

„Strefy i kanały” w sieciach automatyki: zabezpieczenia gwarancją bezpieczeństwa

Bezpieczeństwo jest naszym najwyższym priorytetem

Ostfildern, lipiec 2026 – **Rozporządzenie w sprawie maszyn nakłada taki obowiązek: zabezpieczenia przemysłowe mają na celu ochronę funkcji bezpieczeństwa przed manipulacją – innymi słowy, zabezpieczenia są warunkiem koniecznym dla prawidłowego działania systemów bezpieczeństwa. Ale jak zapewnić kompleksową ochronę sieci automatyki? Normy takie jak IEC 62443-3-2 oraz przyszła norma EN 50742 wyznaczają jasny kierunek: podział systemów na strefy oraz monitorowanie złączy – zasada ta przewija się we wszystkich aktualnych zaleceniach organizacji branżowych i ekspertów. Firma Pilz jest przekonana, że klucz do skutecznego bezpieczeństwa maszyn stanowi ściśle rozdzielenie bezpieczeństwa od tzw. standardowej automatyki – oparte na zasadzie Defence-in-Depth i realizowane poprzez podejście oparte na strefach i kanałach.**

Dom można zbudować w taki sposób, aby był solidny i bezpieczny: z solidnymi ścianami, materiałami ognioodpornymi, niezawodną instalacją elektryczną i sprawnymi czujnikami dymu. To bezpieczeństwo konstrukcyjne stanowi doskonały przykład bezpieczeństwa maszyn, gdzie rozwiązania konstrukcyjne, technologia czujników i mechanizmy zabezpieczające mają na celu zapobieganie niepożądanym zagrożeniom. Jednak taki dom pozostaje bezpieczny tylko wtedy, gdy nie jest narażony na celowe

zakłócenia. Manipulowanie elementami sterującymi ogrzewaniem, sabotaż obwodów elektrycznych lub wyłączenie systemów alarmowych może sprawić, że budynek zaprojektowany z myślą o bezpieczeństwie stanie się zagrożeniem. W świecie maszyn nawet najlepsze rozwiązania konstrukcyjne zapewniające bezpieczeństwo tracą swoją skuteczność, jeśli elementy związane z bezpieczeństwem zostaną naruszone lub wyłączone bez autoryzacji.

W tym kontekście security pełni stanowisko ochrony zewnętrznej: solidne drzwi, zabezpieczone punkty przyłączeniowe, monitorowane złącza oraz bariery chroniące przed nieuprawnionymi ingerencjami. Zatem security nie chroni przed samymi wypadkami, lecz zapobiega wyłączeniu mechanizmów ochronnych – na przykład przez osoby, które uzyskują dostęp przez nieuprawniony wybór trybu pracy lub wykonanie nieuprawnionej czynności. Tylko w ten sposób można zapewnić niezawodną skuteczność środków bezpieczeństwa – Security for Safety.

Od wymogów regulacyjnych do proponowanego rozwiązania

Po raz pierwszy rozporządzenie w sprawie maszyn (UE) 2023/1230 wprowadza wymóg, zgodnie z którym zabezpieczenia muszą stanowić obowiązkowy element zapewniający bezpieczeństwo podczas eksploatacji maszyn i instalacji: funkcji bezpieczeństwa nie wolno naruszać w wyniku manipulacji, niezależnie od tego, czy są zamierzone, czy też nie. Właśnie tutaj pojawia się nowa norma EN 50742; pomoże wyjaśnić podstawowe wymagania w zakresie zabezpieczeń określone w Rozporządzeniu w sprawie maszyn. Norma określa dane techniczne dotyczące zabezpieczeń przed uszkodzeniami oraz jasne wymagania dotyczące sprzętu, oprogramowania i danych, które mogą mieć wpływ na funkcje bezpieczeństwa. Norma obejmuje cały cykl życia – od etapu

projektowania, przez eksploatację aż po wycofanie z eksploatacji. Kluczową rolę odgrywa również istniejąca seria standardów IEC 62443, która określa systematyczne podejście do cyberbezpieczeństwa w przemysłowych systemach automatyzacji i sterowania. Stanowi ustrukturyzowane ramy dla analizy ryzyka, „Defence-in-Depth” oraz zasady segmentacji („strefy i kanały”) i jest jednoznacznie uznana w normie EN 50742 jako alternatywne lub uzupełniające podejście do zapewnienia security. Wszystkie te normy stanowią normatywny trzon koncepcji „Security for Safety”: wymagają, aby integralność cyfrowa maszyny była uznawana za warunek konieczny jej bezpieczeństwa funkcjonalnego i była odpowiednio chroniona.

Dlaczego „strefy i kanały” zwiększają bezpieczeństwo maszyn

Wracając do przykładu domu: kotłownia symbolizuje strefę, natomiast złącze z bramką inteligentnego domu – odpowiadający jej przewód. Manipulacje przy tym złączu mogą mieć wpływ na cały system – nawet jeśli pomieszczenie jest doskonale zabezpieczone. Dlatego też kluczowe znaczenie ma nie tylko ochrona poszczególnych stref, lecz także zabezpieczenia tras, które je łączą. Właśnie w tym momencie do gry wkracza zasada „stref i kanałów”. Strefy są wyraźnie oddzielone od siebie, a przejścia między nimi zostały zaprojektowane w taki sposób, aby umożliwić ich monitorowanie. Podobnie jak w domu, gdzie drzwi i przypisane do nich klucze decydują o tym, kto ma dostęp do poszczególnych pomieszczeń, tak w zakładzie przemysłowym ochrona wewnętrzna (bezpieczeństwo) i ochrona zewnętrzna przed manipulacją (zabezpieczenie) są ze sobą strukturalnie powiązane.

W rezultacie powstała koncepcja zabezpieczeń oparta na zasadzie Defence-in-Depth: bezpieczeństwa nie zapewnia pojedyncza bariera,

lecz szereg kolejnych warstw zabezpieczeń. Jeśli uda się pokonać jedną warstwę, kolejna pozostaje nienaruszona. Strefy tworzą te wielopoziomowe przestrzenie, natomiast kanały stanowią monitorowane przejścia między nimi. W ten sposób pojedyncza wrażliwość nie może narazić na niebezpieczeństwo całego systemu – zwłaszcza gdy w grę wchodzi bezpieczeństwo, a tym samym ochrona ludzi.

Firma PILZ konsekwentnie realizuje tę koncepcję pod hasłem „Security for Safety”, gdzie bezpieczeństwo (Safety) stanowi nadrzędny cel ochrony zapewnianej przez systemy zabezpieczeń (Security). Najważniejsze jest zapewnienie bezpieczeństwa, które z kolei chroni ludzi. Właśnie dlatego firma Pilz oddziela systemy bezpieczeństwa od ogólnego sterowania maszyną, czyli standardowej automatyki, ograniczając w ten sposób narażenie funkcji związanych z bezpieczeństwem. Im wyraźniej te „komponenty podlegające ochronie” są oddzielone pod względem funkcjonalnym, tym mniej dodatkowych środków bezpieczeństwa potrzeba, aby zapewnić niezawodną ochronę.

Korzyści płynące z tego podejścia są widoczne na każdym etapie cyklu życia maszyny. Jeśli funkcje bezpieczeństwa i funkcje standardowe są oddzielone, nie ma potrzeby ponownej certyfikacji ani dostosowywania funkcji bezpieczeństwa równoległe z aktualizacją funkcji standardowych. Pozwala to znacznie ograniczyć nakłady

związane z konserwacją i serwisowaniem. Klasyczne sterowniki bezpieczeństwa wymagają również znacznie mniej aktualizacji o znaczeniu krytycznym dla bezpieczeństwa niż sterowniki standardowe, więc takie rozdzielanie eliminuje konieczność wielu zbędnych interwencji. Rozdzielenie tych elementów ma również zalety techniczne: samodzielny system bezpieczeństwa, taki jak mały sterownik bezpieczeństwa PNOZmulti 2, można dowolnie łączyć z systemami sterowania różnych producentów, podczas gdy systemy zintegrowane są często powiązane z konkretnymi technologiami. Jednocześnie oddzielne rozwiązania w zakresie bezpieczeństwa podnoszą poprzeczkę dla intruzów, ponieważ każdy z tych systemów trzeba przejść osobno, co znacznie utrudnia manipulację. Co więcej, standardowy system w razie potrzeby można podłączyć do sieci, podczas gdy rzeczywiste funkcje bezpieczeństwa pozostają odizolowane, co znacznie ogranicza powierzchnię ataku.

Takie rozdzielanie automatyki bezpieczeństwa i zabezpieczeń – przy idealnie skoordynowanych poziomach zabezpieczeń – zwiększa również wydajność, ułatwiając planowanie działań związanych z bezpieczeństwem, konserwacją i rozbudową. W związku z tym zmiany w standardowym programie nie wymagają żadnych modyfikacji w części dotyczącej bezpieczeństwa, co znacznie ogranicza nakład pracy związany z programowaniem i dostosowywaniem. Współdziałanie oznacza, że takie rozdzielanie ma pozytywny wpływ na koszty oprogramowania i wsparcia technicznego, ponieważ oddzielne systemy często wiążą się z niższymi opłatami licencyjnymi i serwisowymi.

Ochrona dzięki izolacji – kompetencje dzięki szkoleniom

Wyraźne rozdzielanie funkcji bezpieczeństwa od standardowej automatyki nie tylko zapewnia niezawodność techniczną, lecz także

ogranicza liczbę błędów operatorów i zmniejsza wymagania szkoleniowe. Funkcje związane z bezpieczeństwem działają na dedykowanym sprzęcie i są jednoznacznie oddzielone pod względem organizacyjnym, dlatego pozostają chronione nawet w przypadku wprowadzenia zmian w standardowym oprogramowaniu. Dzięki temu błędy w codziennej pracy nie zagrażają Bezpieczeństwu, a obowiązki można przydzielać w sposób bardziej przejrzysty.

Firma Pilz oferuje kompleksowy program szkoleń i usług, który ma pomóc przedsiębiorstwom we wdrażaniu tej architektury. Należą do nich szkolenia „Podstawy bezpieczeństwa przemysłowego” i „CESA – Certified Expert for Security in Automation”, a także usługi z zakresu bezpieczeństwa przemysłowego. Wyjaśniają, jak opracowywać solidne koncepcje zabezpieczeń technicznych w oparciu o poszczególne moduły, ale idą też znacznie dalej: pokazują, jak systematycznie zarządzać ryzykiem związanym z zabezpieczeniami i opracowywać całościowe koncepcje bezpieczeństwa, jak uwzględnić wymagania normy IEC 62443, jak zorganizować architekturę bezpiecznej sieci maszyn oraz jak oceniać i stale poprawiać skuteczność podejmowanych działań.

Jedną z głównych zalet tego podejścia jest to, że operatorzy u użytkownika końcowego nie muszą szczegółowo zagłębiać się w kwestie zabezpieczeń, ponieważ ochrona funkcji bezpieczeństwa jest już zagwarantowana przez samą konstrukcję systemu. Z tego powodu szkolenia skierowane są przede wszystkim do osób podejmujących decyzje dotyczące zabezpieczeń lub projektujących systemy – natomiast operatorzy nadal mogą bezpiecznie wykonywać swoją pracę bez konieczności przechodzenia dodatkowych szkoleń z zakresu bezpieczeństwa przemysłowego. W rezultacie uzyskujemy

praktyczny podział stanowisk, który upraszcza obsługę instalacji, a jednocześnie trwale podnosi poziom bezpieczeństwa.

Większe bezpieczeństwo dzięki przejrzystej strukturze – i odpowiedniej wiedzy specjalistycznej

Skutecznej strategii „Security for Safety” nie da się osiągnąć przez pojedyncze działania, lecz dzięki przemyślanej strukturze, jasno określonym zakresom odpowiedzialności oraz sprecyzowanemu rozwojowi umiejętności. Właśnie na tym polu wkracza firma Pilz. Dzięki konsekwentnemu skupieniu się na Defence-in-Depth oraz wyraźnemu rozdzieleniu bezpieczeństwa od standardowej automatyki firma Pilz tworzy podstawy pod niezawodne maszyny – a wszystko to uzupełnione jest praktycznymi szkoleniami i doradztwem, które pozwalają przedsiębiorstwom podążać tą drogą z pełnym przekonaniem. W rezultacie uzyskujemy poziom bezpieczeństwa, który nie tylko spełnia wymagania standardów, lecz także zapewnia wymierną wartość dodaną w codziennej eksploatacji: prostsze, solidniejsze i skuteczniejsze rozwiązanie w dłuższej perspektywie.

((liczba znaków: 9640))

Pilz – The Spirit of Safety

Firma Pilz jest globalnym dostawcą produktów, systemów i usług w dziedzinie technologii automatyzacji. Jako pionier w dziedzinie bezpieczeństwa automatyzacji firma Pilz tworzy rozwiązania zapewniające bezpieczeństwo ludzi, maszyn i środowiska. Założona w 1948 r. firma rodzinna z Ostfildern zatrudnia obecnie około 2500 osób w 42 oddziałach na całym świecie.

Jako lider technologii przedsiębiorstwo oferuje kompletne rozwiązania automatyzacji dla bezpieczeństwa i ochrony przemysłowej maszyn. Obejmują one technologie czujników, sterowania i napędów – w tym systemy komunikacji, diagnostyki i wizualizacji przemysłowej. Uzupełnieniem oferty są świadczone na całym świecie usługi doradcze, inżynierskie i szkoleniowe. Rozwiązania firmy Pilz są

wykorzystywane w wielu branżach poza inżynierią mechaniczną, takich jak:
intrałogistyka, maszyny pakujące, technologia kolejowa czy robotyka.

www.pilz.com

Firma Pilz w mediach społecznościowych:

Na naszych kanałach w mediach społecznościowych udostępniamy podstawowe informacje o firmie i personelu firmy Pilz oraz przekazujemy najświeższe aktualności ze świata technologii automatyzacji.



www.pilz.com/facebook

www.pilz.com/xing

www.pilz.com/youtube

www.pilz.com/linkedin

Kontakt z mediami:

Martin Kurth

Corporate and Technical
Press
Tel.: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

Prasa korporacyjna
i techniczna
Tel.: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

Prasa techniczna
Tel.: +49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Rößle

Prasa techniczna
Tel.: +49 711 3409-7147
e.roessle@pilz.de