane ramy projektu Samurai Project's Security Testing Framework for Utilities, które wykorzystują najlepsze narzędzia bezpieczeństwa do tradycyjnych testów penetracyjnych sieci i stron internetowych oraz dodają specjalistyczne narzędzia do testowania systemów wbudowanych i RF, a także uwzględniają kontekst sektora energetycznego, dokumentację i przykładowe pliki. Zawiera również emulatory dla SCADA, inteligentnych liczników i innych typów systemów sektora energetycznego, aby zapewnić możliwość wykorzystania pełnego laboratorium testowego.

Właściciele systemów ICS muszą uświadomić osobom korzystającym z narzędzi do oceny podatności, że ciągłość działania ma krytyczne znaczenie oraz, że przeprowadzanie takich testów na działających systemach wiąże się z ryzykiem. Możliwe jest ograniczenie tego ryzyka poprzez przeprowadzenie testów na komponentach ICS, takich jak redundantne serwery lub niezależne systemy testowe w warunkach laboratoryjnych. Testy laboratoryjne można wykorzystać do wykluczenia

procedur testowych, które mogą wpłynąć negatywnie na system pracujący operacyjnie. Nawet przy bardzo dobrym zarządzaniu konfiguracją, aby zapewnić wysoką reprezentatywność systemu testowego, testy na rzeczywistym systemie prawdopodobnie ujawnią wady, które nie zostały wykryte w laboratorium.

ZAŁĄCZNIK F - REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[68]	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B

[68] Narodowe Standardy Cyberbezpieczeństwa - Baza wiedzy - Portal Gov.pl (www.gov.pl)

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[68]	
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61

PUBLIKACJE ANGLOJĘZYCZNE[69]

[1] Fraser, Roy E., *Process Measurement and Control: Introduction to Sensors, Communication, Adjustment, and Control*, Upper Saddle River, New Jersey: Prentice-Hall, Inc., 2001.

[2] Falco, Joe, et al., *IT Security for Industrial Control Systems*, NIST Internal Report (NISTIR) 6859, February 2002, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=821684 [accessed 4/16/15].

[3] Bailey, David, and Edwin Wright, *Practical SCADA for Industry*, Vancouver: IDC Technologies, 2003.

[4] Boyer, Stuart, *SCADA: Supervisory Control and Data Acquisition.* 4th ed. Research Triangle Park, North Carolina: International Society of Automation, 2010.

[5] American Gas Association, AGA Report No. 12, *Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan*, September, March 14, 2006.

[6] Erickson, Kelvin, and John Hedrick, *Plantwide Process Control*, New York: John Wiley & Sons, Inc., 1999.

[7] Berge, Jonas, *Fieldbuses for Process Control: Engineering, Operation, and Maintenance*, Research Triangle Park, North Carolina: ISA, 2002.

[8] Peerenboom, James, "Infrastructure Interdependencies: Overview of Concepts and Terminology," invited paper, *NSF/OSTP Workshop on Critical Infrastructure: Needs in Interdisciplinary Research and Graduate Training*, Washington, D.C., June 14-15, 2001.

[69] Publikacje anglojęzyczne zostały podane w celach uzupełniających dla osób zainteresowanych.

PUBLIKACJE ANGLOJĘZYCZNE[69]

[9] Rinaldi, Steven, et al., "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, (December 2001), pp. 11-25, http://dx.doi.org/10.1109/37.969131.

[10] GAO-04-354, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, U.S. GAO, 2004, http://www.gao.gov/new.items/d04354.pdf.

[11] Weiss, Joseph, "Current Status of Cybersecurity of Control Systems," Presentation to Georgia Tech Protective Relay Conference, May 8, 2003.

[12] Keeney, Michelle et al., *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, United States Secret Service and Carnegie Mellon Software Institute, 2005, http://www.cert.org/archive/pdf/insidercross051105.pdf.

[13] Federal Information Security Management Act of 2002, Pub. L. 107-347 (Title III), 116 Stat 2946, http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf [accessed 4/16/15].

[14] Federal Information Security Management Act Implementation Project [Web site], http://csrc.nist.gov/groups/SMA/fisma/index.html [accessed 4/16/15].

U.S. Department of Commerce, Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf [accessed 4/16/15].

[16] U.S. Department of Commerce, Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006, http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf [accessed 4/16/15].

PUBLIKACJE ANGLOJĘZYCZNE[69]

[17] Knapp, Eric, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, Waltham, Massachusetts: Syngress, 2011.

[18] U.S. Government Accountability Office (GAO), GAO-15-6, *Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems*, December 12, 2014, http://www.gao.gov/products/GAO-15-6 [accessed 4/16/15].

[19] Swanson, Marianne, et al., NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-18 [accessed 4/16/15].

[20] Joint Task Force Transformation Initiative, NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-39 [accessed 4/16/15].

[21] Joint Task Force Transformation Initiative, NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*, February 2010 (updated June 5, 2014), http://dx.doi.org/10.6028/NIST.SP.800-37r1.

[22] Joint Task Force Transformation Initiative, NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated January 22, 2015), http://dx.doi.org/10.6028/NIST.SP.800-53r4.

PUBLIKACJE ANGLOJĘZYCZNE[69]

[23] Joint Task Force Transformation Initiative, NIST SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, December 2014 (updated December 18, 2014), http://dx.doi.org/10.6028/NIST.SP.800-53Ar4.

[24] Barker, William, NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-59 [accessed 4/16/15].

[25] Stine, Kevin, et al., NIST SP 800-60 Revision 1 (2 vols.), *Guide for Mapping Types of Information and Information systems to Security Categories*, August 2008, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-60 [accessed 4/16/15].

26] Quinn, Stephen, et al., NIST SP 800-70 Revision 2, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*, February 2011, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-70 [accessed 4/16/15].

[27] Bowen, Pauline, et al., NIST SP 800-100, *Information Security Handbook: a Guide for Managers*, October 2006 (updated March 7, 2007), http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-100 [accessed 4/16/15].

[28] NIST Security Configurations Checklists Program for IT Products [Web site], http://web.nvd.nist.gov/view/ncp/repository [accessed 4/16/15].

PUBLIKACJE ANGLOJĘZYCZNE[69]

[29] Stamp, Jason, et al., *Common Vulnerabilities in Critical Infrastructure Control Systems*, Sandia National Laboratories, 2003, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.132.3264&rep=rep1&type=pdf.

[30] *SCADA Security - Advice for CEOs*, IT Security Expert Advisory Group (ITSEAG)

[31] Franz, Matthew, *Vulnerability Testing of Industrial Network Devices*, Critical Infrastructure Assurance Group, Cisco Systems, 2003, http://blogfranz.googlecode.com/files/franz-isa-device-testing-oct03.pdf.

[32] Duggan, David, et al., *Penetration Testing of Industrial Control Systems*, Sandia National Laboratories, Report No SAND2005-2846P, 2005.

[33] President's Critical Infrastructure Protection Board, and U.S. Department of Energy, Office of Energy Assurance, *21 Steps to Improve Cybersecurity of SCADA Networks*, [2002], http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf [accessed 4/16/15].

[34] ISA-62443[multiple parts], *Security for Industrial Automation and Control Systems*, Research Triangle Park, North Carolina: International Society of Automation, http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx [accessed 4/16/15].

[35] Centre for the Protection of National Infrastructure (CPNI), *Firewall Deployment for SCADA and Process Control Networks: Good Practice Guide*, February 15, 2005, http://energy.gov/sites/prod/files/Good%20Practices%20Guide%20for%20Firewall%20Deployment.pdf [accessed 4/16/15].

PUBLIKACJE ANGLOJĘZYCZNE[69]

[36] U.S. Department of Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*, October 2009, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf [accessed 4/16/15].

[37] Industrial Automation Open Networking Association (IAONA), *The IAONA Handbook for Network Security*, Version 1.3, 2005, http://www.iaona.org/pictures/files/1122888138-IAONA_HNS_1_3-reduced_050725.pdf [accessed 4/16/15].

[38] U.S. Department of Homeland Security, *Common Cybersecurity Vulnerabilities in Industrial Control Systems*, May 2011, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf [accessed 4/16/15].

[39] NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, 1995, http://csrc.nist.gov/publications/PubsSPs.html.

[40] Souppaya, Murugiah, and Karen Scarfone, NIST SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*, July 2013, http://dx.doi.org/10.6028/NIST.SP.800-40r3.

[41] Scarfone, Karen, et al., NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-115 [accessed 4/16/15].

PUBLIKACJE ANGLOJĘZYCZNE[69]

[42] Roback, Edward, NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/ Use of Tested/Evaluated Products*, August 2000, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-23 [accessed 4/16/15].

[43] Stoneburner, Gary, et al., NIST SP 800-27 Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-27A [accessed 4/16/15].

[44] Grance, Tim, et al., NIST SP 800-35, *Guide to Information Technology Security Services*, October 2003, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-35 [accessed 4/16/15].

[45] Grance, Tim, et al., NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, October 2003, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-36 [accessed 4/16/15].

[46] Grance, Tim, et al., NIST SP 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-64 [accessed 4/16/15].

[47] Hash, Joan, et al., NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, January 2005, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-65 [accessed 4/16/15].

PUBLIKACJE ANGLOJĘZYCZNE[69]

[48] U.S. Department of Homeland Security, *Department of Homeland Security: Cyber Security Procurement Language for Control Systems*, September 2009 https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf [accessed 4/16/15]

[49] Dray, James, et al., NIST SP 800-73-3, *Interfaces for Personal Identity Verification* (4 parts), February 2010, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-73 [accessed 4/16/15].

[50] Grother, Patrick, et al., NIST SP 800-76-2, *Biometric Data Specification for Personal Identity Verification*, July 2013, http://dx.doi.org/10.6028/NIST.SP.800-76-2.

[51] Kuhn, D. Richard, et al., NIST SP 800-46 Revision 1, *Guide to Enterprise Telework and Remote Access Security*, June 2009, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-46 [accessed 4/16/15].

[52] Swanson, Marianne, et al., NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-34 [accessed 4/16/15].

[53] Burr, William, et al., NIST SP 800-63-2, *Electronic Authentication Guideline*, August 2013, http://dx.doi.org/10.6028/NIST.SP.800-63-2.

[54] Bace, Rebecca, and Mell, Peter, NIST SP 800-31, *Intrusion Detection Systems*, 2001, http://csrc.nist.gov/publications/PubsSPs.html.

PUBLIKACJE ANGLOJĘZYCZNE[69]

[55] Scarfone, Karen, and Peter Mell, NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-94 [accessed 4/16/15].

[56] Falco, Joe, et al., NIST SP 1058, *Using Host-based Anti-virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts*, September 18, 2006, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=823596 [accessed 4/16/15].

[57] Peterson, Dale, "Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks," *ISA Automation West (AUTOWEST 2004)*, Long Beach, California, April 2004, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.121.3420&rep=rep1&type=pdf [accessed 4/16/15].

[58] Symantec Corporation, "Symantec Expands SCADA Protection for Electric Utilities," [press release], September 14, 2005, http://www.symantec.com/about/news/release/article.jsp?prid=20050914_01 [accessed 4/16/15].

[59] Grance, Tim, et al., NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*, August 2012, http://dx.doi.org/10.6028/NIST.SP.800-61r2.

[60] Mell, Peter, et al., NIST SP 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, July 2013, http://dx.doi.org/10.6028/NIST.SP.800-83r1.

PUBLIKACJE ANGLOJĘZYCZNE[69]

[61] Wilson, Mark, and Joan Hash, NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-50 [accessed 4/16/15].

[62] Mix, S., *Supervisory Control and Data Acquisition (SCADA) Systems Security Guide*, Electric Power Research Institute (EPRI), 2003.

[63] Scarfone, Karen, et al., NIST SP 800-48 Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, July 2008, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-48 [accessed 4/16/15].

[64] Frankel, Sheila, et al, NIST SP 800-97, *Establishing Wireless Robust Security Networks: a Guide to IEEE 802.11i*, February 2007, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-97 [accessed 4/16/15].

[65] U.S. Department of Commerce, Federal Information Processing Standards (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013, http://dx.doi.org/10.6028/NIST.FIPS.201-2.

[66] Dray, James, et al, NIST SP 800-96, *PIV Card to Reader Interoperability Guidelines*, September 2006, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-96 [accessed 4/16/15].

[67] Polk, W. Timothy, et al, NIST SP 800-78-3, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, December 2010, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-78 [accessed 4/16/15].

PUBLIKACJE ANGLOJĘZYCZNE[69]

[68] Kent, Karen, and Murugiah Souppaya, NIST SP 800-92, *Guide to Computer Security Log Management*, September 2006, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-92 [accessed 4/16/15].

[69] Jansen, Wayne, et al., NIST SP 800-28 Version 2, *Guidelines on Active Content and Mobile Code*, March 2008, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-28 [accessed 4/16/15].

[70] Polk, Tim, et al., NIST SP 800-52 Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, April 2014, http://dx.doi.org/10.6028/NIST.SP.800-52r1.

[71] Barker, Elaine, et al., NIST SP 800-56A Revision 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, May 2013, http://dx.doi.org/10.6028/NIST.SP.800-56Ar2.

[72] Baker, Elaine, et al., NIST SP 800-57 (3 parts), *Recommendation for Key Management*: Part 1 Revision 3, *General*, July 2012 http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-57pt1; Part 2, *Best Practices for Key Management Organization*, August 2005, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-57pt2; Part 3 Revision 1, *Application-Specific Key Management Guidance*, January 2015, http://dx.doi.org/10.6028/NIST.SP.800-57pt3r1.

[73] Kuhn, D. Richard, et al., NIST SP 800-58, *Security Considerations for Voice Over IP Systems*, January 2005, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-58 [accessed 4/16/15].

PUBLIKACJE ANGLOJĘZYCZNE[69]

[74] Frankel, Sheila, et al., NIST SP 800-77, *Guide to IPsec VPNs*, December 2005, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-77 [accessed 4/16/15].

[75] Shirey, R., *Internet Security Glossary, Version 2*, RFC 4949, August 2007, http://www.rfc-editor.org/rfc/rfc4949.txt [accessed 4/16/15].

[76] Franz, Matthew, and Venkat Pothamsetty, *ModbusFW: Deep Packet Inspection for Industrial Ethernet*, Critical Infrastructure Assurance Group, Cisco Systems, 2004, http://blogfranz.googlecode.com/files/franz-niscc-modbusfw-may04.pdf [accessed 4/16/15].

[77] Duggan, David, *Penetration Testing of Industrial Control Systems*, SAND2005-2846P, Sandia National Laboratories, March 2005, http://energy.sandia.gov/wp/wp-content/gallery/uploads/sand_2005_2846p.pdf [accessed 4/16/15].

[78] Kissel, Richard, et al., NIST SP 800-88 Revision 1, *Guidelines for Media Sanitization*, December 2014, http://dx.doi.org/10.6028/NIST.SP.800-88r1.

[79] Joint Task Force Transformation Initiative, NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, September 2012, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-30 [accessed 4/16/15].

[80] Johnson, Arnold, et al., NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-128 [accessed 4/16/15].

PUBLIKACJE ANGLOJĘZYCZNE[69]

[81] Dempsey, Kelley, et al., NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-137 [accessed 4/16/15].

[82] Waltermire, David, et al., NIST SP 800-126 Revision 2, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*, September 2011 (updated March 19, 2012), http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-126-rev2 [accessed 4/16/15].

[83] Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf [accessed 4/16/15].

[84] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.0, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [accessed 4/16/15].

[85] Scarfone, Karen, and Paul Hoffman, NIST SP 800-41 Revision 1, *Guidelines on Firewalls and Firewall Policy*, September 2009, http://csrc.nist.gov/publications/PubsSPs.html#800-41 [accessed 4/16/15].

[86] Office of Management and Budget, OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf [accessed 4/16/15].

PUBLIKACJE ANGLOJĘZYCZNE[69]

[87] Office of Management and Budget, OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, June 25, 2010, https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf [accessed 4/16/15].

[88] McCallister, Erika, et al., NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010, http://csrc.nist.gov/publications/PubsSPs.html#800-122 [accessed 4/16/15].

[89] *Federal Enterprise Architecture Security and Privacy Profile, Version 3.0*, September 2010, https://cio.gov/wp-content/uploads/downloads/2012/09/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf [accessed 4/16/15].

[90] U.S. Department of Commerce, Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001 (Change Notice 2, 12/3/2002), http://csrc.nist.gov/publications/PubsFIPS.html#140-2 [accessed 4/16/15].

[91] Tracy, Miles, et al., NIST SP 800-45 Version 2, Guidelines on Electronic Mail Security, February 2007, http://csrc.nist.gov/publications/PubsSPs.html#800-45 [accessed 4/16/15].

[92] Grance, Tim, et al., NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002, http://csrc.nist.gov/publications/PubsSPs.html#800-47 [accessed 4/16/15].

[93] Kent, Karen, et al., NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response, August 2006, http://csrc.nist.gov/publications/PubsSPs.html#800-86 [accessed 4/16/15].

PUBLIKACJE ANGLOJĘZYCZNE[69]

[94] Scarfone, Karen, et al., NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices, November 2007, http://csrc.nist.gov/publications/PubsSPs.html#800-111 [accessed 4/16/15].

[95] Scarfone, Karen, et al., NIST SP 800-123, Guide to General Server Security, July 2008, http://csrc.nist.gov/publications/PubsSPs.html#800-123 [accessed 4/16/15].

[96] Scarfone, Karen, et al., NIST SP 800-127, Guide to Securing WiMAX Wireless Communications, September 2010, http://csrc.nist.gov/publications/PubsSPs.html#800-127 [accessed 4/16/15].

[97] Johnson, Arnold, et al., NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, August 2011, http://csrc.nist.gov/publications/PubsSPs.html#800-128 [accessed 4/16/15].

[98] Smart Grid Interoperability Panel, Smart Grid Cybersecurity Committee, NISTIR 7628 Revision 1, Guidelines for Smart Grid Cybersecurity, September 2014, http://dx.doi.org/10.6028/NIST.IR.7628r1 [accessed 4/16/15].

[99] Kissel, Richard (ed.), NISTIR 7298 Revision 2, Glossary of Key Information Security Terms, May 2013, http://dx.doi.org/10.6028/NIST.IR.7298r2 [accessed 4/16/15].

ZAŁĄCZNIK G - NAKŁADKI NA SYSTEM ICS

Informacje dla Czytelników

Nakładka ICS bazuje na dostosowaniu środków bezpieczeństwa i zabezpieczeń bazowych zawartych w publikacji NSC 800-53 wer. 1 (odpowiednik publikacji specjalnej NIST SP 800-53, Revision 4, Appendix I) oraz standardzie NSC 800-53B i stanowi uzupełnienie wytycznych specyficznych dla ICS. Nakładka ICS jest przeznaczona do stosowania w odniesieniu do wszystkich systemów ICS we wszystkich sektorach przemysłu. W celu dostosowania do konkretnego sektora (np. rurociągów, energetyki) można zastosować dalsze uszczegółowienia. Docelowo, nakładka może zostać opracowana dla konkretnego systemu (np. firmy XYZ). Ta nakładka ICS stanowi uzupełniające rekomendacje i dostosowanie do specyfikacji zawartych w dokumencie NIST SP 800-53, Revision 4 (NSC 800-53 wer. 1). Należy upewnić się, że przeglądana jest właściwa wersja NIST SP 800-53 (NSC 800-53). Powielanie Załącznika F standardu NIST SP 800-53 zwiększyłoby objętość tego Załącznika. W związku z tym komitet redakcyjny postanowił nie powielać Załącznika F. Czytelnik powinien dysponować dokumentem SP 800-53, Revision 4. Zespół autorski wziął również pod uwagę, że ta nakładka ICS może służyć jako model dla innych nakładek. Mile widziane byłyby informacje zwrotne dotyczące struktury tego załącznika, szczególnie w następujących obszarach: poziom abstrakcji oraz to, czy przykłady podane w wytycznych uzupełniających są wystarczające/przydatne do wdrożenia.

Ponieważ nakładka ICS powstała w kontekście standardu NIST SP 800-53, Revision 4, ważne jest, aby zapoznać się z tym dokumentem. Stanowi on najbardziej kompleksową aktualizację katalogu środków bezpieczeństwa od czasu jego powstania w 2005 roku. Aktualizacja ta była podyktowana przede wszystkim rozszerzającym się obszarem zagrożeń, charakteryzującym się rosnącym wyrafinowaniem cyberataków i tempem operacyjnym przeciwników (tj. częstotliwością takich ataków, profesjonalizmem atakujących i uporczywością ataków). Opracowano i włączono do katalogu najnowocześniejsze środki bezpieczeństwa i rozszerzenia zabezpieczeń w takich obszarach, jak: mobilność i chmury obliczeniowe, bezpieczeństwo aplikacji,

wiarygodność, rzetelność i odporność systemów informacyjnych, zagrożenia wewnętrzne, bezpieczeństwo łańcucha dostaw oraz zaawansowane trwałe zagrożenia.

W celu wykorzystania rozszerzonego zestawu środków bezpieczeństwa i ochrony prywatności oraz zapewnienia organizacjom większej elastyczności i sprawności w obronie ich systemów informacyjnych, w niniejszym wydaniu wprowadzono pojęcie nakładek. Nakładki zapewniają ustrukturyzowane podejście, które pomaga organizacjom dostosować bazowe środki bezpieczeństwa i opracować wyspecjalizowane plany bezpieczeństwa, które można zastosować do konkretnych misji/funkcji biznesowych, środowisk działania i/lub technologii. Takie specjalistyczne podejście ma istotne znaczenie w miarę zwiększania się w katalogu liczby zabezpieczeń i zabezpieczeń rozszerzonych wynikających z zagrożeń oraz opracowywania przez organizacje strategii zarządzania ryzykiem w celu zaspokojenia ich specyficznych potrzeb w zakresie ochrony w ramach określonych tolerancji ryzyka.

Identyfikacja

Nakładka ta może być określana jako NIST Special Publication 800-82 Revision 2 Industrial Control System Overlay ("NIST SP 800-82 Rev 2 ICS Overlay"). Jest ona oparta na NIST SP 800-53 Revision 4 [22].

NIST opracował tę nakładkę w ramach realizacji swoich ustawowych obowiązków wynikających z Federal Information Security Modernization Act (FISMA) z 2014 roku (Public Law 113-283), Presidential Policy Directive (PPD)-21 oraz Executive Order 13636. NIST jest odpowiedzialny za opracowanie norm i wytycznych, w tym minimalnych wymagań, dotyczących zapewnienia odpowiedniego bezpieczeństwa informacji dla wszystkich operacji i aktywów organizacji, jednak takie normy i wytyczne nie będą miały zastosowania do systemów bezpieczeństwa narodowego bez wyraźnej zgody odpowiednich władz państwowych sprawujących kontrolę nad takimi systemami.

Charakterystyka nakładki

Systemy sterowania przemysłowego (ICS) są zwykle stosowane w takich branżach, jak elektryczna, wodno-kanalizacyjna, paliwowa i gazu ziemnego, transportowa, chemiczna, farmaceutyczna, celulozowo-papiernicza, spożywcza i produkcji napojów oraz w produkcji jednostkowej (np. motoryzacyjnej, lotniczej i dóbr trwałych). Systemy kontroli nadzorczej i pozyskiwania danych (SCADA) są zwykle stosowane do sterowania rozproszonymi zasobami przy użyciu scentralizowanego pozyskiwania danych i kontroli nadzorczej. Rozproszone systemy sterowania (DCS) są zwykle stosowane do sterowania systemami produkcyjnymi w obrębie lokalnego obszaru, takiego jak fabryka, z wykorzystaniem kontroli nadzorczej i regulacyjnej. Programowalne sterowniki logiczne (PLC) są zazwyczaj wykorzystywane do sterowania dyskretnego w określonych zastosowaniach i na ogół zapewniają sterowanie regulacyjne. Te systemy sterowania mają zasadnicze znaczenie dla funkcjonowania infrastruktury krytycznej, która często jest silnie powiązana i wzajemnie zależna. Należy zauważyć, że znaczny procent krajowej infrastruktury krytycznej jest własnością prywatną i jest ona eksploatowana przez podmioty prywatne. Podmioty publiczne również obsługują wiele z wymienionych wyżej systemów ICS; przykładem może być kontrola ruchu lotniczego i przeładunek materiałów (np. obsługa korespondencji pocztowej).

Zastosowanie

Celem tej nakładki jest dostarczenie wytycznych do zabezpieczania ICS, w tym systemów SCADA i DCS, sterowników PLC i innych systemów wykonujących funkcje sterowania przemysłowego. Nakładka ta została przygotowana do użytku przez podmioty państwowe. Może być stosowana przez organizacje pozarządowe na zasadzie dobrowolności.

Zestawienie nakładek

Tabela G-1 zawiera podsumowanie środków bezpieczeństwa i rozszerzenia zabezpieczeń zawartych w NSC 800-53 wer. 1 (NIST SP 800-53 [22, App. F]), które zostały przypisane do wstępnych zabezpieczeń bazowych (tj. wpływu na system na

poziomie niskim, umiarkowanym i wysokim), wraz ze wskazaniem wytycznych uzupełniających dotyczących ICS oraz dostosowaniem do ICS. Zabezpieczenia i rozszerzenia zabezpieczeń, dla których istnieją wytyczne uzupełniające ICS, zostały oznaczone **pogrubioną** czcionką. Jeśli zabezpieczenia bazowe są uzupełnione przez wprowadzenie dodatkowego środka bezpieczeństwa do zabezpieczenia bazowego, to zabezpieczenie lub zabezpieczenie rozszerzone jest wyróżnione poprzez podkreślenie. Jeśli zabezpieczenie lub zabezpieczenie rozszerzone zostały usunięte z zabezpieczenia bazowego, zostały one zaznaczone ~~przekreśleniem~~.

Przykład:

AU-4	Pojemność pamięci zapisów audytu	AU-4 **(1)**	AU-4 **(1)**	AU-4 **(1)**

W tym przykładzie wytyczne uzupełniające dotyczące ICS zostały dodane do zabezpieczenia rozszerzonego 1 w zabezpieczeniu AU-4 (pogrubienie). Ponadto do zabezpieczenia bazowego AU-4 i niskim, umiarkowanym i wysokim poziomie wpływu na system dodano zabezpieczenie rozszerzone o numerze 1 (podkreślone).

Tabela G-1. Zabezpieczenia bazowe.

Numer zabezpieczenia	**Nazwa zabezpieczenia**	**Wstępne zabezpieczenia bazowe**		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-1	Polityka i procedury kontroli dostępu	**AC-1**	**AC-1**	**AC-1**
AC-2	Zarządzanie kontem	**AC-2**	**AC-2 (1) (2) (3) (4)**	**AC-2 (1) (2) (3) (4) (5)** (11) (12) (13)
AC-3	Egzekwowanie uprawnień dostępu	**AC-3**	**AC-3**	**AC-3**
AC-4	Egzekwowanie zasad przepływu informacji	Nie wybrano	AC-4	AC-4

Numer zabezpieczenia	**Nazwa zabezpieczenia**	**Wstępne zabezpieczenia bazowe**		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-5	Rozdział obowiązków	Nie wybrano	**AC-5**	**AC-5**
AC-6	Zasada wiedzy koniecznej	Nie wybrano	**AC-6 (1) (2) (5) (9) (10)**	**AC-6 (1) (2) (3) (5) (9) (10)**
AC-7	Nieudane próby logowania	**AC-7**	**AC-7**	**AC-7**
AC-8	Powiadomienie o zasadach użycia systemu	**AC-8**	**AC-8**	**AC-8**
AC-10	Kontrola ilości równoczesnych sesji	Nie wybrano	Nie wybrano	**AC-10**
AC-11	Zamknięcie / Blokada sesji	Nie wybrano	**AC-11 (1)**	**AC-11 (1)**
AC-12	Zakończenie sesji	Nie wybrano	**AC-12**	**AC-12**
AC-14	Działania dozwolone bez identyfikacji lub uwierzytelnienia	AC-14	AC-14	AC-14
AC-17	Zdalny dostęp	**AC-17**	**AC-17 (1) (2) (3) (4)**	**AC-17 (1) (2) (3) (4)**
AC-18	Dostęp bezprzewodowy	**AC-18**	**AC-18 (1)**	**AC-18 (1) (4)** (5)
AC-19	Kontrola dostępu realizowanego z urządzeń przenośnych (mobilnych)	**AC-19**	**AC-19** (5)	**AC-19** (5)
AC-20	Wykorzystanie zewnętrznych systemów informacyjnych	**AC-20**	**AC-20** (1) (2)	**AC-20** (1) (2)

Numer zabezpieczenia	Nazwa zabezpieczenia	Wstępne zabezpieczenia bazowe		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-21	Udostępnianie informacji	**AC-21**	**AC-21**	**AC-21**
AC-22	Treści publicznie dostępne	**AC-22**	**AC-22**	**AC-22**
AT-1	Świadomość bezpieczeństwa, polityka i procedury szkoleniowe	**AT-1**	**AT-1**	**AT-1**
AT-2	Szkolenie w zakresie uświadamiania bezpieczeństwa	**AT-2**	**AT-2** (2)	**AT-2** (2)
AT-3	Szkolenie w zakresie bezpieczeństwa opartego na rolach	**AT-3**	**AT-3**	**AT-3**
AT-4	Rejestrowanie szkoleń z zakresu bezpieczeństwa	AT-4	AT-4	AT-4
AU-1	Polityka oraz procedury w zakresie audytu i rozliczalności	**AU-1**	**AU-1**	**AU-1**
AU-2	Audyt zdarzeń	**AU-2**	**AU-2** (3)	**AU-2** (3)
AU-3	Zawartość rejestrów audytu	**AU-3**	**AU-3** (1)	**AU-3** (1) (2)
AU-4	Pojemność pamięci zapisów audytu	AU-4 **(1)**	AU-4 **(1)**	AU-4 **(1)**
AU-5	Reakcja na błędy procesów audytu	AU-5	AU-5	AU-5 (1) (2)
AU-6	Przegląd audytu, analiza i raportowanie	AU-6	AU-6 **(1)** (3)	AU-6 **(1)** (3) (5) (6)

Numer zabezpieczenia	Nazwa zabezpieczenia	Wstępne zabezpieczenia bazowe		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
AU-7	Redukcja treści zapisów audytu i generowanie raportów	Nie wybrano	AU-7 (1)	AU-7 (1)
AU-8	Znaczniki czasu	**AU-8**	**AU-8 (1)**	**AU-8 (1)**
AU-9	Ochrona informacji audytowych	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Niezaprzeczalność	Nie wybrano	Nie wybrano	**AU-10**
AU-11	Retencja zapisów audytu	AU-11	AU-11	AU-11
AU-12	Tworzenie zapisów audytu	AU-12	AU-12	AU-12 **(1) (3)**
CA-1	Ocena bezpieczeństwa i autoryzacja - polityka i procedury	**CA-1**	**CA-1**	**CA-1**
CA-2	Ocena bezpieczeństwa	**CA-2**	**CA-2** (1)	**CA-2** (1) **(2)**
CA-3	Połączenia międzysystemowe	**CA-3**	**CA-3** (5)	**CA-3** (5)
CA-5	Plan i etapy działania	CA-5	CA-5	CA-5
CA-6	Autoryzacja bezpieczeństwa	CA-6	CA-6	CA-6
CA-7	Ciągłość monitorowania	**CA-7**	**CA-7** (1)	**CA-7** (1)
CA-8	Testy penetracyjne	Nie wybrano	Nie wybrano	**CA-8**
CA-9	Połączenia wewnątrzsystemowe	**CA-9**	**CA-9**	**CA-9**
CM-1	Zarządzanie konfiguracją – polityka i procedury	**CM-1**	**CM-1**	**CM-1**

Numer zabezpieczenia	**Nazwa zabezpieczenia**	**Wstępne zabezpieczenia bazowe**		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
CM-2	Konfiguracja podstawowa	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Zabezpieczanie zmian konfiguracji	Nie wybrano	CM-3 (2)	CM-3 (1) (2)
CM-4	Analiza zmian wpływających na bezpieczeństwo	**CM-4**	**CM-4**	**CM-4** (1)
CM-5	Ograniczenia możliwości wykonywania zmian	Nie wybrano	CM-5	CM-5 **(1) (2) (3)**
CM-6	Ustawienia konfiguracji	CM-6	CM-6	CM-6 (1) (2)
CM-7	Zasada minimalnej funkcjonalności	**CM-7 (1)**	**CM-7** (1) (2) ~~(4)~~ (5)	**CM-7** (1) (2) (5)
CM-8	Inwentaryzacja komponentów systemu informacyjnego	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Plan zarządzania konfiguracją	Nie wybrano	CM-9	CM-9
CM-10	Ograniczenia w użyciu oprogramowania	**CM-10**	**CM-10**	**CM-10**
CM-11	Oprogramowanie instalowane przez użytkownika	CM-11	CM-11	CM-11
CP-1	Polityka i procedury planowania ciągłości działania	**CP-1**	**CP-1**	**CP-1**
CP-2	Plan ciągłości działania	**CP-2**	**CP-2 (1) (3) (8)**	**CP-2 (1) (2) (3) (4) (5) (8)**

Numer zabezpieczenia	**Nazwa zabezpieczenia**	**Wstępne zabezpieczenia bazowe**		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
CP-3	Szkolenie z zakresie planowania ciągłości działania	CP-3	CP-3	CP-3 (1)
CP-4	Testowanie planu ciągłości działania	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-6	Zapasowe miejsce przechowywania kopii	Nie wybrano	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Zapasowe miejsce przetwarzania	Nie wybrano	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Usługi telekomunikacyjne	Nie wybrano	**CP-8** (1) (2)	**CP-8** (1) (2) (3) (4)
CP-9	Kopia zapasowa	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)
CP-10	Odzyskiwanie i odtwarzanie systemu	**CP-10**	**CP-10** (2)	**CP-10** (2) (4)
CP-12	Tryb bezpieczny	**CP-12**	**CP-12**	**CP-12**
IA-1	Identyfikacja i uwierzytelnianie – polityka i procedury	**IA-1**	**IA-1**	**IA-1**
IA-2	Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni)	**IA-2 (1) (12)**	**IA-2 (1) (2) (3) (8)** (11) **(12)**	**IA-2 (1) (2) (3) (4) (8) (9)** (11) **(12)**
IA-3	Identyfikacja i uwierzytelnianie urządzenia	**IA-3**	**IA-3 (1) (4)**	**IA-3 (1) (4)**
IA-4	Zarządzanie identyfikatorem	IA-4	IA-4	IA-4
IA-5	Zarządzanie metodami uwierzytelniania	**IA-5** (1) (11)	**IA-5** (1) (2) (3) (11)	**IA-5** (1) (2) (3) (11)

Numer zabezpieczenia	Nazwa zabezpieczenia	Wstępne zabezpieczenia bazowe		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
IA-6	Ochrona procesu uwierzytelniania	**IA-6**	**IA-6**	**IA-6**
IA-7	Uwierzytelnianie modułu kryptograficznego	IA-7	IA-7	IA-7
IA-8	Identyfikacja i uwierzytelnianie (użytkownicy spoza organizacji)	**IA-8 (1) (2) (3) (4)**	**IA-8 (1) (2) (3) (4)**	**IA-8 (1) (2) (3) (4)**
IR-1	Polityka i procedury reagowania na incydenty	**IR-1**	**IR-1**	**IR-1**
IR-2	Szkolenie w zakresie reagowania na incydenty	IR-2	IR-2	IR-2 (1) (2)
IR-3	Testowanie reagowania na incydenty	Nie wybrano	IR-3 (2)	IR-3 (2)
IR-4	Obsługa incydentów	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	Monitorowanie incydentów	IR-5	IR-5	IR-5 (1)
IR-6	Raportowanie incydentu	**IR-6**	**IR-6 (1)**	**IR-6 (1)**
IR-7	Wsparcie reagowania na incydenty	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Plan reagowania na incydenty	IR-8	IR-8	IR-8
MA-1	Polityka i procedury utrzymania systemu	**MA-1**	**MA-1**	**MA-1**
MA-2	Nadzór nad utrzymaniem	MA-2	MA-2	MA-2 (2)

Numer zabezpieczenia	Nazwa zabezpieczenia	Wstępne zabezpieczenia bazowe		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
MA-3	Narzędzia utrzymaniowe	Nie wybrano	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	Utrzymanie zdalne	MA-4	MA-4 (2)	MA-4 (2) **(3)**
MA-5	Personel utrzymaniowy	MA-5	MA-5	MA-5 (1)
MA-6	Terminowość przeprowadzania konserwacji	Nie wybrano	MA-6	MA-6
MP-1	Polityka i procedury ochrony nośników danych	**MP-1**	**MP-1**	**MP-1**
MP-2	Dostęp do nośników	MP-2	MP-2	MP-2
MP-3	Oznakowanie nośników	Nie wybrano	MP-3	MP-3
MP-4	Przechowywanie nośników	Nie wybrano	MP-4	MP-4
MP-5	Transport nośników	Nie wybrano	MP-5 (4)	MP-5 (4)
MP-6	Sanityzacja nośników	MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	Używanie nośników	MP-7	MP-7 (1)	MP-7 (1)
PE-1	Polityka i procedury ochrony fizycznej i środowiskowej	**PE-1**	**PE-1**	**PE-1**
PE-2	Zezwolenie na dostęp fizyczny	PE-2	PE-2	PE-2
PE-3	Kontrola dostępu fizycznego	PE-3	PE-3	PE-3 (1)
PE-4	Kontrola dostępu do medium transmisyjnego	Nie wybrano	PE-4	PE-4

Numer zabezpieczenia	Nazwa zabezpieczenia	Wstępne zabezpieczenia bazowe		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-5	Kontrola dostępu do urządzeń wejścia - wyjścia	Nie wybrano	PE-5	PE-5
PE-6	Monitorowanie dostępu fizycznego	**PE-6**	**PE-6** (1) **(4)**	**PE-6** (1) **(4)**
PE-8	Rejestracja dostępu gości	PE-8	PE-8	PE-8 (1)
PE-9	Wyposażenie energetyczne i okablowanie	Nie wybrano	PE-9 (1)	PE-9 (1)
PE-10	Wyłączenia awaryjne	Nie wybrano	PE-10	PE-10
PE-11	Zasilanie awaryjne	PE-11 (1)	PE-11 (1)	PE-11 (1) (2)
PE-12	Oświetlenie awaryjne	PE-12	PE-12	PE-12
PE-13	Ochrona przeciwpożarowa	**PE-13**	**PE-13** (3)	**PE-13** (1) (2) (3)
PE-14	Kontrola temperatury i wilgotności	PE-14	PE-14	PE-14
PE-15	Ochrona przed zalaniem	**PE-15**	**PE-15**	**PE-15** (1)
PE-16	Dostawa i usuwanie	PE-16	PE-16	PE-16
PE-17	Zapasowe miejsca pracy	Nie wybrano	PE-17	PE-17
PE-18	Lokalizacja elementów systemu informacyjnego	Nie wybrano	Nie wybrano	PE-18
PL-1	Polityka i procedury planowania bezpieczeństwa	**PL-1**	**PL-1**	**PL-1**

Numer zabezpieczenia	Nazwa zabezpieczenia	Wstępne zabezpieczenia bazowe		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
PL-2	Plan bezpieczeństwa systemu	PL-2 (3)	PL-2 (3)	PL-2 (3)
PL-4	Zasady postępowania	PL-4	PL-4 (1)	PL-4 (1)
PL-7	Koncepcja bezpieczeństwa działań operacyjnych		PL-7	PL-7
PL-8	Architektura bezpieczeństwa informacji	Nie wybrano	PL-8	PL-8
PS-1	Bezpieczeństwo osobowe – polityka i procedury	**PS-1**	**PS-1**	**PS-1**
PS-2	Określanie ryzyka dla stanowiska pracy	PS-2	PS-2	PS-2
PS-3	Dobór personelu	PS-3	PS-3	PS-3
PS-4	Zakończenie zatrudnienia	PS-4	PS-4	PS-4 (2)
PS-5	Obsadzenie lub przeniesienie stanowiska	PS-5	PS-5	PS-5
PS-6	Umowy dostępu / współpracy	PS-6	PS-6	PS-6
PS-7	Bezpieczeństwo osobowe stron trzecich	PS-7	PS-7	PS-7
PS-8	Sankcje personalne	PS-8	PS-8	PS-8
RA-1	Polityka i procedury szacowania ryzyka	**RA-1**	**RA-1**	**RA-1**
RA-2	Kategoryzacja bezpieczeństwa	RA-2	RA-2	RA-2

Numer zabezpieczenia	**Nazwa zabezpieczenia**	**Wstępne zabezpieczenia bazowe**		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
RA-3	Szacowanie ryzyka	RA-3	RA-3	RA-3
RA-5	Skanowanie podatności	**RA-5**	**RA-5** (1) (2) (5)	**RA-5** (1) (2) (4) (5)
SA-1	Polityka i procedury nabywania systemu i usług	**SA-1**	**SA-1**	**SA-1**
SA-2	Przydział zasobów	SA-2	SA-2	SA-2
SA-3	Cykl życia systemu	SA-3	SA-3	SA-3
SA-4	Proces nabycia	**SA-4 (10)**	**SA-4 (1) (2) (9) (10)**	**SA-4 (1) (2) (9) (10)**
SA-5	Dokumentacja systemu informacyjnego	SA-5	SA-5	SA-5
SA-8	Zarządzanie bezpieczeństwem informacji	Nie wybrano	SA-8	SA-8
SA-9	Usługi zewnętrznego systemu informacyjnego	SA-9	SA-9 (2)	SA-9 (2)
SA-10	Zarządzanie konfiguracją dewelopera	Nie wybrano	SA-10	SA-10
SA-11	Testowanie i ocena bezpieczeństwa przez dewelopera	Nie wybrano	SA-11	SA-11
SA-12	Bezpieczeństwo łańcucha dostaw	Nie wybrano	Nie wybrano	SA-12
SA-15	Proces rozwoju, standardy i narzędzia	Nie wybrano	Nie wybrano	SA-15

Numer zabezpieczenia	**Nazwa zabezpieczenia**	**Wstępne zabezpieczenia bazowe**		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
SA-16	Szkolenie dostarczone przez dewelopera	Nie wybrano	Nie wybrano	SA-16
SA-17	Architektura i projekt bezpieczeństwa dewelopera	Nie wybrano	Nie wybrano	SA-17
SC-1	Polityka i procedury ochrony systemów i sieci telekomunikacyjnych	**SC-1**	**SC-1**	**SC-1**
SC-2	Separacja	Nie wybrano	**SC-2**	**SC-2**
SC-3	Izolacja funkcji bezpieczeństwa	Nie wybrano	Nie wybrano	**SC-3**
SC-4	Informacje we współdzielonych zasobach	Nie wybrano	**SC-4**	**SC-4**
SC-5	Ochrona przed blokadą usług (DoS)	**SC-5**	**SC-5**	**SC-5**
SC-7	Ochrona połączeń brzegowych	SC-7	SC-7 (3) (4) (5) (7) **(18)**	SC-7 (3) (4) (5) (7) (8) **(18) (**21)
SC-8	Poufność i integralność transmisji	Nie wybrano	SC-8 **(1)**	SC-8 **(1)**
SC-10	Zakończenie połączenia sieciowego	Nie wybrano	**SC-10**	**SC-10**
SC-12	Generowanie i zarządzanie kluczami kryptograficznymi	**SC-12**	**SC-12**	**SC-12** (1)
SC-13	Ochrona kryptograficzna	SC-13	SC-13	SC-13

Numer zabezpieczenia	Nazwa zabezpieczenia	Wstępne zabezpieczenia bazowe		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-15	Współpracujące urządzenia komputerowe	SC-15	SC-15	SC-15
SC-17	Certyfikaty infrastruktury klucza publicznego	Nie wybrano	SC-17	SC-17
SC-18	Kod mobilny	Nie wybrano	SC-18	SC-18
SC-19	Protokół transmisji pakietowej (VoIP)	Nie wybrano	**SC-19**	**SC-19**
SC-20	Bezpieczeństwo nazw domen / adresów IP (autentyczność pochodzenia)	**SC-20**	**SC-20**	**SC-20**
SC-21	Bezpieczeństwo nazw domen / usługa ustalania adresu IP	SC-21	SC-21	SC-21
SC-22	Architektura nazw domen / adresów IP / zamawianie usług DNS	**SC-22**	**SC-22**	**SC-22**
SC-23	Autentyczność sesji	Nie wybrano	**SC-23**	**SC-23**
SC-24	Przejście do określonego stanu systemu po błędzie	Nie wybrano	**SC-24**	**SC-24**
SC-28	Ochrona danych w składowaniu / kopie konfiguracji systemu	Nie wybrano	**SC-28**	**SC-28**
SC-39	Izolacja procesów	**SC-39**	**SC-39**	**SC-39**
SC-41	Dostęp do portów i urządzeń wejścia / wyjścia	**SC-41**	**SC-41**	**SC-41**

Numer zabezpieczenia	**Nazwa zabezpieczenia**	**Wstępne zabezpieczenia bazowe**		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-1	Polityka i procedury integralności systemu i informacji	**SI-1**	**SI-1**	**SI-1**
SI-2	Usuwanie usterek	**SI-2**	**SI-2 (2)**	**SI-2** (1) **(2)**
SI-3	Zabezpieczenie przed złośliwym kodem	**SI-3**	**SI-3 (1) (2)**	**SI-3 (1) (2)**
SI-4	Monitorowanie systemu informacyjnego	**SI-4**	**SI-4 (2) (4) (5)**	**SI-4 (2) (4) (5)**
SI-5	Alerty bezpieczeństwa, porady i dyrektywy	**SI-5**	**SI-5**	**SI-5** (1)
SI-6	Weryfikacja funkcji bezpieczeństwa	Nie wybrano	Nie wybrano	**SI-6**
SI-7	Aplikacje, oprogramowanie układowe i integralność informacji	Nie wybrano	**SI-7 (1) (7)**	**SI-7 (1) (2) (5) (7)** (14)
SI-8	Ochrona przed spamem	Nie wybrano	**SI-8 (1) (2)**	**SI-8 (1) (2)**
SI-10	Weryfikacja wprowadzanych informacji	Nie wybrano	SI-10	SI-10
SI-11	Obsługa błędów	Nie wybrano	SI-11	SI-11
SI-12	Przechowywanie i retencja informacji	SI-12	SI-12	SI-12
SI-13	Przewidywanie awarii	Nie wybrano	Nie wybrano	**SI-13**
SI-14	Zapobieganie zaawansowanym	Nie wybrano	Nie wybrano	Nie wybrano

Numer zabezpieczenia	Nazwa zabezpieczenia	Wstępne zabezpieczenia bazowe		
		Poziom wpływu na system informacyjny na system informacyjny		
		Niski	Umiarkowany	Wysoki
	długotrwałym atakom (ataki typu APT)			
SI-15	Filtrowanie informacji wyjściowych	Nie wybrano	Nie wybrano	Nie wybrano
SI-16	Ochrona pamięci	Nie wybrano	SI-16	SI-16
SI-17	Bezpieczne procedury	SI-17	SI-17	SI-17

Kategoria Programy bezpieczeństwa informacji (*ang. Program management – PM*) jest wdrażana w całej organizacji wspierając program bezpieczeństwa informacji. Nie jest ona związana z zabezpieczeniami bazowymi i jest niezależna od poziomu wpływu na system.

PM-1	Plan programu bezpieczeństwa informacji	PM-1
PM-2	Osoba odpowiedzialna za bezpieczeństwo informacji (CSO)	PM-2
PM-3	Środki bezpieczeństwa informacji	**PM-3**
PM-4	Plan działania i etapy wprowadzania zabezpieczeń	**PM-4**
PM-5	Inwentaryzacja systemu informacyjnego	PM-5
PM-6	Skuteczność środków bezpieczeństwa informacji	PM-6
PM-7	Struktura organizacyjna	**PM-7**
PM-8	Plan infrastruktury krytycznej	**PM-8**
PM-9	Strategia zarządzania ryzykiem	**PM-9**
PM-10	Proces autoryzacji zabezpieczeń	**PM-10**
PM-11	Definicja misji / procesu biznesowego	**PM-11**
PM-12	Zagrożenia wewnętrzne	PM-12
PM-13	Personel bezpieczeństwa informacji	**PM-13**
PM-14	Testowanie, szkolenia i monitorowanie	PM-14
PM-15	Kontakty z grupami i stowarzyszeniami zajmującymi się bezpieczeństwem informacji	PM-15
PM-16	Ostrzeganie i zagrożeniach	PM-16

Uwagi dotyczące dostosowywania

Ze względu na unikatowe cechy ICS, systemy te mogą wymagać szerszego stosowania kompensacyjnych środków bezpieczeństwa niż ma to miejsce w przypadku systemów informacyjnych ogólnego przeznaczenia. Kompensacyjne środki bezpieczeństwa[70] nie są wyjątkami, ani odstępstwami od bazowych środków bezpieczeństwa; są to alternatywne zabezpieczenia i środki zaradcze stosowane w ICS, które realizują cel pierwotnych środków bezpieczeństwa, które nie mogły być skutecznie zastosowane.

W sytuacjach, w których system ICS nie może obsługiwać lub organizacja stwierdza, że nie jest wskazane wdrożenie określonych środków bezpieczeństwa lub zabezpieczeń rozszerzonych w ICS (np. niekorzystny wpływ na wydajność, bezpieczeństwo lub niezawodność), organizacja przedstawia pełne i przekonujące uzasadnienie tego, w jaki sposób wybrane kompensacyjne środki bezpieczeństwa zapewniają równoważną zdolność bezpieczeństwa lub poziom ochrony ICS oraz dlaczego nie można było zastosować odpowiednich bazowych środków bezpieczeństwa.

Zgodnie z "Technology-related Considerations of the Scoping Guidance" dokumentu NIST SP 800-53 Rev. 4, sekcja 3.2, jeśli zautomatyzowane mechanizmy nie są łatwo dostępne, opłacalne lub technicznie wykonalne w ICS, stosuje się kompensacyjne środki bezpieczeństwa, wdrażane za pomocą niezautomatyzowanych mechanizmów lub procedur [22].

Zabezpieczenia kompensacyjne to alternatywne środki bezpieczeństwa stosowane przez organizacje w miejsce poszczególnych zabezpieczeń bazowych - środki, które zapewniają równoważną lub porównywalną ochronę systemów informacyjnych organizacji oraz informacji przetwarzanych, przechowywanych lub przesyłanych przez te systemy.[71] Może to nastąpić na przykład wtedy, gdy organizacje nie są w stanie

[70] Patrz: "Wybór zabezpieczeń kompensacyjnych" w sekcji 2.4.3 dokumentu NSC 800-53B.

[71] Organizacje powinny dołożyć wszelkich starań, aby wybierać zabezpieczenia kompensacyjne określone w katalogu zabezpieczeń w publikacji NSC 800-53B. Zdefiniowane przez organizację zabezpieczenia kompensacyjne są stosowane tylko wtedy, gdy organizacja stwierdzi, że katalog środków bezpieczeństwa nie zawiera odpowiednich zabezpieczeń kompensacyjnych.

skutecznie wdrożyć określonych zabezpieczeń bazowych lub gdy ze względu na specyfikę ICS lub środowisk działania zabezpieczenia bazowe nie są efektywnym kosztowo sposobem uzyskania wymaganego ograniczenia ryzyka. Zabezpieczenia kompensacyjne mogą obejmować zabezpieczenia rozszerzone, które uzupełniają zabezpieczenia bazowe. Stosowanie zabezpieczeń kompensacyjnych może wiązać się z zachowaniem kompromisu między dodatkowym ryzykiem a zmniejszoną funkcjonalnością. Każde zastosowanie zabezpieczeń kompensacyjnych powinno obejmować określenie na podstawie ryzyka: (I) akceptowalnego poziomu ryzyka szczątkowego, oraz (II) stopnia ograniczenia funkcjonalności. Zabezpieczenia kompensacyjne mogą być stosowane przez organizacje pod następującymi warunkami:

- Organizacje wybierają zabezpieczenia kompensacyjne określone w NSC 800-53B. Jeśli odpowiednie zabezpieczenia kompensacyjne nie są dostępne, organizacje dostosowują ustawienia zabezpieczeń pochodzących z innych źródeł[72].
- Organizacje przedstawiają argumentację potwierdzającą, w jaki sposób zabezpieczenia kompensacyjne zapewniają równoważne możliwości ochrony systemów informacyjnych organizacji oraz uzasadniają, dlaczego nie można było zastosować zabezpieczeń bazowych.
- Organizacje szacują i akceptują ryzyko związane z wdrożeniem zabezpieczeń kompensacyjnych w ICS.

Decyzje organizacyjne dotyczące stosowania zabezpieczeń kompensacyjnych są dokumentowane w planie bezpieczeństwa danego ICS.

Zabezpieczenia zawierające przyporządkowanie (np. *Realizacja: warunki zdefiniowane przez organizację lub zdarzenia uruchamiające*) mogą zostać wyłączone z zestawu zabezpieczeń bazowych. Jest to równoznaczne z przypisaniem wartości "brak".

[72] Organizacje powinny dołożyć wszelkich starań, aby wybrać zabezpieczenia kompensacyjne z katalogu środków bezpieczeństwa NSC 800-53B. Zdefiniowane przez organizację zabezpieczenia kompensacyjne są stosowane *tylko* wtedy, gdy organizacje stwierdzą, że katalog środków bezpieczeństwa nie zawiera odpowiednich zabezpieczenia kompensacyjnych.

Realizacja przyporządkowania może przyjmować różne wartości oddziaływania dla poszczególnych zabezpieczeń bazowych.

Komunikacja bezadresowa i nietrasowana

Unikalne właściwości sieci w ramach ICS wymagają szczególnej uwagi przy stosowaniu określonych środków bezpieczeństwa. Wiele z zabezpieczeń zawartych w NSC SP 800-53, które dotyczą komunikacji, urządzeń i interfejsów, zakłada domyślnie zastosowanie adresowalnych i routowalnych protokołów, takich jak zestaw protokołów internetowych TCP/IP[73] lub warstwy 1, 2 i 3 modelu OSI[74] (ISO/IEC 7498-1). Wyjątkiem od tego założenia są niektóre urządzenia lub podsystemy stosowane w systemach ICS. W tej części omówiono, w jaki sposób można odpowiednio dostosować zabezpieczenia do potrzeb tych systemów. Dostosowanie środków bezpieczeństwa jest wymagane przede wszystkim w następujących sytuacjach:

- Brak odpowiednich możliwości. Cel niektórych zabezpieczeń można łatwiej osiągnąć za pomocą zabezpieczeń kompensacyjnych ze względu na pewne właściwości sieci lub możliwości, które nie są dostępne w podsystemie ICS. Przykładowo, ochrona fizyczna (np. zamykane obudowy) może być użyta do zabezpieczenia całego kanału komunikacyjnego punkt-punkt, jako środek kompensujący brak protokołów obsługujących uwierzytelnianie. Środki bezpieczeństwa mogą gwarantować dodatkowe wsparcie, dzięki któremu wdrożenie zabezpieczeń lub zabezpieczeń kompensacyjnych zapewni odpowiedni poziom ochrony.
- Brak zastosowania. Wiele protokołów komunikacyjnych występujących w ICS może mieć ograniczoną funkcjonalność (np. nie są adresowalne lub routowane). Środki bezpieczeństwa związane z adresowaniem i trasowaniem mogą nie mieć zastosowania do tych protokołów.

Środki bezpieczeństwa stosowane w urządzeniach komunikujących się w układzie punkt-punkt przy użyciu standardów i protokołów nieobejmujących adresowania

[73] Obecnie pakietem protokołów TCP/IP zarządza organizacja Internet Engineering Task Force (IETF).

[74] Open Systems Interconnection.

wymagają na ogół indywidualnego dostosowania. Przykładem jest modem podłączony do komputera za pomocą interfejsu RS-232. Interfejs RS-232 był powszechnie stosowany w obecnie używanym sprzęcie ICS, nawet jeśli został on zastąpiony przez nowszy sprzęt. W telekomunikacji, RS-232 jest tradycyjną nazwą serii standardów dla szeregowych, binarnych, jednokońcówkowych sygnałów danych i sterowania, łączących urządzenia końcowe transmisji danych (*ang. data terminal equipment - DTE*) i urządzenia komutacji łączy (*ang. data circuit terminal - DCE*, pierwotnie określane jako urządzenia do transmisji danych). Obecnie obowiązującą wersją standardu jest Telecommunications Industry Association (TIA)-232-F, Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange, wydana w 1997 roku.

Port szeregowy RS-232 był standardowym wyposażeniem małych urządzeń komputerowych, takich jak podsystemy ICS, służącym do łączenia się z urządzeniami peryferyjnymi. Jednak niska szybkość transmisji, duże wahania napięcia i duże rozmiarowo standardowe złącza zmotywowały do opracowania uniwersalnej magistrali szeregowej (*ang. Universal Serial Bus - USB*), która wyparła RS-232 z większości jego funkcji interfejsu peryferyjnego. Urządzenia RS-232 są wciąż spotykane, zwłaszcza w maszynach przemysłowych, sprzęcie sieciowym i instrumentach naukowych.

Modele warstwowe sieci

Modele warstwowe sieci stosowane zarówno w TCP/IP, jak i OSI mogą stanowić podstawę do zrozumienia różnych właściwości komunikacji sieciowej i pomogą określić, w jaki sposób środki bezpieczeństwa mogą być stosowane w systemach i sieciach. W poniższej tabeli przedstawiono kluczowe właściwości warstw: fizycznej, łącza danych i sieciowej dotyczące stosowania środków bezpieczeństwa.

Warstwa sieciowa	Właściwości warstwy
Warstwa fizyczna	***Nośnik fizyczny*** - fizyczny nośnik sieci, a konkretnie to, czy jest to sieć przewodowa czy bezprzewodowa, może wpłynąć na zastosowanie lub dostosowanie poszczególnych środków bezpieczeństwa. Połączenia bezprzewodowe nie mogą być fizycznie chronione, dlatego nie można stosować zabezpieczeń kompensacyjnych koncentrujących się na bezpieczeństwie fizycznym. ***Topologia*** - topologie fizyczne mogą również wpływać na sposób dostosowywania środków bezpieczeństwa. Na przykład, topologie typu punkt-punkt (np. RS-232) na ogół nie wymagają fizycznie adresowalnych interfejsów, podczas gdy topologie wielopunktowe (np. IEEE 802.3 Ethernet) wymagają stosowania fizycznie adresowalnych interfejsów.
Warstwa łącza danych	***Fizycznie adresowalne*** - protokoły wykorzystujące protokół wielopunktowy wymagają fizycznie adresowalnych interfejsów, aby umożliwić komunikację między wieloma systemami. Systemy, które nie są fizycznie adresowalne, mogą być dostępne tylko dla tych systemów, z którymi mają wspólne połączenia typu punkt-punkt.
Warstwa sieciowa	***Adresowane/routowane systemy sieciowe*** - do systemów adresowalnych/routowalnych można uzyskać dostęp za pomocą dowolnego systemu podłączonego do sieci internetowej. Oznacza to, że komunikacja może być kierowana między sieciami. Jeśli system nie jest adresowalny/routowany, dostęp do niego mogą mieć tylko systemy, z którymi ma wspólne połączenie w sieci lokalnej.

Definicje

Terminy użyte w tym dokumencie są zdefiniowane w Załączniku B.

Dodatkowe informacje lub wskazówki

Obecnie brak. Organizacje mogą podać wszelkie dodatkowe informacje lub wskazówki dotyczące nakładki, które nie zostały uwzględnione w poprzednich sekcjach.

Szczegółowe specyfikacje weryfikacji nakładek

Nakładka jest oparta na dokumentach NSC 800-53 oraz NSC 800-53B, zawierających katalog środków bezpieczeństwa i ochrony prywatności systemów informacyjnych i organizacji oraz proces ich wyboru w celu ochrony działań organizacji (w tym misji, funkcji, wizerunku i reputacji), aktywów organizacji, osób, innych organizacji i państwa przed różnego rodzaju zagrożeniami, w tym wrogimi cyberatakami, klęskami żywiołowymi, usterkami strukturalnymi i błędami ludzkimi (zarówno zamierzonymi, jak i niezamierzonymi). Środki bezpieczeństwa i ochrony prywatności są przystosowywane i wdrażane jako część ogólnoorganizacyjnego procesu zarządzania ryzykiem związanym z bezpieczeństwem informacji i ochroną prywatności. Zabezpieczenia dotyczą różnorodnych wymagań związanych z bezpieczeństwem i ochroną prywatności w organizacjach publicznych i infrastrukturze krytycznej, wynikających z przepisów prawa, rozporządzeń wykonawczych, polityk, dyrektyw, regulacji, standardów i/lub potrzeb biznesowych. Publikacja opisuje również sposoby tworzenia specjalistycznych zestawów zabezpieczeń lub nakładek, dostosowywanych do konkretnych rodzajów misji/funkcji biznesowych, technologii lub środowisk działania. Ponadto katalog zabezpieczeń uwzględnia bezpieczeństwo zarówno z perspektywy funkcjonalności (skuteczność zapewnianych funkcji i mechanizmów zabezpieczeń), jak i poziomu pewności (miary zaufania do wdrożonych zabezpieczeń). Uwzględnienie zarówno funkcjonalności, jak i poziomu pewności bezpieczeństwa pomaga zapewnić, że komponenty technologii informacyjnej oraz systemy informacyjne zbudowane z tych komponentów z wykorzystaniem solidnych zasad inżynierii systemowej i bezpieczeństwa są wystarczająco wiarygodne.

Przygotowując się do wyboru i określenia odpowiednich środków bezpieczeństwa stosowanych w organizacyjnych systemach informacyjnych i środowiskach ich działania, organizacje najpierw określają krytyczność i wrażliwość informacji, które mają być przetwarzane, przechowywane lub przekazywane przez te systemy. Proces ten nazywany jest kategoryzacją zabezpieczeń. Standard NSC199 umożliwia organizacjom określanie kategorii bezpieczeństwa zarówno dla informacji, jak

i systemów informacyjnych. Inne dokumenty, takie jak te opracowane przez ISA[75] i CNSS[76], również zawierają wytyczne dotyczące określania niskiego, umiarkowanego i wysokiego poziomu wpływu na bezpieczeństwa. Kategorie bezpieczeństwa opierają się na potencjalnym wpływie na organizację lub na ludzi (pracowników i/lub społeczeństwo) w przypadku wystąpienia określonych zdarzeń, które zagrażają informacjom i systemom informacyjnym wykorzystywanym przez organizację do wypełniania przydzielonej jej misji, ochrony jej aktywów, wypełniania obowiązków prawnych, utrzymywania jej codziennych funkcji oraz ochrony indywidualnego bezpieczeństwa, zdrowia i życia. Kategorie bezpieczeństwa powinny być stosowane w połączeniu z informacjami i podatnościach i zagrożeniach uzyskiwanych podczas szacowania ryzyka ponoszonego przez organizację.

Niniejsza nakładka zawiera wytyczne uzupełniające ICS dotyczące środków bezpieczeństwa i zabezpieczeń rozszerzonych zalecanych dla systemu informacyjnego lub organizacji, zaprojektowanych w celu ochrony poufności, integralności i dostępności informacji oraz w celu spełnienia zestawu określonych wymagań bezpieczeństwa. Nakładka ta zawiera dostosowanie zabezpieczeń bazowych; jej specyfikacja może być bardziej lub mniej rygorystyczna niż oryginalne zabezpieczenie bazowe i może być stosowana do różnorodnych systemów informacyjnych. Nakładka ta jest wysokopoziomowa i ma zastosowanie do wszystkich ICS; może być wykorzystywana jako element bazowy do opracowania bardziej szczegółowych nakładek. Przypadki zastosowania w konkretnych systemach i w określonych środowiskach, mogą być publikowane w odrębny sposób (np. jako raport NISTIR).

Na rysunku G-1 przedstawiono zabezpieczenie AU-4, jako przykład ilustrujący format i zawartość szczegółowej specyfikacji nakładki na zabezpieczenie.

❶ Numer i nazwa zabezpieczenia.
❷ Kolumna zawierająca numer zabezpieczenia i zabezpieczenia rozszerzonego.
❸ Kolumna zawierająca nazwę zabezpieczenia i zabezpieczenia rozszerzonego.

[75] International Society of Automation.

[76] Committee on National Security Systems.

❹ Kolumny określające zabezpieczenia bazowe. Jeśli zabezpieczenia bazowe zostały dodatkowo rozszerzone, wówczas podana jest informacja uzupełniająca.

❺ Wiersz zawierający informacje i danym zabezpieczeniu lub zabezpieczeniu rozszerzonym.

❻ Kolumny określające wpływ zabezpieczenia bazowego na system: NISKI, ŚREDNI i WYSOKI.

❼ "Wybrane" oznacza, że zabezpieczenie zostało wybrane z NSC SP 800-53. "Dodane" oznacza, że zabezpieczenie została dodana do zabezpieczenia bazowego w nakładce ICS. Pusta komórka oznacza, że zabezpieczenie nie jest wybierane. "Usunięte" oznacza, że zabezpieczenie zostało usunięta z zabezpieczenia bazowego.

❽ Wytyczne uzupełniające do ICS. Jeśli nie występują, jest to odpowiednio zaznaczone.

❾ Zabezpieczenia rozszerzone. Zawarte są wskazówki uzupełniające zabezpieczenie rozszerzone ICS. Jeśli nie występują, jest to odpowiednio zaznaczone.

❿ Uzasadnienie zmiany zabezpieczenia bazowego. Pozycja zawiera uzasadnienie zmiany występującej w zabezpieczeniu bazowym lub zabezpieczeniu rozszerzonym.

❶ **AU-4 POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU**

❷ ❸ ❹

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu		
		Niski	Umiarkowany	Wysoki
AU-4	**Pojemność pamięci zapisów audytu**	Wybrane	Wybrane	Wybrane
AU-4(1)	Transfer rekordów do alternatywnych urządzeń magazynujących	Dodane	Dodane	Dodane

❺ ❻ ❼

❽ Wytyczne uzupełniające do ICS: brak wskazówek uzupełniających do ICS.

❾ Zabezpieczenia rozszerzone:

(1) Wskazówki uzupełniające dotyczące systemów ICS: Przestarzałe systemy ICS są zazwyczaj zaprojektowane do pracy z możliwością zdalnego przechowywania danych w oddzielnym systemie informatycznym (np. program historyzujący w DMZ gromadzi historyczne dane operacyjne ICS, a ich kopie zapasowe są przechowywane w innej lokalizacji). Aktualnie systemy ICS korzystają z usług tworzenia kopii zapasowych online i coraz częściej przechodzą na usługi oparte na chmurze obliczeniowej i zwirtualizowane. Zachowanie niektórych danych (np. telemetrii SCADA) może być wymagane przez organy regulacyjne.

❿ Uzasadnienie zmiany zabezpieczenia bazowego: Przestarzałe komponenty ICS zazwyczaj nie mają możliwości przechowywania lub analizowania danych z audytów. Okresy retencji niektórych danych, zwłaszcza danych dotyczących zgodności z przepisami, mogą wymagać dużej ilości pamięci masowej.

Rysunek G-1. Przykładowa specyfikacja nakładki na zabezpieczenia.

NSC 800-53 zawiera dodatkowe wskazówki dotyczące wszystkich zabezpieczeń i zabezpieczeń rozszerzonych. Wskazówki uzupełniające ICS zamieszczone w nakładkach dostarczają organizacjom dodatkowych informacji na temat zastosowania w systemach ICS i środowiskach, w których te wyspecjalizowane systemy działają, zabezpieczeń i zabezpieczeń rozszerzonych zawartych w publikacji NSC 800-53. Wskazówki uzupełniające ICS dostarczają również informacji i tym, dlaczego dane zabezpieczenie lub zabezpieczenie rozszerzone mogą nie mieć zastosowania w niektórych środowiskach ICS i mogą kwalifikować się do wprowadzenia indywidualnego dostosowania (tj. procedur ustalania zakresu działania systemu i/lub zabezpieczeń kompensacyjnych).

KATEGORIA AC – KONTROLA DOSTĘPU

Uwagi dotyczące dostosowania do kategorii kontroli dostępu

Przed wdrożeniem zabezpieczeń z kategorii AC, należy rozważyć kompromisy[77] między bezpieczeństwem, ochroną prywatności, opóźnieniami, wydajnością, przepustowością i niezawodnością systemu. Na przykład, organizacja rozważa, czy opóźnienia wynikające z zastosowania mechanizmów poufności i integralności wykorzystujących mechanizmy kryptograficzne będą miały negatywny wpływ na wydajność operacyjną ICS.

W sytuacjach, gdy system ICS nie może spełnić określonych wymagań zabezpieczeń kontroli dostępu, organizacja stosuje zabezpieczenia kompensacyjne zgodnie z ogólnymi wskazówkami dotyczącymi dostosowania. Zależnie od potrzeb, przy każdym zabezpieczeniu przedstawione są przykłady zabezpieczeń kompensacyjnych.

Zabezpieczenia powiązane

Zabezpieczenia powiązane dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zawartych w NSC 800-53, powinny być stosowane w połączeniu z wytycznymi uzupełniającymi ICS zawartymi w tej nakładce, jeśli takie istnieją.

AC-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta dotyczy w szczególności wyjątkowych właściwości i wymagań ICS oraz ich związku z systemami innymi niż ICS. Dostęp dostawców i personelu obsługi serwisowej do ICS może mieć charakter

[77] Działania decyzyjne, polegające na wyborze spośród różnych wymagań i alternatywnych rozwiązań na podstawie wartości dodanej dla zainteresowanych stron.

rozległy i obejmować bardzo duży obszar obiektu lub obszar geograficzny, a także przestrzenie nieobjęte nadzorem, takie jak pomieszczenia techniczne i elektrotechniczne, sufity, podłogi, podstacje terenowe, skrzynki z przełącznikami i zaworami oraz stacje przepompowni.

AC-2 ZARZĄDZANIE KONTAMI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-2	**ZARZĄDZANIE KONTAMI**	Wybrane	Wybrane	Wybrane
AC-2 (1)	AUTOMATYCZNE ZARZĄDZANIE KONTEM SYSTEMU		Wybrane	Wybrane
AC-2 (2)	AUTOMATYCZNE ZARZĄDZANIE KONTEM CZASOWYM | AWARYJNYM		Wybrane	Wybrane
AC-2 (3)	WYŁĄCZANIE KONT		Wybrane	Wybrane
AC-2 (4)	AUTOMATYCZNE DZIAŁANIA AUDYTOWE		Wybrane	Wybrane
AC-2 (5)	WYLOGOWANIE PRZEZ UŻYTKOWNIKA PO OKREŚLONYM OKRESIE NIEAKTYWNOŚCI			Wybrane
AC-2 (11)	WARUNKI UŻYTKOWANIA			Wybrane
AC-2 (12)	MONITOROWANIE KONTA POD WZGLĘDEM NIETYPOWYCH ZASTOSOWAŃ			Wybrane
AC-2 (13)	WYŁĄCZANIE KONT DOSTĘPOWYCH UŻYTKOWNIKOM WYSOKIEGO RYZYKA			Wybrane

Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują podniesienie poziomu bezpieczeństwa fizycznego, bezpieczeństwa personelu, wykrywanie włamań, środki audytu.

Zabezpieczenia rozszerzone:

(1, 3, 4) Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują stosowanie niezautomatyzowanych mechanizmów lub procedur.

(2) Wytyczne uzupełniające dotyczące ICS: w sytuacjach, w których ICS (np. urządzenia obiektowe) nie mogą obsługiwać kont tymczasowych lub awaryjnych, to rozszerzenie nie ma zastosowania. Przykładowe zabezpieczenia kompensacyjne obejmują stosowanie niezautomatyzowanych mechanizmów lub procedur.

(5) Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują stosowanie niezautomatyzowanych mechanizmów lub procedur.

(11, 12, 13) Brak wskazówek uzupełniających do ICS.

AC-3 EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-3	**EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują hermetyzację (enkapsulację). Polityka logicznej kontroli dostępu do zasobów systemowych typu nieadresowanego i nieroutowanego oraz związanych z nimi informacji jest wyraźnie określona. Mechanizmy kontroli dostępu obejmują sprzęt, oprogramowanie układowe i software, które kontroluje lub umożliwia dostęp do urządzeń, np. sterowniki urządzeń i kontrolery komunikacyjne. Fizyczna kontrola dostępu może służyć jako zabezpieczenie uzupełniające logiczną kontrolę dostępu, jednak może nie zapewniać wystarczającej precyzji w sytuacjach, gdy użytkownicy wymagają dostępu do różnych funkcjonalności. Logiczna kontrola dostępu może być realizowana za pomocą sprzętu i oprogramowania enkapsulującego.

AC-4 EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-4	**EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Adresy fizyczne (np. port szeregowy) mogą być pośrednio lub bezpośrednio powiązane z etykietami lub atrybutami (np. adres we/wy sprzętu). Metody ręczne są zazwyczaj statyczne. Mechanizmy polityki etykiet lub atrybutów mogą być zaimplementowane w sprzęcie, oprogramowaniu układowym i aplikacjach, które kontrolują urządzenia lub mają do nich dostęp, takich jak sterowniki urządzeń i kontrolery komunikacyjne. Zasady przepływu informacji mogą być wspierane przez etykietowanie lub koloryzowanie złączy fizycznych dla ułatwienia ręcznego podłączania. Kontrolowanie treści komunikatów może wymuszać przestrzeganie zasad przepływu informacji. Na przykład, komunikat zawierający polecenie skierowane do siłownika może nie uzyskać zezwolenia na przepływ między siecią sterowania a jakąkolwiek inną siecią.

AC-5 ROZDZIAŁ OBOWIĄZKÓW

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-5	**ROZDZIAŁ OBOWIĄZKÓW**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują zwiększenie bezpieczeństwa personelu i przeprowadzanie audytów. Organizacja dokładnie analizuje stosowność pełnienia wielu krytycznych ról przez jedną osobę.

AC-6 ZASADA WIEDZY KONIECZNEJ

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-6	**ZASADA WIEDZY KONIECZNEJ**		Wybrane	Wybrane
AC-6 (1)	UPOWAŻNIONY DOSTĘPU DO FUNKCJI BEZPIECZEŃSTWA		Wybrane	Wybrane
AC-6 (2)	NIEUPRZYWILEJOWANY DOSTĘP DLA FUNKCJI NIEZWIĄZANYCH Z BEZPIECZEŃSTWEM		Wybrane	Wybrane
AC-6 (3)	DOSTĘP SIECIOWY DO UPRZYWILEJOWANYCH POLECEŃ			Wybrane
AC-6 (5)	UPRZYWILEJOWANE KONTA		Wybrane	Wybrane
AC-6 (9)	KONTROLA WYKORZYSTANIA UPRZYWILEJOWANYCH FUNKCJI		Wybrane	Wybrane
AC-6 (10)	ODMOWA WYKONYWANIA PRZEZ NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW UPRZYWILEJOWANYCH FUNKCJI		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensujące obejmują zapewnienie zwiększonego bezpieczeństwa personelu i audytu. Organizacja starannie rozważa stosowność posiadania przez jedną osobę wielu krytycznych przywilejów. Modele przywilejów systemowych mogą być dostosowane w celu egzekwowania integralności i dostępności (np. niższe przywileje obejmują dostęp do odczytu, a wyższe przywileje obejmują dostęp do zapisu).

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: w sytuacjach, w których system ICS nie może wspierać kontroli dostępu do funkcji bezpieczeństwa, organizacja stosuje niezautomatyzowane mechanizmy lub procedury jako zabezpieczenia kompensacyjne, zgodnie z ogólnymi wytycznymi dotyczącymi procesu dostosowania.

(2) Wytyczne uzupełniające dotyczące ICS: w sytuacjach, w których system ICS nie może wspierać kontroli dostępu do funkcji niezwiązanych z bezpieczeństwem, organizacja stosuje niezautomatyzowane mechanizmy lub procedury jako zabezpieczenia kompensacyjne, zgodnie z ogólnymi wytycznymi dotyczącymi procesu dostosowania.

(3) Wytyczne uzupełniające dotyczące ICS: w sytuacjach, w których system ICS nie może wspierać kontroli dostępu sieciowego do uprzywilejowanych poleceń, organizacja stosuje niezautomatyzowane mechanizmy lub procedury jako zabezpieczenia kompensacyjne, zgodnie z ogólnymi wytycznymi dotyczącymi procesu dostosowania.

(5) Wytyczne uzupełniające dotyczące ICS: w sytuacjach, w których system ICS nie może wspierać kontroli dostępu do kont uprzywilejowanych, organizacja stosuje niezautomatyzowane mechanizmy lub procedury jako zabezpieczenia kompensacyjne, zgodnie z ogólnymi wytycznymi dotyczącymi procesu dostosowania.

(9) Wytyczne uzupełniające dotyczące ICS: Na ogół przetwarzanie zapisów audytowych nie odbywa się w ICS, lecz w oddzielnym systemie informacyjnym. Przykładowe zabezpieczenia kompensacyjne obejmują zapewnienie możliwości przeprowadzania audytu w oddzielnym systemie informacyjnym.

(10) Wytyczne uzupełniające dotyczące systemów ICS: Przykładowe zabezpieczenia kompensacyjne obejmują rozszerzony audyt.

AC-7 NIEUDANE PRÓBY LOGOWANIA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-7	**NIEUDANE PRÓBY LOGOWANIA**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Wiele systemów ICS musi pozostawać stale włączonych, a operatorzy muszą być zalogowani do systemu przez cały czas. Można zastosować funkcję "log-over". Przykładowe zabezpieczenia kompensacyjne obejmują rejestrowanie lub zapisywanie wszystkich nieudanych prób logowania oraz ostrzeganie pracowników odpowiedzialnych za bezpieczeństwo ICS za pośrednictwem alertów lub innych sposobów w przypadku przekroczenia zdefiniowanej przez organizację liczby kolejnych nieudanych prób dostępu.

AC-8 POWIADOMIENIE i ZASADACH UŻYCIA SYSTEMU

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-8	**POWIADOMIENIE I ZASADACH UŻYCIA SYSTEMU**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Wiele systemów ICS musi być włączonych przez cały czas, a powiadamianie i użyciu systemu może być nieuzasadnione lub nieskuteczne. Przykładowe zabezpieczenia kompensacyjne obejmują umieszczanie ogłoszeń wewnętrznych w obiektach ICS.

AC-10 KONTROLA ILOŚCI JEDNOCZESNYCH SESJI

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-10	**KONTROLA ILOŚCI JEDNOCZESNYCH SESJI**			Wybrane

Wytyczne uzupełniające dotyczące ICS: Liczba, typ konta i uprawnienia do równoczesnych sesji uwzględniają role i obowiązki osób, których dotyczą. Przykładowe zabezpieczenia kompensacyjne obejmują zapewnienie zwiększonej ilości audytowanych środków.

AC-11 BLOKADA URZĄDZENIA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-11	**BLOKADA URZĄDZENIA**		Wybrane	Wybrane
AC-11 (1)	WYGASZACZ EKRANU		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Zabezpieczenie to zakłada istnienie środowiska pracy, w którym użytkownicy mają kontakt z wyświetlaczami systemów informacyjnych. Jeśli założenie to nie ma zastosowania, organizacja odpowiednio dostosowuje zabezpieczenie (np. system ICS może być fizycznie chroniony przez umieszczenie go w zamkniętej obudowie). Zabezpieczenie może być również dostosowane do systemów ICS, które nie są wyposażone w wyświetlacze, ale mają możliwość ich używania (np. systemy ICS, do których serwisant może podłączyć wyświetlacz). W niektórych przypadkach nie zaleca się blokowania sesji na stacjach roboczych/węzłach operatora systemu ICS (np. jeżeli w sytuacjach awaryjnych wymagana jest natychmiastowa reakcja operatora). Przykładowe zabezpieczenia

kompensacyjne obejmują umieszczanie wyświetlacza w obszarze objętym fizycznymi środkami kontroli dostępu, które ograniczają dostęp do wyświetlanych informacji tylko do osób posiadających odpowiednie uprawnienia i wyznaczonych do tego celu.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: ICS może stosować ochronę fizyczną w celu uniemożliwienia dostępu do wyświetlacza lub uniemożliwienia jego podłączenia. W sytuacjach, w których system ICS nie może zamaskować wyświetlanych informacji, organizacja stosuje niezautomatyzowane mechanizmy lub procedury jako zabezpieczenia kompensacyjne pozostające w zgodzie z ogólnymi wytycznymi dotyczącymi dostosowania do indywidualnych potrzeb.

AC-12 ZAKOŃCZENIE SESJI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-12	**ZAKOŃCZENIE SESJI**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują zapewnienie zwiększonych środków kontroli lub ograniczenie uprawnień zdalnego dostępu do kluczowego personelu.

AC-14 DOZWOLONE DZIAŁANIA BEZ IDENTYFIKACJI LUB UWIERZYTELNIENIA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-14	**DOZWOLONE DZIAŁANIA BEZ IDENTYFIKACJI LUB UWIERZYTELNIENIA**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak

AC-17 DOSTĘP ZDALNY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-17	**DOSTĘP ZDALNY**	Wybrane	Wybrane	Wybrane
AC-17 (1)	AUTOMATYCZNE MONITOROWANIE I KONTROLA		Wybrane	Wybrane
AC-17 (2)	OCHRONA POUFNOŚCI I INTEGRALNOŚCI Z WYKORZYSTANIEM SZYFROWANIA		Wybrane	Wybrane
AC-17 (3)	ZARZĄDZANE PUNKTY KONTROLI DOSTĘPU		Wybrane	Wybrane
AC-17 (4)	POLECENIA UPRZYWILEJOWANE I DOSTĘP		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: w sytuacjach, gdy system ICS nie może wdrożyć któregokolwiek z elementów tego zabezpieczenia, organizacja stosuje inne mechanizmy lub procedury stanowiące zabezpieczenia kompensacyjne, z uwzględnieniem ogólnych wytycznych dotyczących procesów dostosowywania.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują stosowanie nieautomatycznych mechanizmów lub procedur jako zabezpieczeń kompensacyjnych (np. po uwierzytelnieniu osobistym [patrz: zabezpieczenie IA-2] można na określony czas włączyć zdalny dostęp wdzwaniany (ang. dial-in) lub nawiązać połączenie telekomunikacyjne z obiektu ICS do uwierzytelnionego podmiotu zdalnego).

(2) Wytyczne uzupełniające dotyczące systemów ICS: Cele związane z bezpieczeństwem ICS często przedkładają poufność nad dostępność i integralność. Organizacja bada wszystkie możliwe do zastosowania mechanizmy kryptograficzne

(np. szyfrowanie, podpis cyfrowy, funkcja skrótu). Każdy mechanizm ma inny wpływ na czas opóźnienia. Przykładowe zabezpieczenia kompensacyjne obejmują zapewnienie zwiększonego audytu sesji zdalnych lub ograniczenie uprawnień kluczowego personelu do korzystania ze zdalnego dostępu).

(3) Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują manualne uwierzytelnianie podmiotu zdalnego dla określonego połączenia.

(4) Wytyczne uzupełniające dotyczące ICS: Brak dodatkowych wytycznych dla ICS.

Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują stosowanie niezautomatyzowanych mechanizmów lub procedur jako zabezpieczeń kompensacyjnych, z uwzględnieniem ogólnych wytycznych dotyczących procesów dostosowywania.

AC-18 DOSTĘP BEZPRZEWODOWY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-18	**DOSTĘP BEZPRZEWODOWY**	Wybrane	Wybrane	Wybrane
AC-18 (1)	UWIERZYTELNIANIE ORAZ SZYFROWANIE		Wybrane	Wybrane
AC-18 (4)	OGRANICZENIE DOKONYWANIE KONFIGURACJI PRZEZ UŻYTKOWNIKÓW			Wybrane
AC-18 (5)	POZIOMY MOCY ANTEN / TRANSMISJI			Wybrane

Wytyczne uzupełniające dotyczące ICS: w sytuacjach, gdy system ICS nie może wdrożyć któregokolwiek z elementów tego zabezpieczenia, organizacja stosuje inne mechanizmy lub procedury stanowiące zabezpieczenia kompensacyjne, z uwzględnieniem ogólnych wytycznych dotyczących procesów dostosowywania.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Patrz zabezpieczenie AC-17 (1). Przykładowe zabezpieczenia kompensacyjne obejmują zapewnienie zwiększonego audytu dostępu do sieci bezprzewodowej lub ograniczanie przywilejów dostępu kluczowego personelu do sieci bezprzewodowej.

(4) (5) Wytyczne uzupełniające dotyczące ICS: Brak.

AC-19 KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-19	**KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH**	Wybrane	Wybrane	Wybrane
AC-19 (5)	SZYFROWANIE ZAWARTOŚCI CAŁEGO URZĄDZENIA / WYBRANYCH ZASOBÓW URZĄDZENIA		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak

AC-20 WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-20	**WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH**	Wybrane	Wybrane	Wybrane
AC-20 (1)	OGRANICZENIA AUTORYZOWANEGO DOSTĘPU		Wybrane	Wybrane
AC-20 (2)	PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE - OGRANICZONE ZASTOSOWANIE		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Organizacje doprecyzowują definicję pojęcia "zewnętrzny", aby odzwierciedlić zakres uprawnień i odpowiedzialności; stopień rozbudowania jednostki organizacyjnej oraz wzajemne relacje. Organizacja może uznać system za zewnętrzny, jeśli posiada różne funkcje, wdraża różne polityki, podlega różnym zarządcom lub nie zapewnia wystarczającego dostępu do wdrażania środków bezpieczeństwa, co pozwoliłoby na ustanowienie zadowalającej relacji zaufania. Na przykład, system sterowania procesami i system przetwarzania danych biznesowych są zazwyczaj uważane za zewnętrzne względem siebie. Innym częstym przykładem jest dostęp do ICS w celu uzyskania wsparcia ze strony partnera biznesowego, np. dostawcy lub wykonawcy wsparcia. Definicja i wiarygodność zewnętrznych systemów informacyjnych jest ponownie analizowana w odniesieniu do funkcji, celów, technologii i ograniczeń ICS w celu ustanowienia jednoznacznie udokumentowanego technicznego lub biznesowego uzasadnienia zastosowania oraz akceptacji ryzyka związanego z zastosowaniem zewnętrznego systemu informacyjnego.

Zabezpieczenia rozszerzone: (1, 2) Brak wytycznych uzupełniających dotyczących ICS.

AC-21 UDOSTĘPNIANIE INFORMACJI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-21	**UDOSTĘPNIANIE INFORMACJI**	Dodane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Organizacja powinna współpracować i na bieżąco dzielić się informacjami i potencjalnych incydentach[78]. Organizacje powinny rozważyć posiadanie zarówno możliwości dzielenia się informacjami jawnymi, jak i niejawnymi.

[78] Patrz: NSC 800-61.

Uzasadnienie zmiany zabezpieczenia bazowego: Systemy ICS zapewniają istotne usługi i funkcje sterowania i często są połączone z innymi systemami ICS lub systemami biznesowymi, które mogą stanowić wektory ataku. Dlatego konieczne jest zapewnienie jednolitej obrony obejmującej zabezpieczenia bazowe na wszystkich poziomach wpływu.

AC-22 TREŚCI PUBLICZNIE DOSTĘPNE

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AC-22	**TREŚCI PUBLICZNIE DOSTĘPNE**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Zasadniczo, publiczny dostęp do systemów ICS nie jest dozwolony. Wybrane informacje mogą być przekazywane do publicznie dostępnego systemu informacyjnego, po ewentualnym zastosowaniu dodatkowych środków bezpieczeństwa.

KATEGORIA AT - UŚWIADAMIANIE i SZKOLENIA

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

AT-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AT-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta dotyczy w szczególności wyjątkowych właściwości i wymagań ICS oraz ich związku z systemami innymi niż ICS.

AT-2 SZKOLENIE w ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AT-2	**SZKOLENIE w ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA**	Wybrane	Wybrane	Wybrane
AT-2 (2)	ZAGROŻENIE WEWNĘTRZNE		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Szkolenie w zakresie uświadamiania bezpieczeństwa obejmuje wstępny i okresowy przegląd polityk, standardowych procedur operacyjnych, trendów w zakresie bezpieczeństwa i podatności na zagrożenia, specyficznych dla danego systemu ICS. Program podnoszenia świadomości

w zakresie bezpieczeństwa ICS jest zgodny z ustanowionymi przez organizację wymaganiami polityki uświadamiania i szkolenia w zakresie bezpieczeństwa informacji.

Zabezpieczenia rozszerzone:

(2) Brak wytycznych uzupełniających dotyczących ICS.

AT-3 SZKOLENIE w ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AT-3	**SZKOLENIE w ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Szkolenie w zakresie bezpieczeństwa obejmuje wstępny i okresowy przegląd polityk, standardowych procedur operacyjnych, trendów w zakresie bezpieczeństwa i podatności na zagrożenia, specyficznych dla danego systemu ICS. Program szkolenia w zakresie bezpieczeństwa ICS jest zgodny z ustanowionymi przez organizację wymaganiami polityki uświadamiania i szkolenia w zakresie bezpieczeństwa informacji.

AT-4 DOKUMENTACJA SZKOLENIOWA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AT-4	**DOKUMENTACJA SZKOLENIOWA**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak

KATEGORIA AU - AUDYT i ROZLICZALNOŚĆ

Uwagi dotyczące dostosowania do kategorii audytu i rozliczalności

Na ogół informacje i narzędzia audytowe nie są dostępne w istniejących ICS, ale w oddzielnym systemie informacyjnym (np. W systemie archiwalnym). W sytuacjach, w których system ICS nie może wspierać określonych wymagań zabezpieczeń w zakresie audytu i rozliczalności, organizacja stosuje zabezpieczenia kompensacyjne zgodnie z ogólnymi wskazówkami dotyczącymi dostosowania. Przykłady zabezpieczeń kompensacyjnych są podane przy każdym zabezpieczeniu, stosownie do potrzeb.

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

AU-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AU-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta dotyczy w szczególności wyjątkowych właściwości i wymagań ICS oraz ich związku z systemami innymi niż ICS.

AU-2 AUDYT ZDARZEŃ

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AU-2	**AUDYT ZDARZEŃ**	Wybrane	Wybrane	Wybrane

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AU-2 (3)	OPINIE I AKTUALIZACJE		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Organizacja może określić zdarzenia ICS jako zdarzenia podlegające audytowi, wymagając, aby dane i/lub telemetria ICS były rejestrowane jako dane podlegające audytowi.

Zabezpieczenia rozszerzone:

(3) Brak wytycznych uzupełniających dotyczących ICS.

AU-3 ZAWARTOŚĆ REJESTRÓW AUDYTU

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AU-3	**ZAWARTOŚĆ REJESTRÓW AUDYTU**	Wybrane	Wybrane	Wybrane
AU-3 (1)	DODATKOWE INFORMACJE KONTROLNE		Wybrane	Wybrane
AU-3 (2)	CENTRALNE ZARZĄDZANIE TREŚCIĄ PLANOWANEGO REJESTRU AUDYTU			Wybrane

Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują zapewnienie możliwości przeprowadzania audytu w wydzielonym systemie informacyjnym.

Zabezpieczenia rozszerzone:

(1, 2) Brak wytycznych uzupełniających dotyczących ICS.

AU-4 POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AU-4	**POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU**	Wybrane	Wybrane	Wybrane
AU-4 (1)	TRANSFER REKORDÓW DO ALTERNATYWNYCH URZĄDZEŃ MAGAZYNUJĄCYCH	Dodane	Dodane	Dodane

Wytyczne uzupełniające dotyczące ICS: Brak.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Starsze systemy ICS są zazwyczaj skonfigurowane pod kątem zdalnego przechowywania danych w oddzielnym systemie informacyjnym (np. system archiwizacji gromadzi historyczne dane operacyjne ICS, a ich kopie zapasowe są przechowywane w oddzielnym miejscu). Obecnie systemy ICS korzystają z usług tworzenia kopii zapasowych online i coraz częściej przechodzą na usługi oparte na chmurze i zwirtualizowane. Przechowywanie niektórych danych (np. telemetrii SCADA) może być wymagane przez organy regulacyjne.

Uzasadnienie zmiany zabezpieczenia bazowego (1): Starsze komponenty ICS zazwyczaj nie mają zdolności do przechowywania lub analizowania danych audytowych. Okresy przechowywania niektórych danych, w szczególności danych dotyczących zgodności, mogą wymagać dużych ilości pamięci masowej.

AU-5 REAKCJA NA BŁĘDY PROCESÓW AUDYTU

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AU-5	**REAKCJA NA BŁĘDY PROCESÓW AUDYTU**	Wybrane	Wybrane	Wybrane
AU-5 (1)	OSTRZEŻENIA DOTYCZĄCE LIMITU PAMIĘCI PRZECHOWYWANIA REKORDÓW AUDYTU			Wybrane
AU-5 (2)	ALERTY CZASU RZECZYWISTEGO			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

AU-6 PRZEGLĄD AUDYTU, ANALIZA i RAPORTOWANIE

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AU-6	**PRZEGLĄD AUDYTU, ANALIZA i RAPORTOWANIE**	Wybrane	Wybrane	Wybrane
AU-6 (1)	ZAUTOMATYZOWANA INTEGRACJA PROCESÓW		Wybrane	Wybrane
AU-6 (3)	KORELACJA ZBIORÓW AUDYTU		Wybrane	Wybrane
AU-6 (5)	ZINTEGROWANA ANALIZA ZAPISÓW z AUDYTU			Wybrane
AU-6 (6)	KORELACJA AUDYTU z MONITOROWANIEM FIZYCZNYM			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują ręczne mechanizmy lub procedury.

(3, 5, 6) Brak wytycznych uzupełniających dotyczących ICS.

AU-7 REDUKCJA TREŚCI ZAPISÓW z AUDYTU i GENEROWANIE RAPORTÓW

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AU-7	**REDUKCJA TREŚCI ZAPISÓW z AUDYTU i GENEROWANIE RAPORTÓW**		Wybrane	Wybrane
AU-7 (1)	AUTOMATYZACJA PROCESU		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

Zabezpieczenia rozszerzone:

(1) Brak wytycznych uzupełniających dotyczących ICS.

AU-8 ZNACZNIKI CZASU

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AU-8	**ZNACZNIKI CZASU**	Wybrane	Wybrane	Wybrane
AU-8 (1)	SYNCHRONIZACJA z AUTORYZOWANYM ŹRÓDŁEM CZASU ODNIESIENIA		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują korzystanie z niezależnego systemu informacyjnego uznanego za autoryzowane źródło czasu odniesienia.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: w systemach ICS stosowane są odpowiednie mechanizmy (np. GPS, IEEE 1588) służące do określania znaczników czasu.

AU-9 OCHRONA INFORMACJI AUDYTOWYCH

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AU-9	**OCHRONA INFORMACJI AUDYTOWYCH**	Wybrane	Wybrane	Wybrane
AU-9 (2)	BACKUP AUDYTU w ODSEPAROWANYM FIZYCZNIE SYSTEMIE / KOMPONENCIE			Wybrane
AU-9 (3)	OCHRONA KRYPTOGRAFICZNA			Wybrane
AU-9 (4)	DOSTĘP DO PODZBIORU UPRZYWILEJOWANYCH UŻYTKOWNIKÓW		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

AU-10 NIEZAPRZECZALNOŚĆ

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AU-10	**NIEZAPRZECZALNOŚĆ**			Wybrane

Wytyczne uzupełniające dotyczące ICS:- Przykładowe zabezpieczenia kompensacyjne obejmują zapewnienie niezaprzeczalności w odseparowanym systemie informacyjnym.

AU-11 RETENCJA ZAPISÓW AUDYTU

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AU-11	**RETENCJA ZAPISÓW AUDYTU**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

AU-12 TWORZENIE ZAPISÓW AUDYTU

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
AU-12	**TWORZENIE ZAPISÓW AUDYTU**	Wybrane	Wybrane	Wybrane
AU-12 (1)	OGÓLNOSYSTEMOWE / SKORELOWANE w CZASIE ŚCIEŻKI AUDYTU			Wybrane
AU-12 (3)	ZMIANY DOKONYWANE PRZEZ UPRAWNIONE OSOBY			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują dostarczanie powiązanych czasowo zapisów audytowych do oddzielnego systemu informacyjnego.

(3) Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują stosowanie niezautomatyzowanych mechanizmów lub procedur.

KATEGORIA CA - OCENA, AUTORYZACJA i MONITOROWANIE

Uwagi dotyczące dostosowania do kategorii oceny, autoryzacji i monitorowania

W sytuacjach, w których system ICS nie może wspierać określonych wymagań zabezpieczeń w zakresie oceny, autoryzacji i monitorowania, organizacja stosuje zabezpieczenia kompensacyjne zgodnie z ogólnymi wskazówkami dotyczącymi dostosowania. Przykłady zabezpieczeń kompensacyjnych są podane przy każdym zabezpieczeniu, stosownie do potrzeb.

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

CA-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CA-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Zasady te w szczególny sposób odnoszą się do wyjątkowych właściwości i wymagań ICS oraz relacji z systemami innymi niż ICS.

CA-2 OCENA ZABEZPIECZEŃ

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CA-2	**OCENA ZABEZPIECZEŃ**	Wybrane	Wybrane	Wybrane
CA-2 (1)	NIEZALEŻNI AUDYTORZY		Wybrane	Wybrane

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CA-2 (2)	OCENY SPECJALISTYCZNE			Wybrane

Wytyczne uzupełniające dotyczące ICS: Oceny są wykonywane i dokumentowane przez wykwalifikowany personel oceniający (tj. posiadający doświadczenie w ocenie ICS) upoważniony przez organizację. Organizacja zapewnia, że przeprowadzanie ocen nie koliduje z funkcjonalnością ICS. Osoba/grupa przeprowadzająca ocenę w pełni rozumie polityki i procedury bezpieczeństwa informacji organizacji, polityki i procedury bezpieczeństwa ICS oraz specyficzne zagrożenia dla zdrowia, bezpieczeństwa i środowiska związane z danym obiektem i/lub procesem. Organizacja zapewnia, że ocenianie nie wpłynie na działanie systemu lub nie spowoduje niezamierzonej modyfikacji systemu. Jeżeli działania związane z oceną muszą być przeprowadzone na produkcyjnym ICS, może zaistnieć konieczność wyłączenia go z eksploatacji przed przeprowadzeniem oceny. Jeżeli w celu przeprowadzenia oceny konieczne jest wyłączenie ICS z eksploatacji, przeprowadzenie tych czynności planowane jest w miarę możliwości podczas planowanych przestojów ICS.

Zabezpieczenia rozszerzone:

(1) Brak wytycznych uzupełniających dotyczących ICS.

(2) Wytyczne uzupełniające dotyczące ICS: Organizacja przeprowadza analizę ryzyka w celu wsparcia wyboru przedmiotu oceny (np. system operacyjny, replika off-line, symulacja).

CA-3 WYMIANA INFORMACJI

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CA-3	**WYMIANA INFORMACJI**	Wybrane	Wybrane	Wybrane
CA-3 (5)	POŁĄCZENIA JAWNYCH BEZPIECZNYCH SYSTEMÓW TRANSGRANICZNYCH		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Organizacje przeprowadzają analizę ryzyka i korzyści w celu uzasadnienia decyzji, czy system ICS powinien zostać połączony z innym system informacyjnym. Osoba autoryzująca ma pełną świadomość zasad i procedur bezpieczeństwa informacji w organizacji; zasad i procedur bezpieczeństwa ICS; zagrożeń wynikających z połączenia z innymi systemami informacyjnymi związanych z działalnością i aktywami organizacji, osobami, innymi organizacjami i państwem; oraz szczególnych zagrożeń dla zdrowia, bezpieczeństwa i środowiska związanych z danym połączeniem. OA dokumentuje akceptację ryzyka w planie bezpieczeństwa systemu ICS.

Zabezpieczenia rozszerzone:

(5) Brak wytycznych uzupełniających ICS.

CA-5 PLAN i ETAPY DZIAŁANIA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CA-5	**PLAN i ETAPY DZIAŁANIA**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

CA-6 AUTORYZACJA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CA-6	**AUTORYZACJA**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

CA-7 CIĄGŁE MONITOROWANIE

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CA-7	**CIĄGŁE MONITOROWANIE**	Wybrane	Wybrane	Wybrane
CA-7 (1)	NIEZALEŻNA OCENA		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Programy ciągłego monitorowania ICS są zaprojektowane, udokumentowane i wdrożone przez wykwalifikowany personel (tj. posiadający doświadczenie w zakresie ICS) wybrany przez organizację. Organizacja zapewnia, że ciągłe monitorowanie nie zakłóca funkcji ICS. Osoba/grupa projektująca i prowadząca ciągłe monitorowanie w pełni rozumie polityki i procedury bezpieczeństwa informacji organizacji, polityki i procedury bezpieczeństwa ICS oraz specyficzne zagrożenia dla zdrowia, bezpieczeństwa i środowiska związane z danym obiektem i/lub procesem. Organizacja zapewnia, że ciągłe monitorowanie nie wpływa na działanie systemu, ani nie prowadzi do zamierzonej lub niezamierzonej modyfikacji systemu. Przykładowe zabezpieczenia kompensacyjne obejmują monitorowanie zewnętrzne.

Zabezpieczenia rozszerzone:

(1) Brak wytycznych uzupełniających ICS.

CA-8 TESTY PENETRACYJNE

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CA-8	**TESTY PENETRACYJNE**			Wybrane

Wytyczne uzupełniające dotyczące ICS: Testy penetracyjne są przeprowadzane w sieciach ICS z zachowaniem szczególnej ostrożności, tak aby proces testowania nie miał negatywnego wpływu na funkcje ICS. Ogólnie rzecz biorąc, systemy ICS są bardzo wrażliwe na ograniczenia czasowe i mają ograniczone zasoby. Przykładowe zabezpieczenia kompensacyjne obejmują wykorzystanie replikowanego, zwirtualizowanego lub symulowanego systemu do przeprowadzenia testów penetracyjnych. Może zaistnieć konieczność wyłączenia produkcyjnego ICS z eksploatacji przed przeprowadzeniem testów. Jeśli w celu przeprowadzenia testów wyłączane są systemy ICS, testy planuje się w miarę możliwości podczas planowanych przestojów ICS. Jeżeli testy penetracyjne są przeprowadzane w sieciach innych niż ICS, należy zachować szczególną ostrożność, aby testy nie rozciągnęły się na sieć ICS.

CA-9 POŁĄCZENIA WEWNĄTRZSYSTEMOWE

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CA-9	**POŁĄCZENIA WEWNĄTRZSYSTEMOWE**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Organizacje przeprowadzają analizę ryzyka i korzyści w celu określenia, czy system ICS powinien być połączony z innymi wewnętrznymi systemami informacyjnymi i (oddzielnymi) komponentami systemów. Osoba autoryzująca w pełni rozumie polityki i procedury bezpieczeństwa informacji organizacji; polityki i procedury bezpieczeństwa ICS; ryzyko związane z połączeniem

z innymi systemami informacyjnymi i wydzielonymi częściami składowymi systemu dla działań i aktywów organizacji, osób, innych organizacji i państwa, niezależnie od tego, czy chodzi i zezwolenie na każde indywidualne połączenie wewnętrzne, czy i zezwolenie na połączenia wewnętrzne dla grupy komponentów i wspólnych cechach i/lub konfiguracjach; oraz szczególne ryzyko dla zdrowia, bezpieczeństwa i środowiska związane z danym połączeniem. Osoba autoryzująca dokumentuje akceptację ryzyka w planie bezpieczeństwa systemu ICS.

KATEGORIA CM - ZARZĄDZANIE KONFIGURACJĄ

Uwagi dotyczące dostosowania do kategorii zarządzania konfiguracją

W sytuacjach, w których system ICS nie może być skonfigurowany w celu ograniczenia użycia nieprzydatnych funkcji lub nie może wspierać użycia zautomatyzowanych mechanizmów do wdrożenia funkcji zarządzania konfiguracją, organizacja stosuje niezautomatyzowane mechanizmy lub procedury jako zabezpieczenia kompensacyjne zgodnie z ogólnymi wskazówkami dotyczącymi dostosowania. Przykłady zabezpieczeń kompensacyjnych są podane przy każdym zabezpieczeniu, stosownie do potrzeb.

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

CM-1 POLITYKA I PROCEDURY

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CM-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta uwzględnia specyficzne właściwości i wymagania ICS oraz relacje z systemami innymi niż ICS.

CM-2 KONFIGURACJA BAZOWA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CM-2	**KONFIGURACJA BAZOWA**	Wybrane	Wybrane	Wybrane

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CM-2 (1)	PRZEGLĄDY I AKTUALIZACJE		Wybrane	Wybrane
CM-2 (2)	AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ / SZCZEGÓŁOWOŚĆ			Wybrane
CM-2 (3)	RETENCJA ZACHOWANYCH KONFIGURACJI		Wybrane	Wybrane
CM-2 (7)	KONFIGURACJA SYSTEMÓW I KOMPONENTÓW W OBSZARACH WYSOKIEGO RYZYKA		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

CM-3 ZABEZPIECZANIE ZMIAN KONFIGURACJI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CM-3	**ZABEZPIECZANIE ZMIAN KONFIGURACJI**		Wybrane	Wybrane
CM-3 (1)	AUTOMATYCZNA DOKUMENTACJA / POWIADAMIANIE / ZAKAZ WPROWADZANIA ZMIAN			Wybrane
CM-3 (2)	TESTY, WALIDACJA I ZMIANY DOKUMENTÓW		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

CM-4 ANALIZY WPŁYWU

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CM-4	**ANALIZY WPŁYWU**	Wybrane	Wybrane	Wybrane
CM-4 (1)	ODDZIELNE ŚRODOWISKA BADAWCZE			Wybrane

Wytyczne uzupełniające dotyczące ICS: Organizacja uwzględnia wzajemne zależności między bezpieczeństwem i ochroną systemu ICS.

Zabezpieczenia rozszerzone:

(1) Brak wytycznych uzupełniających ICS.

CM-5 OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CM-5	**OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN**		Wybrane	Wybrane
CM-5 (1)	AUTOMATYCZNE EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU I ZAPISY Z AUDYTU			Wybrane
CM-5 (2)	PRZEGLĄD ZMIAN W SYSTEMIE			Wybrane
CM-5 (3)	PODPISANE KOMPONENTY			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

CM-6 USTAWIENIA KONFIGURACJI

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CM-6	**USTAWIENIA KONFIGURACJI**	Wybrane	Wybrane	Wybrane
CM-6 (1)	AUTOMATYCZNE ZARZĄDZANIE, STOSOWANIE I WERYFIKACJA			Wybrane
CM-6 (2)	ODPOWIEDŹ NA NIEAUTORYZOWANE ZMIANY			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

CM-7 ZASADA MINIMALNEJ FUNKCJONALNOŚCI

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CM-7	**ZASADA MINIMALNEJ FUNKCJONALNOŚCI**	Wybrane	Wybrane	Wybrane
CM-7 (1)	PRZEGLĄDY OKRESOWE	Dodane	Wybrane	Wybrane
CM-7 (2)	ZAPOBIEGANIA WYKONYWANIU PROGRAMU		Wybrane	Wybrane
CM-7 (4)	NIEAUTORYZOWANE OPROGRAMOWANIE („CZARNA LISTA”)		Usunięte	
CM-7 (5)	AUTORYZOWANE OPROGRAMOWANIE („BIAŁA LISTA”)		Dodane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Porty, w rozumieniu NSC 800-53, są wykorzystywane jako część przestrzeni adresowej w protokołach sieciowych i są często związane z określonymi protokołami lub funkcjami. Jako takie, porty nie są istotne dla protokołów i urządzeń nieroutowanych. W przypadku protokołów i urządzeń nieroutowanych i nieadresowanych, zakaz lub ograniczenie korzystania z określonych funkcji, protokołów i/lub usług musi być wdrożony z uwzględnieniem dostępnej granulacji (pod)systemowej (np. na niskim poziomie można wyłączyć przerwania; na wysokim poziomie funkcje mogą być dostępne tylko do odczytu, z wyjątkiem użytkowników uprzywilejowanych). Przykładowe zabezpieczenia kompensacyjne obejmują stosowanie niezautomatyzowanych mechanizmów lub procedur.

Zabezpieczenia rozszerzone:

(1, 2, 5) Brak wytycznych uzupełniających ICS.

Uzasadnienie zmiany zabezpieczeń bazowych:

(1) Okresowy przegląd i usuwanie zbędnych i/lub niezabezpieczonych funkcji, portów, protokołów i usług dodaje się do systemów i niskim poziomie wpływu, ponieważ wiele komponentów ICS i niskim poziomie wpływu może mieć negatywne oddziaływanie na systemy, z którymi są połączone.

(4, 5) „Biała lista” (CM-7 (5)) jest bardziej skuteczna niż „czarna lista” (CM-7 (4)). Zestaw aplikacji działających w ICS jest w zasadzie niezmienny, co czyni "białą listę" rozwiązaniem praktycznym. Zaleca się wdrażanie "białej listy" aplikacji w systemach ICS.

Referencje: http://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B

CM-8 INWENTARYZACJA KOMPONENTÓW SYSTEMU

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CM-8	**INWENTARYZACJA KOMPONENTÓW SYSTEMU**	Wybrane	Wybrane	Wybrane
CM-8 (1)	AKTUALIZACJE INSTALACJI I USUWANIA KOMPONENTÓW		Wybrane	Wybrane
CM-8 (2)	AUTOMATYCZNA KONSERWACJA (UTRZYMYWANIE)			Wybrane
CM-8 (3)	AUTOMATYCZNE WYKRYWANIE KOMPONENTÓW NIEAUTORYZOWANYCH		Wybrane	Wybrane
CM-8 (4)	INFORMACJE DOTYCZĄCE ODPOWIEDZIALNOŚCI I ROZLICZALNOŚCI			Wybrane
CM-8 (5)	BRAK DUPLIKACJI KOMPONENTÓW		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

CM-9 PLAN ZARZĄDZANIA KONFIGURACJĄ

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CM-9	**PLAN ZARZĄDZANIA KONFIGURACJĄ**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

CM-10 OGRANICZENIA w UŻYCIU OPROGRAMOWANIA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CM-10	**OGRANICZENIA w UŻYCIU OPROGRAMOWANIA**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

CM-11 OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CM-11	**OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

KATEGORIA CP - PLANOWANIE AWARYJNE / CIĄGŁOŚĆ DZIAŁANIA

Uwagi dotyczące dostosowania do kategorii planowania awaryjnego / ciągłości działania

Systemy ICS często zawierają fizyczny komponent znajdujący się w stałej lokalizacji. Komponentów takich nie można logicznie przemieszczać. Niektóre komponenty zastępcze mogą być trudno dostępne. Kontynuacja istotnych misji i funkcji biznesowych z niewielką lub żadną utratą ciągłości działania może być niemożliwa. W sytuacjach, gdy organizacja nie może zapewnić niezbędnych podstawowych usług, wsparcia lub zautomatyzowanych mechanizmów podczas operacji awaryjnych, organizacja zapewnia niezautomatyzowane mechanizmy lub wcześniej ustalone procedury jako zabezpieczenia kompensacyjne zgodnie z ogólnymi wytycznymi dotyczącymi dostosowań Przykłady zabezpieczeń kompensacyjnych są podane przy każdym zabezpieczeniu, odpowiednio do potrzeb.

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

CP-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CP-1	POLITYKA i PROCEDURY	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta uwzględnia specyficzne właściwości i wymagania ICS oraz relacje z systemami innymi niż ICS.

CP-2 PLAN CIĄGŁOŚCI DZIAŁANIA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CP-2	**PLAN CIĄGŁOŚCI DZIAŁANIA**	Wybrane	Wybrane	Wybrane
CP-2 (1)	KOORDYNACJA z POWIĄZANYMI PLANAMI		Wybrane	Wybrane
CP-2 (2)	PLANOWANIE ZDOLNOŚCI FUNKCJONOWANIA			Wybrane
CP-2 (3)	WZNAWIANIE PODSTAWOWYCH DZIAŁAŃ i FUNKCJI BIZNESOWYCH		Wybrane	Wybrane
CP-2 (4)	PRZYWRÓCENIE DZIAŁANIA WSZYSTKICH FUNKCJI BIZNESOWYCH			Wybrane
CP-2 (5)	KONTYNUACJA NIEZBĘDNYCH DZIAŁAŃ i FUNKCJI BIZNESOWYCH			Wybrane
CP-2 (8)	IDENTYFIKACJA ZASOBÓW KRYTYCZNYCH		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Organizacja definiuje plany ciągłości działania dla poszczególnych kategorii zakłóceń lub awarii. W przypadku utraty możliwości przetwarzania danych w ICS lub komunikacji z obiektami operacyjnymi, ICS wykonuje wcześniej ustalone procedury (np. powiadamia operatora o awarii a następnie nie podejmuje żadnych działań; powiadamia operatora a następnie bezpiecznie zamyka proces przemysłowy; powiadamia operatora a następnie podtrzymuje ostatnie ustawienia operacyjne sprzed momentu wystąpienia awarii).

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Elementy organizacyjne odpowiedzialne za powiązane plany mogą obejmować dostawców energii elektrycznej, paliwa, wody pitnej i odprowadzających ścieki.

(2) Wytyczne uzupełniające dotyczące ICS: Brak.

(3, 4) Wytyczne uzupełniające dotyczące ICS: Plany wznowienia podstawowych misji i funkcji biznesowych oraz wznowienia wszystkich misji i funkcji biznesowych uwzględniają skutki zakłócenia środowiska organizacji. Plany przywracania i wznawiania działalności powinny uwzględniać priorytetyzację działań. Zakłócenia mogą wpłynąć na jakość i ilość zasobów w środowisku, takich jak energia elektryczna, paliwo, słodka woda i ścieki, oraz na zdolność tych dostawców do wznowienia świadczenia podstawowych funkcji misji i działalności. Plany ciągłości działania na wypadek wystąpienia rozległych zakłóceń mogą obejmować wyspecjalizowane organizacje (np. służby zarządzania kryzysowego, służby ratownicze, organy regulacyjne).

Referencje: NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs.

(5, 8) Wytyczne uzupełniające dotyczące ICS: Brak.

CP-3 SZKOLENIE w ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CP-3	**SZKOLENIE w ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA**	Wybrane	Wybrane	Wybrane
CP-3 (1)	WYDARZENIA SYMULOWANE			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

CP-4 TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CP-4	**TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA**	Wybrane	Wybrane	Wybrane
CP-4 (1)	KOORDYNACJA z POWIĄZANYMI PLANAMI		Wybrane	Wybrane
CP-4 (2)	ZAPASOWE MIEJSCE PRZETWARZANIA			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

CP-6 ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CP-6	**ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII**		Wybrane	Wybrane
CP-6 (1)	SEPARACJA OD MIEJSCA GŁÓWNEGO		Wybrane	Wybrane
CP-6 (2)	CZAS ODZYSKIWANIA I PUNKT ODTWORZENIA DANYCH			Wybrane
CP-6 (3)	DOSTĘPNOŚĆ		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

CP-7 ZAPASOWE MIEJSCE PRZETWARZANIA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CP-7	**ZAPASOWE MIEJSCE PRZETWARZANIA**		Wybrane	Wybrane
CP-7 (1)	ODSEPAROWANIE OD LOKALIZACJI PODSTAWOWEJ		Wybrane	Wybrane
CP-7 (2)	DOSTĘPNOŚĆ		Wybrane	Wybrane
CP-7 (3)	PRIORYTET USŁUG		Wybrane	Wybrane
CP-7 (4)	GOTOWOŚĆ DO UŻYCIA			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

CP-8 USŁUGI TELEKOMUNIKACYJNE

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CP-8	**USŁUGI TELEKOMUNIKACYJNE**		Wybrane	Wybrane
CP-8 (1)	PRIORYTETY ŚWIADCZENIA USŁUG		Wybrane	Wybrane
CP-8 (2)	POJEDYNCZE PUNKTY AWARII		Wybrane	Wybrane
CP-8 (3)	ROZDZIELENIE DOSTAWCÓW PODSTAWOWYCH i ALTERNATYWNYCH			Wybrane
CP-8 (4)	PLAN AWARYJNY DOSTAWCY			Wybrane

Wytyczne uzupełniające dotyczące ICS: Współczynniki jakości usług (QoS) systemu ICS obejmują opóźnienia i przepustowość.

Zabezpieczenia rozszerzone:

(1, 2, 3, 4) Wytyczne uzupełniające dotyczące ICS: Brak.

CP-9 KOPIA ZAPASOWA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CP-9	**KOPIA ZAPASOWA**	Wybrane	Wybrane	Wybrane
CP-9 (1)	BADANIE NIEZAWODNOŚCI NOŚNIKÓW / INTEGRALNOŚCI INFORMACJI		Wybrane	Wybrane
CP-9 (2)	TESTY ODTWORZENIOWE z WYKORZYSTANIEM PRÓBEK DANYCH			Wybrane
CP-9 (3)	SEPARACJA PRZECHOWYWANIA INFORMACJI KRYTYCZNYCH			Wybrane
CP-9 (5)	PRZEKAZANIE KOPII DO ALTERNATYWNEJ LOKALIZACJI			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

CP-10 ODZYSKIWANIE i ODTWARZANIE SYSTEMU

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CP-10	**ODZYSKIWANIE i ODTWARZANIE SYSTEMU**	Wybrane	Wybrane	Wybrane

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CP-10 (2)	ODTWARZANIE TRANSAKCJI		Wybrane	Wybrane
CP-10 (4)	PRZYWRACANIE w OKREŚLONYM PRZEDZIALE CZASOWYM			Wybrane

Wytyczne uzupełniające dotyczące ICS: Rekonstrukcja systemu ICS obejmuje rozważenie, czy zmienne stanu systemu powinny zostać przywrócone do wartości początkowych lub wartości sprzed zakłócenia (np. czy zawory powinny zostać przywrócone do stanu pełnego otwarcia, pełnego zamknięcia lub ustawień sprzed zakłócenia). Przywrócenie zmiennych stanu systemu może zakłócić trwające procesy fizyczne (np. początkowo zamknięte zawory mogą mieć negatywny wpływ na chłodzenie systemu).

Zabezpieczenia rozszerzone:

(2, 4) Wytyczne uzupełniające dotyczące ICS: Brak.

CP-12 TRYB BEZPIECZNY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
CP-12	**TRYB BEZPIECZNY**	Dodane	Dodane	Dodane

Wytyczne uzupełniające dotyczące ICS: Zdefiniowane przez organizację warunki i odpowiadające im ograniczenia bezpiecznego trybu pracy mogą być różne dla różnych zabezpieczeń bazowych. Te same warunki mogą powodować różne reakcje w zależności od poziomu wpływu. Mogą to być warunki zewnętrzne w stosunku do ICS (np. przerwa w dostawie energii elektrycznej).Powiązane zabezpieczenia: SI-17.

Uzasadnienie zmiany zabezpieczenia bazowego: Zabezpieczenie to stanowi ramy służące organizacji do opracowania polityki i procedur postępowania w przypadku wystąpienia w środowisku działania okoliczności pozostających poza jej kontrolą. Tworzenie pisemnego zapisu procesu decyzyjnego dotyczącego wyboru zdarzeń i odpowiedniej reakcji stanowi część zarządzania ryzykiem w świetle zmieniającego się środowiska działania.

KATEGORIA IA - IDENTYFIKACJA i UWIERZYTELNIANIE

Uwagi dotyczące dostosowania do kategorii identyfikacji i uwierzytelniania

Przed wdrożeniem zabezpieczeń z kategorii IA należy rozważyć kompromisy między bezpieczeństwem, prywatnością, opóźnieniami, wydajnością i przepustowością. Na przykład, organizacja rozważa, czy opóźnienia wynikające z zastosowania mechanizmów uwierzytelniania wykorzystujących techniki kryptograficzne będą miały negatywny wpływ na wydajność operacyjną ICS.

W sytuacjach, gdy ICS nie może spełnić określonych wymagań identyfikacji i uwierzytelniania zawartych w danym zabezpieczeniu, organizacja stosuje zabezpieczenia kompensacyjne zgodnie z ogólnymi wytycznymi dotyczącymi procesu dostosowywania. Przykłady zabezpieczeń kompensacyjnych są podane przy każdym z zabezpieczeń, stosownie do potrzeb.

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

IA-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IA-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta uwzględnia specyficzne właściwości i wymagania ICS oraz relacje z systemami innymi niż ICS.

IA-2 IDENTYFIKACJA i UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI)

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IA-2	**IDENTYFIKACJA i UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI)**	Wybrane	Wybrane	Wybrane
IA-2 (1)	UWIERZYTELNIANIE WIELOSKŁADNIKOWE DOSTĘPU DO KONT UPRZYWILEJOWANYCH	Wybrane	Wybrane	Wybrane
IA-2 (2)	UWIERZYTELNIANIE WIELOSKŁADNIKOWE DOSTĘPU DO KONT NIEUPRZYWILEJOWANYCH		Wybrane	Wybrane
IA-2 (3)	DOSTĘP LOKALNY DO KONT UPRZYWILEJOWANYCH		Wybrane	Wybrane
IA-2 (4)	DOSTĘP LOKALNY DO KONT NIEUPRZYWILEJOWANYCH			Wybrane
IA-2 (8)	DOSTĘP DO KONT – ODPORNOŚĆ NA POWTARZANIE		Wybrane	Wybrane
IA-2 (9)	DOSTĘP SIECIOWY DO KONT NIEUPRZYWILEJOWANYCH - ODPORNOŚĆ NA POWTARZANIE			Wybrane
IA-2 (11)	ZDALNY DOSTĘP - ODSEPAROWANE URZĄDZENIE		Wybrane	Wybrane
IA-2 (12)	AUTORYZACJA DANYCH DOSTĘPOWYCH	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: w przypadku, gdy użytkownicy funkcjonują jako jedna grupa (np. operatorzy sterowni), ich identyfikacja i uwierzytelnianie mogą

być oparte na rolach, grupach lub urządzeniach. W przypadku niektórych systemów ICS możliwość natychmiastowej interakcji z operatorem ma krytyczne znaczenie. Wymogi dotyczące identyfikacji lub uwierzytelniania nie mają wpływu na prowadzenie działań w sytuacjach awaryjnych w systemach ICS. Dostęp do tych systemów może być ograniczony przez odpowiednie fizyczne środki bezpieczeństwa. Przykładowe zabezpieczenia kompensacyjne obejmują wzmocnienie bezpieczeństwa fizycznego, bezpieczeństwa osobowego oraz środków audytu. Na przykład, do ustanowienia zdalnego dostępu może być wymagane manualne uwierzytelnienie głosowe zdalnego personelu i lokalne, osobiste czynności. Patrz: wytyczne uzupełniające zabezpieczenia AC-17 dotyczące ICS. Dostęp użytkowników lokalnych do komponentów ICS jest możliwy tylko wtedy, gdy jest niezbędny, zatwierdzony i uwierzytelniony.

Zabezpieczenia rozszerzone:

(1, 2, 3, 4) Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują wdrożenie środków bezpieczeństwa fizycznego.

(8, 9) Wytyczne uzupełniające dotyczące systemów ICS: Przykładowe zabezpieczenia kompensacyjne obejmują zapewnienie odporności na powtórzenia w systemie zewnętrznym.

(11) Wytyczne uzupełniające dotyczące systemów ICS: Brak.

(12) Wytyczne uzupełniające dotyczące systemów ICS: Przykładowe zabezpieczenia kompensacyjne obejmują wdrożenie obsługi identyfikacji użytkownika poza systemem ICS.

IA-3 IDENTYFIKACJA i UWIERZYTELNIANIE URZĄDZENIA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IA-3	**IDENTYFIKACJA i UWIERZYTELNIANIE URZĄDZENIA**	Dodane	Wybrane	Wybrane

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IA-3 (1)	DWUKIERUNKOWE UWIERZYTELNIANIE KRYPTOGRAFICZNE		Dodane	Dodane
IA-3 (4)			Dodane	Dodane

Wytyczne uzupełniające dotyczące ICS: Organizacja może zezwolić na podłączenie do swojego ICS urządzeń znanych również jako jednostki nieosobowe (*ang. non-person entities - NPE*)[79], należących do innej organizacji i przez nią autoryzowanych (np. partnerów biznesowych). W szczególności, gdy są to urządzenia nielokalne, ich identyfikacja i uwierzytelnianie mogą mieć kluczowe znaczenie. Organizacje mogą przeprowadzić analizę ryzyka i wpływu w celu określenia wymaganej siły mechanizmów uwierzytelniania. Przykładowe zabezpieczenia kompensacyjne urządzeń i protokołów, które nie zapewniają uwierzytelniania w przypadku zdalnych połączeń sieciowych, obejmują wdrożenie środków bezpieczeństwa fizycznego.

Zabezpieczenia rozszerzone:

(1, 4) Wytyczne uzupełniające dotyczące ICS: w zarządzaniu konfiguracją urządzeń do identyfikacji i uwierzytelniania NPE zwykle bierze udział człowiek, który zastępuje NPE lub jest jego przedstawicielem. Urządzenia otrzymują swoje poświadczenia identyfikacji i uwierzytelniania na podstawie oświadczeń dokonanych przez surogata[80]. Surogat reaguje także na zdarzenia i anomalie (np. wygaśnięcie danych uwierzytelniających). Dane uwierzytelniające podmiotów oprogramowania (np. autonomicznych procesów niezwiązanych z konkretną osobą) oparte na właściwościach tego oprogramowania (np. podpisach cyfrowych) mogą się zmieniać za

[79] NPE - Podmiot i tożsamości cyfrowej, który działa w cyberprzestrzeni, ale nie jest człowiekiem. Mogą to być organizacje, urządzenia sprzętowe, aplikacje i artefakty informacyjne.

[80] Zastępuje kogoś innego lub jest używany zamiast czegoś innego.

każdym razem, gdy oprogramowanie jest zmieniane lub poprawiane. Sprzęt specjalnego przeznaczenia (np. niestandardowe układy scalone i płytki obwodów drukowanych) może wykazywać podobne zależności. Definicja konfiguracji parametrów może być różna dla poszczególnych poziomów wpływu.

Uzasadnienie zmiany zabezpieczenia bazowego (1, 4): Systemy ICS mogą wymieniać informacje z szeregiem systemów i urządzeń zewnętrznych. Identyfikacja i uwierzytelnianie urządzeń wprowadzają okoliczności, które nie występują w przypadku działań podejmowanych przez ludzi. Te zabezpieczenia obejmują przypisywanie, które umożliwia organizacji kategoryzowanie urządzeń według typów, modeli lub innych cech grupowych. Przypisywanie umożliwia również organizacjom wybór odpowiednich mechanizmów kontroli dla połączeń lokalnych, zdalnych i sieciowych.

IA-4 ZARZĄDZANIE IDENTYFIKATOREM

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IA-4	**ZARZĄDZANIE IDENTYFIKATOREM**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

IA-5 ZARZĄDZANIE METODAMI UWIERZYTELNIANIA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IA-5	**ZARZĄDZANIE METODAMI UWIERZYTELNIANIA**	Wybrane	Wybrane	Wybrane
IA-5 (1)	UWIERZYTELNIANIE OPARTE I HASŁA	Wybrane	Wybrane	Wybrane

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IA-5 (2)	UWIERZYTELNIANIE OPARTE I INFRASTRUKTURĘ KLUCZA PUBLICZNEGO		Wybrane	Wybrane
IA-5 (3)	REJESTRACJA OSOBISTA LUB PRZEZ ZAUFANĄ TRZECIĄ STRONĘ		Wybrane	Wybrane
IA-5 (11)	UWIERZYTELNIANIE PRZY UŻYCIU TOKENA	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują fizyczną kontrolę dostępu, hermetyzację ICS w celu zapewnienia uwierzytelniania zewnętrznego w stosunku do ICS.

Zabezpieczenia rozszerzone:

(1, 2, 3, 11) Wytyczne uzupełniające dotyczące ICS: Brak.

IA-6 OCHRONA PROCESU UWIERZYTELNIANIA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IA-6	**OCHRONA PROCESU UWIERZYTELNIANIA**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Niniejsze zabezpieczenie wymaga zastosowania interfejsu wizualnego, który w trakcie procesu uwierzytelniania przekazuje informacje zwrotne dotyczące uwierzytelniania. Jeśli uwierzytelnianie ICS wykorzystuje interfejs, który nie obsługuje wizualnego sprzężenia zwrotnego (np. uwierzytelnianie oparte na protokołach), zabezpieczenie to może zostać dostosowana do potrzeb.

IA-7 MODUŁU KRYPTOGRAFICZNEGO

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IA-7	**UWIERZYTELNIANIE MODUŁU KRYPTOGRAFICZNEGO**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

IA-8 IDENTYFIKACJA i UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IA-8	**IDENTYFIKACJA i UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)**	Wybrane	Wybrane	Wybrane
IA-8 (1)	AKCEPTACJA POŚWIADCZEŃ TOŻSAMOŚCI WYDANYCH PRZEZ INNE ORGANIZACJE	Wybrane	Wybrane	Wybrane
IA-8 (2)	AKCEPTACJA POŚWIADCZEŃ STRON TRZECICH[81]	Wybrane	Wybrane	Wybrane
IA-8 (3)	WYKORZYSTANIE CERTYFIKOWANYCH PRODUKTÓW	Wybrane	Wybrane	Wybrane

[81] Dotyczy rynku USA.

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IA-8 (4)	WYKORZYSTANIE PROFILI WYDAWANYCH PRZEZ STOSOWNE INSTYTUCJE	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Do użytkowników spoza organizacji mają zastosowanie wytyczne uzupełniające do ICS dotyczące zabezpieczenia IA-2, *Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni).*

Zabezpieczenia rozszerzone:

(1, 2, 3, 4) Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują wdrożenie wsparcia zewnętrznego systemu ICS oraz uwierzytelnianie wieloskładnikowe.

KATEGORIA IR - REAGOWANIE NA INCYDENTY

Uwagi dotyczące dostosowania do kategorii reagowania na incydenty

Zautomatyzowane mechanizmy wykorzystywane do śledzenia incydentów bezpieczeństwa zwykle nie są elementami ICS ani nie są z nim połączone.

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

IR-1 POLITYKA I PROCEDURY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IR-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta uwzględnia specyficzne właściwości i wymagania ICS oraz relacje z systemami innymi niż ICS.

IR-2 SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IR-2	**SZKOLENIE w ZAKRESIE REAGOWANIA NA INCYDENTY**	Wybrane	Wybrane	Wybrane
IR-2 (1)	WYDARZENIA SYMULOWANE			Wybrane

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IR-2 (2)	ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

IR-3 TESTOWANIE REAGOWANIA NA INCYDENTY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IR-3	**TESTOWANIE REAGOWANIA NA INCYDENTY**		Wybrane	Wybrane
IR-3 (2)	KOORDYNACJA z POWIĄZANYMI PLANAMI		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

IR-4 OBSŁUGA INCYDENTÓW

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IR-4	**OBSŁUGA INCYDENTÓW**	Wybrane	Wybrane	Wybrane
IR-4 (1)	AUTOMATYCZNE PROCESY OBSŁUGI ZDARZEŃ		Wybrane	Wybrane
IR-4 (4)	KORELACJA INFORMACJI			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

IR-5 MONITOROWANIE INCYDENTÓW

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IR-5	**MONITOROWANIE INCYDENTÓW**	Wybrane	Wybrane	Wybrane
IR-5 (1)	AUTOMATYCZNE ŚLEDZENIE, ZBIERANIE DANYCH I ANALIZA			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

IR-6 ZGŁASZANIE INCYDENTÓW

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IR-6	**ZGŁASZANIE INCYDENTÓW**	Wybrane	Wybrane	Wybrane
IR-6 (1)	ZGŁASZANIE AUTOMATYCZNE		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Organizacja powinna zgłaszać incydenty w odpowiednim czasie. Organizacja powinna współpracować i na bieżąco dzielić się informacjami i potencjalnych incydentach[82].

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Zautomatyzowane mechanizmy wykorzystywane do wspierania procesu zgłaszania incydentów nie muszą być częścią ICS, ani nie są z nim połączone.

[82] Patrz: NSC 800-61.

IR-7 WSPARCIE REAGOWANIA NA INCYDENTY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IR-7	**WSPARCIE REAGOWANIA NA INCYDENTY**	Wybrane	Wybrane	Wybrane
IR-7 (1)	AUTOMATYCZNE WSPARCIE DOSTĘPNOŚCI INFORMACJI / OBSŁUGI		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

IR-8 PLAN REAGOWANIA NA INCYDENTY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
IR-8	**PLAN REAGOWANIA NA INCYDENTY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

KATEGORIA MA – UTRZYMANIE i WSPARCIE

Uwagi dotyczące dostosowania do kategorii utrzymania i wsparcia

Zautomatyzowane mechanizmy wykorzystywane do planowania, przeprowadzania i dokumentowania procesów utrzymania i wsparcia, zazwyczaj nie stanowią części ICS i nie są z nim połączone.

W sytuacjach, gdy system ICS nie może spełnić określonych wymagań zabezpieczeń w zakresie utrzymania, organizacja stosuje zabezpieczenia kompensacyjne zgodnie z ogólnymi wskazówkami dotyczącymi procesu dostosowania. Przykłady zabezpieczeń kompensacyjnych są podane przy każdym zabezpieczeniu, stosownie do potrzeb.

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

MA-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
MA-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta uwzględnia specyficzne właściwości i wymagania ICS oraz relacje z systemami innymi niż ICS.

MA-2 NADZÓR NAD UTRZYMANIEM

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
MA-2	**NADZÓR NAD UTRZYMANIEM**	Wybrane	Wybrane	Wybrane
MA-2 (2)	AUTOMATYCZNE DZIAŁANIA KONSERWACYJNE			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

MA-3 NARZĘDZIA UTRZYMANIOWE

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
MA-3	**NARZĘDZIA UTRZYMANIOWE**		Wybrane	Wybrane
MA-3 (1)	SPRAWDZANIE NARZĘDZI		Wybrane	Wybrane
MA-3 (2)	SPRAWDZANIE NOŚNIKÓW DANYCH		Wybrane	Wybrane
MA-3 (3)	ZAPOBIEGANIE NIEAUTORYZOWANEMU USUWANIU			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

MA-4 UTRZYMANIE ZDALNE

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
MA-4	**UTRZYMANIE ZDALNE**	Wybrane	Wybrane	Wybrane
MA-4 (2)	AUDYT I PRZEGLĄD		Wybrane	Wybrane
MA-4 (3)	PORÓWNYWALNE POZIOMY BEZPIECZEŃSTWA / SANITYZACJA			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

Zabezpieczenia rozszerzone:

(2) Wytyczne uzupełniające dotyczące ICS: Brak.

(3) Wytyczne uzupełniające dotyczące ICS: w sytuacjach kryzysowych lub awaryjnych, organizacja może potrzebować natychmiastowego dostępu do nielokalnych usług utrzymaniowych i diagnostycznych w celu przywrócenia istotnych operacji lub usług ICS. Przykładowe zabezpieczenia kompensacyjne obejmują ograniczanie zakresu usług utrzymaniowych i diagnostycznych do minimum niezbędnych działań, wnikliwe monitorowanie i audytowanie nielokalnych działań utrzymaniowych i diagnostycznych.

MA-5 PERSONEL UTRZYMANIOWY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
MA-5	**PERSONEL UTRZYMANIOWY**	Wybrane	Wybrane	Wybrane
MA-5 (1)	OSOBY NIEPOSIADAJĄCE STOSOWNYCH PRAW DOSTĘPU			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

MA-6 TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
MA-6	**TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

KATEGORIA MP – OCHRONA NOŚNIKÓW DANYCH

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

MP-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
MP-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta uwzględnia specyficzne właściwości i wymagania ICS oraz relacje z systemami innymi niż ICS.

MP-2 DOSTĘP DO NOŚNIKÓW DANYCH

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
MP-2	**DOSTĘP DO NOŚNIKÓW DANYCH**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

MP-3 OZNAKOWANIE NOŚNIKÓW DANYCH

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
MP-3	**OZNAKOWANIE NOŚNIKÓW DANYCH**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

MP-4 PRZECHOWYWANIE NOŚNIKÓW DANYCH

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
MP-4	**PRZECHOWYWANIE NOŚNIKÓW DANYCH**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

MP-5 TRANSPORT NOŚNIKÓW DANYCH

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
MP-5	**TRANSPORT NOŚNIKÓW DANYCH**		Wybrane	Wybrane
MP-5 (4)	OCHRONA KRYPTOGRAFICZNA		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

MP-6 SANITYZACJA NOŚNIKÓW DANYCH

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
MP-6	**SANITYZACJA NOŚNIKÓW DANYCH**	Wybrane	Wybrane	Wybrane
MP-6 (1)	PRZEGLĄD / ZATWIERDZANIE / ŚLEDZENIE / DOKUMENTOWANIE / WERYFIKACJA			Wybrane
MP-6 (2)	TESTOWANIE SPRZĘTU			Wybrane
MP-6 (3)	TECHNIKI NIEDESTRUKCYJNE			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

MP-7 UŻYWANIE NOŚNIKÓW DANYCH

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
MP-7	**UŻYWANIE NOŚNIKÓW DANYCH**	Wybrane	Wybrane	Wybrane
MP-7 (1)			Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

KATEGORIA PE – OCHRONA FIZYCZNA i ŚRODOWISKOWA

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

PE-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta uwzględnia w szczególności wyjątkowe właściwości i wymagania ICS oraz relacje z systemami innymi niż ICS. Komponenty ICS mogą być rozmieszczone w obrębie dużego obiektu lub obszaru geograficznego i mogą stanowić punkt wejścia do całej sieci organizacyjnej ICS. Zastosowanie mogą mieć również zabezpieczenia regulacyjne.

PE-2 ZEZWOLENIA NA DOSTĘP FIZYCZNY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-2	**ZEZWOLENIA NA DOSTĘP FIZYCZNY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

PE-3 KONTROLA DOSTĘPU FIZYCZNEGO

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-3	**KONTROLA DOSTĘPU FIZYCZNEGO**	Wybrane	Wybrane	Wybrane
PE-3 (1)	DOSTĘP DO SYSTEMU			Wybrane

Wytyczne uzupełniające dotyczące ICS: Organizacja rozważa współzależności bezpieczeństwa i ochrony ICS. Organizacja rozważa wymagania dostępu w sytuacjach awaryjnych. Podczas zdarzenia związanego z sytuacją awaryjną, organizacja może ograniczyć dostęp do obiektów i aktywów ICS tylko dla upoważnionych osób. ICS są często zbudowane z urządzeń, które albo nie mają, albo nie mogą korzystać z kompleksowych możliwości kontroli dostępu ze względu na czasowe ograniczenia bezpieczeństwa. Fizyczne kontrole dostępu i środki „obrona w głąb" są stosowane przez organizację, gdy jest to konieczne i możliwe, w celu uzupełnienia bezpieczeństwa ICS, gdy mechanizmy elektroniczne nie są w stanie spełnić wymagań planu bezpieczeństwa organizacji. Węzły główne, szafy dystrybucyjne oraz pomieszczenia techniczne/elektryczne powinny być zamknięte i wymagać fizycznej lub elektronicznej kontroli dostępu oraz zawierać czujniki wykrywające włamania.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Brak.

PE-4 KONTROLA DOSTĘPU DO MEDIUM TRANSMISYJNEGO

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-4	**KONTROLA DOSTĘPU DO MEDIUM TRANSMISYJNEGO**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

PE-5 KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-5	**KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

PE-6 MONITOROWANIE DOSTĘPU FIZYCZNEGO

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-6	**MONITOROWANIE DOSTĘPU FIZYCZNEGO**	Wybrane	Wybrane	Wybrane
PE-6 (1)	ALARMY WŁAMANIOWE I URZĄDZENIA NADZORUJĄCE		Wybrane	Wybrane
PE-6 (4)	MONITOROWANIE DOSTĘPU FIZYCZNEGO DO SYSTEMÓW		Dodane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Fizyczne zabezpieczenia dostępu oraz środki "obrony w głąb" są stosowane przez organizację jako zabezpieczenia kompensacyjne, i ile jest to konieczne i możliwe, w celu uzupełnienia zabezpieczeń ICS w sytuacji, gdy mechanizmy elektroniczne nie są w stanie monitorować, wykrywać i ostrzegać i uzyskaniu dostępu do ICS. Tego rodzaju zabezpieczenia kompensacyjne stanowią uzupełnienie środków bezpieczeństwa PE-6 (np. poprzez zastosowanie zabezpieczenia rozszerzonego PE-3(4), Zamykane obudowy i/lub zabezpieczenia rozszerzonego PE-3(5), Ochrona przed manipulacją).

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Brak.

(4) Wytyczne uzupełniające dotyczące ICS: Lokalizacje komponentów ICS (np. urządzeń terenowych, zdalnych jednostek końcowych) mogą obejmować różne lokalizacje zdalne (np. podstacje, przepompownie).

Uzasadnienie zmiany zabezpieczenia bazowego (4): Wiele komponentów systemu ICS jest zlokalizowanych w odległych geograficznie i rozproszonych miejscach, co powoduje, że możliwości monitorowania wszystkich komponentów systemu ICS są ograniczone. Niektóre elementy mogą być zainstalowane na sufitach, podłogach lub w szafach dystrybucyjnych i wyposażone w minimalne zabezpieczenia fizyczne pozwalające na wykrycie, opóźnienie lub uniemożliwienie dostępu do urządzeń a także pozbawione możliwości nadzoru elektronicznego nadzoru elektronicznego lub reagowania przez służby ochrony.

PE-8 REJESTRACJA DOSTĘPU GOŚCI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-8	**REJESTRACJA DOSTĘPU GOŚCI**	Wybrane	Wybrane	Wybrane
PE-8 (1)	AUTOMATYCZNA REJESTRACJA / PRZEGLĄD			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

PE-9 WYPOSAŻENIE ENERGETYCZNE i OKABLOWANIE

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-9	**WYPOSAŻENIE ENERGETYCZNE i OKABLOWANIE**	Wybrane	Wybrane	
PE-9 (1)	REDUNDANCJA OKABLOWANIA	Dodane	Dodane	

Wytyczne uzupełniające dotyczące ICS: Brak.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Brak.

Uzasadnienie zmiany zabezpieczenia bazowego (1): Zapewnienie ciągłości działania systemu ICS wymaga posiadania redundantnego okablowania zasilającego.

PE-10 WYŁĄCZENIE AWARYJNE

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-10	**WYŁĄCZENIE AWARYJNE**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Wyłączenie zasilania niektórych ICS może być niemożliwe lub niewskazane. Przykładowe zabezpieczenia kompensacyjne obejmują uszkodzenia w znanym stanie i procedury awaryjne.

PE-11 ZASILANIE AWARYJNE

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-11	**ZASILANIE AWARYJNE**	Dodane	Wybrane	Wybrane
PE-11 (1)	ALTERNATYWNE ZASILANIE - MINIMALNA ZDOLNOŚĆ OPERACYJNA	Dodane	Dodane	Wybrane
PE-11 (2)	ALTERNATYWNE SAMOOBSŁUGOWE ŹRÓDŁO ZASILANIA			Dodane

Wytyczne uzupełniające dotyczące ICS: Systemy wytwarzania, przesyłu i dystrybucji energii elektrycznej w sytuacjach awaryjnych to kategoria systemów ICS, od których wymaga się spełnienia niezwykle wysokich parametrów eksploatacyjnych. Systemy te podlegają międzynarodowym, krajowym i lokalnym zasadom budowlanym, muszą być poddawane ciągłym testom, a także naprawiane i przywracane do działania w możliwie najkrótszym czasie. Zazwyczaj zasilanie awaryjne jest dostarczane przez agregaty prądotwórcze do zasilania krótko- i średnioterminowego (zazwyczaj dla systemów przeciwpożarowych i ochrony życia, niektórych urządzeń informacyjnych i transportu ewakuacyjnego) oraz zestawy baterii UPS umieszczone w szafach dystrybucyjnych i obszarach roboczych, w celu zapewnienia określonego poziomu ciągłości działania i umożliwienia uporządkowanego wyłączenia mniej istotnych systemów informacyjnych i systemów znajdujących się w obiekcie. Tradycyjne systemy zasilania awaryjnego pozostają w trybie off-line do momentu utraty zasilania i są zazwyczaj podłączone do oddzielnej sieci i systemu kontrolnego właściwego dla obsługiwanego obiektu. Nowe metody wytwarzania i magazynowania energii (np. fotowoltaika, energia geotermalna, elektrownie wiatrowe, mikrosieci elektroenergetyczne, kogeneracja rozproszona), które umożliwiają podłączenie w czasie rzeczywistym do lokalnych sieci energetycznych lub do sieci połączonych z wieloma obiektami, powinny być dokładnie przeanalizowane, aby zapewnić, że dostarczana moc będzie

wystarczająca do pokrycia obciążenia i zapewnienia odpowiedniej jakości energii bez zakłócania istotnych funkcji realizowanych przez dany obiekt.

Zabezpieczenia rozszerzone: (1) Wytyczne uzupełniające dotyczące ICS: Brak.

Uzasadnienie zmiany zabezpieczenia bazowego: System ICS może wspierać działania i znaczeniu krytycznym, które będą niezbędne do zapewnienia bezpieczeństwa i niezawodności nawet w przypadku braku bezprzerwowego zasilania z sieci publicznej.

PE-12 OŚWIETLENIE AWARYJNE

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-12	**OŚWIETLENIE AWARYJNE**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

PE-13 OCHRONA PRZECIWPOŻAROWA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-13	**OCHRONA PRZECIWPOŻAROWA**	Wybrane	Wybrane	Wybrane
PE-13 (1)	SYSTEMY DETEKCJI - AUTOMATYCZNA AKTYWACJA I POWIADAMIANIE			Wybrane
PE-13 (2)	SYSTEMY GASZĄCE - AUTOMATYCZNA AKTYWACJA I POWIADOMIENIE			Wybrane
PE-13 (3)	AUTOMATYCZNE GASZENIE POŻARU		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Mechanizmy gaszenia pożarów powinny uwzględniać środowisko ICS (np. systemy zraszaczy wodnych mogą stanowić zagrożenie w określonych środowiskach).

Zabezpieczenia rozszerzone:

(1, 2, 3) Wytyczne uzupełniające dotyczące ICS: Brak.

PE-14 ZABEZPIECZENIA ŚRODOWISKOWE

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-14	**ZABEZPIECZENIA ŚRODOWISKOWE**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Regulatory temperatury i wilgotności są zazwyczaj składnikami innych systemów ICS, takich jak HVAC[83], systemy technologiczne lub oświetleniowe. Mogą też stanowić samodzielny i unikalny system ICS. Systemy ICS mogą pracować w ekstremalnych środowiskach i w lokalizacjach zarówno wewnętrznych, jak i zewnętrznych. Parametry eksploatacyjne konkretnego systemu ICS zależą od temperatury i wilgotności oraz parametrów roboczych. Ponieważ systemy ICS i IS stają się wzajemnie połączone, a sieć zapewnia łączność w przestrzeni hybrydowej, obwody zasilania, szafy rozdzielcze, routery i przełączniki obsługujące systemy ppoż. i ochrony życia muszą być eksploatowane w odpowiedniej temperaturze i wilgotności.

[83] NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.*

PE-15 OCHRONA PRZED ZALANIEM

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-15	**OCHRONA PRZED ZALANIEM**	Wybrane	Wybrane	Wybrane
PE-15 (1)	AUTOMATYCZNE WYKRYWANIE			Wybrane

Wytyczne uzupełniające dotyczące ICS: Ochrona przed szkodami wyrządzonymi przez wodę oraz stosowanie zaworów odcinających i izolacyjnych jest zarówno działaniem i znaczeniu proceduralnym, jak i specyficznym sposobem ochrony ICS. Systemy ICS stosowane w przemyśle wytwórczym, energetyce wodnej, transporcie/nawigacji, gospodarce wodnokanalizacyjnej opierają się na przepływie wody i są specjalnie zaprojektowane do sterowania ilością/przepływem i ciśnieniem wody. Ponieważ ICS i IS zaczynają być ze sobą powiązane, a sieć zapewnia komunikację w całej przestrzeni hybrydowej, obwody zasilania, szafy rozdzielcze, routery i przełączniki obsługujące systemy ochrony przeciwpożarowej i ochrony życia powinny gwarantować, że woda nie spowoduje wyłączenia systemu (np. pożar, który aktywuje system tryskaczy, nie spowoduje rozpylenia wody na serwery sterujące systemem przeciwpożarowym, router, przełączniki i nie wyłączy sygnalizatorów, systemów ewakuacyjnych, oświetlenia awaryjnego i systemów gaszenia).

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Brak.

PE-16 DOSTAWA i USUWANIE

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-16	**DOSTAWA i USUWANIE**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

PE-17 ZAPASOWE MIEJSCE PRACY

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-17	**ZAPASOWE MIEJSCE PRACY**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

PE-18 LOKALIZACJA KOMPONENTÓW SYSTEMU

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PE-18	**LOKALIZACJA KOMPONENTÓW SYSTEMU**			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

KATEGORIA PL – PLANOWANIE

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

PL-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PL-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta uwzględnia w szczególności wyjątkowe właściwości i wymagania ICS oraz relacje z systemami innymi niż ICS.

PL-2 PLANY BEZPIECZEŃSTWA SYSTEMU i OCHRONY PRYWATNOŚCI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PL-2	**PLANY BEZPIECZEŃSTWA SYSTEMU i OCHRONY PRYWATNOŚCI**	Wybrane	Wybrane	Wybrane
PL-2 (3)	PLANOWANIE / KOORDYNACJA z INNYMI PODMIOTAMI ORGANIZACYJNYMI	Dodane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

Zabezpieczenia rozszerzone:

(3) Wytyczne uzupełniające dotyczące ICS: Brak.

Uzasadnienie zmiany zabezpieczenia bazowego: w przypadku systemów silnie ze sobą powiązanych niezbędne jest prowadzenie skoordynowanego planowania. System i małym wpływie może mieć negatywny wpływ na system i większym wpływie.

PL-4 ZASADY POSTĘPOWANIA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PL-4	**ZASADY POSTĘPOWANIA**	Wybrane	Wybrane	Wybrane
PL-4 (1)	MEDIA SPOŁECZNOŚCIOWE I OGRANICZENIA KORZYSTANIA ZE STRON / APLIKACJI ZEWNĘTRZNYCH		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

PL-7 KONCEPCJA BEZPIECZEŃSTWA DZIAŁAŃ OPERACYJNYCH

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PL-7	**KONCEPCJA BEZPIECZEŃSTWA DZIAŁAŃ OPERACYJNYCH**		Dodane	Dodane

Wytyczne uzupełniające dotyczące ICS: Brak.

Uzasadnienie zmiany zabezpieczenia bazowego: Systemy ICS są systemami złożonymi. Organizacje zazwyczaj stosują CONOPS, co pozwala zdefiniować system i udostępnić te informacje personelowi obsługującemu ten system i inne systemy, z którymi on współpracuje. CONOPS często pomaga określić wymagania dotyczące ochrony informacji.

PL-8 ARCHITEKTURY BEZPIECZEŃSTWA i OCHRONY PRYWATNOŚCI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PL-8	**ARCHITEKTURY BEZPIECZEŃSTWA i OCHRONY PRYWATNOŚCI**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

KATEGORIA PM – PROGRAMY ZARZĄDZANIA

Uwagi dotyczące dostosowania do kategorii programów zarządzania

Programy zarządzania bezpieczeństwa informacji są wprowadzane w całej organizacji i wspierają program bezpieczeństwa informacji. Nie są one związane z zabezpieczeniami bazowymi i są niezależne od poziomu wpływu na system.

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

PM-1 PLAN PROGRAMU BEZPIECZEŃSTWA INFORMACJI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-1	**PLAN PROGRAMU BEZPIECZEŃSTWA INFORMACJI**

Wytyczne uzupełniające dotyczące ICS: Plan programu bezpieczeństwa informacji dotyczy głównie unikatowych właściwości i wymagań ICS, relacji z systemami innymi niż systemy ICS oraz z innymi programami związanymi z charakterystyką operacyjną ICS (np. ochrona, efektywność, niezawodność, odporność).

PM-2 ROLE KIEROWNICZE PROGRAMU BEZPIECZEŃSTWA INFORMACJI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-2	**ROLE KIEROWNICZE PROGRAMU BEZPIECZEŃSTWA INFORMACJI**

Wytyczne uzupełniające dotyczące ICS: Brak.

PM-3 ZASOBY w ZAKRESIE BEZPIECZEŃSTWA INFORMACJI i OCHRONY PRYWATNOŚCI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-3	**ZASOBY w ZAKRESIE BEZPIECZEŃSTWA INFORMACJI i OCHRONY PRYWATNOŚCI**

Wytyczne uzupełniające dotyczące ICS: Planowanie budżetowe i decyzje inwestycyjne dotyczą wszystkich istotnych technologii i wszystkich faz cyklu życia i muszą być podejmowane przez ekspertów w dziedzinie ICS oraz ekspertów w innych dziedzinach (np. W dziedzinie bezpieczeństwa informacji). Tworzenie interdyscyplinarnych roboczych zespołów doradczych w zakresie planowania finansowego i decyzji inwestycyjnych może pomóc w osiągnięciu kompromisu i równowagi między kolidującymi interesami, celami i obowiązkami, takimi jak zdolność, adaptacyjność, odporność, bezpieczeństwo, ochrona, użyteczność i efektywność.

PM-4 PLAN DZIAŁANIA i ETAPY WPROWADZANIA ZABEZPIECZEŃ

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-4	**PLAN DZIAŁANIA i ETAPY WPROWADZANIA ZABEZPIECZEŃ**

Wytyczne uzupełniające dotyczące ICS: Plan działania i etapy wprowadzania zabezpieczeń obejmują zarówno składniki rachunkowe, jak i materialne ICS. Zapisy zaobserwowanych niedociągnięć i odpowiednich działań zaradczych mogą być przechowywane w jednym dokumencie lub w wielu skoordynowanych dokumentach (np. przyszłych planach inżynieryjnych).

PM-5 INWENTARYZACJA SYSTEMU

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-5	**INWENTARYZACJA SYSTEMU**

Wytyczne uzupełniające dotyczące ICS: Brak.

PM-6 MIARY SKUTECZNOŚCI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-6	**MIARY SKUTECZNOŚCI**

Wytyczne uzupełniające dotyczące ICS: Brak.

PM-7 STRUKTURA ORGANIZACYJNA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-7	**STRUKTURA ORGANIZACYJNA**

Wytyczne uzupełniające dotyczące ICS: Brak.

PM-8 PLAN INFRASTRUKTURY KRYTYCZNEJ

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-8	**PLAN INFRASTRUKTURY KRYTYCZNEJ**

Wytyczne uzupełniające dotyczące ICS: Brak.

PM-9 STRATEGIA ZARZĄDZANIA RYZYKIEM

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-9	**STRATEGIA ZARZĄDZANIA RYZYKIEM**

Wytyczne uzupełniające dotyczące ICS: Zarządzanie ryzykiem w odniesieniu do ICS jest uwzględniane wraz z innymi rodzajami ryzyka organizacyjnego wpływającego na powodzenie misji/biznesu w perspektywie całej organizacji. Ogólnoorganizacyjna strategia zarządzania ryzykiem uwzględnia wytyczne dotyczące poszczególnych sektorów, jeśli jest to uzasadnione.

PM-10 PROCES AUTORYZACJI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-10	**PROCES AUTORYZACJI**

Wytyczne uzupełniające dotyczące ICS: Procesy upoważnienia do działania systemu ICS obejmują różnorodne dziedziny, w których stosowane są obowiązujące procedury zatwierdzania i zarządzania ryzykiem (np. bezpieczeństwo fizyczne, ochrona). Zarządzanie ryzykiem w całej organizacji wymaga harmonizacji między tymi dziedzinami.

PM-11 DEFINICJA MISJI i PROCESU BIZNESOWEGO

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-11	**DEFINICJA MISJI i PROCESU BIZNESOWEGO**

Wytyczne uzupełniające dotyczące ICS: w ramach udoskonalania misji/procesów biznesowych konieczna jest ochrona aktywów fizycznych przed szkodami pochodzącymi z cyberprzestrzeni. Wymagania te wynikają z potrzeb misji/biznesu zdefiniowanych przez organizację, procesów misji/biznesu wybranych w celu zaspokojenia określonych potrzeb oraz strategii zarządzania ryzykiem organizacyjnym.

PM-12 ZAGROŻENIE WEWNĘTRZNE

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-12	**ZAGROŻENIA WEWNĘTRZNE**

Wytyczne uzupełniające dotyczące ICS: Brak.

PM-13 PERSONEL BEZPIECZEŃSTWA i OCHRONY i PRYWATNOŚCI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-13	**PERSONEL BEZPIECZEŃSTWA i OCHRONY i PRYWATNOŚCI**

Wytyczne uzupełniające dotyczące ICS: Wszystkie aspekty programów rozwoju i doskonalenia pracowników zajmujących się bezpieczeństwem informacji obejmują podnoszenie wiedzy i umiejętności w zakresie zarówno obliczeniowych, jak i fizycznych komponentów ICS.

PM-14 TESTOWANIE, SZKOLENIA i MONITOROWANIE

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-14	**TESTOWANIE, SZKOLENIA i MONITOROWANIE**

Wytyczne uzupełniające dotyczące ICS: Brak.

PM-15 GRUPY i STOWARZYSZENIA ZAJMUJĄCE SIĘ BEZPIECZEŃSTWEM I OCHRONĄ PRYWATNOŚCI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-15	**GRUPY i STOWARZYSZENIA ZAJMUJĄCE SIĘ BEZPIECZEŃSTWEM i OCHRONĄ PRYWATNOŚCI**

Wytyczne uzupełniające dotyczące ICS: Brak.

PM-16 OSTRZEGANIE O ZAGROŻENIACH

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego
PM-16	**OSTRZEGANIE O ZAGROŻENIACH**

Wytyczne uzupełniające dotyczące ICS: Organizacja powinna współpracować i na bieżąco dzielić się informacjami i potencjalnych incydentach[84]. Organizacje powinny rozważyć posiadanie zarówno możliwości dzielenia się informacjami jawnymi, jak i niejawnymi.

[84] Patrz: NSC 800-61.

KATEGORIA PS – BEZPIECZEŃSTWO OSOBOWE

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

PS-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PS-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta uwzględnia w szczególności wyjątkowe właściwości i wymagania ICS oraz relacje z systemami innymi niż ICS.

PS-2 OKREŚLANIE RYZYKA DLA STANOWISKA PRACY

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PS-2	**OKREŚLANIE RYZYKA DLA STANOWISKA PRACY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

PS-3 DOBÓR PERSONELU

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PS-3	**DOBÓR PERSONELU**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

PS-4 ZAKOŃCZENIE ZATRUDNIENIA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PS-4	**ZAKOŃCZENIE ZATRUDNIENIA**	Wybrane	Wybrane	Wybrane
PS-4 (2)				Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

PS-5 OBSADZENIE LUB PRZENIESIENIE STANOWISKA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PS-5	**OBSADZENIE LUB PRZENIESIENIE STANOWISKA**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

PS-6 UMOWY DOSTĘPU / WSPÓŁPRACY

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PS-6	**UMOWY DOSTĘPU / WSPÓŁPRACY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

PS-7 BEZPIECZEŃSTWO OSOBOWE STRON TRZECICH

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PS-7	**BEZPIECZEŃSTWO OSOBOWE STRON TRZECICH**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

PS-8 SANKCJE PERSONALNE

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
PS-8	**SANKCJE PERSONALNE**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

KATEGORIA RA – OCENA RYZYKA

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

RA-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
RA-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta uwzględnia w szczególności wyjątkowe właściwości i wymagania ICS oraz relacje z systemami innymi niż ICS.

RA-2 KATEGORYZACJA BEZPIECZEŃSTWA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
RA-2	**KATEGORYZACJA BEZPIECZEŃSTWA**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

RA-3 SZACOWANIE RYZYKA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
RA-3	**SZACOWANIE RYZYKA**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

RA-5 MONITOROWANIE i SKANOWANIE PODATNOŚCI

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
RA-5	**MONITOROWANIE i SKANOWANIE PODATNOŚCI**	Wybrane	Wybrane	Wybrane
RA-5 (1)	AKTUALIZACJA NARZĘDZI		Wybrane	Wybrane
RA-5 (2)	NADZOROWANIE WYKRYTYCH PODATNOŚCI		Wybrane	Wybrane
RA-5 (4)	WYKRYWANIE SKANOWANIA			Wybrane
RA-5 (5)	DOSTĘP UPRZYWILEJOWANY		Wybrane	Wybrane

Wytyczne uzupełniające dla systemów ICS: Aktywne skanowanie podatności wprowadzanych przez ruch sieciowy, jest przeprowadzane w systemach ICS z zachowaniem szczególnej ostrożności. Celem tego procesu jest uniknięcie negatywnego wpływu na funkcje ICS. Organizacja podejmuje decyzję i zastosowaniu aktywnego skanowania na podstawie szacowania ryzyka. Pasywne monitorowanie / podsłuchiwanie może być stosowane jako element zabezpieczenia kompensacyjnego. Przykładowe zabezpieczenia kompensacyjne obejmują zapewnienie replikowanego, zwirtualizowanego lub symulowanego systemu do przeprowadzenia skanowania.

Przed przeprowadzeniem skanowania może być konieczne wyłączenie produkcyjnego ICS. Jeśli ICS są wyłączone z eksploatacji w celu przeprowadzenia skanowania, skanowanie jest planowane w miarę możliwości podczas zamierzonych przestojów ICS. Jeśli narzędzia do skanowania podatności są używane w sieciach innych niż ICS, należy zachować szczególną ostrożność, aby nie przeskanowały one sieci ICS. Skanowanie sieci nie ma zastosowania do komunikacji nieadresowanej. W celu identyfikacji badanych obiektów, sprawdzanie podatności może być przeprowadzane z wykorzystaniem innych mechanizmów niż skanowanie. Przykładem zabezpieczenia kompensacyjnego jest analiza podatności oparta na hostach.

Zabezpieczenia rozszerzone:

(1, 2, 4, 5) Wytyczne uzupełniające dla systemów ICS: Brak.

KATEGORIA SA – NABYWANIE SYSTEMU i USŁUG

Uwagi dotyczące dostosowania do kategorii nabywania systemu i usług

W sytuacjach, gdy system ICS nie może spełnić określonych wymagań zabezpieczeń nabywania systemu i usług, organizacja stosuje zabezpieczenia kompensacyjne zgodnie z ogólnymi wskazówkami dotyczącymi dostosowania. Zależnie od potrzeb, przy każdym zabezpieczeniu przedstawione są przykłady zabezpieczeń kompensacyjnych.

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

SA-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SA-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta uwzględnia w szczególności wyjątkowe właściwości i wymagania ICS oraz relacje z systemami innymi niż ICS.

SA-2 PRZYDZIAŁ ZASOBÓW

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SA-2	**PRZYDZIAŁ ZASOBÓW**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SA-3 CYKL ŻYCIA SYSTEMU

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SA-3	**CYKL ŻYCIA SYSTEMU**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SA-4 PROCES NABYCIA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SA-4	**PROCES NABYCIA**	Wybrane	Wybrane	Wybrane
SA-4 (1)	WŁAŚCIWOŚCI FUNKCJONALNE ZABEZPIECZEŃ		Wybrane	Wybrane
SA-4 (2)	IMPLEMENTACJA ZABEZPIECZEŃ		Wybrane	Wybrane
SA-4 (9)	FUNKCJE, PORTY, PROTOKOŁY / USŁUGI		Wybrane	Wybrane
SA-4 (10)	WYKORZYSTANIE ZATWIERDZONYCH PRODUKTÓW	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Ponieważ bezpieczeństwo ICS historycznie koncentrowało się na ochronie fizycznej i izolacji, dostawcy i deweloperzy mogą być nieobeznani z zagadnieniami cyberbezpieczeństwa. Organizacje powinny przewidzieć potrzebę nawiązania współpracy z dostawcami ICS w celu zwiększenia świadomości potrzeb w zakresie cyberbezpieczeństwa. Projekt SCADA/Control Systems Procurement Project zawiera przykładowe języki składania zamówień w zakresie cyberbezpieczeństwa systemów ICS. Referencje:

https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf

Zabezpieczenia rozszerzone:

(1, 2, 9) Wytyczne uzupełniające dotyczące ICS: Deweloperzy mogą nie mieć dostępu do wymaganych informacji.

(10) Wytyczne uzupełniające dotyczące systemów ICS: Przykładowe zabezpieczenia kompensacyjne obejmują zastosowanie produktów firm zewnętrznych znajdujących się na liście zatwierdzonych produktów weryfikacji tożsamości osobistej (PIV) powiązanych z produktami ICS.

SA-5 DOKUMENTACJA SYSTEMU

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SA-5	**DOKUMENTACJA SYSTEMU**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SA-8 ZASADY INŻYNIERII BEZPIECZEŃSTWA i OCHRONY PRYWATNOŚCI

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SA-8	**ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SA-9 USŁUGI SYSTEMU ZEWNĘTRZNEGO

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SA-9	**USŁUGI SYSTEMU ZEWNĘTRZNEGO**	Wybrane	Wybrane	Wybrane
SA-9 (2)			Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SA-10 ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SA-10	**ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SA-11 TESTOWANIE i OCENA PRZEZ DEWELOPERA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SA-11	**TESTOWANIE i OCENA PRZEZ DEWELOPERA**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SA-12 BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SA-12	**BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW**			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SA-15 PROCES ROZWOJU, STANDARDY i NARZĘDZIA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SA-15	**PROCES ROZWOJU, STANDARDY i NARZĘDZIA**			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SA-16 SZKOLENIA PROWADZONE PRZEZ DEWELOPERA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SA-16	**SZKOLENIA PROWADZONE PRZEZ DEWELOPERA**			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SA-17 ARCHITEKTURA ORAZ PROJEKT BEZPIECZEŃSTWA i OCHRONY PRYWATNOŚCI DEWELOPERA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SA-17	**ARCHITEKTURA ORAZ PROJEKT BEZPIECZEŃSTWA i OCHRONY PRYWATNOŚCI DEWELOPERA**			Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

KATEGORIA SC – OCHRONA SYSTEMÓW i SIECI TELEKOMUNIKACYJNYCH

Uwagi dotyczące dostosowania do kategorii ochrony systemów i sieci telekomunikacyjnych

Zastosowanie kryptografii jest poprzedzone dokładnym rozważeniem potrzeb w zakresie bezpieczeństwa i potencjalnych konsekwencji dla wydajności systemu. Na przykład, organizacja rozważa, czy opóźnienia wynikające z zastosowania kryptografii będą miały negatywny wpływ na wydajność operacyjną ICS. Chociaż starsze urządzenia powszechnie występujące w systemach ICS często nie obsługują bezpośrednio funkcji kryptograficznych, można zastosować zabezpieczenia kompensacyjne (np. enkapsulacje[85]) w celu spełnienia założeń zabezpieczenia.

W sytuacjach, gdy ICS nie może spełnić określonych wymagań ochrony systemu i sieci telekomunikacyjnych, organizacja stosuje zabezpieczenia kompensacyjne zgodnie z ogólnymi wytycznymi dotyczącymi procesu dostosowania. Przykłady zabezpieczeń kompensacyjnych są podane przy każdym zabezpieczeniu, stosownie do potrzeb.

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

[85] Enkapsulacja, inaczej zwana hermetyzacją (kapsułkowaniem), jest jednym z głównych założeń programowania obiektowego. Polega na ukrywaniu metod i atrybutów dla klas zewnętrznych. Dostęp do nich możliwy jest tylko z wewnątrz klasy, do której należą, z klas zaprzyjaźnionych lub z klas dziedziczących.

SC-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta uwzględnia w szczególności wyjątkowe właściwości i wymagania ICS oraz relacje z systemami innymi niż ICS.

SC-2 ROZDZIELENIE FUNKCJONALNOŚCI SYSTEMU i UŻYTKOWNIKA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-2	**ROZDZIELENIE FUNKCJONALNOŚCI SYSTEMU i UŻYTKOWNIKA**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Systemy używane do zarządzania ICS powinny być oddzielone od operacyjnych komponentów ICS Przykładowe zabezpieczenia kompensacyjne obejmują wprowadzenie zaostrzonych środków audytu.

SC-3 IZOLACJA FUNKCJI BEZPIECZEŃSTWA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-3	**IZOLACJA FUNKCJI BEZPIECZEŃSTWA**			Wybrane

Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują wprowadzenie zaostrzonych środków audytu, ograniczenie łączności sieciowej, przydziały architektoniczne.

SC-4 INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-4	**INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują zaprojektowanie wykorzystania systemu ICS w taki sposób, aby zapobiec współdzieleniu zasobów systemowych.

SC-5 OCHRONA PRZED BLOKADĄ USŁUG (DoS)

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-5	**OCHRONA PRZED BLOKADĄ USŁUG (DoS)**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują zapewnienie, że utrata komunikacji spowoduje, że system ICS będzie działał w trybie nominalnym lub bezpiecznym. Polityka i procedury są określane na podstawie analizy ryzyka.

SC-7 OCHRONA POŁĄCZEŃ BRZEGOWYCH

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-7	**OCHRONA POŁĄCZEŃ BRZEGOWYCH**	Wybrane	Wybrane	Wybrane
SC-7 (3)	PUNKTY DOSTĘPOWE		Wybrane	Wybrane
SC-7 (4)	ZEWNĘTRZNE USŁUGI TELEKOMUNIKACYJNE		Wybrane	Wybrane
SC-7 (5)	ODRZUĆ DOMYŚLNIE / POZWÓL NA WYJĄTEK		Wybrane	Wybrane
SC-7 (7)	DZIELONE TUNELOWANIE URZĄDZEŃ ZDALNYCH			Wybrane
SC-7 (8)	RUCH TELEKOMUNIKACYJNY DO AUTORYZOWANYCH SERWERÓW PROXY		Dodane	Wybrane
SC-7 (18)	BŁĄD BEZPIECZEŃSTWA			Wybrane
SC-7 (21)	IZOLACJA KOMPONENTÓW SYSTEMU		Wybrane	

Wytyczne uzupełniające dotyczące ICS: Brak.

Zabezpieczenia rozszerzone:

(3, 4, 5, 7, 8, 21) Wytyczne uzupełniające dotyczące ICS: Brak.

(18) Wytyczne uzupełniające dotyczące ICS: Organizacja wybiera odpowiedni tryb awaryjny (np. zezwolenie lub zablokowanie całej komunikacji).

Uzasadnienie zmiany zabezpieczenia bazowego: Podczas tworzenia architektury i projektowania ICS organizacja określa właściwy tryb awaryjny, zgodny z funkcją pełnioną przez ICS i środowiskiem operacyjnym. Możliwość wyboru trybu awaryjnego

dla fizycznej części ICS odróżnia ICS od innych systemów informacyjnych. Wybór ten może mieć istotny wpływ na złagodzenie skutków awarii.

SC-8 POUFNOŚĆ i INTEGRALNOŚĆ TRANSMISJI

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-8	**POUFNOŚĆ i INTEGRALNOŚĆ TRANSMISJI**		Wybrane	Wybrane
SC-8 (1)	OCHRONA KRYPTOGRAFICZNA		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Organizacja bada wszystkie możliwe mechanizmy integralności kryptograficznej (np. podpis cyfrowy, funkcja hash). Każdy z mechanizmów ma inny wpływ na opóźnienia.

SC-10 ZAKOŃCZENIE POŁĄCZENIA SIECIOWEGO

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-10	**ZAKOŃCZENIE POŁĄCZENIA SIECIOWEGO**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują zapewnienie zwiększonych środków audytowych lub ograniczenie uprawnień w zakresie zdalnego dostępu dla kluczowego personelu.

SC-12 GENEROWANIE i ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-12	**GENEROWANIE i ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI**	Wybrane	Wybrane	Wybrane
SC-12 (1)				Wybrane

Wytyczne uzupełniające dotyczące ICS: Zarządzania kluczami kryptograficznymi w ICS ma na celu wewnętrzne, niepubliczne wykorzystanie.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Brak.

SC-13 OCHRONA KRYPTOGRAFICZNA

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-13	**OCHRONA KRYPTOGRAFICZNA**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SC-15 WSPÓŁPRACUJĄCE URZĄDZENIA i APLIKACJE

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-15	**WSPÓŁPRACUJĄCE URZĄDZENIA i APLIKACJE**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SC-17 CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-17	**CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SC-18 KOD MOBILNY

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-18	**KOD MOBILNY**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SC-19 PROTOKÓŁ TRANSMISJI PAKIETOWEJ (VoIP)

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-19	**PROTOKÓŁ TRANSMISJI PAKIETOWEJ (VoIP)**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Wykorzystanie technologii VoIP jest ustalane po dokładnym rozważeniu i po sprawdzeniu, czy nie ma to negatywnego wpływu na wydajność operacyjną systemu ICS.

SC-20 BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA)

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-20	**BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA)**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Korzystanie z bezpiecznych usług rozdzielania nazw/adresów jest określane po dokładnym rozważeniu i po sprawdzeniu, czy nie ma to negatywnego wpływu na działanie ICS.

SC-21 BEZPIECZEŃSTWO NAZW DOMEN / USŁUGA USTALANIA ADRESU IP

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-21	**BEZPIECZEŃSTWO NAZW DOMEN / USŁUGA USTALANIA ADRESU IP**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Korzystanie z bezpiecznych usług rozdzielania nazw/adresów jest określane po dokładnym rozważeniu i po sprawdzeniu, czy nie ma to negatywnego wpływu na działanie ICS.

SC-22 ARCHITEKTURA NAZW DOMEN / ADRESÓW IP / ZAMAWIANIE USŁUGI DNS

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-22	**ARCHITEKTURA NAZW DOMEN / ADRESÓW IP / ZAMAWIANIE USŁUGI DNS**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Korzystanie z bezpiecznych usług rozdzielania nazw/adresów jest określane po dokładnym rozważeniu i po sprawdzeniu, czy nie ma to negatywnego wpływu na wydajność operacyjną ICS.

SC-23 AUTENTYCZNOŚĆ SESJI

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-23	**AUTENTYCZNOŚĆ SESJI**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują środki służące do przeprowadzania audytów.

SC-24 PRZEJŚCIE DO OKREŚLONEGO STANU SYSTEMU PO BŁĘDZIE

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-24	**PRZEJŚCIE DO OKREŚLONEGO STANU SYSTEMU PO BŁĘDZIE**		Dodane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Organizacja określa właściwy stan sytemu po wystąpieniu błędu. Zachowanie informacji i stanie ICS obejmuje zachowanie zgodności między zmiennymi stanu ICS a stanem fizycznym, który reprezentuje ICS (np. czy zawory są otwarte lub zamknięte, komunikacja dozwolona lub zablokowana, kontynuacja operacji).

Uzasadnienie zmiany zabezpieczenia bazowego: Podczas projektowania i opracowywania architektury systemu ICS organizacja wybiera stosowny stan po wystąpieniu błędu systemu ICS zgodnie z funkcją pełnioną przez system ICS i środowiskiem operacyjnym. Możliwość wyboru trybu awaryjnego dla fizycznej części ICS odróżnia ICS od innych systemów informacyjnych. Wybór ten może mieć istotny wpływ na złagodzenie skutków awarii, ponieważ może ona zakłócić trwające procesy fizyczne (np. awaria zaworów w pozycji zamkniętej może mieć negatywny wpływ na chłodzenie systemu).

SC-28 OCHRONA DANYCH w SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-28	**OCHRONA DANYCH w SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Wykorzystanie mechanizmów kryptograficznych jest określane po dokładnym rozważeniu oraz po sprawdzeniu, że nie ma to negatywnego wpływu na wydajność operacyjną ICS.

SC-39 IZOLACJA PROCESÓW

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-39	**IZOLACJA PROCESÓW**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: zabezpieczenia kompensacyjne obejmują rozdzielenie procesów na odrębne platformy.

SC-41 DOSTĘP DO PORTÓW i URZĄDZEŃ WEJŚCIA / WYJŚCIA

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SC-41	**DOSTĘP DO PORTÓW i URZĄDZEŃ WEJŚCIA / WYJŚCIA**	Dodane	Dodane	Dodane

Wytyczne uzupełniające dotyczące ICS: Brak.

Uzasadnienie zmiany zabezpieczenia bazowego: Funkcja systemu ICS może być z góry łatwo określona, co ułatwia identyfikację portów i urządzeń we/wy, które są zbyteczne. Wyłączenie lub usunięcie takich portów zwiększa bezpieczeństwo.

KATEGORIA SI – INTEGRALNOŚĆ SYSTEMU i INFORMACJI

Uwagi dotyczące dostosowania do kategorii integralności systemu i informacji

W sytuacjach, gdy system ICS nie może spełnić określonych wymagań zabezpieczeń integralności systemu i informacji, organizacja stosuje zabezpieczenia kompensacyjne zgodnie z ogólnymi wskazówkami dotyczącymi dostosowania. Zależnie od potrzeb, przy każdym zabezpieczeniu przedstawione są przykłady zabezpieczeń kompensacyjnych.

Wytyczne uzupełniające

Wytyczne uzupełniające dla wszystkich zabezpieczeń i zabezpieczeń rozszerzonych zamieszczonych w publikacji NSC 800-53 powinny być stosowane łącznie z wytycznymi uzupełniającymi dla systemów ICS zawartymi w tej nakładce, jeśli takie istnieją.

SI-1 POLITYKA i PROCEDURY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-1	**POLITYKA i PROCEDURY**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Polityka ta uwzględnia w szczególności wyjątkowe właściwości i wymagania ICS oraz relacje z systemami innymi niż ICS.

SI-2 USUWANIE USTEREK

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-2	**USUWANIE USTEREK**	Wybrane	Wybrane	Wybrane
SI-2 (1)	ZARZĄDZANIE CENTRALNE			Wybrane

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-2 (2)	ZAUTOMATYZOWANE USUWANIE USTEREK		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Usuwanie usterek jest procesem złożonym, ponieważ wiele systemów ICS korzysta z systemów operacyjnych i innego oprogramowania, które nie jest aktualne, nie jest już aktualizowane przez dostawców i nie jest odporne na bieżące zagrożenia. Operatorzy systemów ICS są często uzależnieni od producentów produktów w zakresie sprawdzania poprawności działania poprawki a czasami także przeprowadzania jej instalacji. Często usterki nie mogą być usunięte ze względu na okoliczności pozostające poza kontrolą operatora ICS (np. niedostępność poprawki wydanej przez producenta). Czasami organizacja nie ma wyboru i musi zaakceptować dodatkowe ryzyko. W takich sytuacjach należy wdrożyć zabezpieczenia kompensacyjne (np. ograniczyć ekspozycję podatnego systemu). Mogą być również pożądane inne zabezpieczenia kompensacyjne, które nie zmniejszają ryzyka szczątkowego, ale zwiększają zdolność do reagowania (np. zapewnienie szybkiej reakcji w przypadku incydentu; opracowanie planu zapewniającego, że system ICS będzie w stanie zidentyfikować wykorzystanie luki). Testowanie usuwania usterek w systemie ICS może wymagać większych zasobów niż organizacja jest w stanie przeznaczyć.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Brak.

(2) Wytyczne uzupełniające dotyczące ICS: w sytuacjach, gdy ICS nie może wspierać użycia zautomatyzowanych mechanizmów do przeprowadzania i raportowania statusu usuwania usterek, organizacja stosuje niezautomatyzowane mechanizmy lub procedury, które zawierają metody wdrażania, śledzenia i weryfikowania działań łagodzących jako zabezpieczeń kompensacyjnych zgodnych z ogólnymi wytycznymi dotyczącymi procesów dostosowania.

SI-3 ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-3	**ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM**	Wybrane	Wybrane	Wybrane
SI-3 (1)	ZARZĄDZANIE CENTRALNE		Wybrane	Wybrane
SI-3 (2)	AUTOMATYCZNE AKTUALIZACJE		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Użycie i wdrożenie zabezpieczenia przed złośliwym kodem jest określane po dokładnym rozważeniu i po sprawdzeniu, że nie ma to negatywnego wpływu na działanie ICS. Narzędzia do ochrony przed złośliwym kodem powinny być skonfigurowane tak, aby zminimalizować ich potencjalny wpływ na ICS (np. stosować powiadomienia zamiast kwarantanny). Przykładowe zabezpieczenia kompensacyjne obejmują wzmożone monitorowanie ruchu i audyty.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Organizacja wdraża centralne zarządzanie ochroną przed złośliwym kodem z uwzględnieniem wpływu na działanie ICS. Przykładowe zabezpieczenia kompensacyjne obejmują wzmożoną obserwację działań audytowych.

(2) Wytyczne uzupełniające dotyczące ICS: Organizacja implementuje automatyczne aktualizacje zabezpieczeń przed złośliwym kodem z uwzględnieniem wpływu na działanie ICS. W sytuacjach, w których system ICS nie może wspierać użycia automatycznej aktualizacji zabezpieczeń przed złośliwym kodem, organizacja stosuje jako zabezpieczenia kompensacyjne nieautomatyczne procedury, wprowadzane zgodnie z ogólnymi wytycznymi dotyczącymi procesów dostosowania.

SI-4 MONITOROWANIE SYSTEMU

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-4	**MONITOROWANIE SYSTEMU**	Wybrane	Wybrane	Wybrane
SI-4 (2)	AUTOMATYCZNE NARZĘDZIA i MECHANIZMY ANALIZY w CZASIE RZECZYWISTYM		Wybrane	Wybrane
SI-4 (4)	WEJŚCIOWY / WYJŚCIOWY RUCH TELEKOMUNIKACYJNY		Wybrane	Wybrane
SI-4 (5)	ALERTY SYSTEMOWE		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Organizacja zapewnia, że stosowanie narzędzi i technik monitorowania nie ma negatywnego wpływu na wydajność operacyjną ICS. Przykładowe zabezpieczenia kompensacyjne obejmują wdrożenie skutecznego monitorowania sieci.

Zabezpieczenia rozszerzone:

2) Wytyczne uzupełniające dotyczące ICS: w sytuacjach, w których ICS nie może wspierać użycia zautomatyzowanych narzędzi do wspierania analizy zdarzeń w czasie zbliżonym do rzeczywistego, organizacja stosuje zabezpieczenia kompensacyjne (np. zapewnienie możliwości audytu w oddzielnym systemie, niezautomatyzowane mechanizmy lub procedury) zgodnie z ogólnymi wytycznymi dotyczącymi procesu dostosowania.

4) Wytyczne uzupełniające dotyczące ICS: w sytuacjach, w których ICS nie może monitorować przychodzącego i wychodzącego ruchu telekomunikacyjnego, organizacja stosuje zabezpieczenia kompensacyjne obejmujące zapewnienie możliwości monitorowania w odseparowanym systemie informacyjnym.

(5) Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia kompensacyjne obejmują ręczne metody generowania ostrzeżeń.

SI-5 ALERTY BEZPIECZEŃSTWA, PORADY i DYREKTYWY

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-5	**ALERTY BEZPIECZEŃSTWA, PORADY i DYREKTYWY**	Wybrane	Wybrane	Wybrane
SI-5 (1)	AUTOMATYCZNE ALERTY i PORADY			Wybrane

Wytyczne uzupełniające dotyczące ICS: Zespół reagowania na cyberzagrożenia związane z systemami sterowania przemysłowego generuje alerty i ostrzeżenia dotyczące bezpieczeństwa systemów ICS.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Brak.

SI-6 WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA i OCHRONY PRYWATNOŚCI

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-6	**WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA i OCHRONY PRYWATNOŚCI**			Wybrane

Wytyczne uzupełniające dotyczące ICS: Wyłączenie i ponowne uruchomienie ICS może nie zawsze być wykonalne po zidentyfikowaniu anomalii; działania te powinny być zaplanowane zgodnie z wymaganiami operacyjnymi ICS.

SI-7 APLIKACJE, OPROGRAMOWANIE UKŁADOWE i INTEGRALNOŚĆ INFORMACJI

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-7	**APLIKACJE, OPROGRAMOWANIE UKŁADOWE i INTEGRALNOŚĆ INFORMACJI**		Wybrane	Wybrane
SI-7 (1)	KONTROLE INTEGRALNOŚCI		Wybrane	Wybrane
SI-7 (2)	AUTOMATYCZNE POWIADOMIENIA I NARUSZENIACH INTEGRALNOŚCI			Wybrane
SI-7 (5)	AUTOMATYCZNA ODPOWIEDŹ NA NARUSZENIA INTEGRALNOŚCI			Wybrane
SI-7 (7)	INTEGRACJA WYKRYWANIA i ODPOWIEDZI		Wybrane	Wybrane
SI-7 (14)	KOD WYKONYWALNY BINARNY LUB MASZYNOWY			Wybrane

Wytyczne uzupełniające dotyczące ICS: Organizacja określa, czy użycie aplikacji do weryfikacji integralności wpłynęłoby negatywnie na działanie ICS i stosuje zabezpieczenia kompensacyjne (np. ręczne weryfikacje integralności), które nie wpływają na działanie ICS.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Organizacja zapewnia, że użycie aplikacji do weryfikacji integralności nie ma negatywnego wpływu na wydajność operacyjną ICS.

(2) Wytyczne uzupełniające dotyczące ICS: w sytuacjach, gdy organizacja nie może zastosować zautomatyzowanych narzędzi, które zapewniają powiadamianie

i naruszeniach integralności, stosowane są niezautomatyzowane mechanizmy lub procedury. Przykładowe zabezpieczenia kompensacyjne obejmują przeprowadzanie zaplanowanych manualnych inspekcji pod kątem naruszeń integralności.

(5) Wytyczne uzupełniające dotyczące ICS: Wyłączenie i ponowne uruchomienie ICS może nie zawsze być wykonalne po zidentyfikowaniu anomalii; działania te powinny być zaplanowane zgodnie z wymaganiami operacyjnymi ICS.

(7) Wytyczne uzupełniające dotyczące ICS: w sytuacjach, w których system ICS nie jest w stanie wykryć nieuprawnionych zmian istotnych z punktu widzenia bezpieczeństwa, organizacja stosuje zabezpieczenia kompensacyjne (np. procedury ręczne) zgodnie z ogólnymi wytycznymi dotyczącymi procesu dostosowania.

(14) Brak wytycznych uzupełniających ICS.

SI-8 OCHRONA PRZED SPAMEM

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-8	**OCHRONA PRZED SPAMEM**		Wybrane	Wybrane
SI-8 (1)	ZARZĄDZANIE CENTRALNE		Wybrane	Wybrane
SI-8 (2)	AUTOMATYCZNE AKTUALIZACJE		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Ochrona ICS przed spamem może zostać wdrożona poprzez usunięcie z ICS mechanizmów, funkcji i usług umożliwiających przekazywanie spamu (np. poczty elektronicznej, dostępu do Internetu). Jeśli jakiekolwiek mechanizmy, funkcje i usługi transportujące spam są obecne w ICS, ochrona przed spamem w ICS uwzględnia właściwości operacyjne ICS, które różnią się od systemów informacyjnych ogólnego przeznaczenia (np. nietypowy przepływ ruchu, który może być błędnie zinterpretowany i wykryty jako spam). Przykładowe zabezpieczenia kompensacyjne obejmują „białą listę” serwerów poczty elektronicznej

(*ang. whitelist mail transfer agent - MTA*), wiadomości podpisane cyfrowo, akceptowalne źródła i typy wiadomości.

Zabezpieczenia rozszerzone:

(1) Wytyczne uzupełniające dotyczące ICS: Przykładowe zabezpieczenia wyrównawcze obejmują stosowanie wewnętrznych mechanizmów lub procedur.

(2) Wytyczne uzupełniające dotyczące ICS: Brak.

SI-10 WERYFIKACJA WPROWADZANYCH INFORMACJI

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-10	**WERYFIKACJA WPROWADZANYCH INFORMACJI**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SI-11 OBSŁUGA BŁĘDÓW

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe**		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-11	**OBSŁUGA BŁĘDÓW**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SI-12 ZARZĄDZANIE i RETENCJA DANYCH

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-12	**ZARZĄDZANIE i RETENCJA DANYCH**	Wybrane	Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SI-13 PRZEWIDYWANIE AWARII

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-13	**PRZEWIDYWANIE AWARII**			Dodane

Wytyczne uzupełniające dotyczące ICS: Awarie w systemach ICS mogą być zarówno stochastyczne, jak i deterministyczne. Awarie stochastyczne można analizować z wykorzystaniem teorii prawdopodobieństwa, natomiast analiza awarii deterministycznych opiera się na nielosowych właściwościach systemu. Rozważane są znane tryby i przyczyny awarii systemów ICS. Obliczanie i stosowanie statystycznych wskaźników opisowych, takich jak średni czas międzyawaryjny (ang. Mean Time To Failure - MTTF), powinno obejmować dodatkową analizę mającą na celu określenie sposobu objawiania się tych awarii w cyberprzestrzeni i domenie fizycznej. Znajomość tych możliwych przejawów może być niezbędna do wykrycia, czy w systemie ICS doszło do awarii, ponieważ awarie systemów informacyjnych mogą nie być łatwe do zidentyfikowania. Do analizy należy włączyć pojawiające się właściwości, które mogą powstawać zarówno w systemach informacyjnych, jak i w procesach fizycznych, i które mogą potencjalnie powodować awarie systemu. Na przykład skumulowane efekty wyczerpania zasobów (np. ulotność pamięci) lub błędy (np. zaokrąglanie i obcinanie) mogą wystąpić, gdy procesy ICS są wykonywane przez nieoczekiwanie długi czas.

Awariom deterministycznym (np. przepełnienie całkowitej pamięci licznika), po ich zidentyfikowaniu, można zapobiec.

Często komponenty zastępcze mogą nie być dostępne lub mogą być niewystarczające do ochrony przed błędami występującymi przed przewidywaną usterką. W celu ochrony przed takimi awariami należy stosować niezautomatyzowane mechanizmy lub zabezpieczenia fizyczne.

Oprócz informacji dotyczących nowo odkrytych podatności (tj. ukrytych wad) potencjalnie wpływających na system/aplikacje, które są wykrywane w trakcie badań z użyciem technik kryminalistycznych, nowe podatności mogą być identyfikowane przez organizacje odpowiedzialne za upowszechnianie informacji i podatnościach (np. ICS-CERT[86]) na podstawie analizy podobnego schematu zgłoszonych im incydentów lub podatności zgłoszonych przez innych analityków.

Powiązane zabezpieczenia: IR-5, IR-6, RA-5, SI-2, SI-5, SI-11.

Uzasadnienie zmiany zabezpieczenia bazowego: ICS są projektowane i budowane z uwzględnieniem określonych warunków brzegowych, parametrów projektowych oraz założeń dotyczących ich środowiska i sposobu działania. ICS mogą działać znacznie dłużej niż konwencjonalne systemy, co pozwala na urzeczywistnienie się ukrytych wad, które nie ujawniają się w innych środowiskach. Na przykład, przepełnienie rejestratora może nigdy nie wystąpić w systemach, które są ponownie inicjowane z częstotliwością większą niż czas wystąpienia przepełnienia. Doświadczenie i analizy analityczne anomalii i incydentów w systemach ICS mogą prowadzić do identyfikacji nowych właściwości, które wcześniej były nieznane, nieoczekiwane lub nieprzewidziane. Działania prewencyjne i naprawcze (np. ponowne uruchomienie systemu lub aplikacji) są uzasadnione, ale mogą być niedopuszczalne ze względów operacyjnych związanych z ICS.

[86] Np. CERT Polska
ICS-CERT Advisories | CISA
ICS-CERT Alerts | CISA

SI-16 OCHRONA PAMIĘCI

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-16	**OCHRONA PAMIĘCI**		Wybrane	Wybrane

Wytyczne uzupełniające dotyczące ICS: Brak.

SI-17 PROCEDURY TESTOWANIA AWARYJNEGO „FAIL-SAFE”

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe		
		Poziom wpływu na system informacyjny		
		Niski	Umiarkowany	Wysoki
SI-17	**PROCEDURY TESTOWANIA AWARYJNEGO „FAIL-SAFE”**	Dodane	Dodane	Dodane

Wytyczne uzupełniające dotyczące ICS: Wybrane stany awarii i powiązane z nimi procedury mogą być różne dla różnych zabezpieczeń bazowych. To samo zdarzenie powodujące awarię może wywołać różne reakcje w zależności od poziomu wpływu na system. System mechaniczny i analogowy można wykorzystać do stworzenia procedur zapewniających bezpieczeństwo w przypadku awarii. Stany awaryjne powinny uwzględniać potencjalne oddziaływania na bezpieczeństwo ludzi, systemy fizyczne i środowisko.

Powiązane zabezpieczenia: CP-6.

Uzasadnienie zmiany zabezpieczenia bazowego: Zabezpieczenie to zapewnia organizacji warunki do określenia jej polityki i procedur postępowania w przypadku awarii i innych zdarzeń. Tworzenie pisemnego zapisu procesu decyzyjnego dotyczącego selekcjonowania incydentów i odpowiedniego reagowania, jest częścią zarządzania ryzykiem w świetle zmieniającego się środowiska działania.