

IEC 62443-3-3:2013 Wymagania bezpieczeństwa systemów dla automatyki przemysłowej

Siedem wymagań podstawowych, 51 wymagań systemowych

100 wymagań. Ta norma może zostać certyfikowana przez akredytowaną jednostkę. Stan na 07/2026.

Normę IEC 62443-3-3 można certyfikować, a przedmiotem certyfikacji jest system, nie organizacja i nie osoba. Ścieżki certyfikacji to ISASecure SSA oraz IECCEB Scheme. Kto chce certyfikować organizację, potrzebuje normy 62443-2-1 lub 2-4, kto ma na myśli komponent, potrzebuje normy 62443-4-2. Ta lista zawiera 51 wymagań systemowych oraz 49 rozszerzeń wymagań. To, które z nich mają zastosowanie, zależy od docelowego poziomu bezpieczeństwa: 38 od SL 1, 60 od SL 2, 90 od SL 3, wszystkie 100 na SL 4. Żadne rozszerzenie nie ma zastosowania już na SL 1. Ta lista jest pomocą roboczą do samooceny, nie dowodem.

Firma

Data

Opracował

5 FR 1: Kto lub co żąda dostępu i czy rzeczywiście jest tym, za kogo się podaje

24

SR 1.1 Użytkownicy będący ludźmi są identyfikowani, a ich tożsamość jest weryfikowana przed uzyskaniem dostępu, w każdym punkcie, w którym mogą obsługiwać lub konfigurować system automatyki. Dotyczy to paneli operatorskich przy maszynie, dostępu inżynierskiego oraz usług sieciowych.

Jak to wykazać: Inwentaryzacja wszystkich punktów logowania w systemie, czyli HMI, sterownia, dostęp do programowania sterownika PLC, switch, VPN oraz klient zdalnej obsługi serwisowej, każdy z mechanizmem uwierzytelniania stosowanym w tym miejscu. Dodać wyciąg z konfiguracji lub zrzut ekranu okna logowania dla każdej klasy urządzeń. Mały zakład zaczyna od jednej tabeli na urządzenie, kolumny: urządzenie, interfejs, uwierzytelnianie obecne tak lub nie, uzasadnienie w przypadku nie. Wymagane od SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 1.1 RE 1 Każdy użytkownik będący człowiekiem pracuje pod indywidualnym identyfikatorem przypisanym wyłącznie tej osobie. Konta współdzielone i zmianowe są wyłączone, pozostałe wyjątki są uzasadniane indywidualnie i wspierane dodatkowymi środkami.

Jak to wykazać: Eksport kont z systemu z przypisaniem identyfikatora do osoby, lista wyjątków z uzasadnieniem i środkiem kompensującym, na przykład kamera lub rejestr obecności na stanowisku operatora. Ta pozycja jest rozszerzeniem wymagania i dlatego nigdy nie jest obowiązkowa na SL 1, jest wymagana od SL 2.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 1.1 RE 2 Każdy, kto loguje się z niezaufanej sieci, na przykład z internetu lub przez połączenie zdalnej obsługi serwisowej, potwierdza swoją tożsamość przy użyciu co najmniej dwóch niezależnych czynników.

Jak to wykazać: Konfiguracja dostępu zdalnego z włączonym drugim czynnikiem, przykładowy zapis logowania pokazujący oba czynniki oraz lista wydanych tokenów lub rejestracji aplikacji. Mały zakład korzysta z drugiego czynnika istniejącej bramy VPN lub aplikacji uwierzytelniającej, co nie kosztuje nic poza czasem konfiguracji. Rozszerzenie wymagania, wymagane od SL 3, nie na SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 1.1 RE 3 Potwierdzenie dwoma niezależnymi czynnikami dotyczy nie tylko dostępu z zewnątrz, ale każdego logowania użytkownika będącego człowiekiem, w tym logowań wewnątrz sieci sklasyfikowanej jako zaufana.

Jak to wykazać: Wyciąg z polityki centralnej usługi uwierzytelniania pokazujący, że drugi czynnik jest egzekwowany bez żadnego wyjątku sieciowego, wraz z przykładowymi zapisami logowania ze sterowni i panelu operatorskiego. Rozszerzenie wymagania, wymagane dopiero od SL 4.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 1.2 Nie tylko ludzie, ale także procesy programowe i urządzenia uwierzytelniają się w systemie, zanim zostanie im pozwolone na wymianę danych lub korzystanie z usług. Dotyczy to sprzężeń między sterownikami, łączących dane do systemów nadrzędnych oraz narzędzi diagnostycznych.

Jak to wykazać: Lista połączeń maszyna do maszyny ze źródłem, celem, protokołem i danymi uwierzytelniającymi użytymi w każdym przypadku, na przykład certyfikat, konto usługowe lub klucz współdzielony. Dodać wyciąg z konfiguracji jednego sprzężenia, który uwidacznia uwierzytelnianie. Wymagane od SL 2, nie wymagane na SL 1.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 1.2 RE 1 Każdy proces programowy i każde urządzenie posługuje się własnym unikalnym identyfikatorem. Współdzielone konta usługowe lub jeden klucz stosowany w całym systemie dla wielu urządzeń są niedozwolone.

[Dokument](#)

Jak to wykazać: Mapowanie urządzenia na identyfikator lub numer seryjny certyfikatu pokazujące, że żaden identyfikator nie występuje dwukrotnie. Rozszerzenie wymagania, wymagane od SL 3 i dlatego nienależące do SL 1.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 1.3 Konta są zarządzane w całym swoim cyklu życia: tworzenie, zmiana uprawnień, wyłączenie przy odejściu oraz usuwanie są regulowane zasadami i wspierane przez zaangażowane systemy. Dotyczy to kont użytkowników, kont usługowych i kont awaryjnych.

[Dokument](#)

Jak to wykazać: Rejestr kont z typem, właścicielem, celem i statusem, wraz z dowodami dotyczącymi osób przyjmowanych i odchodzących, na przykład podpisane przekazanie lub zgłoszenie pokazujące wyłączenie z jego datą. Wskazany jest cykliczny przegląd kont, a w małym zakładzie wystarcza coroczne uzgodnienie listy kont z listą personelu. Wymagane od SL 1.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 1.3 RE 1 Zarządzanie kontami jest ujednolicone we wszystkich komponentach systemu, tak aby wyłączenie konta w jednym miejscu nie pozostawało bezskuteczne na poszczególnych urządzeniach.

Jak to wykazać: Dowód integracji z centralnym katalogiem, na przykład usługa katalogowa lub RADIUS, z listą podłączonych komponentów oraz jawną listą urządzeń, których nie można podłączyć, wraz z ich procedurą alternatywną. Zapis testu wyłączenia, które staje się skuteczne we wszystkich podłączonych systemach. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 1.4 Identyfikatory są wydawane według ustalonych zasad, przypisywane jednoznacznie osobie, urządzeniu lub roli, wycofywane, gdy nie są już używane, i nigdy nie są ponownie nadawane innemu posiadaczowi w późniejszym czasie.

Jak to wykazać: Reguła nazewnictwa identyfikatorów, na przykład nazwisko plus inicjał lub kod zakładu plus numer, wraz z historią wycofanych identyfikatorów pokazującą, że nie są one ponownie wykorzystywane. Mały zakład prowadzi jedną bieżącą listę z datą wydania i datą wycofania. Wymagane od SL 1.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 1.5 Elementy uwierzytelniające, takie jak hasła, klucze, certyfikaty i tokeny, są wydawane w uporządkowany sposób, zmieniane w razie podejrzenia ujawnienia i unieważniane w razie potrzeby. Konta domyślne i hasła fabryczne w stanie dostawy są zmieniane przed uruchomieniem.

Jak to wykazać: Lista wydanych tokenów i certyfikatów z odbiorcą i datą, dowody zmian i unieważnień, wraz z listą kontrolną uruchomienia dla każdego urządzenia z pozycją hasła fabryczne zmienione, podpisaną. Wymagane od SL 1.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 1.5 RE 1 Dane uwierzytelniające procesów programowych nie są przechowywane jako czytelny plik na nośniku danych, lecz w pamięci sprzętowej, która uniemożliwia odczytanie tajnej części.

Jak to wykazać: Dowód typu zastosowanego komponentu bezpieczeństwa, na przykład TPM, secure element lub HSM, wraz z wyciągiem z konfiguracji dowodzącym, że klucz jest przechowywany wewnątrz komponentu. Jako dowód typu wystarczy zapis zakupu lub karta katalogowa. Rozszerzenie wymagania, wymagane od SL 3, nie wymagane na SL 1 i SL 2.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 1.6 Bezprzewodowy dostęp do systemu, na przykład WLAN, radiowe zdalne sterowanie lub diagnostyka Bluetooth, jest możliwy do wykorzystania dopiero po identyfikacji i uwierzytelnieniu zarówno użytkownika, jak i urządzenia, i jest świadomie zarządzany.

Jak to wykazać: Inwentaryzacja wszystkich łącz bezprzewodowych z celem, zasięgiem i metodą szyfrowania, wyciąg z konfiguracji punktu dostępowego oraz lista zatwierdzonych urządzeń końcowych. Mały zakład dodatkowo dokumentuje, które interfejsy bezprzewodowe urządzeń zostały świadomie wyłączone. Wymagane od SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 1.6 RE 1 Każdy dostęp bezprzewodowy musi być możliwy do przypisania do jednego konkretnego użytkownika lub jednego konkretnego urządzenia, współdzielony klucz sieciowy dla wszystkich uczestników nie jest wystarczający.

Jak to wykazać: Dowód metody z indywidualnymi danymi uwierzytelniającymi, na przykład uwierzytelnianie WLAN typu enterprise wobec katalogu lub certyfikaty dla poszczególnych urządzeń, wraz z dziennikiem połączeń pokazującym indywidualny identyfikator. Rozszerzenie wymagania, wymagane od SL 2 i dlatego nie na SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 1.7 Wszędzie tam, gdzie stosowane są hasła, można konfigurować ich minimalną siłę, na przykład minimalną długość i wymagane typy znaków, a skonfigurowane wartości obowiązują wszystkie odnośne konta.

Jak to wykazać: Wyciąg z konfiguracji polityki haseł dla każdego systemu z faktycznie ustawionymi wartościami, na przykład długość ≥ 10 znaków i co najmniej trzy typy znaków, wraz z listą systemów, które technicznie nie mogą obsługiwać tego ustawienia, wraz z ich środkiem kompensującym. Wymagane od SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 1.7 RE 1 Dla użytkowników będących ludźmi obowiązują dodatkowe zasady dotyczące generowania i ważności haseł: ponowne użycie wcześniejszych haseł jest uniemożliwione, a ważność jest ograniczona w czasie.

Jak to wykazać: Wyciąg z konfiguracji pokazujący historię haseł, na przykład zablokowane ponowne użycie ostatnich pięciu haseł, oraz skonfigurowaną maksymalną ważność. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 1.7 RE 2 Ograniczenie ważności haseł dotyczy nie tylko ludzi, ale wszystkich kont, w tym kont usługowych, serwisowych i kont urządzeń.

Jak to wykazać: Plan rotacji dla kont technicznych z ostatnią i następną datą zmiany dla każdego konta, wraz z dowodami zmian, na przykład zapis zmiany lub zgłoszenie. Rozszerzenie wymagania, wymagane dopiero od SL 4.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 1.8

Tam, gdzie stosowane są certyfikaty, pochodzą one z uporządkowanego zarządzania certyfikatami z określonymi zasadami wnioskowania, wydawania, okresu ważności, odnawiania i unieważniania.

[Dokument](#)

Jak to wykazać: Polityka certyfikatów lub krótka pisemna zasada określająca odpowiedzialność, okresy ważności i ścieżkę unieważniania, wraz z inwentaryzacją wydanych certyfikatów z ich terminami ważności. Mały zakład prowadzi tabelę z certyfikatem, urządzeniem, terminem ważności i datą przypomnienia, co zapobiega cichym przestojom zakładu spowodowanym wygasłymi certyfikatami. Wymagane od SL 2.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

[Dowód / uzasadnienie](#)

SR 1.9

Gdy do uwierzytelniania stosowane są pary kluczy, system w pełni waliduje certyfikat: łańcuch zaufania, okres ważności, status unieważnienia oraz dowód, że druga strona rzeczywiście posiada klucz prywatny. Powiązanie między certyfikatem a kontem jest jednoznaczne.

Jak to wykazać: Wyciąg z konfiguracji z włączonym sprawdzaniem unieważnień, na przykład CRL lub OCSP, zapis testu odrzuconego logowania z certyfikatem wygasłym lub unieważnionym, wraz z tabelą mapowania certyfikatu na konto. Wymagane od SL 3, nie wymagane na SL 1 i SL 2.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

[Dowód / uzasadnienie](#)

SR 1.9 RE 1

Klucze prywatne znajdują się wyłącznie w pamięci sprzętowej, z której nie można ich odczytać, i są również używane wewnątrz tej pamięci.

Jak to wykazać: Karta katalogowa lub dowód certyfikacji zastosowanego komponentu bezpieczeństwa oraz wyciąg z konfiguracji pokazujący, że klucz jest generowany wewnątrz komponentu, tak że klucz prywatny nigdy go nie opuszcza. Rozszerzenie wymagania, wymagane dopiero od SL 4.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

[Dowód / uzasadnienie](#)

SR 1.10

Podczas logowania system nie ujawnia żadnych informacji, które mogłyby zostać wykorzystane. Wprowadzane hasła są maskowane, a komunikaty o błędach nie ujawniają, czy błędny był identyfikator, czy hasło.

Jak to wykazać: Zrzut ekranu okna logowania z zamaskowanym wprowadzaniem oraz zrzut ekranu komunikatu o błędzie po nieudanej próbie. Dla urządzeń, które nie potrafią tego technicznie, na przykład starsze panele operatorskie, dodać krótką notatkę o środku kompensującym, na przykład ograniczony dostęp fizyczny do miejsca instalacji. Wymagane od SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

[Dowód / uzasadnienie](#)

SR 1.11

Liczba kolejnych nieudanych prób logowania jest ograniczona, a reakcja na nie jest konfigurowalna, na przykład tymczasowa blokada. Wybrana reakcja nie utrudnia eksploatacji zakładu związanej z bezpieczeństwem funkcjonalnym.

Jak to wykazać: Wyciąg z konfiguracji z progiem, na przykład blokada po ≤ 5 nieudanych próbach, oraz czasem trwania blokady, wraz z krótką oceną, dlaczego blokada nie uniemożliwia obsługi awaryjnej ani bezpiecznego wyłączenia zakładu. Na stanowiskach operatorskich z funkcją bezpieczeństwa blokada czasowa jest preferowana wobec trwałej blokady konta. Wymagane od SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

[Dowód / uzasadnienie](#)

SR 1.12

Przed zalogowaniem można wyświetlić komunikat o użytkowaniu, wskazujący zasady użytkowania i monitorowania systemu. Treść i sposób wyświetlania są konfigurowalne przez właściciela zasobu.

Jak to wykazać: Zrzut ekranu wyświetlanego tekstu komunikatu oraz zatwierdzonego brzmienia z datą zatwierdzenia. Małe zakłady krótko uzgadniają brzmienie z przedstawicielstwem pracowników lub z kierownictwem, wystarczy jeden akapit. Wymagane od SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

[Dowód / uzasadnienie](#)

SR 1.13 Dostęp z niezauważanych sieci, na przykład zdalna obsługa serwisowa przez dostawców, jest ograniczony do określonych ścieżek, jest monitorowany i w każdej chwili można go przerwać.

Jak to wykazać: Inwentaryzacja ścieżek dostępu zdalnego z celem, stroną zdalną, osobą kontaktową i wykorzystywaną ścieżką, wraz z dziennikami połączeń i dowodem możliwości rozłączenia, na przykład przełącznik klawiszowy, reguła zapory sieciowej lub router zdalnej obsługi serwisowej możliwy do wyłączenia. Wymagane od SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 1.13 RE 1 Każda pojedyncza sesja z niezauważanej sieci jest jawnie zatwierdzana przez osobę odpowiedzialną przed nawiązaniem połączenia, stale otwarte połączenie nie jest wystarczające.

Jak to wykazać: Zapisy zatwierdzeń dla każdej sesji zdalnej obsługi serwisowej z czasem, powodem, osobą zatwierdzającą i czasem trwania, technicznie na przykład przez przełącznik klawiszowy przy routerze dostępowym lub przez portal zatwierdzeń. W małym zakładzie wystarczy dziennik zdalnej obsługi serwisowej przy szafie sterowniczej, podpisywany przez technika serwisowego dla każdej sesji. Rozszerzenie wymagania, wymagane od SL 2 i dlatego nigdy na SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

6 FR 2: Kontrola użycia (uprawnienia, sesje, zapisy audytu)

24

SR 2.1 System technicznie wymusza przyznane uprawnienia: każda zalogowana osoba, każde urządzenie i każdy proces programowy otrzymuje dokładnie taki dostęp, jaki został mu przypisany, a każda próba wykraczająca poza to jest odrzucana.

Jak to wykazać: Konceptcja uprawnień przypisująca konta do uprawnień, wraz ze zrzutem ekranu lub wyciągiem z konfiguracji dla każdego systemu sterowania, HMI i stacji inżynierskiej, pokazującym aktywne uprawnienia. Dodatkowo zapis testu, w którym konto o niskich uprawnieniach próbuje wykonać zablokowaną czynność i zostaje odrzucone. Wymagane od SL 1. Mały zakład radzi sobie z dwiema lub trzema rolami, na przykład obsługa, utrzymanie ruchu, inżynieria, i dokumentuje je na jednej stronie.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 2.1 RE 1 Egzekwowanie uprawnień dotyczy nie tylko operatorów będących ludźmi, ale w równym stopniu procesów programowych i urządzeń, które samodzielnie uzyskują dostęp do systemu.

Jak to wykazać: Lista kont technicznych i usługowych, na przykład klienci OPC UA, połączenia historian, usługi kopii zapasowych, każde z przypisanym zestawem uprawnień. Wyciąg z zarządzania uprawnieniami pokazujący, że te konta nie działają z uprawnieniami administratora. Rozszerzenie wymagania, wymagane od SL 2, nie na SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 2.1 RE 2 Uprawnienia nie są nadawane osobom pojedynczo, lecz poprzez role, a przypisanie roli do dozwolonych czynności jest udokumentowane w sposób możliwy do prześledzenia.[Dokument](#)

Jak to wykazać: Macierz ról i uprawnień w formie tabeli: wiersze to role, kolumny to czynności, takie jak zmiana wartości zadanej, wgranie programu, potwierdzenie alarmu, utworzenie konta. Wraz z listą przypisania osób do ról. Rozszerzenie wymagania, wymagane od SL 2. W pełni wystarczający jako dowód jest prowadzony arkusz kalkulacyjny z datą zmiany.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 2.1 RE 3 W wąsko określonych przypadkach wyjątkowych upoważniony przełożony może zniesić ograniczenie uprawnień na czas ograniczony, a każde takie odstępstwo jest rejestrowane w dzienniku audytu.

Jak to wykazać: Opis procedury zatwierdzania wyjątku określający, kto może go udzielić i jak długo pozostaje ważny, wraz z zapisami audytu już udzielonych odstępstw, pobranymi z dziennika systemu. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 2.1 RE 4 Szczególnie krytyczne ingerencje wymagają zatwierdzenia przez dwie niezależne upoważnione osoby przed wykonaniem czynności.

Jak to wykazać: Lista czynności podlegających podwójnemu zatwierdzeniu, na przykład zmiana parametrów bezpieczeństwa lub wgranie nowego programu sterującego, wraz z dowodem konfiguracji i zapisami audytu wskazującymi obie osoby zatwierdzające. Rozszerzenie wymagania, wymagane dopiero od SL 4.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 2.2 Wykorzystanie połączeń bezprzewodowych w sieci automatyki jest związane z jawną autoryzacją, a wymianę danych lub ingerencję drogą radiową mogą prowadzić wyłącznie zatwierdzeni uczestnicy.

Jak to wykazać: Inwentaryzacja wszystkich łączy bezprzewodowych, na przykład punkty dostępowe WLAN, parowania Bluetooth, routery komórkowe, każde z celem i zatwierdzonymi uczestnikami. Wraz z konfiguracją kontroli dostępu na punkcie dostępowym. Wymagane od SL 1. Kto nie eksploatuje żadnego łącza bezprzewodowego w sieci procesowej, stwierdza to dokładnie na piśmie i popiera widokiem konfiguracji pokazującym łączność bezprzewodową wyłączoną.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 2.2 RE 1 Nieautoryzowane urządzenia bezprzewodowe w pobliżu sieci automatyki są wykrywane i zgłaszane.

Jak to wykazać: Zapis z monitorowania sieci bezprzewodowej lub cyklicznego skanowania bezprzewodowego z datą, listą wyników i notatką o każdym nieznanym urządzeniu. Wskazana jest ścieżka zgłaszania do odpowiedzialnej funkcji. Rozszerzenie wymagania, wymagane od SL 2, nie na SL 1. Mały zakład może przeprowadzać kwartalne skanowanie za pomocą notebooka i zapisywać wynik jako protokół.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 2.3 Wykorzystanie urządzeń przenośnych i mobilnych w systemie, na przykład notebooki serwisowe, pamięci USB lub tablety, jest regulowane zasadami i technicznie ograniczone do jawnie zatwierdzonych urządzeń.

Jak to wykazać: Zbiór zasad użytkowania urządzeń, lista zatwierdzonych urządzeń serwisowych z ich identyfikatorami oraz dowód technicznego ograniczenia, na przykład porty USB na HMI i stacji inżynierskiej wyłączone lub ograniczone do konkretnych urządzeń. Wymagane od SL 1. Mały zakład pracuje z dwoma oznakowanymi pendrive'ami serwisowymi, które są zapisywane wyłącznie na jednej stacji transferowej.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 2.3 RE 1 Przed podłączeniem sprawdzany jest stan bezpieczeństwa urządzenia przenośnego lub mobilnego, a urządzeniom niespełniającym wymagań uniemożliwia się uzyskanie dostępu.

Jak to wykazać: Kryteria sprawdzania stanu urządzenia, na przykład aktualna ochrona przed złośliwym oprogramowaniem i poziom poprawek, wraz z zapisami sprawdzeń dla każdego urządzenia serwisowego oraz dowodem technicznego wymuszenia, na przykład poprzez stację transferową lub kontrolę dostępu do sieci. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 2.4 Dla kodu mobilnego wykonywanego w systemie, na przykład skrypty w interfejsach operatorskich lub treści aktywne w raportach, określone jest, które typy są dozwolone, a typom niedozwolonym uniemożliwia się wykonanie.[Dokument](#)

Jak to wykazać: Definicja, jaki kod mobilny jest dozwolony w jakich systemach, wraz z dowodem konfiguracji ograniczenia, na przykład wykonywanie skryptów w przeglądarce HMI wyłączone, makra w plikach analiz zablokowane. Wymagane od SL 1. Wystarczy jednostronicowa definicja obejmująca trzy lub cztery faktycznie występujące przypadki.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 2.4 RE 1 Przed wykonaniem kodu mobilnego weryfikuje się, że pochodzi on ze spodziewanego źródła i nie został zmieniony.

Jak to wykazać: Dowód konfiguracji weryfikacji podpisu lub kontroli sumy kontrolnej, wraz z zapisem testu, w którym kod zmanipulowany lub niepodpisany zostaje odrzucony. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 2.5 Sesja jest blokowana po określonym czasie bez działania operatora i zostaje odblokowana ponownie dopiero po ponownym uwierzytelnieniu, bez utraty wyświetlania informacji procesowych istotnych dla bezpieczeństwa.

Jak to wykazać: Wyciąg z konfiguracji z ustawionym czasem blokady dla każdego stanowiska, wraz z uzasadnieniem dla stanowisk w stale obsadzonych sterowniach, gdzie blokada jest świadomie ustawiona inaczej. Wymagane od SL 1. Dowód wizualny: zrzut ekranu blokady z nadal widocznym paskiem alarmowym.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 2.6 Sesje zdalne są kończone po określonym czasie bez aktywności lub na żądanie operatora, tak aby żadne otwarte połączenie zdalne nie pozostawało bez nadzoru.

Jak to wykazać: Konfiguracja dostępu zdalnego z limitem czasu bezczynności, zapisy audytu zakończonych sesji zdalnych oraz opis, w jaki sposób operator może natychmiast rozłączyć trwającą sesję zdalnej obsługi serwisowej, na przykład przez przełącznik kluczykowy lub zwolnienie dla poszczególnej sesji. Wymagane od SL 2, nie na SL 1.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 2.7 Liczba równoczesnych sesji dla konta lub roli jest ograniczona, a próby logowania przekraczające ten limit są odrzucane.

Jak to wykazać: Wyciąg z konfiguracji z określonym limitem górnym dla każdej roli, na przykład ≤ 1 równoczesna sesja dla kont inżynierskich, wraz z zapisem testu odrzuconej drugiej próby logowania. Wymagane od SL 3.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 2.8 Zdarzenia istotne dla bezpieczeństwa są rejestrowane, a każdy wpis wskazuje co najmniej czas, źródło, konto wyzwalające, rodzaj zdarzenia i wynik.[Dokument](#)

Jak to wykazać: Definicja rejestrowanych rodzajów zdarzeń, na przykład logowanie, nieudane logowanie, zmiana uprawnień, zmiana programu, zmiana konfiguracji, wraz z autentycznym wyciągiem z dziennika audytu pokazującym wymienione pola. Wymagane od SL 1. Mały zakład gromadzi dzienniki z systemu sterowania, HMI i zapory sieciowej w jednym folderze z ustalonym okresem przechowywania.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 2.8 RE 1 Zapisy audytu poszczególnych komponentów są gromadzone w jednym centralnym miejscu i tworzą jeden, obejmujący cały system rejestr, który można ocenić jako całość.

Jak to wykazać: Szkic architektury gromadzenia dzienników pokazujący wszystkie podłączone źródła, wraz z analizą umieszczającą zdarzenia z co najmniej dwóch komponentów na jednej osi czasu. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 2.9 Zapewniona jest wystarczająca przestrzeń przechowywania dla zapisów audytu, tak aby zdarzenia były zachowywane przez określony okres przechowywania i nie były niezamierzenie nadpisywane.

Jak to wykazać: Obliczenie lub oszacowanie zapotrzebowania na przestrzeń na podstawie dziennego wolumenu dzienników pomnożonego przez okres przechowywania, wraz ze skonfigurowanym rozmiarem przestrzeni i zasadą archiwizacji. Wymagane od SL 1. W praktyce wystarczy codzienna kopia do osobnej lokalizacji przechowywania z udokumentowanym okresem przechowywania.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 2.9 RE 1 Po osiągnięciu określonego progu wypełnienia przestrzeni przechowywania audytu wydawane jest ostrzeżenie do odpowiedzialnej funkcji, zanim pojemność przechowywania zostanie w pełni wyczerpana.

Jak to wykazać: Wyciąg z konfiguracji progu, na przykład ostrzeżenie od ≥ 80 procent wykorzystania, wraz z przykładem wywołanego powiadomienia i listą odbiorców. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 2.10 Jeśli rejestrowanie audytu zawiedzie lub przestrzeń przechowywania audytu wypełni się, system reaguje w z góry określony sposób, a odpowiedzialna funkcja zostaje poinformowana, bez zagrożenia dla bezpiecznej eksploatacji zakładu.

Jak to wykazać: Określona reakcja dla każdego przypadku awarii, na przykład nadpisanie starszych wpisów i wywołanie powiadomienia zamiast zatrzymania zakładu, z uzasadnieniem z punktu widzenia procesu. Dowód poprzez wywołane testowe powiadomienie i odpowiadający mu wpis audytu. Wymagane od SL 1.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 2.11 Każdy zapis audytu zawiera znacznik czasu pochodzący z nazwanego źródła czasu, tak aby zdarzenia z różnych komponentów można było uporządkować względem siebie.

Jak to wykazać: Wskazanie źródła czasu stosowanego dla każdego komponentu oraz wyciąg z dziennika z widocznym znacznikiem czasu wraz ze strefą czasową. Wymagane od SL 2, nie na SL 1.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 2.11 RE 1 Zegary wszystkich uczestniczących komponentów są synchronizowane wobec wspólnego źródła czasu, tak aby odchylenie pozostawało w określonej granicy.

Jak to wykazać: Konfiguracja synchronizacji czasu, na przykład serwer NTP i interwał synchronizacji, wraz z zapisem sprawdzenia ze zmierzonym odchyleniem dla każdego komponentu wobec określonej granicy, na przykład ≤ 1 sekunda. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 2.11 RE 2 Samo źródło czasu jest chronione przed manipulacją, a nieprawdopodobne lub zmienione odniesienie czasowe jest wykrywane i zgłaszane.

Jak to wykazać: Opis sposobu ochrony źródła czasu, na przykład uwierzytelniona synchronizacja czasu, ograniczenie do źródła wewnętrznego, monitorowanie skoków czasu, wraz z powiadomieniami lub zapisami audytu wykrytego odchylenia. Rozszerzenie wymagania, wymagane dopiero od SL 4.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 2.12 Dla określonych czynności krytycznych można później bez wątpliwości ustalić, kto je wywołał, tak aby działająca osoba nie mogła w wiarygodny sposób temu zaprzeczyć.

[Dokument](#)

Jak to wykazać: Lista czynności, których dotyczy ten dowód, na przykład zmiana receptury, zwolnienie partii, zmiana wartości granicznych, wraz z odpowiednimi zapisami z unikalnym identyfikatorem osoby oraz dowodem, że konta grupowe są wykluczone dla tych czynności. Wymagane od SL 3.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 2.12 RE 1 Niezaprzeczalne przypisanie działającej osoby dotyczy nie tylko wybranych czynności krytycznych, ale wszystkich użytkowników i wszystkich wywoływanych przez nich czynności.

Jak to wykazać: Dowód, że każde konto jest powiązane z jedną osobą i że nie pozostają żadne współdzielone loginy, wraz z wyciągiem z dziennika dowolnych czynności, w którym w każdym przypadku pojawia się unikalny identyfikator osoby. Rozszerzenie wymagania, wymagane dopiero od SL 4.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

7 FR 3: Integralność systemu, ochrona danych, oprogramowania i sesji przed nieautoryzowaną modyfikacją

19

SR 3.1 System sterowania wykrywa, kiedy informacja została zmieniona podczas przesyłania przez kanał komunikacyjny, i robi to zarówno dla danych sterujących, danych konfiguracyjnych, jak i ruchu zarządzającego. Ochrona obejmuje również połączenia opuszczające system lub przechodzące przez niezaufane segmenty sieci.

Jak to wykazać: Przegląd sieci i protokołów wskazujący, który kanał wykorzystuje jaki mechanizm integralności (suma kontrolna, kod uwierzytelniania wiadomości, podpisane telegramy), wyciąg z konfiguracji ustawień bezpieczeństwa magistrali polowej lub OPC UA oraz zapis testu pokazujący, że zmanipulowany telegram został wykazywalnie odrzucony. Mały zakład ujmuje to w tabeli dla każdego połączenia z kolumnami źródło, cel, protokół i mechanizm integralności, i jednorazowo wykazuje skuteczność za pomocą przechwyty ruchu. Wymagane od SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 3.1 RE 1 Ochrona integralności podczas przesyłania opiera się na mechanizmach kryptograficznych, tak aby celowa manipulacja przez atakującego posługującego się własnymi środkami nie mogła przejść niezauważona. Zwykła suma kontrolna przed błędami transmisji nie jest tu wystarczająca.

Jak to wykazać: Lista stosowanych mechanizmów kryptograficznych i długości kluczy dla każdego kanału, odniesienie do leżącego u podstaw zarządzania kluczami oraz wyciągi z konfiguracji (na przykład zestawy szyfrów TLS, OPC UA SecurityPolicy, profile IPsec). Małe zakłady opierają się na bezpiecznych profilach domyślnych swoich sterowników i archiwizują zrzut ekranu aktywnego ustawienia. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 3.2 Wdrożone są mechanizmy ochrony przed złośliwym kodem, które uniemożliwiają wykonanie niepożądanego kodu programowego na komponentach systemu i zgłaszają każde wykrycie. Mechanizmy są dobrane tak, aby nie zakłócały zamierzonej eksploatacji zakładu, i są utrzymywane w aktualności.

Jak to wykazać: Przegląd dla każdego komponentu, jaki mechanizm ma zastosowanie (antywirus, biała lista aplikacji, utwardzony system operacyjny bez praw wykonywania), dowód aktualizacji sygnatur lub białych list oraz alerty z systemu ochrony. Tam, gdzie antywirus nie jest wykonalny, na przykład na sterowniku, rejestrowany jest środek kompensujący wraz z uzasadnieniem. Małym zakładom dobrze sprawdza się biała lista na komputerze operatorskim i pisemna zasada dla nośników USB. Wymagane od SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 3.2 RE 1 Ochrona przed złośliwym kodem działa dodatkowo w punktach wejścia i wyjścia zakładu, w których dane wchodzi lub wychodzi, a nie tylko na samych urządzeniach końcowych.

Jak to wykazać: Lista wszystkich punktów wejścia i wyjścia (dostęp zdalnej obsługi serwisowej, brama transferu danych, nośniki wymienne, przekazanie do sieci biurowej, ścieżka poczty elektronicznej dla wersji programów) wraz z mechanizmem skanowania obowiązującym w każdym z nich oraz zapisami sprawdzonych przekazów. Małe zakłady tworzą jeden komputer przekazujący ze skanowaniem antywirusowym jako bramę i utrwalają to w instrukcji roboczej. Rozszerzenie wymagania, wymagane od SL 2.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 3.2 RE 2 Mechanizmy ochrony przed złośliwym kodem są zarządzane z jednego centralnego miejsca, aktualizacje są dystrybuowane centralnie, a wykrycia są gromadzone w jednym miejscu do oceny.

Jak to wykazać: Konfiguracja centralnej konsoli zarządzania, raport o stanie aktualizacji wszystkich podłączonych komponentów oraz analiza zgłoszonych wykryć w danym okresie czasu. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 3.3

Funkcje bezpieczeństwa systemu są weryfikowane w zaplanowanych odstępach czasu oraz po zmianach, aby potwierdzić, że faktycznie działają. Testy są planowane tak, aby nie zagrażały eksploatacji zakładu, a wyniki są rejestrowane.

[Dokument](#)

Jak to wykazać: Plan testów wskazujący przedmiot testu, odstęp czasu i okno czasowe, wraz z zapisami testów pokazującymi datę, osobę testującą, zachowanie oczekiwane i zachowanie zaobserwowane. Przydatne pojedyncze testy to: logowanie kontem wyłączonym kończy się niepowodzeniem, antywirus reaguje na plik testowy, dostęp zdalnej obsługi serwisowej jest nieosiągalny bez zwolnienia. Małe zakłady dołączają testowanie do postępu konserwacyjnego, który i tak jest planowany, i przechodzą przez ustaloną listę kontrolną. Wymagane od SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

[Dowód / uzasadnienie](#)

SR 3.3 RE 1

Weryfikacja funkcji bezpieczeństwa przebiega za pomocą środków zautomatyzowanych, tak aby była powtarzalna bez wysiłku ręcznego i dawała spójny wynik.

Jak to wykazać: Skrypty lub narzędzia testowe wraz z ich harmonogramem, plikami wynikowymi oraz porównaniem kilku przebiegów pokazującym, że odchylenia są wykrywane. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

[Dowód / uzasadnienie](#)

SR 3.3 RE 2

Weryfikacja funkcji bezpieczeństwa jest możliwa również podczas normalnej eksploatacji, bez konieczności zatrzymywania zakładu lub wprowadzania go w stan specjalny.

Jak to wykazać: Opis procedury testowej wraz z dowodem, że nie wywiera niekorzystnego wpływu na proces, na przykład analiza wpływu na czasy cykli i obciążenie sieci, wraz z zapisami testów pobranymi z eksploatacji produkcyjnej. Rozszerzenie wymagania, wymagane od SL 4.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

[Dowód / uzasadnienie](#)

SR 3.4

Nieautoryzowane zmiany oprogramowania, firmware'u i informacji przechowywanych są wykrywane. Dotyczy to w równym stopniu programów sterujących, zestawów parametrów, receptur i plików konfiguracyjnych.

Jak to wykazać: Inwentaryzacja wersji wymagających ochrony wraz z przechowywanymi wartościami kontrolnymi lub podpisami, wyniki porównań integralności oraz udokumentowane uzgodnienie z wersją przechowywaną w kontroli wersji. Małe zakłady przechowują zwolnioną wersję programu wraz z jej sumą kontrolną w lokalizacji zabezpieczonej przed zapisem i porównują w razie podejrzenia lub po konserwacji. Wymagane od SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

[Dowód / uzasadnienie](#)

SR 3.4 RE 1

Jeśli wykryte zostanie naruszenie integralności oprogramowania lub informacji, system zgłasza to automatycznie do odpowiedzialnego punktu, bez konieczności aktywnego wyszukiwania tego przez kogokolwiek.

Jak to wykazać: Konfiguracja ścieżek powiadamiania (alarm w sterowni, e-mail, komunikat do systemu monitorowania), lista odbiorców z ustawieniami zastępstwa oraz co najmniej jeden alarm testowy z udokumentowanym czasem reakcji. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

[Dowód / uzasadnienie](#)

SR 3.5

Dane wejściowe przyjmowane przez system z danych procesowych, interfejsów lub interfejsów użytkownika są sprawdzane pod kątem dozwolonej składni, dozwolonego zakresu wartości i dozwolonej długości przed przetworzeniem. Nieprawidłowe dane wejściowe nie prowadzą do niekontrolowanego zachowania.

Jak to wykazać: Specyfikacja granic i formatów dla każdego wejścia, wyciągi z logiki walidacji w sterowniku lub aplikacji oraz przypadki testowe z celowo nieprawidłowymi danymi wejściowymi (wartość zbyt duża, błędny typ danych, zbyt długi ciąg znaków) wraz z udokumentowanym zachowaniem systemu. Małe zakłady rejestrują granice wiarygodności dla każdego punktu pomiarowego w tabeli i weryfikują je podczas uruchomienia. Wymagane od SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

[Dowód / uzasadnienie](#)

SR 3.6 Na wypadek usterki określone jest, jaki stan przyjmują wyjścia do zakładu, a system przyjmuje dokładnie ten stan. Określony stan jest zgodny z bezpieczeństwem funkcjonalnym zakładu.

Jak to wykazać: Definicja dla każdego wyjścia lub grupy wyjść (utrzymanie wartości, określona wartość zastępcza, bezpieczny stan wyłączenia) z uzasadnieniem z oceny ryzyka, wyciąg z konfiguracji sterownika oraz dowód z testu awarii, na przykład zerwanie przewodu lub utrata komunikacji, pokazujący oczekiwane zachowanie. Wymagane od SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 3.7 System obsługuje warunki błędu w taki sposób, że eksploatacja pozostaje pod kontrolą, a nie zostają ujawnione informacje, które pomogłyby atakującemu. Komunikaty o błędach pokazywane operatorom pozostają zwięzłe, natomiast szczegóły techniczne trafiają wyłącznie do zapisów wewnętrznych.

Jak to wykazać: Przegląd klas błędów z zachowaniem systemu przewidzianym dla każdej z nich, przykłady wyświetlanych komunikatów w zestawieniu z odpowiadającymi im wewnętrznymi wpisami dziennika oraz dowód testowy, że na interfejsie operatorskim nie pojawiają się ścieżki plików, nazwy kont, wyniki bazy danych ani szczegóły wersji. Wymagane od SL 1.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 3.8 Aktywne sesje są chronione przed przejęciem oraz przed wstrzykiwaniem obcych komunikatów. Sesja kończy się po wylogowaniu lub po określonym czasie bez aktywności, a potem nie może zostać ponownie wykorzystana.

Jak to wykazać: Konfiguracja zarządzania sesjami z ustawionymi limitami czasu bezczynności i maksymalnego czasu trwania, dowód mechanizmu chroniącego przed powtórzeniem komunikatu oraz zapis testu, w którym przechwycona sesja przestaje działać po wylogowaniu. Wymagane od SL 2.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 3.8 RE 1 Identyfikatory sesji tracą ważność wraz z zakończeniem sesji i nie są ponownie akceptowane przez system, nawet gdy zostaną ponownie przedstawione z zewnątrz.

Jak to wykazać: Wyciąg z konfiguracji zarządzania sesjami obejmujący unieważnianie, wraz z zapisem testu, w którym wcześniej ważny identyfikator jest ponownie wysyłany po wylogowaniu i zostaje odrzucony przez system. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 3.8 RE 2 Dla każdej nowej sesji generowany jest dedykowany identyfikator jednorazowego użytku. Identyfikatory nie są ponownie wykorzystywane między sesjami, użytkownikami ani urządzeniami.

Jak to wykazać: Opis procedury generowania oraz dowód z dziennika lub przechwyty ruchu, że kilka kolejnych logowań otrzymuje różne identyfikatory. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 3.8 RE 3 Identyfikatory sesji są generowane za pomocą uznanych mechanizmów losowych, tak aby nie można ich było ani odgadnąć, ani wyprowadzić z poprzednich identyfikatorów.

Jak to wykazać: Wskazanie zastosowanego generatora liczb losowych i jego źródła entropii, deklaracja dostawcy lub raport z testu na ten temat oraz statystyczna ocena próbki wygenerowanych identyfikatorów. Rozszerzenie wymagania, wymagane od SL 4.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 3.9

Zapisy związane z bezpieczeństwem oraz narzędzia stosowane do ich oceny są chronione przed nieautoryzowanym dostępem, modyfikacją i usunięciem. Krąg osób uprawnionych do zmiany lub usuwania zapisów jest wąski i nazwany.

[Dokument](#)

Jak to wykazać: Koncepcja uprawnień dla danych dziennika z nazwanym przypisaniem, konfiguracja przekazywania do osobnego systemu rejestrowania, okresy przechowywania oraz dowód testowy, że zwykły operator nie może usunąć wpisów. Małe zakłady przekazują dzienniki na osobne urządzenie, do którego operatorzy zakładu nie mają dostępu do zapisu. Wymagane od SL 2.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 3.9 RE 1

Zapisy związane z bezpieczeństwem są dodatkowo przechowywane na nośniku wykluczającym późniejsze nadpisanie, tak aby raz zapisany wpis nie mógł już zostać zmieniony, nawet z uprawnieniami administracyjnymi.

[Dokument](#)

Jak to wykazać: Opis zastosowanego nośnika przechowywania (nośnik jednokrotnego zapisu, archiwum odporne na manipulacje, stałe rozszerzanie łańcuch podpisów), dowód nieudanej próby zmiany wpisu oraz zasada przechowywania i wyszukiwania nośników. Rozszerzenie wymagania, wymagane od SL 3.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

8 FR 4: Poufność danych

6

SR 4.1

System automatyki chroni informacje poufne przed nieautoryzowanym ujawnieniem, zarówno podczas przesyłania, jak i podczas przechowywania. Określone jest, które dane uznaje się za poufne, na przykład receptury, zestawy parametrów, dane uwierzytelniające, pliki konfiguracyjne lub dane diagnostyczne z odniesieniem do osób.

[Dokument](#)

Jak to wykazać: Lista rodzajów danych wymagających ochrony ze wskazaniem, gdzie są przechowywane i jak są przesyłane, wraz z konkretnym środkiem ochronnym dla każdej pozycji, na przykład połączenie szyfrowane, zaszyfrowany nośnik danych lub udział z ograniczonym dostępem. Mały zakład radzi sobie z jednostronicową tabelą: rodzaj danych, gdzie się znajdują, kto może je zobaczyć, co je chroni. Wymagane od SL 1.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 4.1 RE 1

Dla informacji przesyłanych przez niezaufane sieci lub przechowywanych poza chronionym środowiskiem poufność jest wymuszana środkami technicznymi, a nie jedynie obiecywana w regule organizacyjnej.

Jak to wykazać: Wyciąg z konfiguracji stosowanego szyfrowania transportu lub szyfrowania przechowywania, na przykład profil VPN dla zdalnej obsługi serwisowej, ustawienia TLS interfejsu systemu sterowania lub szyfrowanie nośników kopii zapasowych. Jako dowód wystarczy opatrzonej datą zrzut ekranu aktywnego ustawienia. Wymagane od SL 2, nie od SL 1, ponieważ jest to rozszerzenie wymagania.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 4.1 RE 2

Poufność jest wymuszana również na granicach między strefami, tak aby informacja nie stawała się widoczna jawnym tekstem przy przejściu z jednej strefy do drugiej.

Jak to wykazać: Plan stref i kanałów wskazujący, które przejścia są szyfrowane, wraz z konfiguracją komponentu granicznego, takiego jak brama, zapora sieciowa lub dioda danych. Przechwyt ruchu lub zapis testu pokazujący, że na granicy nie pojawiają się dane w postaci jawnej. Wymagane od SL 4.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 4.2

Określone jest, w jaki sposób informacje poufne są niezawodnie usuwane, gdy urządzenia są wycofywane z eksploatacji, zmieniają właściciela, są przekazywane do naprawy lub są ponownie wykorzystywane, tak aby nie pozostały żadne czytelne dane resztkowe.

[Dokument](#)

Jak to wykazać: Pisemna procedura wycofania z eksploatacji z metodą oczyszczenia danych dla każdego typu urządzenia, wraz z zapisami kasowania podającymi identyfikację urządzenia, datę i osobę, która to wykonała. Mały zakład zapisuje to jako jeden wiersz na urządzenie we wspólnej liście i archiwizuje obok niej certyfikaty zewnętrznych firm utylizacyjnych. Wymagane od SL 2.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 4.2 RE 1 Współdzielone obszary pamięci są czyszczone przed ponownym przydzieleniem innemu użytkownikowi lub procesowi, tak aby zawartość należąca do poprzedniego użytkownika nie mogła zostać odczytana.

Jak to wykazać: Oświadczenie dostawcy lub zapis konfiguracji obejmujący czyszczenie ponownie wykorzystywanej pamięci i obszarów buforowych, uzupełniony zapisem testu z odbioru lub konserwacji. Tam, gdzie komponent nie potrafi tego wykonać, jako dowód służy udokumentowany środek kompensujący, na przykład niedzielenie urządzenia między różne role. Wymagane od SL 3, nie od SL 1, ponieważ jest to rozszerzenie wymagania.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 4.3 Wszędzie tam, gdzie stosowana jest kryptografia, algorytmy, długości kluczy i postępowanie z kluczami są zgodne z uznaną dobrą praktyką, a określone jest, w jaki sposób klucze są generowane, dystrybuowane, przechowywane, rotowane i unieważniane.

[Dokument](#)

Jak to wykazać: Przegląd mechanizmów stosowanych w każdym systemie, z podaniem algorytmu, długości klucza i okresu ważności, wraz z zasadami zarządzania kluczami oraz zapisami rotacji kluczy i odnowień certyfikatów. Jako miernik służą publiczne zalecenia, na przykład wytyczne techniczne niemieckiego BSI. Mały zakład prowadzi listę certyfikatów z terminami ważności i przypomnieniem ≥ 30 dni przed wygaśnięciem. Wymagane od SL 1.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

9 FR 5: Ograniczony przepływ danych, strefy i kanały

11

SR 5.1 System sterowania można podzielić na oddzielne strefy, a ruch między tymi strefami przechodzi wyłącznie przez określone kanały. Podział opiera się na uzasadnieniu, które można wyjaśnić, na przykład potrzebą ochrony, własnością lub funkcją zaangażowanych odcinków zakładu.

[Dokument](#)

Jak to wykazać: Schemat sieci pokazujący strefy i kanały między nimi, lista stref z uzasadnieniem dla każdej granicy oraz konfiguracja komponentów separujących, takich jak definicje VLAN lub interfejsy zapory sieciowej. Mały zakład radzi sobie z jednostronicowym szkicem pokazującym biuro, sieć maszynową i dostęp zdalny jako trzy pola z połączeniami między nimi, wraz ze zrzutem ekranu konfiguracji VLAN przełącznika.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 5.1 RE 1 Separacja stref jest realizowana fizycznie, to znaczy za pomocą dedykowanych komponentów sieciowych i dedykowanego okablowania, i nie opiera się wyłącznie na konfiguracji logicznej wewnątrz współdzielonych urządzeń. Punkt 9.1 na tej liście, wymagane od SL 2. Rozszerzenia wymagań tej normy nigdy nie są obowiązkowe już na SL 1.

Jak to wykazać: Inwentaryzacja komponentów sieciowych wskazująca, który switch lub router obsługuje którą strefę, zdjęcia lub układ szafy rozdzielczych rozdzielni, oznakowanie kabli. Małe zakłady wykazują to za pomocą dwóch oddzielnych, wyraźnie oznakowanych switchy zamiast jednego współdzielonego urządzenia oraz zdjęcia szafy sterowniczej w dokumentacji zakładu.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 5.1 RE 2 Sieć automatyki może być eksploatowana niezależnie od sieci spoza automatyki. Jeśli zawiedzie informatyka biurowa lub łącze zewnętrzne, sterowanie i monitorowanie zakładu nadal działają. Wymagane od SL 3.

Jak to wykazać: Lista zależności usług wykorzystywanych wewnątrz sieci automatyki, takich jak serwer czasu, rozwiązywanie nazw, usługa katalogowa lub serwer licencji, ze wskazaniem, gdzie każda z nich jest hostowana, wraz z zapisem próby rozłączenia, w której odłączono łącze do informatyki biurowej. Mały zakład odnotowuje wynik takiej próby w dzienniku konserwacji: łącze uplink odłączone, zakład nadal działał, brakowało jedynie raportów biurowych.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 5.1 RE 3 Strefy pełniące szczególnie krytyczne funkcje, na przykład funkcje bezpieczeństwa lub ochrony, są oddzielone od pozostałych stref zarówno logicznie, jak i fizycznie. Wymagane od SL 4.

Jak to wykazać: Oznaczenie stref krytycznych na schemacie stref wraz z uzasadnieniem klasyfikacji, dowód dedykowanych komponentów sieciowych i dedykowanego okablowania dla tych stref, konfiguracja kanałów wraz z dowodem, że nie istnieje żadna ścieżka współdzielona.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 5.2 Na granicach stref ruch jest kontrolowany, monitorowany oraz dopuszczany lub odrzucany zgodnie z określonymi regułami. Nie istnieje żadna ścieżka między dwiema strefami, która omijałaby ten punkt kontrolny.

Jak to wykazać: Eksportowany zbiór reguł zapory sieciowej lub urządzenia granicznego, dzienniki połączeń odrzuconych i dopuszczonych, dowód nieistnienia ścieżek bocznych, na przykład poprzez sprawdzenie dodatkowych kart sieciowych, modemów lub routerów komórkowych w komputerach zakładowych. Mały zakład wykazuje to eksportem reguł swojej jedynej zapory sieciowej oraz krótką notatką z obchodu potwierdzającą, że w żadnej szafie sterowniczej nie znajduje się nieplanowany router.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 5.2 RE 1 Zbiór reguł na granicy strefy działa na zasadzie, że wszystko jest zabronione, chyba że zostało jawnie dozwolone. Każda reguła zezwalająca jest indywidualnie uzasadniona i powiązana z celem. Wymagane od SL 2.

Jak to wykazać: Zbiór reguł z widoczną regułą końcową odrzucającą resztę ruchu oraz lista zezwoleń wskazująca źródło, cel, usługę, cel biznesowy i osobę odpowiedzialną dla każdej reguły. Małe zakłady prowadzą tę listę jako pięciokolumnową tabelę obok eksportu zapory sieciowej i przeglądają ją raz w roku pod kątem reguł, których nikt już nie potrzebuje.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 5.2 RE 2 Sieć automatyki można świadomie odciąć od wszystkich połączeń zewnętrznych i utrzymać w trybie wyspowym. Działanie to można wywołać bez konieczności zatrzymywania zakładu. Wymagane od SL 3.

Jak to wykazać: Opis procedury izolacji wskazujący, kto i w jaki sposób może ją wywołać, dowód technicznej realizacji, na przykład awaryjny zbiór reguł lub oznakowany przełącznik izolujący, wraz z zapisem ćwiczenia, w którym izolacja została faktycznie przećwiczona. Mały zakład przeprowadza ćwiczenie raz w roku podczas konserwacji i odnotowuje datę, czas trwania i wszelkie nieprawidłowości.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 5.2 RE 3 Jeśli urządzenie na granicy strefy ulegnie awarii lub utraci swoje reguły, odrzuca ruch zamiast go przepuszczać. Awaria nie może pozostawić po sobie otwartego połączenia. Wymagane od SL 4.

Jak to wykazać: Oświadczenie dostawcy lub dowód konfiguracji dotyczący zachowania komponentu przy usterce i przy ponownym uruchomieniu, zapis testu celowo wywołanej awarii z zaobserwowanym wynikiem, zgodność z oceną ryzyka zakładu, ponieważ granica odrzucająca ruch może sama w sobie mieć konsekwencje zależne od procesu.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 5.3 Ogólne usługi komunikacji między osobami, takie jak poczta elektroniczna, komunikatory lub połączenia wideo, mogą być blokowane na urządzeniach automatyki i wewnątrz sieci automatyki. Zakres blokady jest określony i uzasadniony.

Jak to wykazać: Definicja, które usługi są niedozwolone w sieci automatyki, wraz z realizacją techniczną: zablokowane porty i cele w zbiorze reguł, usunięte lub zablokowane aplikacje na stacjach operatorskich, dowód z inwentaryzacji oprogramowania urządzeń. Mały zakład rozwiązuje to blokadą aplikacji na stacji HMI oraz regułą, że wychodzący ruch pocztowy i internetowy z sieci maszynowej jest zabroniony.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 5.3 RE 1 Takie usługi komunikacji między osobami są zablokowane w całej sieci automatyki, a nie jedynie częściowo ograniczone lub ograniczone do poszczególnych urządzeń. Wymagane od SL 2.

Jak to wykazać: Dowód, że blokada dotyczy każdego urządzenia w strefie, na przykład poprzez przegląd zainstalowanego oprogramowania na każdym komputerze w strefie oraz test połączenia z dowolnego komputera zakładowego. Małe zakłady wykazują to listą urządzeń, w której każdy wiersz jest odznaczony z datą sprawdzenia, oraz zrzutem ekranu nieudanej próby połączenia.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 5.4 Dane aplikacji i funkcje aplikacji są podzielone tak, aby procesy o różnych potrzebach ochrony lub różnych uprawnieniach nie mogły sięgać do tych samych obszarów. Separacja jest zaprojektowana w architekturze systemu, a nie pozostawiona przypadkowi instalacji.

Jak to wykazać: Przegląd aplikacji wskazujący, z jakich danych i usług korzystają i jakie konta za nimi stoja, konfiguracja oddzielnych instancji, baz danych, katalogów lub maszyn wirtualnych oraz lista uprawnień dla każdego obszaru. Mały zakład rozwiązuje to oddzielnymi kontami użytkowników i oddzielnymi folderami danych dla inżynierii i eksploatacji, wraz z notatką, która aplikacja ma dostęp do którego folderu.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

10 FR 6: Terminowa reakcja na zdarzenia

3

SR 6.1 Zapisy audytu zgromadzone w systemie mogą być odczytywane i oceniane przez osoby i role upoważnione do tego celu bez zakłócania bieżącej eksploatacji zakładu, a sam dostęp do tych zapisów jest ograniczony do użytkowników upoważnionych.

Jak to wykazać: Macierz ról i uprawnień pokazująca, kto może przeglądać dane dziennika, wraz ze zrzutem ekranu lub eksportem faktycznie pobranego widoku dziennika, opatrzonym znacznikiem czasu. Dodać krótką notatkę o ścieżce wykorzystanej do pobrania, na przykład interfejs operatorski sterownika, serwer dziennika lub eksport pliku. Małe zakłady radzą sobie z jednostronicowym przeglądem dla każdego zakładu: gdzie znajduje się dziennik, kto ma dostęp do odczytu, jak jest pobierany. Testowe pobranie raz w roku, odnotowane w dzienniku konserwacji, pokazuje, że ścieżka działa. Dotyczy od SL 1 dla wszystkich poziomów bezpieczeństwa.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 6.1 RE 1 Zapisy audytu mogą być pobierane za pośrednictwem interfejsu maszynowego, tak aby narzędzia analityczne mogły je dalej przetwarzać bez ręcznego przepisywania, a dane są udostępniane w udokumentowanym, powszechnie stosowanym formacie.

Jak to wykazać: Opis stosowanego interfejsu wraz z formatem, na przykład syslog, OPC UA Alarms and Conditions, zapytanie REST lub eksport CSV, wraz z przykładowym zapisem i konfiguracją systemu odbiorczego. Dowodem może być wyciąg z konfiguracji SIEM lub kolektora dzienników wraz z potwierdzeniem napływających zapisów. Bez SIEM wystarczy kolektor dzienników na prostym serwerze, który nocą pobiera dzienniki skryptem i je zapisuje; dowodem jest sam skrypt wraz z wykazem katalogu zgromadzonych plików. Jako rozszerzenie jest to wymagane dopiero od SL 3, nie od SL 1.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 6.2 Aktywność istotna dla bezpieczeństwa w systemie jest monitorowana w sposób ciągły, monitorowanie wykrywa próby ataków i nadużycia oraz niezwłocznie zgłasza je nazwanemu punktowi kontaktowemu, a narzędzia, ścieżki zgłaszania i zakresy odpowiedzialności stosowane w tym celu są określone.

Jak to wykazać: Przegląd narzędzi monitorowania dla każdej strefy, na przykład sensor sieciowy, alerty antywirusowe, alarmy zapory sieciowej lub kontrola integralności, ze wskazaniem, kto otrzymuje alert i w jakich ramach czasowych oczekiwana jest reakcja. Jako dowód służą konfiguracje alarmów, lista alertów zgłoszonych w ostatnich miesiącach oraz notatki dotyczące ich obsługi. Małe zakłady nie potrzebują całodobowej sterowni: wystarczy współdzielona skrzynka pocztowa lub skrzynka zgłoszeń gromadząca alerty z istniejących systemów, wraz ze stałą zasadą, że nazwana osoba przegląda ją każdego dnia roboczego, co jest wykazywane historią skrzynki pocztowej. Wymagane od SL 2.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

11 FR 7: Dostępność zasobów

13

SR 7.1 W warunkach przeciążenia lub celowych ataków zalewowych system pozostaje w określonym stanie pracy, zasadnicze funkcje sterujące nadal działają, a awaria pojedynczej usługi nie pociąga za sobą zakładu.

Jak to wykazać: Konfiguracja mechanizmów ochronnych (ograniczenie szybkości, limity połączeń, kontrola sztormu rozgłoszeniowego na switchach), oświadczenia dostawców dotyczące zachowania pod obciążeniem, wraz z zapisem testu obciążeniowego lub rzeczywistego zdarzenia przeciążenia z obserwacją funkcji sterującej. Wymagane od SL 1. Mały zakład pokrywa to zrzutami ekranu ustawień switcha i zapory sieciowej oraz krótką notatką, która funkcja nadal działała podczas testu najważniejszej komórki.

Otwarte W toku Spełnione Nie dotyczy

Dowód / uzasadnienie

SR 7.1 RE 1 Obciążenie komunikacyjne, jakie poszczególne komponenty mogą wprowadzić do sieci, jest ograniczone, tak aby uszkodzony lub przejęty komponent nie mógł zalać segmentu sieci.

Jak to wykazać: Limity przepustowości i multicastu dla każdego portu na komponentach sieciowych, dowód ograniczenia dla każdego połączenia, wraz z pomiarem faktycznego bazowego obciążenia dla każdego urządzenia. Wymagane od SL 2, nie od SL 1. Bez switchy zarządzalnych ta pozycja nie może zostać wykazana, i wtedy jest to punkt otwarty.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 7.1 RE 2 Sytuacja przeciążenia wewnątrz rozpatrywanego systemu nie przenosi się na systemy lub sieci sąsiednie; wpływ na zewnątrz jest technicznie ograniczony.

Jak to wykazać: Reguły segmentacji i filtrowania na granicach, dowód ograniczenia ruchu wychodzącego, wraz z zapisem testu pokazującym, że obciążenie wygenerowane w sieci komórki nie pogorszyło pracy sieci biurowej ani sąsiedniej. Wymagane od SL 3.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 7.2 Wykorzystanie czasu przetwarzania, pamięci, przestrzeni dyskowej i przepustowości sieci jest ograniczone w taki sposób, że pojedynczy proces lub usługa nie może zużyć zasobów potrzebnych do sterowania.

Jak to wykazać: Konfiguracja limitów zasobów (kwoty, priorytety procesów, limity pamięci), ocena monitorowania wykorzystania w reprezentatywnym okresie, wraz z progami, przy których wywoływane jest ostrzeżenie. Wymagane od SL 1. Małe zakłady korzystają z wbudowanych środków systemu operacyjnego oraz prostego monitorowania z alertem o przestrzeni dyskowej i CPU wysyłanym e-mailem.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 7.3 Istnieją kopie zapasowe konfiguracji systemu, danych aplikacji i wersji programów; można je wykonywać bez przerywania bieżącej eksploatacji, a są one chronione przed nieautoryzowanym dostępem i modyfikacją.[Dokument](#)

Jak to wykazać: Koncepcja kopii zapasowych obejmująca zakres, częstotliwość i okres przechowywania, dzienniki kopii zapasowych z najnowszych przebiegów, wraz z dowodem ochrony dostępu do nośników kopii zapasowych (osobne przechowywanie, szyfrowanie, dedykowane uprawnienia). Wymagane od SL 1. Mały zakład wykonuje kopie zapasowe projektów PLC i wersji HMI na zaszyfrowany nośnik, który jest fizycznie odłączany po wykonaniu kopii, i odnotowuje datę oraz wersję na prostej liście.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 7.3 RE 1 Zweryfikowano przydatność kopii zapasowych do użycia; wykazano, że można z nich faktycznie przywrócić działający stan.

Jak to wykazać: Zapis próby przywrócenia z datą, testowaną wersją kopii zapasowej, systemem docelowym i wynikiem, co najmniej dla komponentów krytycznych. Wymagane od SL 2, nie od SL 1. Małe zakłady sprawdzają wrywkowo raz w roku jeden program PLC i jeden obraz HMI na urządzeniu zapasowym i odnotowują wynik w dwóch zdaniach.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 7.3 RE 2 Kopia zapasowa wykonywana jest automatycznie według określonego harmonogramu; nieudany przebieg jest wykrywany i zgłaszany.

Jak to wykazać: Harmonogram zadania kopii zapasowej, dzienniki wykonania bez luk, wraz z dowodem powiadomienia o niepowodzeniu dla przebiegu, który się nie powiódł (alarm, zgłoszenie, e-mail). Wymagane od SL 3.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 7.4

Po zakłóceniu, awarii lub ataku system można przywrócić do znanego, bezpiecznego stanu; przywracanie zostało przećwiczone, a zakresy odpowiedzialności są nazwane.

[Dokument](#)

Jak to wykazać: Plan ponownego uruchomienia dla każdego komponentu krytycznego z kolejnością, wymaganymi nośnikami, kontaktami i czasem docelowym, wraz z zapisem najnowszego ćwiczenia przywracania. Wymagane od SL 1. Mały zakład radzi sobie z jednostronicową kartą ponownego uruchomienia dla każdej linii, przechowywaną w szafie sterowniczej i sprawdzaną przy każdej wymianie części zamiennej.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 7.5

Jeśli zawiedzie regularne zasilanie, system przechodzi w określony stan: albo zasilanie jest utrzymywane przez źródło zapasowe, albo następuje uporządkowane wyłączenie bez utraty bezpiecznego stanu.

Jak to wykazać: Dowód doboru wielkości i konserwacji zasilacza bezprzerwowego lub agregatu awaryjnego, zapis najnowszego testu akumulatora lub testu obciążeniowego, wraz z opisem zachowania przy przełączeniu i przy powrocie zasilania sieciowego. Wymagane od SL 1. Małe zakłady testują UPS pod obciążeniem raz w roku i odnotowują datę testu, czas podtrzymania i wiek akumulatora.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 7.6

Ustawienia sieciowe i bezpieczeństwa systemu są ustalone na zatwierdzony stan docelowy, odchylenia od tego stanu docelowego są wykrywalne, a stan bieżący można w każdej chwili odczytać.

[Dokument](#)

Jak to wykazać: Zatwierdzona konfiguracja docelowa dla każdej klasy urządzeń (specyfikacja utwardzenia), bieżące stany konfiguracji urządzeń, wraz z wynikiem porównania stanu docelowego z rzeczywistym wraz z listą odchyłeń i przyczyną każdego z nich. Wymagane od SL 1. Mały zakład przechowuje eksporty konfiguracji w systemie kontroli wersji i porównuje je przed i po każdej zmianie.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 7.6 RE 1

Bieżący stan ustawień bezpieczeństwa można wyeksportować w formie czytelnej maszynowo, tak aby można go było automatycznie sprawdzić względem stanu docelowego.

Jak to wykazać: Przykładowy wynik w formacie czytelny maszynowo (eksport konfiguracji, plik strukturalny, zapytanie interfejsu) oraz skrypt lub narzędzie wykonujące porównanie ze stanem docelowym, wraz z raportem wyniku jednego przebiegu. Wymagane od SL 3.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 7.7

System jest ograniczony do funkcji potrzebnych do eksploatacji; usługi, porty, protokoły i interfejsy, które nie są wymagane, są wyłączone lub usunięte.

Jak to wykazać: Lista aktywnych usług i otwartych portów dla każdego komponentu wraz z uzasadnieniem potrzeby, dowód, że pozostałe są wyłączone (konfiguracja, wynik skanowania portów), wraz z zasadą dla interfejsów USB i serwisowych. Wymagane od SL 1. Małe zakłady przeprowadzają proste skanowanie portów dla każdego segmentu i uzasadniają każdą otwartą pozycję w jednej linii.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie

SR 7.8

Dostępna jest aktualna inwentaryzacja wszystkich komponentów systemu wraz z producentem, typem, wersją firmware lub oprogramowania oraz adresem sieciowym, i jest ona aktualizowana przy każdej zmianie.

[Dokument](#)

Jak to wykazać: Inwentaryzacja komponentów wraz z datą rewizji i właścicielem, dowód utrzymania poprzez historię zmian, wraz z porównaniem z wynikiem wykrywania sieciowego w celu znalezienia urządzeń niezarejestrowanych. Wymagane od SL 2, nie od SL 1. Mały zakład prowadzi inwentaryzację jako tabelę i aktualizuje ją jako stałą zasadę przy każdej wymianie urządzenia i każdej aktualizacji firmware.

Otwarte	W toku	Spełnione	Nie dotyczy
---------	--------	-----------	-------------

Dowód / uzasadnienie