Bezpieczeństwo 2020

ludzi • maszyn • procesów • danych

Egzoszkielety przemysłowe

Wspomagają pracownika i zapewniają dodatkową ochronę przed obrażeniami

- Obsługa nowoczesnych systemów bezpieczeństwa
- Jak wdrażać systemy LOTO
- Cyberbezpieczeństwo przemysłowych systemów sterowania (ICS)

Dodatek do:

CONTROL ENGINEERING Polska

INŻYNIERIA & UTRZYMANIE RUCHU

Firmy współpracujące:

AnterSystem

SICK Sensor Intelligence.

PROTEKT

EMERSON

RA Controls PROMOTOR INNOWACJI W PRZEMYŚLE

SCHMERSAL Safe solutions for your industry

OEM AUTOMATIC

PILZ THE SPIRIT OF SAFETY

Tworzymy bezpieczne miejsca pracy.

PROTECT PSC1

- Programowalny, modułowy sterownik bezpieczeństwa
- Elastyczne i skalowalne dostosowywanie aplikacji
- Połączenie z systemami magistralowymi za pomocą zintegrowanego interfejsu
- Bezpieczne monitorowanie napędu dla maks. 12 osi

www.schmersal.pl

SCHMERSAL
THE DNA OF SAFETY

Egzoszkielet jako sposób na zwiększenie bezpieczeństwa pracy

Mimo coraz większej automatyzacji i robotyzacji zakładów przemysłowych ich pracownicy nadal muszą wykonywać zadania, podczas których narażeni są na fizyczne obciążenie. Dotyczy to zwłaszcza tych czynności, które są wielokrotnie powtarzane w ciągu dnia pracy oraz wykonywane w niekomfortowej pozycji ciała. Problemy te może rozwiązać pełna automatyzacja, jednak – jak się okazuje – nie zawsze jest ona opłacalna i możliwa do wdrożenia. Przykładem są dynamiczne środowiska produkcyjne lub magazynowe, gdzie stosunkowo niewielkie rozmiary zamówień narzucają wysoki poziom elastyczności.

Optymalnym rozwiązaniem może być połączenie siły i precyzji systemu robotycznego z kreatywnością i elastycznością pracy człowieka. Chodzi tu o zastosowanie egzoszkieletów, o których piszemy na łamach najnowszego numeru specjalnego, przygotowanego przez redakcje magazynów *Control Engineering Polska* oraz *Inżynieria i Utrzymanie Ruchu*. Konstrukcje te, zwane także szkieletami zewnętrznymi lub robotami pomocniczymi, są zaprojektowane pod kątem poszczególnych stanowisk pracy i mają na celu wzmocnienie operatora i zapewnienie mu dodatkowej ochrony przed obrażeniami.

Uniformy w stylu Irona Mana, zwiększające siłę i wytrzymałość pracownika, powoli stają się rzeczywistością. O korzyściach płynących z zastosowania egzoszkieletów przekonują się na co dzień pracownicy takich firm, jak Ford, Toyota czy Boeing. Rozwiązania te są intensywnie rozwijane i testowane na całym świecie, nie tylko w fabrykach. Mimo że obecnie wykorzystywane są w przemyśle na niewielką skalę, wszystko wskazuje na to, że ich popularyzacja w środowisku produkcyjnym jest tylko kwestią czasu.

Zapraszamy do lektury!

Redakcja

Spis treści

2 Egzoszkielet – nowy wymiar bezpieczeństwa
6 Bezpieczeństwo funkcjonalne: zrozumieć podstawy
12 Konwergencja systemów bezpieczeństwa z innymi systemami przemysłowymi
18 Jak wdrażać systemy LOTO
28 Cyberbezpieczeństwo przemysłowych systemów sterowania (ICS)
32 Budowanie bezpiecznych sieci informatycznych jako strategicznych szkieletów cyfryzacji przemysłu
35 Bariery fizyczne i osłony na straży bezpieczeństwa
38 Obsługa nowoczesnych systemów bezpieczeństwa
e1 Jak zbudować kulturę bezpieczeństwa w zakładzie

Spis materiałów reklamowych

Anter System Polska ... III okładka
Emerson Automation Solutions, ASCO Numatics – Polska ... 24, 25, 26, 27
OEM Automatic ... 10, 11
Pilz Polska ... 9
Protekt ... 15
RAControls ... 5
Safety – Konferencja i Wystawa ... 30
Schmersal Polska ... II okładka
SICK ... 16, 17
Smary i Oleje – Konferencja i Wystawa ... 34
Urząd Dozoru Technicznego ... IV okładka

Redakcja

Zespół redakcyjny
Agata Abramczyk
agata.abramczyk@trademedia.pl

Agnieszka Korzeniewska
agnieszka.korzeniewska@utrzymanieruchu.pl

Redaktor merytoryczny
dr inż. Andrzej Ożadowicz

Korekta
Małgorzata Wyrwicz

Reklama
Piotr Wojciechowski
piotr.wojciechowski@trademedia.pl

Beata Kaczmarska
beata.kaczmarska@trademedia.pl

Sales Support Manager
Edyta Sekuła
edyta.sekula@trademedia.pl

Młodszy specjalista ds. marketingu
Aleksandra Fura
aleksandra.fura@trademedia.pl

Prenumerata
Aneta Marciniak
aneta.marciniak@trademedia.pl
prenumerata@controlengineering.pl
www.controlengineering.pl/prenumerata
prenumerata@utrzymanieruchu.pl
www.utrzymanieruchu.pl/prenumerata

DTP
Grzegorz Solecki
grzegorz.solecki@trademedia.pl

Druk i oprawa
EnterDruk

Wydawnictwo

Trade Media International
ul. Rzymowskiego 30, lok. 226
02-697 Warszawa
tel. +48 22 852 44 15
faks +48 22 899 30 23
e-mail: kontakt@trademedia.us
www.trademedia.us

Wydawca
Michael J. Majchrzak
michael.majchrzak@trademedia.pl

Egzoszkielet wspomaga pracownika wykonującego powtarzające się zadania związane z wierceniem otworów w podwoziach na linii montażowej samochodów.

Źródło: RIA/Ford Motor

Egzoszkielet – nowy wymiar bezpieczeństwa

ABI Research w swoim raporcie na temat sektora egzoszkieletów pasywnych przewiduje, że rynek ten do 2025 r. osiągnie wartość 1,8 mld dolarów. Ocenia się, że jeden z najsilniejszych trendów wzrostowych będzie dotyczył egzoszkieletów przemysłowych – rozwiązań, które mają na celu wzmocnienie pracownika i zapewnienie dodatkowej ochrony przed obrażeniami.

Tanya M. Anandan

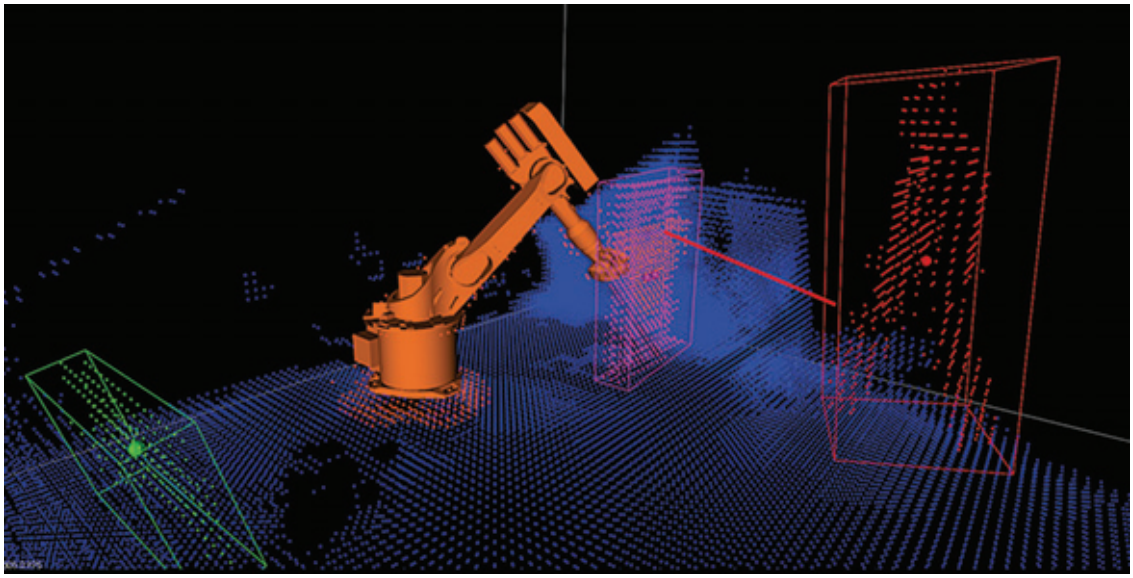
Jednym z wyzwań epoki robotów w przemyśle produkcyjnym jest ułatwianie koegzystencji i współpracy ludzi oraz robotów o zaawansowanych funkcjach i wysokich możliwościach. Veo Robotics – startup z Cambridge w stanie Massachussets w USA opracowuje technologię, która ma temu sprostać.

Wypełnić lukę między człowiekiem a robotem

– Uważamy, że ludzie i roboty doskonale się uzupełniają pod względem możliwości, a umiejętna organizacja współpracy możliwości te jeszcze zwiększa – stwierdza Clara Vu, współzałożycielka i wiceprezes ds. technicznych firmy Veo Robotics. *– W całym przemyśle produkcyjnym istnieją takie zadania, przy realizacji których można efektywnie połączyć ludzkie zdolności manualne, umiejętność oceny sytuacji oraz elastyczność z siłą, szybkością, precyzją i powtarzalnością ruchów robotów.*

– Zasilanie robota oraz jego siła mechaniczna są oczywiście ważnym elemen-

↗ Zrzut ekranu interfejsu użytkownika oprogramowania, które w sposób ciągły monitoruje miejsce pracy człowieka z robotem współpracującym pod względem zapewnienia bezpieczeństwa.



Źródło: Veo Robotics

tem, jednak rozwiązują one tylko część problemu – dodaje Clara Vu. – *Zgłaszają się do nas klienci, którzy np. chcą, by robot podnosił ciężki element i trzymał go w określonej lokalizacji, gdy pracownik będzie wykonywał na nim jakieś operacje*.

Clara Vu dostrzega duże zapotrzebowanie na system, który potrafi wykorzystać niewiarygodną siłę, szybkość i submilimetrową precyzję standardowego robota przemysłowego, ale jednocześnie ma możliwość współpracy z ludźmi. Współzałożyciele firmy Veo Robotics mają ustalone poglądy, jak odpowiedzieć na ten popyt.

Firma Veo Robotics poszukuje rozwiązań wypełniających lukę pomiędzy ludźmi a robotami przez wsparcie rozwoju robotów w zakresie lepszej percepcji swojego otoczenia i umożliwienie im zrozumienia tego, co dzieje się w ich gniazdach.

– *Nasz system różni się od zwykłego, polegającego np. na zainstalowaniu skanera laserowego w funkcjonalnej jednostce bezpieczeństwa. Nasz system rozumie, co dzieje się w gnieździe roboczym oraz co robi sam robot. Realizujemy tę „inteligencję" oraz ruchy robota w technologii 3D, która sprawia, że system jest bardziej elastyczny i inaczej reaguje na kogoś wyciągającego rękę, a inaczej na kogoś wchodzącego do gniazda robota*.

Jak stwierdza Clara Vu, podstawą systemu firmy Veo Robotics jest integralne połączenie sprzętu i oprogramowania.

– *W naszym systemie sprzęt składa się z dopasowanych do aplikacji i posiadających certyfikaty bezpieczeństwa czujników ToF* (time-of-flight – generujących wiązkę światła i mierzących czas, jaki wiązka ta potrzebuje na powrót do czujnika po odbiciu od obiektu – przyp. tłum.)*, wysyłających dane do wbudowanego komputera o dużej mocy obliczeniowej, który obsługuje system wizyjny i algorytmy sterujące robotem. Komputer obsługujący systemy rezyduje w gnieździe robotycznym i komunikuje się bezpośrednio ze sterownikiem robota*.

System jest zaprojektowany tak, aby działał z każdym robotem dowolnego z głównych producentów. Będzie dostarczany z 4 kamerami ToF, które, jak oczekuje firma Veo Robotics, wystarczą dla większości aplikacji gniazd robotycznych w przemyśle produkcyjnym. Clara Vu informuje jednak, że jej firma tworzy obecnie taki system, który będzie mógł być skonfigurowany do pracy z maksymalnie 8 kamerami dla bardziej wymagających środowisk przemysłowych.

– *Nasz system potrafi śledzić roboty, obrabiane elementy i ludzi w gnieździe robotycznym oraz orientować się, czy sytuacja jest bezpieczna w zależności od położenia tych obiektów* – stwierdza Clara Vu.

Jeśli z jakiegoś powodu pole widzenia kamery zostanie zasłonięte, system domyślnie powróci do najbezpieczniejszego położenia. System umożliwi robotowi poruszanie się, jeśli będzie pewien, że ruch ten jest bezpieczny.

Veo Robotics już współpracuje z pewną liczbą firm, w tym producentami samochodów oraz dostawcami ich podzespołów na pierwszy montaż (Tier 1). Ponadto analizuje możliwości zastosowania swojego systemu w transporcie bliskim materiałów, produkcji metali oraz sprzętu AGD, czyli obszarów, w których nadal dominuje tendencja do separacji ludzi i robotów.

– *Jeśli inżynierowie w przemyśle produkcyjnym projektują jakiś proces, to czy jest to proces ręczny, czy zautomatyzowany?* – pyta Clara Vu. I odpowiada: – *Tym, co naprawdę chcemy dokonać, aby pomóc tym inżynierom, i na co dostrzegamy popyt w całej branży, jest umożliwienie określenia, które elementy tego procesu powinny być wykonane przez człowieka, a które przez robota*.

Jest to istota współpracy człowieka z robotem: wykorzystanie unikalnych możliwości obydwu z nich i połączenie ich w optymalne rozwiązanie. Roboty współpracujące (coboty) są obecnie wykorzystywane na hali fabrycznej na różne, interesujące sposoby.

Kamizelka w postaci egzoszkieletu

Co może być lepszym robotem współpracującym od robota, którego pracownik „nosi" na sobie? Egzoszkielet (*exoskeleton*) to rozwiązanie techniczne, które cechuje się najbardziej bliskimi relacjami pomiędzy człowiekiem a robotem. Jedynymi urządzeniami przekraczającymi ten poziom współpracy są robotyczne urzą-

Robot współpracujący aplikuje poliuretan na tylną szybę samochodu, bez potrzeby instalowania tradycyjnej osłony bezpieczeństwa pomiędzy operatorem a robotem, co oszczędza cenną przestrzeń na hali fabrycznej.

Źródło: Esys Automation

dzenia medyczne, które pracują wewnątrz ludzkiego ciała.

Pracownicy linii montażowej w zakładach firmy Ford Motor noszą kamizelki – egzoszkielety produkowane przez firmę Ekso Bionics z Richmond (z Kalifornii), przeznaczone dla pracowników przemysłu i zakładane na górną część ciała.

Mogłoby się wydawać, że egzoszkielety, szczególnie bez zasilania (pasywne), takie jak produkt firmy Ekso Bionics, nie są robotami. Ale działy badawczo-rozwojowe firm na całym świecie pracują nad alternatywnymi rozwiązaniami uzyskiwania siły przez egzoszkielety. Rozwiązania te są często tańsze, lżejsze, bezpieczniejsze i niewymagające zasilania.

Ekso Bionics produkuje egzoszkielety pasywne dla przemysłu oraz egzoszkielety aktywne (zasilane) dla zastosowań w rehabilitacji. Wyroby tej firmy stanowią dobry przykład egzoszkieletów pasywnych, szczególnie wspomagających górną część ciała człowieka.

– Z samej zasady egzoszkielety muszą być współpracujące, ponieważ są zakładane na ludzkie ciało, i jeśli nie sprawdzają się w realizacji wyznaczonego zadania, to człowiek je odrzuci – mówi Claire Cunningham, menedżer ds. doświadczenia użytkownika w firmie Ekso Bionics. – *Chcemy, aby nasze produkty uzupełniały i wspierały użytkowników w wykonywaniu ich zadań, nie zaś im przeszkadzały. Szczególnie kamizelka, która jest zaprojektowana do używania przez cały dzień. Pracownicy firm będących naszymi klientami noszą ją przez 8 godzin dziennie podczas pracy na linii montażowej samochodów, tak więc komfort użytkownika jest dla nas sprawą najwyższej wagi. Jest to naprawdę trudnym wyzwaniem, aby połączyć jednoczesne wzmocnienie siły człowieka z jego komfortem*.

Kamizelka przeznaczona jest do wspierania siły ramion pracownika przy podnoszeniu, co ma pomagać w realizacji zadań wymagających pracy rąk na wysokości od poziomu piersi do ponad głową. Waga kamizelki wynosi nieco poniżej 5 kg, jednak osoba ją nosząca nie odczuwa tego dodatkowego ciężaru, ponieważ jest on rozłożony na różnych strefach ciała. Urządzenie dodaje siłę do 6,8 kg na jedno ramię użytkownika.

– Nosząc tę kamizelkę, nie musimy o niej myśleć – mówi Claire Cunningham. *– Pas biodrowy przenosi dużą część masy urządzenia na biodra i miednicę użytkownika. Natomiast szelki i mankiety kierują siłę pochodzącą z siłownika i systemu sprężyn do rąk, umożliwiając użytkownikowi pracę z siłą 15 lb* (66,7 N – przyp. tłum.) *przez cały dzień roboczy*.

Roboty współpracujące przeznaczone do noszenia na sobie

Firma Ekso Bionics szybko udowadnia, że jej kamizelka nie jest urządzeniem pomocniczym typu „podnieś i trzymaj” (*lift-and-carry*). Nie ma na celu wyposażenia użytkownika tylko w siłę supermana, jak głosi powszechne przekonanie na temat egzoszkieletów.

– Jest to urządzenie maratonowe i wspomagające podnoszenie – mówi Claire Cunningham. *– Zwiększa ono wytrzymałość człowieka, zaś prawdziwe jego zalety dostrzega się po kilku dniach. Człowiek będzie miał więcej energii, jego ramiona będą mniej zmęczone, a samopoczucie lepsze. Naszym celem związanym z tym urządzeniem jest zapobieganie zranieniom pracowników, często występującym podczas pracy z rękami uniesionymi nad głowę przez cały dzień roboczy*.

Gdy użytkownik zaczyna podnosić ramiona, mechaniczny siłownik uruchamia się i zaczyna lekko wzmacniać siłę rąk. Aplikacje kamizelki obejmują każdy typ powtarzających się czynności w pracy z rękami uniesionymi nad głową, takich jak wiercenie otworów w podwoziach czy instalowanie elementów układu wydechowego na linii montażowej samochodów. Kamizelka ta może być także używana w pracach budowlano-konstrukcyjnych,

gdy pracownicy, unosząc ręce nad głową, wykonują zadania związane z instalacjami hydraulicznymi i elektrycznymi, malowaniem przemysłowym, instalowaniem sufitowych paneli akustycznych oraz piaskowaniem przemysłowym.

Firma Ford realizuje pilotażowy program wykorzystania kamizelek od prawie 2 lat oraz wykonuje testy beta różnych wersji tego urządzenia. Claire Cunningham mówi, że współpraca partnerska z Fordem dostarczyła jej firmie wielu pomocnych informacji na temat sprawdzania się konstrukcji egzoszkieletu w praktyce.

– Uzyskaliśmy informacje zwrotne od firmy Ford oraz innych firm realizujących program pilotażowy i przełożyliśmy je na zmiany konstrukcyjne kamizelki. Obecnie pracujemy nad dystrybucją tych kamizelek – mówi Claire Cunningham.

Kamizelka ta może być personalizowana. Elementy wykonane z miękkich materiałów, takie jak pas biodrowy, mankiety i szelki, dostarczane są w różnych rozmiarach. Można także zmieniać wielkość siły wspomagającej użytkownika poprzez regulację sprężyn w siłowniku.

– Możemy regulować siłowniki niezależnie od siebie – mówi Kevin Dacey, główny inżynier projektu. *– Na przykład jeśli ktoś wierci otwory w podwoziach na linii montażowej samochodów, to może trzymać w jednej ręce wiertarkę, zaś drugą operować śrubami i nakrętkami, tak więc może wymagać więcej wspomagania w ręce trzymającej wiertarkę i mniej w drugiej.*

Urządzenie to jest wyposażone w pewną inteligencję, jednak w całości jest mechaniczne. W odróżnieniu od współczesnych elektromechanicznymi robotów przemysłowych, kamizelka jest urządzeniem pasywnym. Nie ma żadnych silników ani innych elementów elektrycznych.

– Nie wszystkie egzoszkielety muszą być zasilane z sieci elektroenergetycznej lub akumulatora – mówi Kevin Dacey. *– Konstrukcja mechaniczna jest tańsza i trwalsza. W środowisku przemysłowym pracownicy noszą tę kamizelkę przez 8 godzin dziennie 5 dni w tygodniu. Nie muszą pamiętać, aby podłączyć ją do sieci na noc w celu naładowania akumulatora.*

– Zmobilizowanie górnych kończyn wymaga znacznie mniej energii niż kończyn dolnych – mówi Claire Cunningham. *– Nasze egzoszkielety rehabilitacyjne są urządzeniami elektromechanicznymi, które wymagają niewiarygodnie dużego momentu obrotowego, aby sprawić, by siedzący użytkownik wstał. Jednak idea wykorzystywania energii elektrycznej w egzoszkieletach noszonych na górnej części ciała nosi już znamiona przesady.*

Egzoszkielety robotyczne są jednak wciąż nowym wyzwaniem. Claire Cunningham mówi, że ta dziedzina techniki ciągle ewoluuje.

– W przyszłości będzie wykorzystywanych więcej egzoszkieletów mechanicznych, ponieważ są dużo tańsze – mówi Cunningham. *– Dzięki niższym cenom egzoszkielety mechaniczne są rozwiązaniem dla każdego. Przewidujemy, że w ciągu kolejnych 10 lat w każdym domu będzie już egzoszkielet. Majsterkowicze będą mogli kupić jeden z różnych dostępnych typów w lokalnym sklepie z narzędziami. Ta relacja ludzi z robotami współpracującymi w najbliższej przyszłości będzie relacją mechaniczną. Roboty mechaniczne, elektromechaniczne, hydrauliczne i inspirowane biologią pracują we wszystkich konfiguracjach. Zupełnie jak ludzie.*

Podsumowanie

Jeśli spędzimy w branży robotycznej wystarczająco dużo czasu, zaczniemy patrzeć na nią inaczej. Zobaczymy próby i niepowodzenia, sukcesy i porażki, zaś nasze oczy będą szeroko otwarte. Łatwo jest zachwycać się postępem, ale także łatwo jest zrozumieć pełną wyzwań drogę, która wciąż przed nami.

Staniemy się w pełni świadomi zdumiewających możliwości ludzkiego ciała i umysłu. Co bardziej zadziwiające, przekonamy się, że będziemy wykorzystywać roboty do tego, by lepiej docenić nasze własne unikalne zdolności, które wykorzystujemy każdego dnia.

Ludzie dysponują kreatywnością, wyobraźnią, percepcją, zdolnościami manualnymi oraz niewiarygodną zdolnością do empatii i myślenia krytycznego. Czy roboty będą mogły z nami kiedykolwiek konkurować? Nie powinny, gdyż ludzie i roboty mają więcej możliwości, gdy stanowią zespół.

Tanya M. Anandan *jest redaktorem współpracującym Stowarzyszenia Przemysłu Robotycznego (RIA) i portalu Robotics Online.* ■

Bezpieczeństwo funkcjonalne: zrozumieć podstawy

Inżynierowie odpowiedzialni za projektowanie i rozwijanie systemów do aplikacji przemysłowych muszą być świadomi praktyk projektowych w zakresie bezpieczeństwa funkcjonalnego, które, jak wykazano, skutecznie zmniejszają ryzyko awarii.

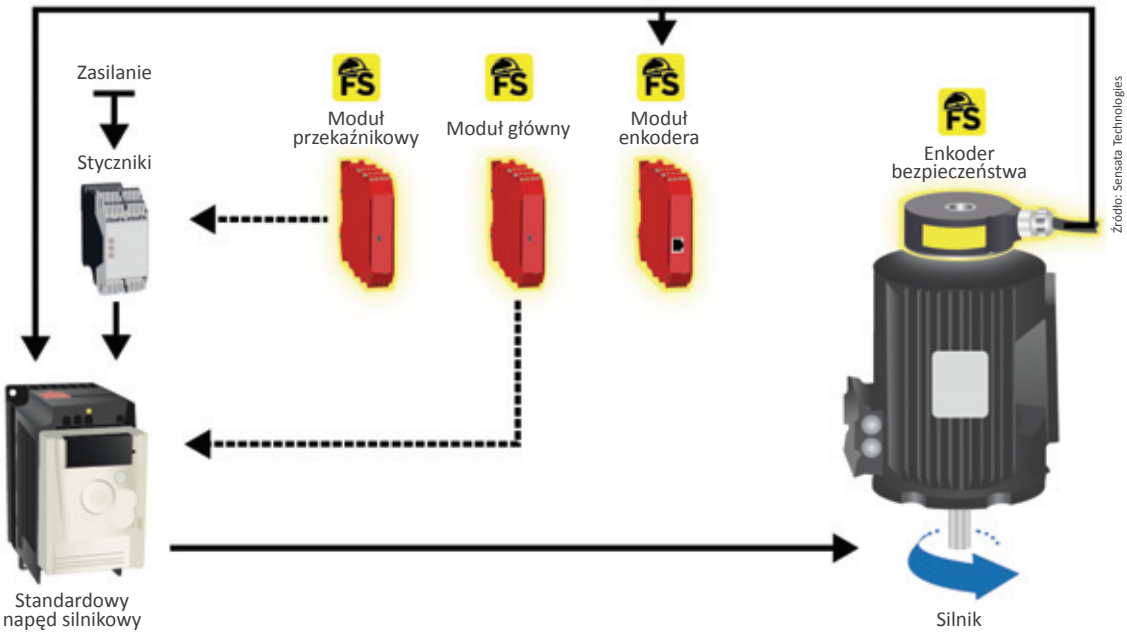
Scott Orlosky
Jean-Marc Hubsch

W sektorze przemysłowym i magazynowym istnieje wiele różnych systemów i instalacji, które mogą i powinny czerpać korzyści z zastosowania procesów i norm bezpieczeństwa funkcjonalnego.

Gdzie bezpieczeństwo funkcjonalne ma kluczowe znaczenie

Wdrożenie bezpieczeństwa funkcjonalnego w systemie sterującym rozlewni może pozwolić na dostosowanie prędkości linii rozlewniczej czy momentu obrotowego do poziomu „bezpiecznego" podczas wykonywania krótkich kontroli czy napraw, bez konieczności całkowitego zatrzymania produkcji. Podobnie w drukarni – wdrożenie procedur i elementów bezpieczeństwa funkcjonalnego dla prasy drukarskiej może pozwolić na czyszczenie wałków przy wprowadzeniu krótkich postojów lub nawet bez przerw w procesie produkcji oraz, co najważniejsze, przy niewielkim lub w zasadzie żadnym zagrożeniu dla operatora.

Aby zapobiec zranieniu pracowników obsługujących przenośnik taśmowy, można zastosować czujnik, który wykrywa obecność osób, gdy obiekt znajdzie się w odległości 8 stóp (243,84 cm) od maszyny i wysyła odpowiedni sygnał do sterownika w celu zmniejszenia prędkości posuwu przenośnika. Zamiast całkowitego wyłączenia takiego przenośnika i zatrzymania produkcji, można ją utrzymać przy zredukowanej prędkości i ogra-



Rys. Takie produkty, jak enkodery i moduły bezpieczeństwa, które posiadają certyfikaty dopuszczenia do stosowania w systemach bezpieczeństwa, mogą być łatwo wykorzystane w modernizacji istniejącego już sprzętu i tym samym zwiększeniu jego bezpieczeństwa.

Bezpieczeństwo funkcjonalne zwiększa wydajność produkcji, ponieważ umożliwia działanie systemów podczas drobnych napraw czy prac konserwacyjnych.

niczonym do minimum zagrożeniu dla bezpieczeństwa ludzi.

Innym przykładem jest przemysł drzewny, w którym systemy bezpieczeństwa funkcjonalnego mogą mieć kluczowe znaczenie dla bezpiecznego funkcjonowania maszyn do ścinania i korowania drzew, ponieważ system monitoruje pozycjonowanie surowej tarcicy, która ma być pocięta na deski.

W hutach stali także wymagane jest rygorystyczne stosowanie zasad i procedur bezpieczeństwa funkcjonalnego. Ma to na celu zapewnienie bezpiecznego i dokładnego realizowania procesów wytopu i przetwarzania stali, np. wylewania stopionej stali, a także kształtowania i walcowania sztab oraz blach.

Z kolei w przypadku schodów ruchomych, chodników ruchomych czy wind niezbędne jest zastosowanie czujników prędkości. W windach konieczna jest kontrola położenia kabiny. W wykorzystywanych od niedawna aplikacjach robotów współpracujących (zwanych również cobotami) zdolność robota do efektywnej współpracy z człowiekiem całkowicie zależy od poprawności i niezawodności elementów bezpieczeństwa – zwłaszcza zdolność do rejestrowania kontaktu z człowiekiem oraz zmniejszania stosowanej przez niego siły.

Przemysłowe obiekty magazynowe mogą być bezpieczniejsze i wydajniejsze dzięki wdrożeniu polityki bezpieczeństwa funkcjonalnego. Na przykład w wielu zakładach wykorzystuje się rozwiązania AGV (*automated guided vehicles*) do szybkiego przemieszczania produktów w magazynie i wokół niego lub na różne części linii produkcyjnych. W konstrukcji takich wózków często wykorzystuje się moduły enkoderów z certyfikatami dopuszczenia do stosowania w aplikacjach bezpieczeństwa, które mierzą prędkość i kierunek ruchu tych pojazdów i pomagają w zapewnieniu ich bezpiecznego funkcjonowania (**rys.**).

We wszystkich wymienionych aplikacjach, a także w wielu innych projektowanie i wdrażanie odpowiednich poziomów bezpieczeństwa funkcjonalnego może się przyczynić do redukcji przestojów i zapobiec poważnym zranieniom pracowników lub uszkodzeniom sprzętu.

Bezpieczeństwo funkcjonalne według norm

Implementacja elementów i procedur bezpieczeństwa funkcjonalnego jest obowiązkowa w systemach projektowanych w Unii Europejskiej, zgodnie z normami EN ISO 13849-1 oraz EN/IEC 62061, w Polsce wprowadzonymi normami: PN-EN ISO 13849-1 – „Bezpieczeństwo maszyn. Elementy systemów sterowania związane z bezpieczeństwem. Część 1: Ogólne zasady projektowania" oraz PN-EN 62061 – „Bezpieczeństwo maszyn. Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem".

Tak zwana dyrektywa maszynowa (dyrektywa 2006/42/WE z dnia 17 maja 2006 r. w sprawie maszyn) stanowi, że systemy i maszyny przemysłowe powinny działać tak bezpiecznie, jak to tylko możliwe, przy minimalnym ryzyku zranienia ludzi. Jednak, jak wszyscy wiemy, w rzeczywistości nie istnieje coś takiego jak „zerowe ryzyko". Zamiast tego wspomniana dyrektywa ustanawia drogę do osiągnięcia poziomu „akceptowalnego ryzyka" w określonych środowiskach przemysłowych.

Dla tych środowisk oraz działających w nich maszyn, jeśli bezpieczeństwo jest zależne od systemów sterowania (enkoderów, czujników itp.), to te podsystemy muszą być tak zaprojektowane, aby zapewniały wystarczająco małe prawdopodobieństwo awarii funkcjonalnych. Jeżeli jednak przy ich implementacji okaże się, że jest to niemożliwe, należy dążyć do tego, aby wszelkie awarie, które w rzeczywistości występują, nie prowadziły do utraty funkcji bezpieczeństwa.

Do niedawna elementy układów sterujących maszyn związane z bezpieczeństwem były projektowane zgodnie z normą EN 954-1, w Polsce wprowadzoną normą PN-EN 954-1 – „Maszyny. Bezpieczeństwo. Elementy systemów sterowania związane z bezpieczeństwem. Część 1: Ogólne zasady projektowania" (zastąpioną przez wspomnianą normę PN-EN ISO 13849-1), na podstawie obliczonego ryzyka. Jednak wraz z pojawieniem się nowych i bardziej zaawansowanych komponentów sprzętu i oprogramowania standardy dokonywania pomiarów i monitorowania bezpieczeństwa zostały zmodernizowane. Obecnie podstawową normą bezpieczeństwa funkcjonalnego jest EN/IEC 61508, wprowadzoną w Polsce normą PN-EN 61508 – „Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem". Zawiera ona kilka odwołań do szczegółowych wymagań i standardów, odnoszących się do specyficznych obszarów produkcji i projektowania, a zwłaszcza zapisów wspomnianych już norm PN-EN ISO 13849-1 oraz PN-EN 62061.

Aby zapobiec zranieniu pracowników obsługujących przenośnik taśmowy, zamiast całkowitego wyłączenia takiego przenośnika i zatrzymania produkcji, można ją utrzymać przy zredukowanej prędkości i ograniczonym do minimum zagrożeniu dla bezpieczeństwa ludzi.

PN-EN ISO 13849-1 (opracowana ze szczególnym odniesieniem do bezpieczeństwa maszyn)
Norma ta może być zastosowana dla związanych z bezpieczeństwem elementów systemów sterowania oraz wszystkich typów maszyn, niezależnie od wykorzystanej technologii oraz rodzaju energii. Elementami tymi mogą być np. przekaźniki, zawory, wyłączniki położeniowe, sterowniki PLC, napędy silnikowe czy czujniki ciśnienia. Działanie funkcji bezpieczeństwa określane jest jako „poziom zapew-

Tabela. Pojęcia poziomu nienaruszalności bezpieczeństwa (SIL) oraz poziomu zapewnienia bezpieczeństwa (PL) opisują możliwości funkcjonalne systemu sterowania, w kategoriach bezpieczeństwa, do zmniejszania czynnika ryzyka.

PFD (*probability of failure on demand* – prawdopodobieństwo wystąpienia awarii na żądanie)	PFH (*probability of failures per hour* – prawdopodobieństwo wystąpienia awarii w ciągu godziny)	SIL (*safety integrity level* – poziom nienaruszalności bezpieczeństwa) – EN 61508, EN 62061	PL (*performance level* – poziom zapewnienia bezpieczeństwa) – EN 13849-1	RRF (*risk reduction factor* – współczynnik zmniejszenia ryzyka)
10^{-2}<PFD<10^{-1}	10^{-6}<PFH<10^{-5}	1	b, c	od 10 do 100
10^{-3}<PFD<10^{-2}	10^{-7}<PFH<10^{-6}	2	d	od 100 do 1000
10^{-4}<PFD<10^{-3}	10^{-8}<PFH<10^{-7}	3	e	od 1000 do 10 000

nienia bezpieczeństwa" (*performance level* – PL), z ustalonym wskaźnikiem poziomu bezpieczeństwa od najniższego „a" do najwyższego „e" (**tabela**).

PN-EN 62061 (opracowana ze szczególnym odniesieniem do elementów i układów elektrycznych/elektronicznych)
Norma ta określa wymagania i podaje zalecenia dotyczące projektowania, integracji oraz certyfikacji związanych z bezpieczeństwem elektrycznych, elektronicznych oraz programowalnych elektronicznych systemów sterowania maszyn. Efektywność wdrożenia procedur bezpieczeństwa według tego standardu charakteryzuje wskaźnik „poziomu nienaruszalności bezpieczeństwa" (*safety integrity level* – SIL), który może przyjąć wartość od 1 do 4, gdzie „4" dotyczy najbardziej złożonych i zaawansowanych systemów na poziomie zakładu, funkcjonujących w środowiskach najwyższego ryzyka[1] (**tabela**).

Projektowanie systemów bezpieczeństwa dla przemysłu

Projektowanie systemów bezpieczeństwa przeznaczonych do zastosowań przemysłowych łączy w sobie zarówno procedury stosowane przez inżyniera podczas projektowania, jak i wdrażane przez użytkownika po zainstalowaniu i uruchomieniu systemu.

Zawsze preferowane są środki podejmowane w początkowej fazie projektowania. Są one zwykle bardziej efektywne od tych, które są stosowane tylko przez operatora maszyny.

Niezależnie od tego, czy dane środki są podejmowane przed zaprojektowaniem systemu, czy po jego zainstalowaniu, w projekcie muszą być uwzględnione następujące czynniki:

- ocena ryzyka i podjęcie decyzji na temat potrzeby zmniejszenia ryzyka,
- identyfikacja zagrożeń oraz wszelkich związanych z projektowanym systemem niebezpiecznych sytuacji,
- oszacowanie ryzyka w odniesieniu do każdego zidentyfikowanego zagrożenia i niebezpiecznej sytuacji,
- ustalenie ograniczeń oraz przeznaczenia maszyn.

Zdefiniowanie funkcji bezpieczeństwa maszyny jest krytycznym aspektem zmniejszania ryzyka. Obejmuje to np. funkcje bezpieczeństwa systemu sterowania, które zabezpieczają maszynę przed nieoczekiwanym uruchomieniem, przekroczeniem dopuszczalnej prędkości czy zbyt powolną pracą.

Podobnie ważne jest rozpoznanie dotyczące różnych stanów operacyjnych maszyn (np. tryby automatyczne i konfiguracji) oraz możliwych do zastosowania środków zabezpieczających w różnych trybach pracy. W praktyce może być tak, że w celu osiągnięcia wymaganych poziomów bezpieczeństwa w systemie będą musiały być zawarte: jeden lub więcej modułów sterujących związanych z bezpieczeństwem oraz kilka różnych funkcji bezpieczeństwa, co zostanie ustalone na podstawie rozpoznanych trybów pracy maszyny i możliwości w zakresie jej sterowania przy określonym trybie pracy.

Podsumowanie

Wśród korzyści wynikających z wdrożenia bezpieczeństwa funkcjonalnego należy wymienić ochronę ludzi, sprzętu i środowiska, w którym pracują. Ponadto bezpieczeństwo funkcjonalne zwiększa wydajność produkcji, ponieważ umożliwia działanie systemów podczas drobnych napraw czy prac konserwacyjnych.

Oczywiście zmiany w procesie inżynieryjnym i projektowym mogą zwiększyć koszty oraz wymagać czasu na wdrożenie. Jednak dzięki dostępnej obecnie nowej generacji czujników, enkoderów i sterowników inżynierowie mają do dyspozycji bloki konstrukcyjne, które umożliwiają im projektowanie bezpieczniejszych systemów z porównywalną łatwością i przy jedynie minimalnie wyższych kosztach.

***Scott Orlosky** – Product Manager w Sensata Technologies, **Jean-Marc Hubsch** – Engineering Manager w Sensata Technologies.* ■

[1] Od autorów: w artykule koncentrujemy się na poziomach SIL od 1 do 3, ponieważ są one stosowane w odniesieniu do maszyn przemysłowych.

PILZ

THE SPIRIT OF SAFETY

O FIRMIE

Pilz jest światowym liderem w dziedzinie bezpieczeństwa maszyn i ludzi. Oferuje na całym świecie rozwiązania dostosowane do indywidualnych wymagań Klientów ze wszystkich gałęzi przemysłu. Obejmują one innowacyjne produkty oraz kompleksowe usługi.

PRODUKTY

W naszej ofercie znajdują się produkty, dzięki którym możliwe jest zabezpieczenie praktycznie każdej maszyny czy linii produkcyjnej, należą do nich:

- przekaźniki bezpieczeństwa realizujące pojedyncze funkcje bezpieczeństwa;
- konfigurowalne przekaźniki bezpieczeństwa (rodzina PNOZmulti);
- kurtyny świetlne i bariery optyczne oraz skanery laserowe;
- wizyjne systemy bezpieczeństwa (w tym system SafetyEye do monitorowania stref 3D);
- czujniki bezpieczeństwa (mechaniczne, magnetyczne oraz kodowane);
- systemy ryglowania drzwi (PSENslock, PSENmlock, PSENsgate);
- przyciski stopu awaryjnego i wyłączniki linkowe;
- panele diagnostyczne oraz wizualizacyjne (rodzina PMI);
- maty bezpieczeństwa z funkcją detekcji położenia;
- serwonapędy z możliwością realizacji funkcji bezpiecznych (seria urządzeń PMC);
- systemy sterowania realizujące także funkcje bezpieczeństwa (PSS 4000).

Nasze rozwiązania doskonale wpisują się w założenia koncepcji Industry 4.0:

- **System PSS4000** wraz z wizualizacją PASvisu;
- **Safety Device Diagnostic** – do diagnostyki czujników safety połączonych szeregowo;
- **Security Bridge** – do zabezpieczenia przed nieuprawnionym dostępem do sterowników bezpieczeństwa PNOZmulti lub PSS4000.

ROZWIĄZANIA

Pomagamy opracować optymalne **rozwiązanie sterowania** – niezależnie od tego, czy głównym celem jego wdrożenia jest standaryzacja zabezpieczeń, zapewnienie bezpieczeństwa i standaryzacja w obrębie jednego systemu czy kompletna automatyzacja.

Koncentrujemy się na opracowywaniu **rozwiązań systemowych**, które w zależności od potrzeb mogą znaleźć zastosowanie zarówno z prostymi, niewielkimi maszynami, jak i z dużymi, pracującymi w sieci instalacjami.

USŁUGI

Tym co nas szczególnie wyróżnia jest bogata **oferta usług** pozwalająca na ocenę istniejącego stanu bezpieczeństwa maszyn i linii produkcyjnych, a także na ich dostosowanie do wymagań minimalnych lub zasadniczych, obejmująca:

- Opracowywanie **analizy ryzyk** dla ocenianych maszyn i linii produkcyjnych;
- Przygotowanie **koncepcji bezpieczeństwa** w celu eliminacji wykrytych zagrożeń i niezgodności;
- **Projektowanie** rozwiązań poprawiających stan bezpieczeństwa;
- **Wdrożenia** pozwalające na zmodernizowanie i dostosowanie istniejących układów bezpieczeństwa;
- **Walidacja** układów bezpieczeństwa po wdrożeniu;
- Analiza **LOTO** – przegląd procedur klienta wraz z propozycją rozwiązań poprawiających istniejący stan;
- **Certyfikacja CE** dla maszyn i linii produkcyjnych;
- **Ocena zakładu (Plant Assesment)**, która pozwala klientom na właściwe zaplanowanie inwestycji;
- Okresowe **przeglądy układów bezpieczeństwa**;
- **Pomiary prędkości i kolizji** dla aplikacji HRC za pomocą urządzenia PROBms
- **Szkolenia** produktowe oraz z zakresu norm i przepisów, w tym nowy program szkoleń **CMSE (Certified Machinery Safety Expert)**.

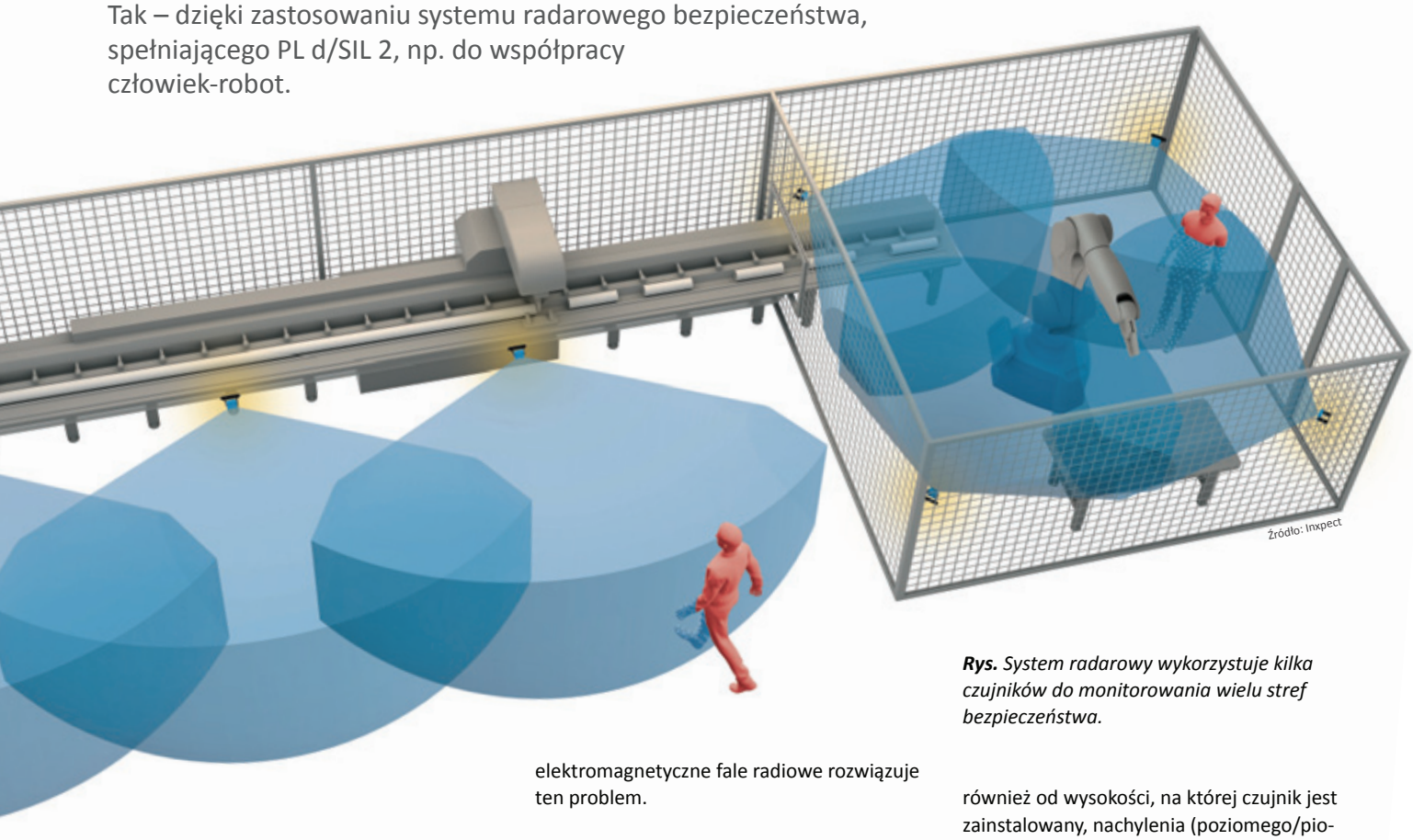
Połączenie oferty produktowej z usługami opartymi na wiedzy i doświadczeniach naszych inżynierów, czyni naszą ofertę unikalną na rynku.

Pilz Polska sp. z o.o.
Ul. Ruchliwa 15
02-182 Warszawa
Tel. 22 884 71 00
Fax 22 884 71 09
www.pilz.pl
info@pilz.pl

System radarowy

do efektywnego nadzorowania stref bezpieczeństwa

Czy można dostosować technologię radarową do rynku przemysłowego? Tak – dzięki zastosowaniu systemu radarowego bezpieczeństwa, spełniającego PL d/SIL 2, np. do współpracy człowiek-robot.



Rys. *System radarowy wykorzystuje kilka czujników do monitorowania wielu stref bezpieczeństwa.*

Systemy radarowe są integralną częścią samolotów. Luca Salgarelli, współzałożyciel i dyrektor generalny Inxpect, wraz ze swoją włoską firmą wprowadza tę technologię także do przemysłu. Jest przekonany, że „na horyzoncie widać prawdziwą rewolucję technologiczną, która zmusi nas do przedefiniowania obszarów zastosowania radaru". Jest nią system radarowy bezpieczeństwa LBK.

Dlaczego radary?

Kurtyny świetlne, skanery laserowe lub kamery zawsze potrzebują bezpośredniej widoczności obiektu, który mają „obserwować". Działa to jednak tylko w czystym środowisku, a nie w pomieszczeniach, które są zanieczyszczone przez zakłócające elementy, takie jak opary, kurz, woda, olej lub wióry. Technologia radarowa wykorzystująca elektromagnetyczne fale radiowe rozwiązuje ten problem.

Centralnym elementem systemu jest sterownik bezpieczeństwa, który zarządza maksymalnie sześcioma czujnikami radarowymi. Ma dwa przekaźnikowe wyjścia bezpieczeństwa, trzy redundantne zintegrowane wejścia bezpieczeństwa i dwa cyfrowe wyjścia sygnałowe. Każdy czujnik monitoruje wąski lub szeroki zakres 50° w poziomie i 15° w pionie lub 110° w poziomie i 30° w pionie. Jeden czujnik pokrywa maksymalny zasięg do 4 m, w którym użytkownicy mogą podzielić monitorowany obszar na strefę ostrzegawczą i strefę bezpieczeństwa.

Elastyczne koncepcje bezpieczeństwa

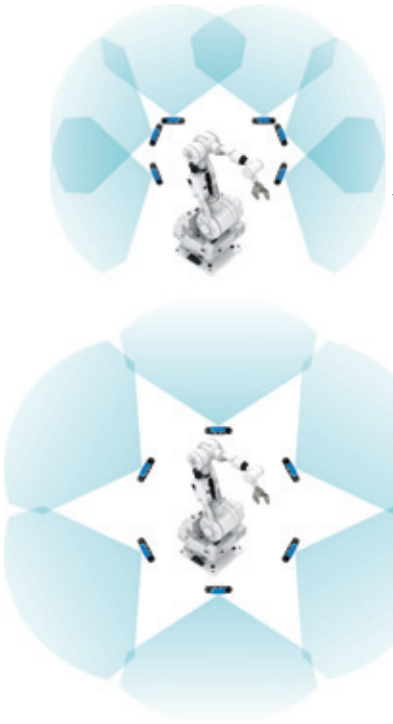
Każdy czujnik może być indywidualnie konfigurowany, mogą być także łączone między sobą. Pozwala to na ustawienie szerokiego lub wąskiego obszaru chronionego. Zależy to również od wysokości, na której czujnik jest zainstalowany, nachylenia (poziomego/pionowego) czujnika i konfiguracji przestrzeni ostrzegawczej. Liczba i rozmieszczenie czujników mogą być też wykorzystane do tworzenia różnych stref ochronnych, z możliwym pokryciem 360°. System można montować do wysokości 3 m. Może czasowo wyłączyć do trzech oddzielnych obszarów (muting), umożliwiając tworzenie elastycznych stref bezpieczeństwa. Pozwala to uniknąć przestojów i zwiększa produktywność. Maksymalna szerokość strefy bezpieczeństwa wynosi 15 m.

System LBK ma dwie funkcje bezpieczeństwa. Dzięki zabezpieczeniu dostępu, przy wejściu w strefę ostrzegawczą system wysyła sygnał, który spowalnia niebezpieczny ruch. Jeśli strefa bezpieczeństwa zostanie naruszona, pojawi się sygnał stop, np. dla robota. Ponadto blokada ponownego uruchomienia zapobiega nieoczekiwanemu, automatycznemu ponownemu uruchomieniu maszyny.

Możliwości wszechstronnego zastosowania

System radarowy przeznaczony jest do wolumetrycznego nadzorowania stref w trzech wymiarach. Głównym obszarem zastosowania systemu radarowego LBK jest zatem ochrona obszaru. W oparciu o ruch obiektu odróżnia on osobę od maszyny. Użytkownicy mogą ustawić czułość systemu tak, że wykrywa on nawet mikroruchy człowieka podczas oddychania. Sterownik bezpieczeństwa systemu LBK posiada możliwość konfigurowania dodatkowych funkcji, może być również podłączony do wyłącznika zatrzymania awaryjnego lub wyłącznika bezpieczeństwa drzwi i przycisku restartu.

Typowym zastosowaniem jest monitorowanie załadunku lub rozładunku palet za pomocą wózka widłowego. Zazwyczaj są tu stosowane systemy mutingu, aby zapobiec przypadkowemu przedostaniu się ludzi do strefy zagrożenia podczas transportu materiałów. Ponadto często wymagane jest manualne resetowanie funkcji. System LBK zastępuje kurtyny świetlne oraz skanery laserowe bezpieczeństwa chroniąc dostęp do niebezpiecznej strefy, i jednocześnie zapobiegając ponownemu uruchomieniu maszyny, gdy



Źródło: Inxpect

operator znajduje się wewnątrz tej strefy.

W przypadku aplikacji z pojazdami AGV możliwe jest takie ustawienie zabezpieczeń, które nie będą wymagać stosowania skanerów laserowych. Z kolei dobrze znane problemy z czujnikami optycznymi w maszynach do obróbki drewna i kamienia, zostały wyeliminowane.

Konfiguracja z komputera poprzez kabel microUSB

Dzięki aplikacji Safety App można szybko i łatwo skonfigurować do sześciu czujników wraz z jednostką sterującą, jak również strefy ostrzegawcze i bezpieczeństwa każdego czujnika. Jeśli jednostka sterująca nie jest dostępna, aplikacja może być wstępnie skonfigurowana za pomocą aplikacji symulującej. Dzięki możliwości wczytania rysunków maszyn, użytkownicy mogą szybko i zgodnie ze skalą zestawić aplikacje w sposób wirtualny.

Aprobata wg dyrektywy maszynowej

Zgodność WE według dyrektywy maszynowej zachodzi dla normy EN/ISO 13849 (PLd) i EN 62061 (SIL 2). Oprogramowanie Safety App zawiera narzędzie i opis producenta na potrzeby walidacji. Automatycznie można wywołać diagnostykę online w celu ustalenia, czy czujniki są prawidłowo ustawione i czy działają bez problemów.

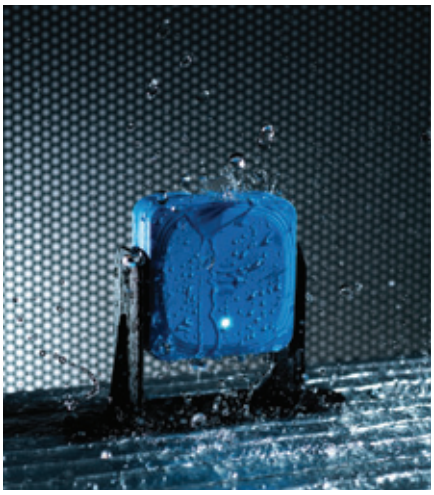
Firma OEM Automatic, dostawca rozwiązań w zakresie bezpieczeństwa funkcjonalnego, jest odpowiedzialna za sprzedaż na terenie Polski. Współpracując z firmą Inxpect i klientami z wielu branż, może służyć pomocą przy rozwiązywaniu problemów w różnych aplikacjach związanych z bezpieczeństwem. Firma OEM Automatic znalazła wiele zastosowań dla systemu LBK i posiada niezbędny know-how w zakresie jego zastosowania, instalacji i uruchomienia. Dzięki bezpośredniej współpracy z producentem firma OEM Automatic posiada również dostęp do najnowszych wersji oprogramowania sprzętowego/warsztatowego.

Źródło: Inxpect

Czy to pył...

Źródło: Inxpect

...mgła...



Źródło: Inxpect

...czy też woda – system radarowy LBK nadzoruje strefy niebezpieczne także w trudnych warunkach.

OEM Automatic Sp. z o.o.
ul. Działkowa 121A, 02-234 Warszawa
tel. +48 (22) 863 27 22
www.oemautomatic.pl

Konwergencja systemów bezpieczeństwa z innymi systemami przemysłowymi

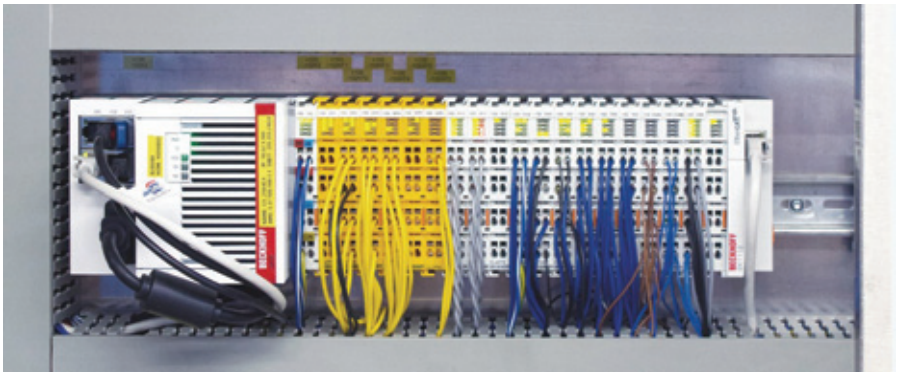
Integrowanie systemów bezpieczeństwa ze standardowymi platformami sterowania maszyn upraszcza obsługę samych maszyn, zwiększa możliwości diagnostyczne i tworzy bezpieczniejsze środowisko pracy dla inżynierów oraz użytkowników końcowych.

Sree Swarna Gutta

Konwergencja poprzednio niezależnych, a często i rozbieżnych technologii nadal jest ważnym tematem w przemyśle ze względu na korzyści, jakie oferuje inżynierom, producentom wyposażenia oryginalnego (OEM) i użytkownikom końcowym. Integrowanie technologii bezpieczeństwa z innymi technologiami sterowania czy transmisji danych może nie wydawać się oczywiste, jednak temat ten zasługuje na uwagę. Podobnie jak w przypadku technologii informatycznej (IT) i technologii operacyjnej (OT), połączenie systemu bezpieczeństwa z innymi dla stworzenia jednego systemu daje większą elastyczność i skalowalność, ulepszoną akwizycję danych we wszystkich systemach oraz lepsze dostosowanie systemów i ich funkcji do potrzeb użytkownika. Co ważniejsze, tworzy bezpieczniejsze środowisko pracy dla operatorów i personelu fabryk poprzez implementację większej ilości technologii bezpieczeństwa w większej liczbie miejsc.

Programowalne urządzenia bezpieczeństwa w formie modułów wejść/wyjść (We/Wy), które są ponadto zintegrowane z architekturą głównego układu sterującego maszyny, umożliwiają dokonanie takiej konwergencji. Te moduły We/Wy mają wbudowaną logikę bezpieczeństwa i komunikują się ze sterownikiem maszyny na bazie komputera typu PC. Komunikacja ta jest realizowana za pomocą wspólnej płyty głównej lub kabla sieci Ethernet. EtherCAT, przemysłowa technologia sieci standardu Ethernet, tworzy nowe obszary dla konwergencji technologii w systemach bezpieczeństwa, takich jak wbudowana diagnostyka i obsługa wielu magistral obiektowych (*fieldbus*). To podejście oznacza zmianę w stosunku do poprzednich architektur, w których systemy, w tym również systemy bezpieczeństwa, funkcjonowały niezależnie, praktycznie w architekturze wyspowej. Konwergencja technologii umożliwia utrzymanie poziomów nienaruszalności bezpieczeństwa (*safety integrity level* – SIL) maszyn oraz jednocześnie oferuje możliwości dostosowania do potrzeb użytkownika.

Aby zrozumieć zasadę tej konwergencji i powody, dla których jest ona korzystna, ważne jest, aby rozważyć 3 poziomy technologii bezpieczeństwa oraz ich role na hali fabrycznej.



Źródło: Beckhoff Automation

↗ W odróżnieniu od tradycyjnych systemów bezpieczeństwa, które były odseparowane od pozostałych komponentów, zabezpieczenia zintegrowane mogą być montowane na tej samej szynie DIN i komunikować się ze sterownikiem na bazie komputera typu PC oraz innymi układami We/Wy za pomocą wspólnej płyty głównej.

1 Podstawowe urządzenia bezpieczeństwa

Tradycyjne podstawowe podejście do bezpieczeństwa polega na odseparowaniu systemów bezpieczeństwa od systemów sterowania maszyn. Do grupy dedykowa-

nych urządzeń bezpieczeństwa zalicza się przede wszystkim przekaźniki i wyłączniki, które w przypadku ich wyzwolenia lub naciśnięcia odłączają zasilanie maszyn lub modułów. Chociaż nie wymagają one programowania, to muszą być bezpośrednio połączone przewodami z każdym modułem oraz każdym innym urządzeniem bezpieczeństwa, aby mieć pewność, że cała maszyna lub linia produkcyjna zostanie wyłączona po zadziałaniu jednego z zabezpieczeń. Instalowanie i oprzewodowanie przekaźników bezpieczeństwa jest praco- i czasochłonne, szczególnie w przypadku dużych maszyn.

Przekaźniki oraz inne podstawowe urządzenia bezpieczeństwa nie są zwykle konfigurowalne, ponieważ nie mają możliwości połączenia z siecią. Nie mogą wysyłać informacji zwrotnych do programowalnych sterowników logicznych (PLC), ani dostarczać danych dotyczących ich działania lub danych diagnostycznych. Mogą tylko sygnalizować stan za pomocą kontrolek LED. Przez wiele lat tego typu urządzenia były jedyną opcją zabezpieczeń w przemyśle, spełniając minimalne wymagania dotyczące ochrony operatorów i sprzętu. Jednak obecnie, w dobie inteligentnych fabryk i Przemysłu 4.0, podstawowe wymagania bezpieczeństwa nie dotrzymują już kroku postępowi technologicznemu w przemyśle. Wykorzystywanie tylko takich podstawowych urządzeń jest nieefektywne, ponieważ wymaga większego nakładu prac przy uruchamianiu i oferuje tylko nieskomplikowane, podstawowe technicznie zabezpieczenia dla pracowników.

Źródło: Beckhoff Automation

↗ Niektóre moduły bezpieczeństwa We/Wy, w tym wszystkie nowe moduły TwinSAFE, mają wbudowaną logikę bezpieczeństwa na poziomie urządzeń i nie wymagają osobnego sterownika PLC bezpieczeństwa.

2 Samodzielne sterowniki bezpieczeństwa

Samodzielne sterowniki bezpieczeństwa mają wbudowaną pewną logikę programowalną oraz umożliwiają rozbudowę, ale przy implementacji wymagają dodatkowych prac inżynierskich. Mogą być podłączane do sieci i dostarczają informacje diagnostyczne pomocne przy rozwiązywaniu problemów, jednak nie umożliwiają konwergencji systemów bezpieczeństwa z innymi systemami.

Podobnie jak podstawowe zabezpieczenia, sterowniki bezpieczeństwa pozostają fizycznie odseparowane od sterowników maszyn. Chociaż obydwa typy sterowników zawierają logikę, to sterownik bezpieczeństwa i sterownik PLC obsługują tylko komunikację asynchroniczną, co oznacza, że kluczowe dane z systemu bezpieczeństwa nie są dostępne do analizy. Ponadto zabezpieczenie wykorzystuje inne oprogramowanie niż sterownik PLC sterujący maszyną, natomiast wymagane szkolenie i konserwacja dla wielu pakietów oprogramowania spowalniają uruchamianie sprzętu i rozwiązywanie problemów.

3 Zintegrowane bezpieczeństwo – programowalne układy We/Wy

Większa konwergencja technologii ma miejsce dzięki zintegrowaniu systemów bezpieczeństwa z programowalnymi modułami We/Wy bezpieczeństwa. Moduły te wyróżniają się na zewnątrz żółtym kolorem obudowy. Wewnątrz mają obwody redundantne i mikrokontrolery, co maksymalizuje niezawodność i umożliwia spełnianie wymagań norm bezpieczeństwa PN-EN IEC 61508 „Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem" oraz PN-EN ISO 13849-1 „Bezpieczeństwo maszyn – Elementy systemów sterowania związane z bezpieczeństwem". Urządzenia te są instalowane na standardowej szynie montażowej, obok modułów i złączek niezwiązanych z bezpieczeństwem. Mogą się komunikować za pomocą systemów ethernetowych takich jak EtherCAT. Zintegrowane bezpieczeństwo może być rozszerzone poza moduły We/Wy w celu wykorzystania logiki bezpieczeństwa w modułach obiektowych, takich jak serwonapędy i serwomotory, z wbudowanymi funkcjami bezpiecznego wyłączenia momentu obrotowego STO (*safe torque off*) i bezpiecznego stopu SS1 (*safe stop 1*). Metoda ta wykorzystuje to samo środowisko inżynierskie co układy sterowania maszyn i zapewnia elastyczność znaną z rozproszonych systemów bezpieczeństwa.

Programowalne moduły We/Wy mogą także obsługiwać zabezpieczenia pojedynczych kanałów sygnałowych. Dzięki zaimplementowanemu i niezbędnemu do tego oprogramowaniu (firmware) do obsługi protokołów bezpiecznej komunikacji moduły te pozwalają inżynierom, szczególnie pracującym w przemyśle procesowym, ustawiać parametry akceptowalnych warunków dla różnych aplikacji, takich jak monitoring temperatury i ciśnienia oraz pomiary poziomu i prędkości.

Opisywane moduły bezpieczeństwa mają żółty pasek na obudowach, co odróżnia 1-kanałową technologię analogową od standardowych, cyfrowych modułów bezpieczeństwa w segmencie We/Wy. Te wyspecjalizowane moduły 1-kanałowe umożliwiają ponadto wykorzystanie układów We/Wy do realizacji zadań związanych z bezpieczeństwem.

Zintegrowane zabezpieczenia są niezbędne we współczesnych aplikacjach przemysłowych, w których coraz częściej

wykorzystuje się roboty, skomplikowany sprzęt sterujący ruchem oraz pojazdy autonomiczne. Nowoczesne fabryki wymagają zarówno prostych urządzeń bezpieczeństwa takich jak przyciski zatrzymania awaryjnego (e-stop), jak i bardziej skomplikowanych, takich jak m.in.: kurtyny świetlne, maty bezpieczeństwa i pulpity sterujące wymagające obsługi dwoma rękami na raz – (dla uniknięcia przypadkowego wciśnięcia, włączenia/wyłączenia).

Oprogramowanie dla automatyki na bazie komputerów typu PC, wyposażone w standardowe bloki funkcyjne bezpieczeństwa, pozwala inżynierom na pisanie programów, które są niezbędne do ochrony pracowników i sprzętu w tych środowiskach pracy. Podczas działania sterownik maszyny na bazie komputera typu PC oraz sterowniki bezpieczeństwa mogą się nawzajem monitorować.

W wyniku opisywanej konwergencji otrzymuje się lepsze funkcjonowanie systemów oraz większe możliwości diagnostyczne. Informacje diagnostyczne mogą być wyświetlane na interfejsie operatorskim (HMI), ponieważ system bezpieczeństwa jest podłączony do systemów sterowania i sterowników PLC. Podczas gdy w przypadku podstawowych systemów bezpieczeństwa wymagane jest więcej programowania, to uruchamianie zintegrowanych systemów jest uproszczone. Ponadto wyeliminowane są komplikacje spowodowane wieloma środowiskami programistycznymi, dodatkowymi sieciami i koniecznością połączenia każdego urządzania przewodami ze wszystkimi innymi. Inne urządzenia oparte na technologii EtherCAT realizują komunikację przy wykorzystaniu protokołu FSoE (*FailSafe over EtherCAT*), mającego certyfikat TÜV.

Bezpieczne przesyłanie danych dotyczących bezpieczeństwa

Protokół FSoE jest przeznaczony do transmisji danych dotyczących bezpieczeństwa przy wykorzystaniu istniejącej w fabryce sieci i za pomocą tzw. czarnego kanału (*black channel*). Ten bezpieczny kanał sieciowy inkrementuje cykliczny kod nadmiarowy (*cyclic redundancy check* – CRC) dla każdych dwóch bajtów danych dotyczących bezpieczeństwa, w celu zapewnienia, że są one wolne od błędów. Zasady funkcjonowania technologii EtherCAT umożliwiają transmisję danych dotyczących bezpieczeństwa oraz pozostałych danych bez ograniczeń prędkości przesyłu i czasu cyklu. Zaprojektowana do komunikacji z dużą prędkością EtherCAT sprawdza urządzenia bezpieczeństwa w czasie rzeczywistym i zatrzymuje operacje po zadziałaniu zabezpieczenia. Ponadto wbudowana diagnostyka pomaga inżynierom w lokalizowaniu problemów fizycznych, takich jak uszkodzenia w kablach, złączkach czy modułach We/Wy.

Źródło: Beckhoff Automation

↗ Zintegrowane bezpieczeństwo może być rozszerzone poza moduły We/Wy w celu wykorzystania logiki bezpieczeństwa w komponentach obiektowych takich jak serwonapędy.

Protokół FSoE jest niezależny od magistrali obiektowej i obsługuje prędkości przesyłu danych ponad 100 Mbit/s w EtherCAT, ale może być także zintegrowany z wieloma innymi przemysłowymi sieciami ethernetowymi lub magistralami obiektowymi. Jeśli fabryki wykorzystują sieci standardów DeviceNet, Profibus, CANopen, EtherNet/IP i Profinet, to wdrożenie zintegrowanych systemów bezpieczeństwa wraz z FSoE wymaga dodania do systemów odpowiednich modułów We/Wy oraz bram sieciowych EtherCAT.

Protokół FSoE ma certyfikat TÜV oraz spełnia wymagania norm PN-EN IEC 61508 PN-EN ISO 13849-1. Te cechy bezpieczeństwa pozostają niezmienione, niezależnie od tego, czy komunikacja odbywa się poprzez istniejącą magistralę obiektową, przemysłową sieć Ethernet czy sieci bezprzewodowe. Ponadto FSoE oraz zintegrowane moduły We/Wy bezpieczeństwa oferują możliwości większego dostosowania do użytkownika.

Konwergencja technologii umożliwia dopasowanie ich do użytkownika

Kluczową korzyścią z integracji systemów bezpieczeństwa z innymi jest możliwość dopasowania zintegrowanego systemu do potrzeb użytkownika. Jeśli klient ma maszynę modułową, to jej producent OEM lub integrator systemów ma możliwość wyłączenia określonego modułu w oprogramowaniu, zamiast przechodzić przez tradycyjną ścieżkę przeprojektowania i przeprogramowania systemu bezpieczeństwa tej maszyny. Poprzednia metoda obejmowała zmianę układów We/Wy, ponowne zaprojektowanie i wykonanie komponentów lub stworzenie prymitywnych obejść przewodami w celu ominięcia niepotrzebnych części systemu bezpieczeństwa. Przy wykorzystaniu oprogramowania dla automatyki opartej na komputerach typu PC dodawanie lub usuwanie modułów albo grup umożliwia szybkie dokonywanie modyfikacji.

Jednak niektóre firmy powoli adaptują zintegrowaną technologię bezpieczeństwa, co jest spowodowane obawami o konsekwencje wynikające z połączenia systemów bezpieczeństwa i pozostałych na jednej platformie. Zintegrowane zabezpieczenia są jednak niezawodne i preferowane w stosunku do podstawowych urządzeń bezpieczeństwa oraz samodzielnych sterowników bezpieczeństwa. Jeśli sterownik PLC bezpieczeństwa i sterownik maszyny pracują w tym samym środowisku, to kontrolują się wzajemnie i mogą komunikować się ze sobą bardziej efektywnie.

Dzięki większej elastyczności i szybszej instalacji możliwe jest projektowanie maszyn i fabryk, które korzystają w większym stopniu z technologii bezpieczeństwa niż dotychczas. Wdrożenie zintegrowanych zabezpieczeń za pomocą programowalnych modułów We/Wy jest najbezpieczniejszym wyborem.

Sree Swarna Gutta *jest specjalistą ds. aplikacji We/Wy w firmie Beckhoff Automation.* ■

PROTEKT®

www.protekt.pl
+48 42 29 29 500

Zobacz film!

Mobilne stanowiska pracy zabezpieczające przed upadkiem z wysokości

RJ500

www.protekt.pl/katalogi

Dobierz skaner do swoich potrzeb

Wprowadzenie: laserowe skanery bezpieczeństwa w automatyce

Laserowe skanery bezpieczeństwa okazały się niezawodnymi urządzeniami ochronnymi, stosowanymi w tysiącach aplikacji przemysłowych od ponad 25 lat. Są bardzo wszechstronne i otwierają różnorodne możliwości zastosowań. Montowane poziomo lub pionowo w aplikacji stacjonarnej monitorują niebezpieczne punkty i obszary, a także punkty dostępu do maszyn i wykrywają osoby chcące wejść w te przestrzenie. W aplikacjach mobilnych zabezpieczają zautomatyzowane trasy pojazdów. Istnieje szereg wariantów skanerów o różnej ilości i różnych zakresach skanowania pola ochronnego, kątach skanowania i opcje integracji.

Laserowe skanery bezpieczeństwa powodują zatrzymanie maszyny lub pojazdu, gdy tylko wykryją osobę, część ciała lub inną przeszkodę wewnątrz pola ochronnego. Zapobiega to narażeniu ludzi na niebezpieczeństwo w wyniku niebezpiecznych ruchów maszyny.

Nowa technologia skanowania: analogowa a cyfrowa

Na podstawie różnicy czasu wysłania i odbioru wiązki (Δt) laserowy skaner bezpieczeństwa oblicza odległość od obiektu. Poprzedni standard technologii skanowania opierał się na pomiarze czasu przelotu z analizą sygnału analogowego. W tego typu pomiarach skanery również muszą być w stanie niezawodnie wykrywać obiekty z remisją zaledwie 1,8%, np. takie jak czarny materiał spodni, czarne obuwie. Te procesy pomiaru czasu „przelotu" wiązki z analizą sygnału analogowego osiągnęły jednak już swój poziom graniczny w trudnych warunkach otoczenia. Dlatego opracowano nowy cyfrowy proces skanowania safeHDDM™ o wysokiej rozdzielczości.

Ta procedura pomiarowa zapewnia znacznie ulepszoną odporność na takie czynniki, jak światło otoczenia, deszcz, mgła i kurz, oraz sprawia, że problem wcześniej niedostępnych trudnych warunków aplikacji mogą być rozwiązany z jej wykorzystaniem. Ten proces został opracowany i opatentowany przez SICK, a jest stosowany w nowej generacji laserowych skanerach bezpieczeństwa microScan3 od początku 2016 r. Koncepcja wieloimpulsowa SafeHDDM™ generuje ok. 80 000 pojedynczych impulsów na każdym skanie – w porównaniu z ok. 500 wygenerowanymi za pomocą konwencjonalnej technologii. W tym procesie cyfrowe echa są kompilowane w pakiety danych, które nakładają się podczas oceny, a dzięki znacznie większej liczbie impulsów laserowych na skan nowa technologia SafeHDDM™ gwarantuje dużo bardziej stabilny pomiar odległości. Jako podstawa bezpiecznego wykrywania ludzi i przedmiotów otwiera to zupełnie nowy poziom jakości i niezawodności wykrywania. Skaner stał się czterokrotnie mniej wrażliwy na światło słoneczne i światło otoczenia do 40 000 luksów.

Laserowe skanery bezpieczeństwa z safeHDDM™ są dlatego odporne na olśnienie – bez względu na to, czy przed jasnym światłem słonecznym, czy wysokiej częstotliwości sztucznym źródła światła, oświetleniem otoczenia lub odbiciem padającym bezpośrednio na optykę. Dzięki zastosowaniu safeHDDM™ indywidualne remisje z kodowania sekwencji impulsów skanera są niezawodnie wykrywane

Fot. *outdoorScan3 – jedyny certyfikowany skaner bezpieczeństwa do aplikacji na zewnątrz budynków*

Fot. *Skanery bezpieczeństwa (od lewej): S3000, microScan3, TiM-S, nanoScan3, S300, outdoorScan3*

i analizowane, nawet gdy siły sygnału są niskie. W zależności od oceny mogą być one wygaszane i dzięki temu cząsteczki pyłu lub osad osadzający się na optyce skanera ma znacznie mniejszy wpływ na niezawodność wykrywania i ciągłość pracy skanera. Ponadto najnowszej generacji laserowe skanery bezpieczeństwa z safeHDDM™ mają również parabolicznie zakrzywioną przednią szybę i wykazują praktycznie brak wzajemnych zakłóceń z innymi skanerami.

Nowe możliwości: skaner bezpieczeństwa poza budynkiem – outdoorScan3

Wózki samojezdne i systemy transportu samojezdnego są obecnie używane w niemal każdym środowisku przemysłowym. Dlatego obecnie wielu specjalistów logistyki, inżynierów i pracowników ds. bezpieczeństwa z niecierpliwością oczekiwało na bezpieczną automatyzację procesów przemysłowych na zewnątrz budynków. Tym wymaganiom sprostał pierwszy laserowy skaner bezpieczeństwa z certyfikatem IEC 62998 do użytku na zewnątrz budynków, stworzony przez SICK – outdoorScan3. Dzięki innowacyjnej technologii skanowania HDDM® outdoorsafe, skaner outdoorScan3 działa bezpiecznie i niezawodnie w każdych warunkach pogodowych, takich jak deszcz, śnieg lub mgła czy silne promienie słoneczne – i w ten sposób zamyka główną lukę w automatyzacji procesów przemysłowych.

Fot. *nanoScan3 – minimalne wymiary a oprócz funkcji bezpieczeństwa przesyła dane nawigacyjne*

Nowe rozwiązanie pozwala, aby pojazdy autonomiczne, samojezdne AGV/AGC mogły jeździć z większą prędkością, a nawet zapewnić ciągłość przepływu materiału między halami produkcyjnymi. Po prostu outdoorScan3 umożliwia zwiększenie wydajności wewnątrz i na zewnątrz budynków i hal produkcyjnych.

Nowe funkcje: bezpieczeństwo i lokalizacja w jednym

Teraz laserowe skanery bezpieczeństwa mają oprócz standardowych funkcji bezpieczeństwa również możliwość przesyłania danych nawigacyjnych. Dane pomiarowe zeskanowanego otoczenia przesyłane są do komputera nawigacyjnego, który wykorzystuje je do lokalizacji i nawigacji. Niezależnie od tego skaner monitoruje cały czas pola ochronne. Umożliwia to zastosowanie laserowych skanerów bezpieczeństwa w kompaktowych i ekonomicznych pojazdach transportowych.

W 2019 r. firma SICK wprowadziła na rynek nowy typ skanera – nanoScan3. Łączy on inteligentne funkcje bezpieczeństwa z doskonałą jakością danych pomiarowych, zapewniając dokładną i niezawodną lokalizację. Skaner nanoScan3 wyróżnia się bardzo małą konstrukcją, dużym zakresem funkcji, a przede wszystkim małą konstrukcją zgodną z oczekiwaniami branży logistycznej.

Programowalne i dynamicznie dostosowujące się pola ochronne, dane wyjściowe o informacjach pomiarowych niezbędnych do obsługi nawigacji, a także sprawdzone technologie skanera, które zapewniają maksymalną niezawodność wykrywania nawet w trudnych warunkach otoczenia, takich jak kurz i brud, charakteryzują czujnik bezpieczeństwa 2D.

Dzięki wymiarom zaledwie 101×101×80 mm nanoScan3 otwiera aplikacje niezwykle ważne dla intralogistyki mobilnej, mobilnej robotyki z autonomicznymi platformami transportowymi, a także dla robotów współpracujących (cobotów). Ponadto nanoScan3 ustanawia nowy punkt odniesienia w stosunku ceny do wydajności w tym segmencie rynku.

Podsumowanie

Nowe laserowe skanery bezpieczeństwa serii microScan3, nanoScan3 oraz outdoorScan3 doskonale wpisują się w oczekiwania nowoczesnego Przemysłu 4.0. Możliwość monitorowania dużej ilości pól pozwala na lepsze dostosowanie zachowania się maszyn w zależności od panującej sytuacji, np. w aplikacjach współpracy człowieka z robotem. Możliwe jest ograniczanie zakresu pracy oraz prędkości, zależnie od miejsca oraz odległości, w jakiej znajduje się człowiek. W aplikacjach mobilnych pola skanera można precyzyjnie dostosować w zależności od kierunku jazdy i prędkości i bezpiecznie wykrywać obiekty oraz wolne przestrzenie magazynowe. Dostępne w skanerach różnorodne interfejsy komunikacyjne pozwalają na szybkie podłączenie do układu sterowania maszyny. Umożliwiają przesyłanie dużej ilości sygnałów „bezpiecznych” – naruszenia stref, sygnałów standardowych – ostrzeżenia, błędy, diagnostykę, informację o zanieczyszczeniu, dane o otoczeniu wykorzystywane do nawigacji oraz konfigurację. Daje to możliwość zbierania dużej ilości informacji o stanie maszyny, a na ich podstawie jeszcze większe możliwości diagnostyczne czy możliwość przewidywania usterek i planowania prac serwisowych.

SICK
Sensor Intelligence.

tel. 22 539 41 00
www.sick.pl

Jak wdrażać systemy LOTO

Prawidłowe wdrożenie systemu LOTO uniemożliwia przypadkowe załączenie maszyny przez ograniczenie dostępu osobom nieuprawnionym lub jej załączenie przez osobę do tego nieupoważnioną i nieprzeszkoloną (inną niż ta, która zablokowała i oznaczyła źródło energii niezbędne do bezpiecznego wykonania czynności). Gwarantuje, że urządzenie nie będzie uruchomione, dopóki prawidłowo zaaplikowany system LOTO nie zostanie usunięty. LOTO stanowi więc jeden z ważniejszych systemów bezpieczeństwa pracy.

Źródło: TagOut Systemy Bezpieczeństwa

↗ Blokada wtyczek siłowych – duża, do stosowania w momencie odłączenia urządzenia na wtyczce. Dostępne są również rozmiary mniejsze, np. do wtyczek jednofazowych.

Aleksandra Solarewicz

LOTO to skrót od angielskiego terminu *lockout/tagout*. *Lockout* obejmuje szereg urządzeń oraz postępowań mających na celu odcięcie i kontrolę wszelkich źródeł energii zasilających daną maszynę lub urządzenie. *Tagout* z kolei ma zadanie informacyjno-ostrzegawcze – komunikuje o istniejącym zagrożeniu, ale również informuje imiennie, kto znajduje się w strefie bezpośredniego zagrożenia. Oba elementy systemu LOTO znacznie zwiększają bezpieczeństwo pracy.

System LOTO został opracowany w USA w 1982 r. z myślą o ochronie pracowników przeprowadzających regularne kontrole, naprawy i serwis maszyn i urządzeń, ale też pracowników obsługi wykonujących codzienne czynności procesowe. Bazuje on na wykorzystaniu nieograniczonego zestawu blokad i zawieszek, mających na celu zabezpieczenie pracowników przed niekontrolowanym włączeniem urządzenia i uwolnieniem energii zasilającej, zmagazynowanej oraz resztkowej, stanowiącej główne zagrożenie dla pracowników zarówno działów technicznych, jak i produkcyjnych. *Lockout* i *tagout* ograniczają możliwość popełnienia błędów wynikających z intensywności i technicznych aspektów wykonywanej pracy, a także – a może przede wszystkim – z błędów powstałych na skutek nieuwagi pracowników.

Źródła zagrożeń

Główne źródła zagrożeń występujące w zakładzie przemysłowym to:

- energia elektryczna,
- energia mechaniczna,
- energia pneumatyczna,
- energia hydrauliczna,
- energia cieplna,

- substancje chemiczne w stanie ciekłym i gazowym,
- gorące powierzchnie i substancje,
- energia potencjalna wynikająca z grawitacji – możliwość upadku urządzeń, elementów z wysokości,
- energia magazynowana,
- energia resztkowa.

Według statystyk Centralnego Instytutu Ochrony Pracy większość wypadków przy pracy związana jest z:

- przygotowywaniem, instalowaniem, montowaniem, demontowaniem, rozbieraniem (ok. 8 tys. wypadków rocznie),
- konserwacją, naprawami i regulacjami (5 tys. wypadków rocznie),
- czyszczeniem i sprzątaniem (5 tys. wypadków rocznie).

Normy i przepisy

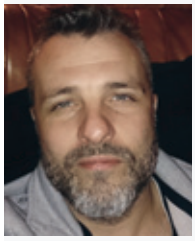
W polskich i europejskich przepisach nie ma wyrażonego wprost nakazu stosowania systemów LOTO, są w nich jednak wymogi dotyczące zapewnienia bezpieczeństwa podczas pracy z maszynami i można je odnieść do LOTO. Chodzi tu mianowicie o:

- Rozporządzenie Ministra Gospodarki z dnia 21 października 2008 r. w sprawie zasadniczych wymagań dla maszyn – rozporządzenie to wdrożyło postanowienia dyrektywy 2006/42/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie maszyn;
- Rozporządzenie Ministra Gospodarki z dnia 30 października 2002 r. w sprawie minimalnych wymagań dotyczących bezpieczeństwa i higieny pracy w zakresie użytkowania maszyn przez pracowników podczas pracy – wdrożyło ono postanowienie dyrektywy Parlamentu Europejskiego i Rady 2009/104/WE z dnia 16 września 2009 r. dotyczącej minimalnych wymagań w dziedzinie bezpieczeństwa i higieny użytkowania sprzętu roboczego przez pracowników podczas pracy.

W rozporządzeniu w sprawie zasadniczych wymagań dla maszyn ujęte są

Artur Chudyga, właściciel firmy TagOut Systemy Bezpieczeństwa

Proces trudny i pracochłonny, ale konieczny do przeprowadzenia



Prawidłowe wdrożenie systemu LOTO nie jest procesem łatwym, biorąc pod uwagę odpowiedzialność spoczywającą na prowadzącym wdrożenie. Jest to wręcz trudny i czasochłonny proces. Dodatkowo wymaga wiedzy z zakresu BHP, utrzymania ruchu, a także budowy maszyn. Wdrożenie może bowiem dotyczyć maszyn, linii produkcyjnych, produkcji gniazdowej, ale też rozdzielni czy ciepłowni, czyli infrastruktur, które wykorzystują jednocześnie różne rodzaje energii oraz ich wielokrotność. A to wymaga szczególnej staranności w planowaniu i przeprowadzeniu wdrożenia.

Niewłaściwe wdrożenie systemu stanowi dodatkowe zagrożenie wynikające z mylnej oceny ryzyka maszynowego, błędnego oznaczenia i tworzenia dokumentacji, ale przede wszystkim podejścia pracowników do zagadnień związanych z samym wdrożeniem.

Wyszkolenie i zdyscyplinowanie pracowników jest trudne, wymaga czasu i niejednokrotnie trudnych, dyscyplinujących decyzji personalnych, lecz pamiętajmy, że stawką jest zdrowie i życie. Odpowiednie szkolenia przygotowujące do pracy z systemem, wsparte zajęciami praktycznymi na maszynach, to podstawa.

Patrząc przez pryzmat wdrożeń, które już wykonałem, mogę powiedzieć, że wraz z intensywnością używania systemu LOTO wzrasta komfort bezpiecznej pracy. A to w rezultacie przekonuje opornych. Przede wszystkim jednak system daje nam możliwość zapobiegania wypadkom, w myśl zasady: „Lepiej zapobiegać, niż leczyć".

Źródło: TagOut Systemy Bezpieczeństwa

→ Skrzynka blokowania grupowego, używana w trakcie prac z zastosowaniem systemu LOTO w celu całkowitego doprowadzenia maszyny lub urządzenia do zerowego stanu energii.

wymogi dotyczące zapewnienia ich bezpiecznej konserwacji. Zgodnie z nimi należy zapewnić możliwość wykonywania regulacji, konserwacji, naprawy, czyszczenia i innych czynności serwisowych podczas postoju maszyny. Jeżeli nie jest to możliwe, powinna być zapewniona możliwość przeprowadzenia tych czynności bez powstania ryzyka związanego z ich wykonywaniem. Ponadto maszyna powinna być wyposażona w łatwo rozpoznawalne – łatwe do identyfikacji – urządzenia odłączające ją od wszystkich źródeł energii, przy czym w urządzeniu należy uwzględnić funkcję zablokowania go, jeżeli ponowne podłączenie zasilania energią mogłoby zagrażać ludziom.

Rozporządzenie w sprawie minimalnych wymagań dotyczących bezpieczeństwa i higieny pracy w zakresie użytkowania maszyn przez pracowników podczas pracy zawiera podobne wymaganie, by prace konserwacyjne prowadzone były podczas postoju maszyny. Jeżeli jest to niemożliwe, należy stosować odpowiednie środki ochronne. Tu również znajduje się zapis, zgodnie z którym maszyny powinny być wyposażone w łatwo rozpoznawalne – identyfikowalne – urządzenia służące do odłączania od źródeł energii, a ponowne przyłączenie nie może stanowić zagrożenia dla pracowników.

Należy tu także wspomnieć o normie PN-EN 1037 – „Bezpieczeństwo maszyn. Zapobieganie niespodziewanemu uruchomieniu". Określono w niej wbudowane środki bezpieczeństwa przeznaczone do zapobiegania niespodziewanemu uruchomieniu maszyny i umożliwiające bezpieczną interwencję pracownika w strefach zagrożenia.

Wdrożenie systemu LOTO

Wdrożenie systemu LOTO powinno być poprzedzone wieloma szczegółowymi czynnościami. Należą do nich:

- inwentaryzacja posiadanych maszyn/urządzeń – tzw. audyt wdrożeniowy;
- wybór zakresu wdrażania systemu i strategii w zależności od liczby posiadanych maszyn/urządzeń, sposobu ich pracy (indywidualny lub w ciągu technologicznym), roku produkcji czy rodzaju energii zasilających;
- opracowanie listy maszyn/urządzeń/instalacji objętych wdrożeniem;
- przeprowadzenie oceny ryzyka dla wszystkich maszyn/urządzeń/instalacji z listy, z uwzględnieniem blokad LOTO. Ocena ryzyka powinna obejmować:
  - weryfikację prac, dla których ma obowiązywać system LOTO,
  - identyfikację, które energie mają być odcinane, a które nie podczas poszczególnych prac;
- określenie wpływu odcięcia energii na otoczenie – sąsiednie maszyny, instalacje;
- określenie, czy dla prac z energiami niebezpiecznymi (niszczącymi) dostępne są techniczne środki bezpieczeństwa ograniczające i monitorujące te energie i czy są dobrane odpowiednie poziomy niezawodności działania;
- określenie, czy jest możliwy wybór trybu pracy;
- sprawdzenie, czy maszyna/urządzenie/instalacja zabezpieczona jest przed niespodziewanym uruchomieniem;
- sprawdzenie, czy może nastąpić kumulacja którejkolwiek z energii, a jeśli tak, to czy dostępne są urządzenia pozwalające unieszkodliwić zakumulowaną energię;
- sprawdzenie środowiska pracy, które może mieć wpływ na dobór wyposażenia LOTO;
- opracowanie instrukcji szczegółowych maszyn/urządzeń;
- opracowanie procedury głównej dla określenia sposobów postępowania w danym zakładzie pracy;
- wybór systemu LOTO – jednolitego systemu dla całego przedsiębiorstwa.

Źródło: TagOut Systemy Bezpieczeństwa

↖ Blokada uniwersalna do zaworów różnego typu i wielkości. W odpowiedniej konfiguracji samej blokady można zastosować ją z ramieniem (jak na zdjęciu) lub z linką albo też sam korpus do zaworów klapowych.

Źródło: TagOut Systemy Bezpieczeństwa

↗ Nylonowa klamra/szekla – przeznaczona do stosowania w sytuacji, gdy jest tylko jedno miejsce do blokowania, a blokujących jest więcej.

System LOTO ma w założeniu chronić pracownika przed niekontrolowaną emisją wszelkiej energii dopływającej do urządzenia. Z tego względu każdy uprawniony pracownik powinien być przygotowany, czyli odpowiednio przeszkolony w zakresie niezbędnym do wykonywanej pracy.

Po wykonaniu wszystkich czynności przygotowawczych można przystąpić do wdrożenia samego systemu. W jego zakres wchodzi:

- dostosowanie i ewentualna modernizacja wytypowanych maszyn/urządzeń/instalacji w celu uzyskania wymaganej liczby punktów blokowania energii,
- program szkoleń dla pracowników,
- oznakowanie wszystkich punktów blokowania energii LOTO wraz z opracowaniem instrukcji postępowania.

Inwentaryzacja sprzętu

Audyt systemu LOTO powinien obejmować zlokalizowanie punktów odcięcia dopływu energii (zaworów, przełączników, wyłączników lub zaślepek) i oznaczenie ich założonymi na stałe i ujednoliconymi etykietami lub zawieszkami. Punkty muszą być wyraźnie oznaczone – to warunek najważniejszy, by system LOTO był skuteczny. Należy również pamiętać, że etykiety lub zawieszki powinny być spójne z procedurami, jakie zostały sporządzone na piśmie lub elektronicznie.

Niezależnie od opisu działań, warto umieścić przy urządzeniu informację graficzną, zdjęcia urządzeń i punktów odcięcia energii. Podpisy muszą być zrozumiałe dla wszystkich pracowników, dlatego niekiedy konieczne jest przygotowanie podpisów w językach obcych.

Opracowanie procedury ogólnej oraz procedur dla wszystkich urządzeń

Opracowanie i udokumentowanie zasad kontroli energii doprowadzanej do urządzeń to najważniejszy dokument dla systemu LOTO, wskazujący urządzenia, które są objęte procedurami. Należy w nim uwzględnić wymagania przepisów i norm, a także wewnętrznych wymagań i zaleceń dla pracowników. Powinien on wyjaśniać, krok po kroku, proces wyłączania, odcinania, blokowania i zabezpieczania urządzeń, a także poszczególne etapy zakładania, usuwania i przekazywania narzędzi LOTO.

Instrukcję do systemu LOTO można stworzyć we własnym zakresie, ale można także skorzystać ze specjalnej aplikacji e-loto do tworzenia e-procedur LOTO. Taka e-aplikacja pozwala tworzyć, utrzymywać i aktualizować instrukcje maszynowe LOTO. Jedna z firm dostarcza takie narzędzie nieodpłatnie wszystkim klientom, u których dokonała wdrożenia systemu. Za jego pomocą można też opracowywać szkolenia.

Dobór sprzętu do blokowania urządzeń

Do punktów kontroli energii zalicza się zawory, przyciski, dźwignie, wyłączniki itp. Dla poszczególnych typów tych punktów produkowane są odpowiednie zabezpieczenia *lockout*, które pozwalają na utrzymanie urządzeń w pozycji bezpiecznej lub wyłączonej.

Urządzenia LOTO powinny spełniać następujące wymagania:

- ich konstrukcja powinna być trwała i uwzględniać warunki – w tym atmosferyczne, w jakich będzie pracować,
- nie mogą ulegać uszkodzeniom spowodowanym środowiskiem korozyjnym,
- powinny być standaryzowane w przedsiębiorstwie w co najmniej jednym z następujących kryteriów: kolor, format, wielkość,

Źródło: TagOut Systemy Bezpieczeństwa

→ Blokada wyłączników nadprądowych typu „S”, zarówno jedno-, jak i trójfazowych.

Źródło: TagOut Systemy Bezpieczeństwa

↙ Blokada zaworów kulowych – mała. Dostępna w różnych rozmiarach i kolorach, w zależności od rozmiaru zaworu oraz medium.

- muszą być tak zaprojektowane, aby ich usunięcie, wyłączenie nie wymagało od pracownika nadmiernej siły fizycznej lub zastosowania nietypowych narzędzi (noży, śrubokrętów itp.),
- ich konstrukcja (kształt, kolor) powinna zapobiegać przypadkowym usunięciom,
- powinny umożliwiać identyfikację pracownika korzystającego z systemu LOTO (np. elektryka, mechanika).

Jednym z rodzajów zabezpieczeń *lockout* są kłódki. W zależności od warunków, w jakich mają być używane, kłódki są wykonywane z różnych materiałów, mają różną wielkość, kolory i obudowy. Kłódki oznaczone danym kolorem mogą np. pomóc zidentyfikować, który zespół utrzymania ruchu serwisuje konkretną maszynę.

Różne obudowy kłódek pozwalają natomiast zoptymalizować trwałość i bezpieczeństwo użytkownika w określonych warunkach. W niektórych branżach wymagane jest stosowanie kłódek o wysokiej odporności na ścieranie, w innych preferowane są kłódki nieprzewodzące. Elementy ruchome i specyficzne punkty można blokować, korzystając z uniwersalnych blokad *lockout*.

Tagouty, czyli przywieszki

Do każdego zabezpieczenia *lockout* dopasowuje się odpowiednie oznakowanie – *tagout*, mówiąc potocznie: przywieszkę. Przywieszki muszą być czytelne i zrozumiałe dla wszystkich pracowników, których dotyczą, powinny zawierać miejsce na wpisanie imienia i nazwiska osoby blokującej, wydział lub firmę, w której pracuje, i numer telefonu, pod którym można się z nim skontaktować.

Znaczniki i ich środki mocowania muszą być wykonane z materiałów odpornych na warunki środowiska, w którym są stosowane. Muszą być mocowane w ten sposób do maszyn/urządzeń, aby nie mogły być przypadkowo usunięte.

Na zawieszce do kłódki może znajdować się informacja, dlaczego maszyna została zablokowana, kto ją serwisuje i przewidywany czas serwisowania. Dzięki temu pracownicy otrzymują istotne dane o blokadzie i wiedzą, do kogo należy się zwrócić po dodatkowe informacje.

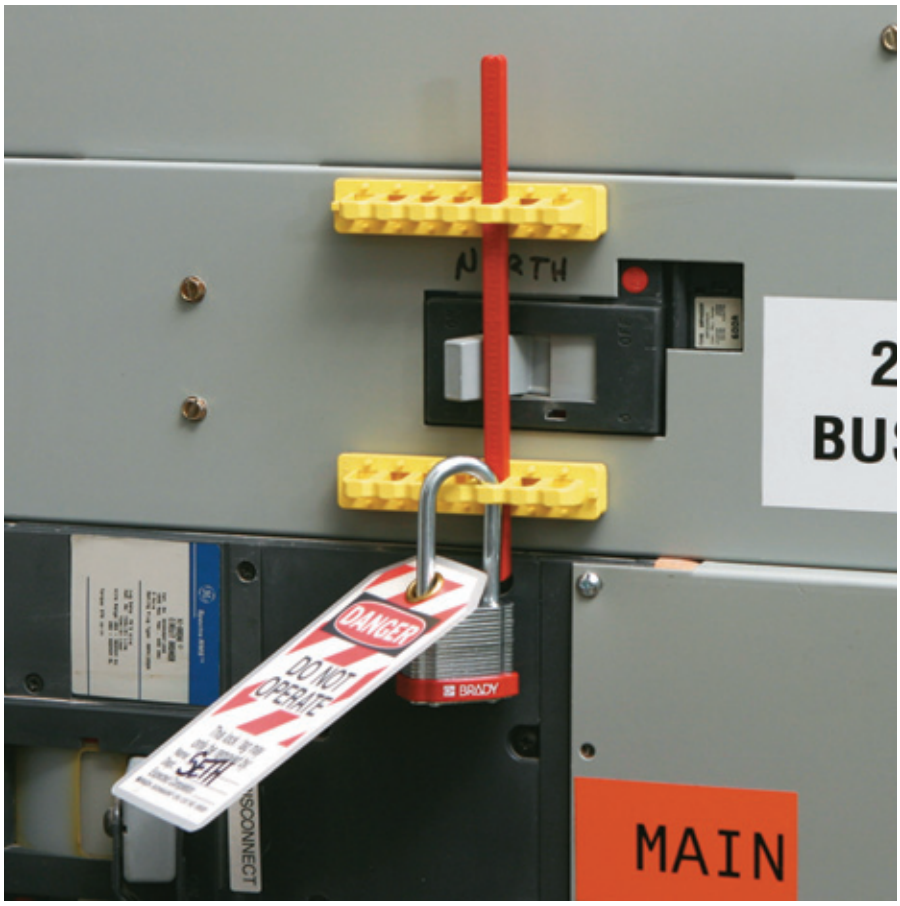
Co ważne, w sytuacji zablokowania energii urządzenia ochronne nie mogą uniemożliwić działań pozaprodukcyjnych, stąd program kontroli energii wymaga zastosowania systemu *tagout*, zgodnego z opracowanymi procedurami. Tagouty nie mogą być usunięte bez zezwolenia osoby do tego uprawnionej.

Jeśli blokada nie jest możliwa…

Nie wszystkie prace serwisowe, diagnostyczne, a szczególnie naprawcze mogą

Źródło: TagOut Systemy Bezpieczeństwa

→ Blokada przycisków operacyjnych na pulpitach sterowniczych, szafach. Szczególnie przydatna do zabezpieczenia w trakcie czynności operatorskich.



Źródło: TagOut Systemy Bezpieczeństwa

↘ Blokada wyłączników, np. „WIS", z krótkim ramieniem – ma szczególne zastosowanie w rozdzielniach NN i ŚN.

być realizowane po odcięciu źródeł energii. Bywa, że pracownik musi wyregulować, zdiagnozować maszynę, pracując w strefie niebezpiecznej. Pracodawca musi zapewnić mu wtedy maksymalne bezpieczeństwo. Oznacza to ograniczenie dopływu energii i nieustanny jej monitoring.

Nowoczesny system bezpieczeństwa jest w stanie zadziałać w sytuacji przekroczenia określonych wartości energii, co w efekcie skutkuje zatrzymaniem pracy maszyny i odłączeniem napędów od źródła zasilania.

Szkolenia

System LOTO ma w założeniu chronić pracownika przed niekontrolowaną emisją wszelkiej energii dopływającej do urządzenia. Z tego względu każdy uprawniony pracownik powinien być przygotowany, czyli odpowiednio przeszkolony w zakresie niezbędnym do wykonywanej pracy.

Dla osób pracujących z blokadami LOTO szkolenie powinno być bardziej szczegółowe, jednak zaleca się, by ogólne informacje w tym zakresie otrzymali wszyscy pracownicy. Tematy szkolenia powinny obejmować: przyczyny wprowadzenia systemu LOTO, jego charakterystykę, informacje o polityce LOTO w zakładzie oraz o procedurach dotyczących konkretnych maszyn. Wśród szczegółowych zagadnień można wymienić: stosowane źródła energii, rodzaje i wielkości dostępnej energii, metody i środki niezbędne do blokowania energii oraz jej kontroli.

Wszyscy pracownicy, którzy w związku z wykonywaną pracą mogą się znajdować w miejscu, gdzie mogą być stosowane procedury kontroli energii, muszą być zaznajomieni z tymi procedurami, a przede wszystkim pouczeni o zakazie ingerowania w zastosowane blokady.

Ponadto pracodawca powinien dokonywać przeglądu procedur kontrolnych niebezpiecznej energii, szczególnie pod kątem ich przestrzegania. Wszelkie odchylenia powinny być odnotowywane, identyfikowane przyczyny niezgodności i wdrażane działania korygujące. Takie okresowe inspekcje dają pewność, że każdy pracownik wykonujący serwisowanie, naprawę lub przegląd maszyny albo urządzenia realizuje zadania zgodnie z procedurą i nieoczekiwane włączenie urządzenia i uwolnienie energii, mogącej spowodować obrażenia lub śmierć pracownika, jest wykluczone.

Aleksandra Solarewicz *– publicystka, od 1997 r. współpracuje z prasą branżową.* ■

Literatura

1. T. Lis, K. Nowacki, H. Kania, S. Jucha, „System Lockout-Tagout dla bezpieczeństwa pracy", Konferencja Innowacje w Zarządzaniu i Inżynierii Produkcji 2016, tom II, www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2016/T2/t2_0413.pdf.
2. Brady, „Bezpieczeństwo podczas prac serwisowych. Przewodnik po blokadach Lockout/Tagout", www.tagout.com.pl/wp-content/uploads/2014/02/LOTO_guide-Book_PL_v3.pdf.
3. A. Humienna-Berta, „Czym jest LOTO", 8.12.2015, https://glowny-mechanik.pl/2015/12/08/czym-jest-loto/.
4. Industriel, „Kompleksowe wdrożenia systemu LOTO: Lock Out Tag Out", www.industriel.pl/services.php?body=article&name=system-loto-lock-out-tag-out&lang=pl.
5. Industriel „e-LOTO oprogramowanie Lockout/Tagout – aplikacja do tworzenia e-procedur LOTO", www.industriel.pl/services.php?body=article&name=e-loto-program-do-instrukcji&lang=pl.

Elastyczne podejście do stref bezpieczeństwa zmniejsza złożoność bezpieczeństwa maszyn oraz poprawia produktywność i całkowitą efektywność wyposażenia

Producenci na całym świecie muszą zapobiegać wypadkom w miejscu pracy, chroniąc swój personel oraz maszyny przed licznymi zagrożeniami. Osiągnięcie odpowiedniego poziomu bezpieczeństwa to wyzwanie, gdyż może zwiększać złożoność oraz prowadzić do obniżenia produktywności. W niniejszym artykule wyjaśniono, jak unikalne podejście do bezpieczeństwa, znane również jako bezpieczeństwo strefowe, zmniejsza złożoność projektowania redundantnych pneumatycznych obwodów bezpieczeństwa, a co więcej, zwiększa wydajność maszyny. W artykule tym omówiono przewagę strategii nad tradycyjną metodą konstrukcji pneumatycznych obwodów bezpieczeństwa, gdzie wykorzystuje się zawory spustowe i wymienia korzyści zarówno dla producentów urządzeń (OEM), jak i dla użytkowników końcowych.

Niedawne badanie przeprowadzone przez Administrację Zdrowia i Bezpieczeństwa Pracy (*Occupational Safety and Health Administration*) wykazało, że przemysł wytwórczy odpowiada za 26% hospitalizacji i 57% amputacji związanych z pracą – są to najwyższe liczby spośród wszystkich branż przemysłu w Stanach Zjednoczonych. Statystyki tego typu wyjaśniają, dlaczego producenci oraz użytkownicy końcowi są bardzo zainteresowani poprawą bezpieczeństwa maszyn produkcyjnych oraz nastawieni na udoskonalenia w tej dziedzinie. Kluczową kwestią dla przedsiębiorstw produkcyjnych jest zapewnienie bezpieczeństwa pracownikom, którzy uczestniczą w instalacji, obsłudze, dostosowywaniu i konserwacji urządzeń produkcyjnych. Są one jednak coraz bardziej złożone, a duża liczba interakcji pomiędzy operatorami i maszynami sprawia, że zapewnienie bezpieczeństwa ludzi i mienia staje się coraz większym wyzwaniem dla wielu przedsiębiorstw na całym świecie.

Silny nacisk na bezpieczeństwo jest niezwykle ważny, zwłaszcza w tych sektorach, gdzie używa się maszyn wykorzystujących ruch poziomy lub pionowy, które wymagają okresowych lub częstych interakcji z operatorem (np. operacje ładowania/rozładowywania). Obejmują one przemysł motoryzacyjny, opakowaniowy, farmaceutyczny, przetwórczy, tłoczenie (obróbkę plastyczną), działalność montażową oraz produkcję opon. Jednak ochrona przed zagrożeniami bezpieczeństwa nie jest łatwa; wprowadzanie zmian mających poprawić bezpieczeństwo maszyn może sprawić, że obsługa stanie się jeszcze bardziej skomplikowana i restrykcyjna. Środki ostrożności często obejmują czasochłonne procedury, takie jak: zatrzymanie pracy maszyny, odłączenie od energii elektrycznej, rozwiązanie problemów i proces ponownego włączania – wszystko to skutkuje stratą czasu produkcyjnego. Mimo to bezpieczeństwo zawsze musi stać na pierwszym miejscu, ponieważ wypadek może skutkować uszkodzeniem sprzętu, nieprzewidzianymi kosztami, utratą produktywności spowodowaną wyłączeniem oraz, co najważniejsze, poważnym uszczerbkiem na zdrowiu pracowników lub w najgorszym wypadku utratą życia.

Poprzez wprowadzenie odpowiednich procedur oraz technologii producenci urządzeń i użytkownicy końcowi mogą stworzyć bezpieczniejsze środowiska produkcyjne, które zmniejszają ryzyko związane z bezpieczeństwem operatorów bez obniżania produktywności. Podczas gdy użytkownicy końcowi są odpowiedzialni za szkolenie pracowników w bezpiecznych praktykach podczas pracy, producenci urządzeń muszą zaprojektować i skonstruować maszyny, które są bezpieczne i zgodne z regulacjami oraz dyrektywami rządowymi i przemysłowymi. Aby sprostać temu zadaniu, producenci maszyn muszą przeprowadzić analizę ryzyka, aby zidentyfikować istniejące zagrożenia zdrowia i bezpieczeństwa. Maszyny muszą zatem zostać zaprojektowane i skonstruowane przy użyciu metod, które obniżają zatem to ryzyko.

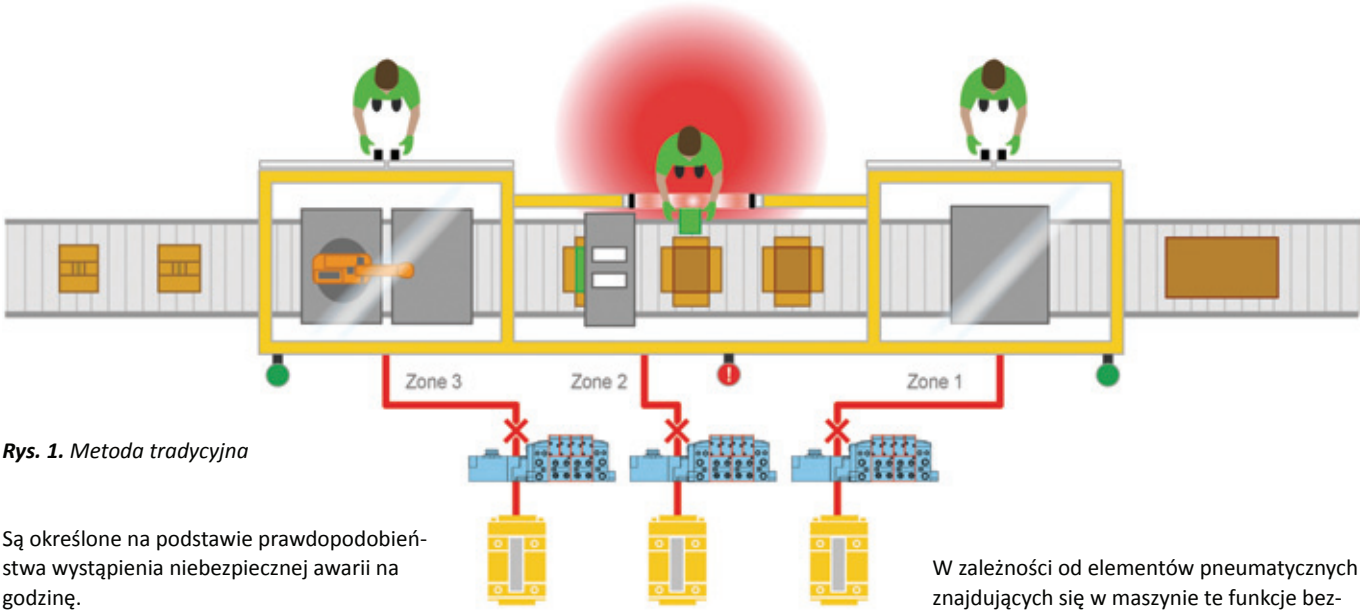
Dyrektywa maszynowa i normy bezpieczeństwa

Przez ostatnie dwadzieścia lat opracowano standardy, które ułatwiają wytwórcom produkcję bezpiecznych urządzeń. W Europie dyrektywa maszynowa 2006/42/WE weszła w życie w 2009 r. Chroni ona zdrowie i bezpieczeństwo osób podczas instalacji, użytkowania, dostosowywania oraz konserwacji maszyn. Dyrektywa jest przeznaczona dla producentów, importerów, a także dealerów maszyn oraz elementów bezpieczeństwa i obowiązuje dla nowo wyprodukowanych lub używanych maszyn w Europie. Ujednolica ona poziom bezpieczeństwa produktów zaprojektowanych i wyprodukowanych przez różnych wytwórców.

Dyrektywę tę uzupełniają różne normy. Na przykład norma ISO 13849-1 obejmuje zasady projektowania i konstrukcji części związanych z bezpieczeństwem elementów sterowniczych maszyn. Zawierają one podstawowe pojęcia, reguły projektowania i aspekty inżynieryjne, które mogą być wykorzystane podczas produkcji urządzeń, aby zapewnić bezpieczeństwo maszyn.

Norma ISO 13849-1 wprowadza trzy kluczowe pojęcia związane z projektowaniem maszyn oraz ich funkcjami dotyczącymi bezpieczeństwa. Są to:

- analiza ryzyka poprzedzająca projekt;
- uwzględnienie aspektów ilościowych funkcji bezpieczeństwa oraz kwestii jakościowych;
- wykorzystanie poziomu wydajności (PL) przy ocenie zdolności części związanych z bezpieczeństwem do realizacji funkcji bezpieczeństwa maszyn w przewidywanych warunkach.



Rys. 1. *Metoda tradycyjna*

Są określone na podstawie prawdopodobieństwa wystąpienia niebezpiecznej awarii na godzinę.

Według europejskich statystyk w zakresie wypadków przy pracy (ESAW) między 2009 r., gdy dyrektywa maszynowa 2006/42/WE weszła w życie, a 2013 r. odnotowano spadek wskaźnika wypadków przy pracy – bez skutku śmiertelnego o 12%, a ze skutkiem śmiertelnym o 15%. W tym samym okresie częstotliwość wypadków (liczba wypadków na 1000 pracowników) w sektorze produkcyjnym spadła o 9%, a liczba wypadków śmiertelnych w sektorze produkcyjnym o 13%.

Nawet jeśli ta dyrektywa została zapoczątkowana i ma swoje zastosowanie w Europie, istotne jest, aby rozwiązania były projektowane globalnie i nie tylko spełniały wymogi europejskiej dyrektywy, lecz przynosiły korzyści producentom i użytkownikom na całym świecie.

Tradycyjna metoda konstruowania pneumatycznych obwodów bezpieczeństwa – wykorzystanie dodatkowych spustowych zaworów bezpieczeństwa

Wyobraźmy sobie linię produkcyjną, gdzie operator ładuje część do maszyny spawalniczej. Gdy operator wchodzi lub sięga w stronę maszyny, cały ruch urządzenia musi zostać zatrzymany, aby zapewnić bezpieczeństwo. Aby spełnić obowiązujące wymogi dotyczące bezpieczeństwa, konstrukcja maszyny z elementami pneumatycznymi tradycyjnie zawierała oddzielne obwody bezpieczeństwa z dodatkowymi zaworami spustowymi, które odcinały dopływ powietrza, wypuszczały powietrze i zatrzymywały działanie całej maszyny.

Rozwiązanie to było stosowane przez wiele lat, jednak ma ono konkretne wady. Marnuje energię przez ciągłe spuszczanie z maszyny całego skompresowanego powietrza, które po wznowieniu działania trzeba ponownie załadować. Powoduje to stratę cennego czasu, gdy operator musi czekać, aż cały system ponownie się uruchomi. Metoda ta znacznie komplikuje konstrukcję maszyny, jej produkcję i instalację oraz zwiększa koszty, ponieważ wymaga droższych elementów i bardziej skomplikowanych struktur sterowniczych z systemem bezpieczeństwa wymaganym dla każdej strefy. Bez tych struktur sterowniczych nagłe ponowne wprowadzenie powietrza do systemu pneumatycznego może spowodować niezamierzone ruchy elementów maszyny, zwiększając przy tym ryzyko jej zniszczenia lub powodując, że produkty mocowane przy użyciu przyrządów montażowych, uchwytów lub zacisków mogą zacząć się ruszać lub odpadać, powodując uszkodzenie, rozlanie, utratę produktu i jego wybrakowanie. Próbując uniknąć uszkodzenia oraz w celu uzyskania oczekiwanego efektu, niektórzy operatorzy mogą niepotrzebnie pozostawiać maszynę włączoną, narażając siebie na wzmożone ryzyko przy wykonywaniu różnych działań.

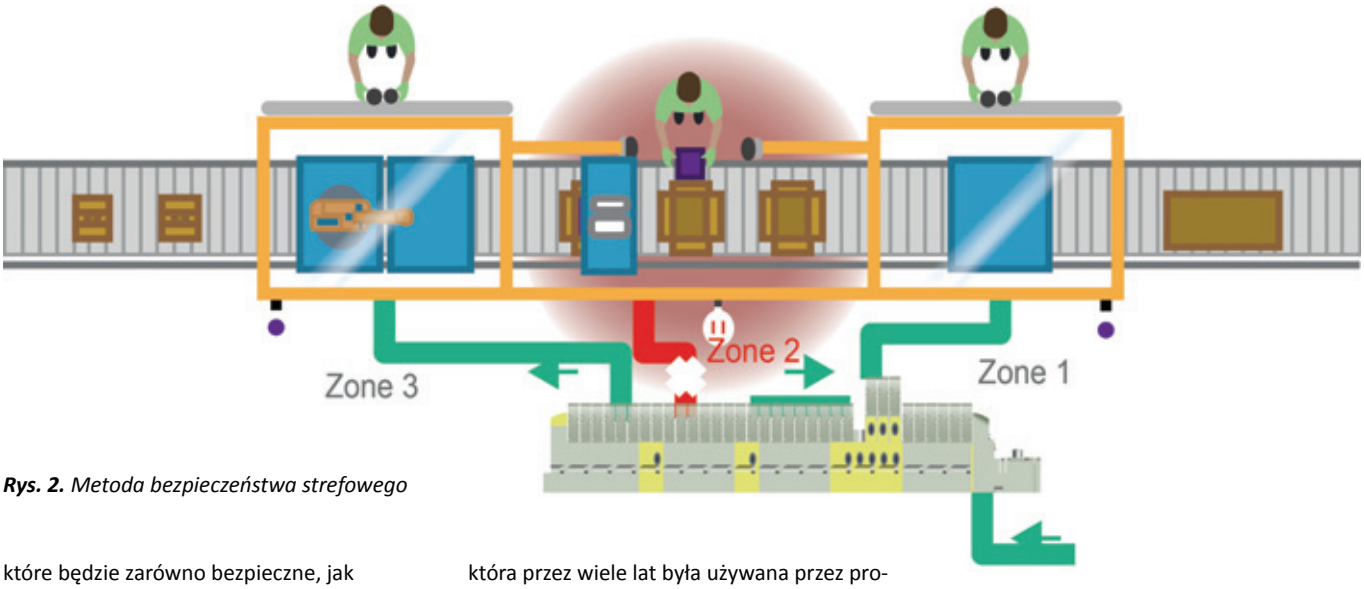
Warto wspomnieć, że jeśli dodatkowy zawór spustowy używany jest w cyklu ciągłym, jak pokazano powyżej (**rys. 1**), jego cykl życia może okazać się niewystarczający do osiągnięcia wymaganego poziomu wydajności (PL).

Lepszy sposób na osiągnięcie bezpieczeństwa obsługi maszyn

Obwody pneumatyczne mają trzy podstawowe funkcje bezpieczeństwa – uwolnienie energii, powrót oraz zatrzymanie ruchu. W zależności od elementów pneumatycznych znajdujących się w maszynie te funkcje bezpieczeństwa mogą być najbardziej wydajną i najbezpieczniejszą metodą. W przypadku niektórych zastosowań tradycyjne wykorzystanie zaworu spustowego jest najlepszym rozwiązaniem. Jednak w wielu innych bardziej wydajne byłoby zatrzymanie ruchu, powrót lub użycie innej kombinacji funkcji bezpieczeństwa, dostosowane do szczegółowych wymogów konkretnego urządzenia. Czasem bardziej wydajne jest zatrzymanie tylko niektórych części maszyny, gdy pozostałe działają normalnie. W związku z tym powstała koncepcja bezpieczeństwa strefowego – innowacyjna technologia, która zapewnia łatwiejszą i tańszą strategię bezpieczeństwa, spełniając jednocześnie wymogi dyrektywy maszynowej 2006/42/WE oraz normy ISO 13849-1.

Technologia bezpieczeństwa strefowego, wprowadzona przez firmę Emerson w systemach zaworowych marki ASCO™, upraszcza konstrukcję dodatkowych pneumatycznych obwodów bezpieczeństwa. Umożliwia to utworzenie maksymalnie trzech niezależnych stref bezpieczeństwa elektropneumatycznych, a jednocześnie istnienie niezależnych sekcji bez zabezpieczeń na jednej wyspie zaworowej. Systemy zaworowe ASCO™ ze strefami bezpieczeństwa zostały ocenione przez jednostkę certyfikującą TÜV Rheinland, która przypisała im kategorię 3 PLd. Jest to odpowiednie rozwiązanie dla większości stacji przeładunkowych oraz innych różnorodnych zastosowań przemysłowych, dostępne z różnymi węzłami Fieldbus. Alternatywne rozwiązania konkurencji pozwalają na odizolowanie tylko jednej strefy w wyspie, przez co są droższe i bardziej złożone.

Wykorzystując koncepcję bezpieczeństwa strefowego, można dostosować rozwiązanie,



Rys. 2. *Metoda bezpieczeństwa strefowego*

które będzie zarówno bezpieczne, jak i wydajne. Ponieważ strefy bezpieczeństwa można konfigurować tak, aby dostęp powietrza był odcinany tylko w konkretnej grupie zaworów, które kontrolują konkretny ruch maszyny w sąsiedztwie operatora, nie ma potrzeby wyłączania całego urządzenia. Zapewnia to bezpieczeństwo operatora, podczas gdy maszyna częściowo kontynuuje produkcję, nawet jeśli włączone są obwody bezpieczeństwa (**rys. 2**).

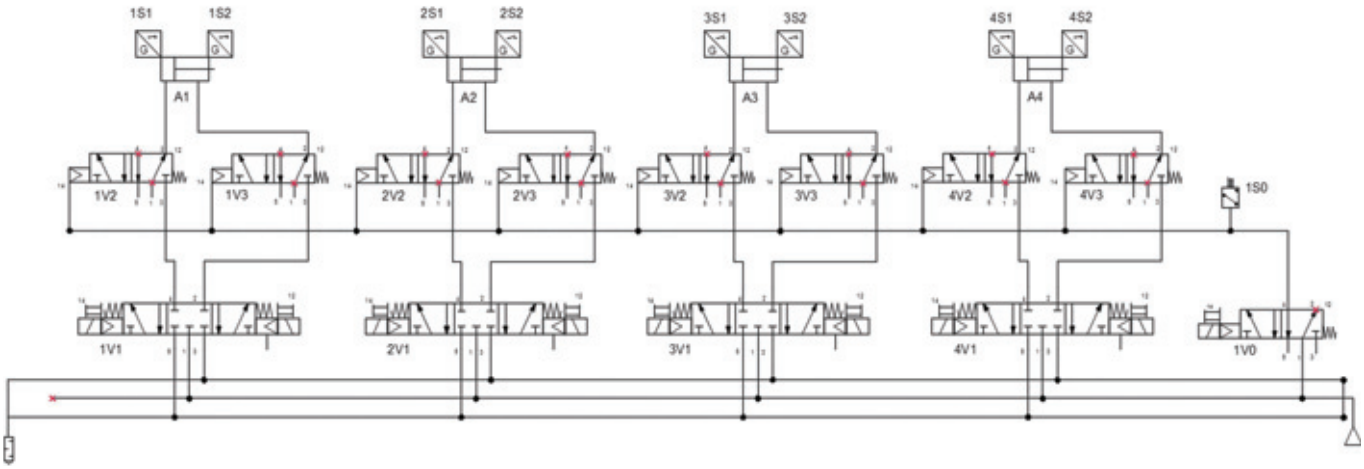
Ponieważ funkcję stref bezpieczeństwa opracowano dla platformy wyspy zaworowej, do kontrolowania strefy nie będzie konieczna rekonfiguracja ani dodatkowy spustowy zawór bezpieczeństwa, natomiast użytkownik posiada optymalną gamę opcji wyboru zaworów, akcesoriów oraz wymogów dotyczących przepływu. Zmontowany produkt jest bardzo podobny do standardowej wyspy zaworowej, która przez wiele lat była używana przez producentów urządzeń oraz konstruktorów maszyn.

Strategia bezpieczeństwa strefowego nie powinna być mylona z programem Lockout-Tagout (LOTO), który jest trybem używanym podczas serwisowania maszyny. W trybie tym personel techniczny włącza zawór spustowy w systemie pneumatycznym maszyny, usuwając i wypuszczając skompresowaną energię powietrza. Następnie odłącza się napięcie i na zaworze spustowym instalowana jest blokada fizyczna. Dzięki temu system pneumatyczny maszyny nie może być przypadkowo uruchomiony ponownie.

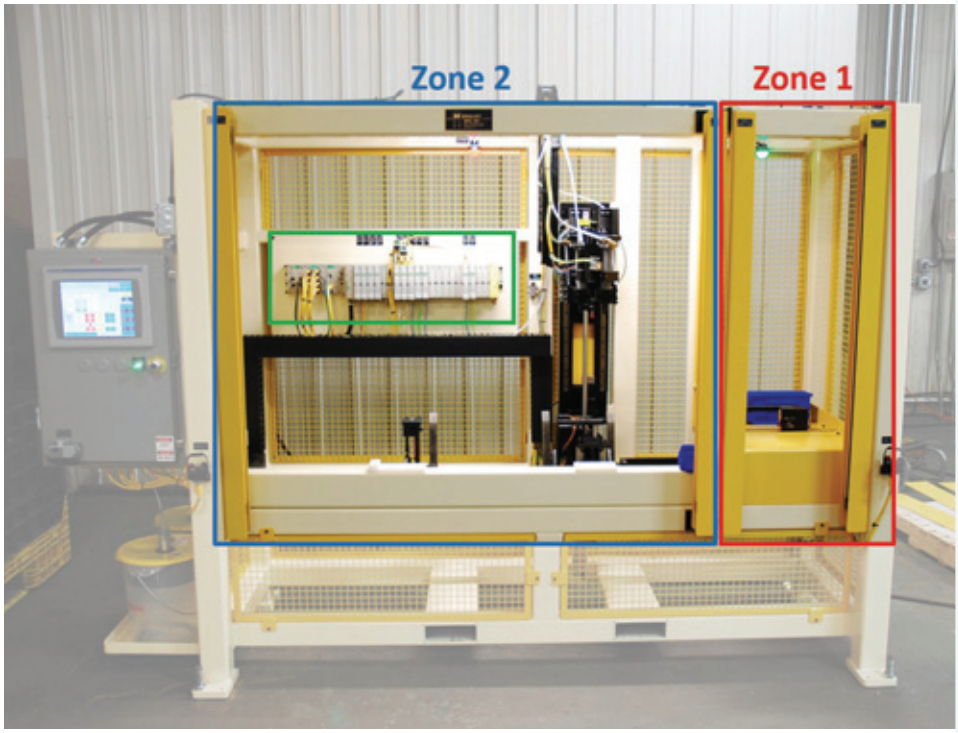
Jakie są korzyści?

Zastosowanie bezpieczeństwa strefowego w wyspie zaworowej zapewnia producentom urządzeń wiele korzyści. Prawdopodobnie najistotniejszą z nich jest możliwość uproszczenia konstrukcji dodatkowego obwodu bezpieczeństwa w systemie wyspy zaworowej. Aby odizolować sekcje maszyny, nie trzeba już stosować oddzielnego obwodu bezpieczeństwa z wieloma dodatkowymi zaworami spustowymi i innymi elementami, które są skomplikowane i kosztowne.

Możliwość łatwej i taniej konstrukcji wielu niezależnych obwodów bezpieczeństwa w jednej pneumatycznej wyspie zaworowej może zmniejszyć liczbę elementów systemu bezpieczeństwa aż o 35%, a dodatkowo



Rys. 3. *Schemat pneumatyczny wyspy zaworowej wyposażonej w system bezpieczeństwa strefowego, który izoluje jedną strefę, używając zaworu wykonawczego i zaworu sterowanego pilotem z zewnętrznymi komponentami dla dodatkowego zatrzymania ruchu.*



Rys. 4. *System strefowych zaworów bezpieczeństwa ASCO™ (zaznaczone na zielono), izolujących dwie strefy podczas zastosowania w branży motoryzacyjnej.*

optymalizuje użytkowanie sieci bezpieczeństwa i wymaga mniej prac hydraulicznych. Strategia ta zmniejsza również system bezpieczeństwa i umożliwia wykorzystanie cennej przestrzeni w maszynie i na wyspie zaworowej do innych celów.

Konstrukcja wielostrefowych obwodów bezpieczeństwa w wyspie zaworowej ze strefami bezpieczeństwa to dla większości producentów urządzeń rozwiązanie znane i przyjazne użytkownikowi.

Do zaworów systemu bezpieczeństwa dodano jedynie możliwość dodatkowego odcięcia napięcia i powietrze pilotujące. Dla właścicieli urządzeń i operatorów bezpieczeństwo strefowe to ułatwienie i niższy koszt przy jednoczesnej optymalizacji bezpieczeństwa maszyn. Co najważniejsze, można zwiększyć produktywność, bo przy włączonych obwodach bezpieczeństwa użytkownik nie musi wyłączać całej maszyny.

Stosowanie bezpieczeństwa strefowego w przypadku automatyzacji pracy

Zautomatyzowana maszyna może posiadać trzy stacje załadunkowe. Podczas gdy elementy poruszają się w dół, operator umieszcza tłoczoną metalową część w zespole spawanym. Aby uniknąć zranienia, nie powinien on zbliżać rąk do działającej powierzchni załadunku. Dla bezpieczeństwa operator musi przejść przez barierę fotokomórek, która odłącza zasilanie i powietrze pilotujące (tylko w dodatkowych zaworach pneumatycznych kontrolujących ruchome elementy na stanowisku pracy), dzięki czemu zatrzymuje niechciany ruch. Operator ładuje część do uchwytu, cofa się przez barierę fotokomórek, rozpoczyna operację i ponownie włącza maszynę.

Bezpieczeństwo operatora przebywającego w strefach załadunku musi zostać zapewnione zgodnie z dyrektywą maszynową 2006/42/WE i normą ISO 13849-1. Konwencjonalnym sposobem realizacji funkcji bezpieczeństwa jest jedna wyspa zaworowa przypadająca na obwód bezpieczeństwa w pierwszej stacji załadunkowej. Zasilanie tej stacji zapewniłby drogi, dodatkowy redundantny zawór bezpieczeństwa.

W obwodach bezpieczeństwa w drugiej i trzeciej strefie załadunku trzeba by zainstalować duplikat wyspy zaworowej oraz zawór spustowy.

Strategia bezpieczeństwa strefowego znacznie upraszcza konstrukcję, dzięki czemu możliwe jest bezpieczne działanie bez potrzeby spuszczania powietrza z całej wyspy. Trzy niezależne strefy w jednej wyspie zaworowej z funkcją bezpieczeństwa strefowego mogą niezależnie kontrolować funkcje bezpieczeństwa w trzech stacjach załadunku. Dodatkowe rozdzielacze, zawory spustowe i węzły sieciowe pokazane na **rys. 1** nie są zatem konieczne.

Wniosek

Wdrożenie dyrektywy maszynowej 2006/42/WE i normy ISO 13849-1 spowodowało nacisk na konstrukcję i produkcję bezpiecznych urządzeń produkcyjnych. Tradycyjnie dyskretne pneumatyczne obwody bezpieczeństwa projektowano z wykorzystaniem zaworów spustowych i innych elementów, aby zapewnić różnorodność. Te systemy bezpieczeństwa są jednak złożone, drogie i często wymagają wyłączenia całej maszyny produkcyjnej.

Konstrukcja bezpieczeństwa strefowego to zintegrowana strategia kontroli bezpieczeństwa, gdzie wiele niezależnych stref bezpieczeństwa może być utworzonych w obrębie jednego systemu pneumatycznej wyspy zaworowej. Powietrze i zasilanie są wyłączane jedynie w elementach kontrolujących urządzenie bezpośrednio przy operatorze. Gdy te obwody bezpieczeństwa są włączone, reszta maszyny może nadal działać.

Bezpieczeństwo strefowe znacznie upraszcza konstrukcję obwodu bezpieczeństwa i zmniejsza liczbę elementów systemu. Rozwiązanie to jest szczególnie polecane do wszystkich urządzeń produkcyjnych sterowanych pneumatycznie, które muszą spełniać wymogi dyrektywy maszynowej 2006/42/WE oraz normy ISO 13849-1.

Dowiedz się więcej na stronie www.Emerson.com lub skontaktuj się z nami.

EMERSON™

Emerson Automation Solutions
ASCO Numatics Sp. z o.o. – Polska
ul. Szturmowa 2A, 02-678 Warszawa
tel.: +48 22 458 92 88
e-mail: Biuro@Emerson.com
www.Emerson.com

Cyberbezpieczeństwo przemysłowych systemów sterowania (ICS)

Stosowanie w przemyśle nieprawidłowych praktyk cyberbezpieczeństwa może przynieść katastrofalne skutki. W artykule opisano metody powszechnie wykorzystywane do przeprowadzania cyberataków, a także sposoby zapobiegania różnym typom cyberataków oraz etapy wprowadzania ulepszeń w cyberzabezpieczeniach.

Osman Ahmed
Asad Rehman
Ahmed Habib

Cyberbezpieczeństwo zawsze było postrzegane przez wszystkich branżowców przemysłowego IT jako zabezpieczanie firm przed utratą danych, szpiegostwem przemysłowym oraz nieplanowanymi przestojami w zakładach. Jednak atak dokonany za pomocą złośliwego oprogramowania Triton (inne nazwy to Trisis lub HatMan) w 2018 roku pokazał inną stronę tego bardzo poważnego zagrożenia: możliwość doprowadzenia do prawdziwej katastrofy. W dalszej części tekstu opisano słabe punkty powszechnie wykorzystywane do przeprowadzania cyberataków oraz informacje na temat poprawy cyberbezpieczeństwa w zakładach przemysłowych.

Tradycyjnie przemysłowe systemy sterowania (ICS) były projektowane do pracy w izolacji, w swoich własnych sieciach sterowania. Jednak wraz z ewolucją innych technologii cyfrowych i komunikacji danych wykorzystywanych w zakładach przemysłowych, w tym: inteligentnych czujników, bezprzewodowych bram sieciowych, zdalnie zarządzanych systemów, wirtualizacji, chmury obliczeniowej, smartfonów oraz różnych inteligentnych aplikacji biznesowych, prawdopodobieństwo pozostawania systemów ICS wolnymi od zakłóceń powodowanych działaniami z zewnątrz zmniejsza się z dnia na dzień.

Pierwszym przypadkiem zewnętrznej manipulacji systemem ICS był atak dokonany za pomocą robaka Stuxnet w 2010 roku. Stuxnet był skryptem napisanym w celu przeprowadzenia sabotażu w sterownikach przemysłowych obsługujących wirówki wzbogacające uran (w Iranie). Następnie w 2013 roku miał miejsce atak za pomocą oprogramowania typu RAT (*remote access trojan*) o nazwie Havex. Jego celem były sieci elektroenergetyczne i zakłady energetyczne. Wskutek tego cyberataku wyciekły duże ilości danych, które wykorzystano w celach szpiegowskich i dokonywania sabotażu.

W 2015 roku pojawiły się dwa kolejne zagrożenia: malware BlackEnergy, które zniszczyło dane i pliki w stacjach elektroenergetycznych na Ukrainie, oraz IronGate – wirus znaleziony przez ekspertów przeglądających źródła publiczne (*Google Virus Total*), który spełniał tę samą funkcję co Stuxnet. Złośliwe oprogramowanie atakujące systemy przemysłowe nazwano Industroyer. Spowodowało ono spustoszenie w systemie elektroenergetycznym na Ukrainie w 2016 roku, kasując dane i wykonując ataki typu DDoS (*distributed denial of service*, rozproszona odmowa usługi) na sieć informatyczną systemu. Spowodowało to wyłączenie wielkiej elektrowni i przerwę w dostawie energii elektrycznej na Ukrainie.

W 2017 roku miał miejsce cyberatak dokonany za pomocą malware o nazwie Triton. Jego wykrycie zapobiegło poważnej katastrofie. Oprogramowanie to mogło zainfekować sterowniki przemysłowego systemu bezpieczeństwa Triconex (firmy Schneider Electric), dając hakerom możliwość zmiany parametrów bezpieczeństwa. Złośliwy atak mógł zmienić bezpieczne nastawy systemu sterującego

↘ Cyberbezpieczeństwo w przemyśle musi być inicjatywą na poziomie całej fabryki, obejmując współpracę nad projektem i platformą, analizę luk, wdrażanie zabezpieczeń oraz przeprowadzanie audytów.

sprzętem przemysłowym, co potencjalnie mogło spowodować wypadek tej samej wielkości co eksplozja w fabryce chemicznej Jiangsu Tianjiayi w Chinach w marcu 2019 roku.

Zrozumienie źródeł cyberataków

Pierwszym krokiem na drodze do zapobiegania zagrożeniom dla cyberbezpieczeństwa jest zrozumienie, skąd mogą pochodzić cyberataki, ponieważ osoby dokonujące ich w pierwszej kolejności prowadzą przez pewien czas swego rodzaju rekonesans – wyszukują i analizują słabe punkty w obiektach, które mają być celem ataku. W dłuższym okresie organizacja może wykonać analizę wektora zagrożenia do zidentyfikowania różnych metod, które mogą być wykorzystane przez hakerów lub na które system może być wrażliwy. Wszystko to musi być oparte na ryzyku wynikającym z analizy BIA (*business impact analysis*, analizy wpływu na biznes) wykonanej dla zasobów firmy. Użytkownicy mogą chcieć wykorzystać niektóre z dostępnych na rynku narzędzi analitycznych, używając ich do segregacji kluczowych zasobów od pozostałych i uzasadnienia tego podziału oraz wykonania analizy luk (*gap analysis*) w celu rozpoczęcia właściwych działań.

Sześć metod najczęściej wykorzystywanych do przeprowadzania cyberataków to:

1. Ataki dokonywane z zewnątrz za pomocą sieci zewnętrznych, Internetu oraz połączeń zdalnych, poprzez oprogramowanie do planowania zasobów przedsiębiorstwa (ERP), bramy sieciowe, repozytoria danych i dokumentów oraz programy do archiwizacji danych online.
2. Wykorzystanie nieprawidłowo skonfigurowanych elementów ochrony sieci lokalnej, tzw. firewalli i bram sieciowych.
3. Kradzież lub wyłudzenie (*phishing*) loginów i haseł dostępu użytkowników do stacji roboczych i komputerów sterujących w firmie.
4. Ataki fizyczne na systemy produkcyjne, w większości przypadków przeprowadzane za pomocą interfejsów operatorskich (HMI) oraz inżynierskich i operatorskich stacji roboczych.
5. Przeprowadzanie ruchu bocznego (poprzecznego) w sieci (*lateral movement*, *lateral network attack*), co ma na celu dokonanie ataku na sieci sterowania, i wykorzystanie przemysłowych protokołów komunikacyjnych do odkrycia innych urządzeń w sieci i rozprzestrzenienia złośliwego kodu.
6. Ataki przy wykorzystaniu inżynierii społecznej (*social engineering*), które koncentrują się na oszukiwaniu pracowników firmy (wykorzystywaniu ich naiwności i łatwowierności), posiadających niejawne i przypisane do nich informacje potrzebne do uzyskania dostępu, otwarcia bram sieciowych czy niezamierzonego uruchomienia skryptów.

Źródło: *Control Engineering* na podstawie informacji z Intech Process Automation

Zapewnienie cyberbezpieczeństwa – osiem środków zapobiegawczych

Do każdego typu ataku można przypisać osobny zestaw środków zapobiegawczych. Do takich środków i metod należą w szczególności:

1. **Segregacja zasobów i segmentacja sieci**

Może to się wydawać oczywiste, jednak staranna analiza luk w zabezpieczeniach sieci systemu sterowania, przy zaangażowaniu wykwalifikowanego personelu i odpowiednich narzędzi, potrafi bardzo często przyczynić się do wykrycia wielu niemonitorowanych punktów dostępu, które są ignorowane podczas realizowania standardowych praktyk zabezpieczania sieci sterowania. Źródłami tych zagrożeń mogą być:

- → brak ograniczeń dostępu do inżynierskich i operatorskich stacji roboczych,
- → nieaktualizowane oprogramowanie antywirusowe,
- → aplikacje i połączenia firm trzecich, które nie zostały odpowiednio zabezpieczone lub zweryfikowane,
- → brak tzw. stref zdemilitaryzowanych (*demilitarized zones* – DMZ) lub diod

danych (*data diodes*) przy eksportowaniu danych z sieci sterujących;
- kluczowe zasoby, które zostały podłączone do wspólnej domeny.

1. **Zarządzanie dostępem użytkowników**
Zadanie to obejmuje działania w celu ograniczenia nieautoryzowanego dostępu oraz śledzenie i zatrzymywanie wszelkiej działalności związanej z nieautoryzowanym dostępem. Są to:
- utrudnienie dostępu dla nieupoważnionego personelu,
- zarządzanie politykami cyberbezpieczeństwa i aktualizacja ich według ścisłego harmonogramu,
- wdrożenie uwierzytelniania wieloetapowego w całej organizacji,
- tworzenie tzw. białych list, dodanie uprzednio zatwierdzonych adresów, lokalizacji i alarmów opartych na portach, do identyfikacji systemów kontroli dostępu użytkowników,
- zmiana wartości domyślnych dla wszystkich haseł i kodów dostępu oraz okresowe, systematyczne zmiany haseł użytkowników.

2. **Częste patchowanie sprzętu sterującego i zabezpieczającego**
Patchowanie, czyli instalowanie najnowszych wersji oprogramowania układowego (*firmware*) całego sprzętu sterującego i zabezpieczającego, musi być wykonywane okresowo. Podczas gdy rutynowe, nieinwazyjne instalowanie tzw. łatek powinno być wykonywane dla wszystkich kluczowych sterowników i kontrolerów, to w najgorszym przypadku patchowanie powinno być wykonywane podczas każdej corocznej konserwacji systemu sterowania.

3. **Dokonywanie weryfikacji i walidacji oprogramowania, logiki i kodów wykonywalnych**
Testy dla celów weryfikacji i walidacji oprogramowania, logiki i kodów wykonywalnych zapewniają, że zmiany w logice, kodach i skryptach zostały wykonane celowo przez upoważnioną osobę. Emulowane środowiska walidacyjne pomagają w monitorowaniu wszelkich niepożądanych zmian w logice i parametrach sterowników, a ponadto pomagają operatorom w szkoleniach z obsługi sprzętu, bez ryzyka uszkodzenia rzeczywistych systemów fizycznych. Dostępne są narzędzia do automatycznego wykrywania wszelkich zmian na poziomie logiki i wszystkie te zmiany są wykonywane w kontrolowanym środowisku, przy utrzymywaniu kopii zapasowej, która jest gotowa do przywrócenia w przypadku powstania cyberzagrożenia dla sterownika lub systemu sterowania.

4. **Dodanie zabezpieczeń fizycznych do sterowników**
Biorąc pod uwagę niedawne cyberataki, niektórzy producenci systemów sterowania dodają obecnie do swoich sterowników blokady fizyczne, które zapobiegają wykonywaniu przez te sterowniki jakichkolwiek dodatkowych kodów, bez uprzed-

niego przejścia przez warstwę zabezpieczeń fizycznych.

5. **Przeprowadzanie szkoleń pracowników z zakresu cyberbezpieczeństwa**
Kluczowa część zagrożenia dla cyberbezpieczeństwa pochodzi od hakerów, którzy wykorzystują błędy popełniane przez personel fabryk. Nie można w zakładzie w pełni wdrożyć żadnego ze środków cyberzabezpieczeń, gdy cały personel związany z systemami sterowania nie jest odpowiednio przeszkolony i świadomy swojej odpowiedzialności. Należy więc przeszkolić personel z metod identyfikacji cyberataków, zabezpieczania swoich osobistych danych, uwierzytelniania oraz zabezpieczania się przed cyberatakami. Szkolenia te powinny być realizowane dla pracowników każdego poziomu: dyrekcji, kierownictwa, działów operacyjnych (OT), administratorów i użytkowników systemów.

6. **Opracowanie planu reagowania na cyberincydenty**
Na wypadek popełnienia błędów lub przeoczeń, które mogą być wykorzystane przez potencjalnych hakerów, działania mające na celu zapewnienie cyberbezpieczeństwa powinny obejmować opracowanie praktycznego planu dla personelu, opisującego działania niezbędne do wykonania po naruszeniu cyberbezpieczeństwa albo zidentyfikowaniu zagrożenia. Plany te po opracowaniu powinny być wypróbowane w praktyce, np. poprzez regularnie prowadzone warsztaty, i udostępniane całemu odpowiedzialnemu personelowi, który w przypadku naruszenia cyberbezpieczeństwa przeprowadzi szybkie działania.

7. **Utrzymywanie aktualizowanego rejestru zasobów**
Aby zmniejszyć ryzyko, należy utrzymywać aktualizowaną listę wszystkich będących na stanie zasobów OT, w tym przełączników sieciowych, routerów, firewalli, różnych usług webowych, oprogramowania dla systemów sterujących SCADA, serwerów danych historycznych, sterowników i kontrolerów lub wszelkich innych urządzeń wykorzystujących protokół internetowy (IP), z których każde może pozostawić lukę dla hakerów mogących wtedy eksplorować niezarządzany system. Zasoby mogą być monitorowane przez sieć pod kątem aktualizacji oprogramowania do najnowszych wersji, natomiast łatki i wszelkie miejsca wrażliwe na cyberataki mogą być monitorowane za pomocą różnych narzędzi administracji i ochrony sieci.

Cztery fazy realizacji inicjatywy cyberbezpieczeństwa

Uruchomienie inicjatywy cyberbezpieczeństwa dla systemów przemysłowych nie jest ani tak trudnym zadaniem, ani tak dużą inwestycją, jak mogłoby się wydawać na początku. Wielkość możliwych szkód sprawia, że nierozważanie przez firmy możliwości zainwestowania w cyberbezpieczeństwo jest po prostu naiwne.

Podobnie jak każda skuteczna inicjatywa na poziomie całej firmy, cyberbezpieczeństwo także wymaga posiadania w firmie odpowiednich specjalistów, którzy pomogą jej w zaadaptowaniu niezbędnych polityk i procedur. W większości przypadków najlepszym sposobem jest wyznaczenie osób odpowiedzialnych (*owners* – „właścicieli") za cyberbezpieczeństwo sieci biurowej oraz sieci systemu sterowania.

Cyberbezpieczeństwo w przemyśle musi być inicjatywą realizowaną na poziomie całej fabryki. Wdrażane jest w czterech fazach:

Faza 1. Projekt i platforma cyberbezpieczeństwa
Projektowanie systemu zarządzania cyberbezpieczeństwem jest najbardziej złożoną fazą, wymagającą najwięcej czasu i wysiłku. Jednak do dyspozycji firm przemysłowych jest na rynku wiele firm konsultingowych z branży cyberbezpieczeństwa. Ich główna działalność polega na pomocy zakładom w projektowaniu infrastruktury, polityk i procedur cyberbezpieczeństwa. Zadanie to obejmuje identyfikację wszystkich systemów i całego personelu powiązanego z cyberbezpieczeństwem, zdefiniowanie ich roli, dostępu i praw w systemach sterowania oraz budowanie polityk na podstawie tych parametrów w celu zapewnienia bezpiecznego realizowania operacji w zakładach. Faza projektowania cyberbezpieczeństwa wymaga znacznego wysiłku i udziału osób zainteresowanych w celu zapewnienia skutecznej realizacji tego projektu.

Faza 2. Odnalezienie i analiza luk w systemach
Faza odnalezienia luk w systemach zasadniczo obejmuje analizę projektu cyberbezpieczeństwa oraz zidentyfikowanie potencjalnych słabych punktów i ryzyk, w zależności od ich wpływu na firmę. Zidentyfikowane luki należy zawrzeć w projekcie i je aktualizować. Analizy mogą być wykonywane przez doświadczony personel oraz przy wykorzystaniu różnych narzędzi typu *Sniffer* (*Packet Sniffer*). Oprogramowanie to przechwytuje pakiety danych przepływających w sieci w celu wykrycia anomalii przepływu oraz luk w zabezpieczeniach systemu.

Faza 3. Opracowanie i wdrożenie polityk, procedur i praktyk cyberbezpieczeństwa
Ta część jest właściwym wdrożeniem polityk, procedur i praktyk cyberbezpieczeństwa. Na tym etapie przydaje się pomoc specjalistów z firm zewnętrznych, którzy mogą przyśpieszyć proces wyboru i wdrożenia oraz zapewnić, że wszystkie listy kontrolne zostaną wypełnione. Kluczową metodą jest tzw. utwardzanie systemu (*system hardening*).

Faza 4. Przeprowadzanie audytów cyberbezpieczeństwa
Audyty cyberbezpieczeństwa obejmują zadania takie jak kompleksowe testy penetracji, które mają zapewnić, że wdrożenie środków cyberbezpieczeństwa przynosi pożądane wyniki. Firmy specjalizujące się w audytach zwykle wykonują te zadania i pomagają swoim klientom w zapewnieniu właściwego poziomu cyberbezpieczeństwa. Ta część wymaga największego udziału specjalistów zewnętrznych w realizacji planu nowego wdrożenia. Jeśli jednak wewnętrzny zespół firmy przemysłowej, wyznaczony do przeprowadzania audytów, zostanie przeszkolony podczas wszystkich faz, to zespół ten może wykorzystać nabytą wiedzę i doświadczenie do przeprowadzania audytów w innych fabrykach i zakładach należących do firmy.

Osman Ahmed *jest dyrektorem ds. rozwoju firmy,* ***Asad Rehman*** *jest inżynierem projektantem oraz inżynierem aplikacji, a* ***Ahmed Habib*** *jest dyrektorem ds. marketingu w firmie Intech Process Automation, zajmującej się integracją systemów.* ■

Budowanie bezpiecznych sieci informatycznych
jako strategicznych szkieletów cyfryzacji przemysłu

Działy firm przemysłowych związane z technologią operacyjną (OT) oraz informatyczną (IT) muszą ze sobą współpracować i budować sieci, które efektywnie wykorzystują cyfryzację do tworzenia wydajnego i bezpiecznego środowiska w zakładzie.

Donald Mannon

Najnowsze osiągnięcia technologiczne branży IT, takie jak dostępność chmury obliczeniowej, zaawansowanej analizy danych i przetwarzania dużych zbiorów danych Big Data, doprowadziły do powstania koncepcji Przemysłowego Internetu Rzeczy (IIoT). Trzeba jednak mieć świadomość i pamiętać, że czynnikiem gwarantującym sprawne działanie IoT jest bezpieczne, niezawodne i deterministyczne usieciowienie nie tylko systemów IT, ale również sterowania i monitoringu. Dlatego przedsiębiorstwa przemysłowe pragnące osiągnąć kompleksową cyfryzację dla realizowanych przez siebie operacji muszą traktować bezpieczne sieci informatyczne jako strategiczny element – szkielet struktury i architektury sieci transmisji danych.

Bez tych sieci w nowoczesnych przedsiębiorstwach przemysłowych doszłoby do zastoju. Firmy muszą podejmować działania zmierzające do łączenia w zintegrowane sieci i platformy sieciowe swoich dużych zasobów strategicznych oraz zaawansowanych technologii informatycznych (IT), które wspierają użytkowników zarówno w biurach, jak i odległych lokalizacjach. Technologie te obejmują systemy planowania zasobów przedsiębiorstwa (ERP), systemy zarządzania relacjami z klientem (CRM), analizę wielkich ilości różnorodnych i zmiennych w czasie danych (Big Data) oraz inne kluczowe aplikacje, rezydujące w centrach danych, w chmurze obliczeniowej albo w obydwu tych lokalizacjach. Bezpieczeństwo danych i sieci oraz dostęp do nich są sprawą najwyższej wagi ze względu na integralność i prywatność danych oraz ochronę przed hakerami.

Źródło: Siemens

Aby utrzymać nieprzerwaną produkcję, technologia informatyczna musi zapewniać bezpieczną pracę połączonych w sieci maszyn i urządzeń, tworzących wspomniane technologie operacyjne. Są one uruchamiane na poziomie obiektowym/w terenie, a także wymagają zazwyczaj sterowania w tzw. czasie rzeczywistym i często pracują w ekstremalnych warunkach otoczenia. Warto dodać, że nowoczesne maszyny i urządzenia są wyposażone w tysiące czujników, siłowników, zaworów, przyrządów pomiarowych oraz innych urządzeń i modułów, zwykle pochodzących od różnych producentów – nie wspominając o samych maszynach, a nawet systemach przenośników, które także pochodzą z różnych źródeł. Jednocześnie wszystkie te komponenty muszą wymieniać dane operacyjne z dynamicznymi infrastrukturami „pionowymi", składającymi się z szerokiej gamy sterowników, systemów operatorskich oraz systemów realizacji produkcji (MES).

Niestety, wiele przedsiębiorstw przemysłowych zbudowało sieci jako komponenty infrastruktury IT/OT, a następnie dodało nowe sieci lub rozbudowało te już istniejące. Wynikiem tego są niewła-

ściwie skonfigurowane, segmentowe, nieoptymalne struktury sieciowe, tworzące „wyspy informacji", co uniemożliwia realizowanie procesów integracji i uzyskanie prawdziwej kompleksowej cyfryzacji. Pofragmentowana topologia sieci może spowodować powstanie słabych punktów w działach operacyjnych fabryk, które mogą wykorzystać hakerzy do uzyskania dostępu do kluczowych zasobów i danych na hali fabrycznej lub poza nią.

Wymagania sieci OT przekraczają wymagania sieci IT

Budowanie strategicznego szkieletu sieci, która będzie efektywnie i niezawodnie obsługiwała przepływ danych cyfrowych w przedsiębiorstwie cyfrowym, oznacza, że działy IT i OT tej firmy muszą ze sobą współpracować w celu spełnienia wymagań zarówno biurowych, teleinformatycznych, jak i produkcyjnych – transmisji danych w czasie rzeczywistym. Wymagania produkcyjne zawsze będą znacznie większe i krytyczne. Przykładowo polecenia z systemów sterowania muszą dotrzeć precyzyjnie do miejsca przeznaczenia i na czas, z dokładnością do milisekund, w celu otwarcia lub zamknięcia zaworu albo uruchomienia czy zatrzymania silnika.

Na poziomie makro wiele systemów sterujących – np. wykorzystywanych w elektroenergetyce, komunikacji publicznej i systemach transportowych, musi działać w czasie rzeczywistym lub zbliżonym do rzeczywistego oraz przy dyspozycyjności co najmniej 99,99%. Niezawodność, trwałość i dyspozycyjność są kluczowe, ponieważ stawką może być skomplikowana awaria urządzeń, procesów lub nawet ludzkie życie. Wypadki przy pracy oraz nieprzestrzeganie wymagań określonych odpowiednimi przepisami mogą ponadto pociągać za sobą wysokie kary pieniężne. W odróżnieniu od tego sieci IT przedsiębiorstw mogą działać na zasadzie dążenia do jak najlepszych osiągów w zakresie szybkości transmisji danych, ale przy opóźnieniach przesyłu danych znacznie większych od tych, jakie są dopuszczalne w sieciach OT. Użytkownicy w biurach nie zauważą 1- lub 2-sekundowego opóźnienia w dostarczeniu e-maila albo uzyskaniu dostępu do bazy danych, jednak tego rzędu opóźnienia mogą już znacząco zaburzyć proces produkcji, a nawet narazić na niebezpieczeństwo personel i środowisko.

Sieci wykorzystują nowoczesne przemysłowe standardy komunikacji

Złożone, zautomatyzowane systemy produkcyjne wymagają możliwości obsługi i poprawnego działania rozproszonego systemu sterowania (DCS). Organizacja struktury hierarchicznej systemu DCS zaczyna się od połączenia małych komponentów i maszyn, które znajdują się na hali fabrycznej, z programowalnymi sterownikami logicznymi (PLC). Z kolei sterowniki PLC łączą się z interfejsami operatorskimi (HMI), za pomocą których operatorzy mogą monitorować pracę maszyn i urządzeń oraz dostrajać parametry robocze według potrzeb.

Jeden lub wiele systemów DCS może być zintegrowanych pionowo w strukturze sieciowej z systemami wyższego rzędu, aby uzyskać możliwość ogólnego zarządzania produkcją i jej kompleksowy monitoring. Aby skutecznie i bezpiecznie przesyłać dane w sposób deterministyczny, nowoczesne przemysłowe protokoły komunikacyjne wykorzystują rozbudowaną priorytetyzację danych oraz techniki cyberzabezpieczeń, takie jak:

Multicasting. Protokół IGMP (*Internet Group Management Protocol*) umożliwia urządzeniom, routerom i przełącznikom w sieci OT transmisję krytycznych danych na zasadzie „jeden do wielu" (*one-to-many*) lub „wiele do wielu" (*many-to-many*).

Redundancja. W przypadku awarii dwa typy redundancji mogą obsługiwać czasy rekonfiguracji wynoszące kilka milisekund lub nawet mikrosekund.

Redundancja systemów. Rezerwowe systemy i podzespoły komunikacyjne pracują równolegle z systemami podstawowymi, przejmując ich zadania w razie ich awarii.

Redundancja mediów. W przypadku przerwania transmisji w sieci fabryka może kontynuować pracę dzięki wykorzystaniu zastępczych ścieżek komunikacyjnych. Dwoma wiodącymi protokołami są tu: zgodny z Profinet protokół MRP (*media redundancy protocol*) oraz HSR (*high-availability seamless redundancy*).

Segmentacja sieci i tworzenie VLAN. Wirtualne sieci lokalne (VLAN) mogą być utworzone przez podział jednej fizycznej sieci LAN na mniejsze sieci logiczne. Te oddzielne sieci separują systemy automatyki OT od systemów IT, co gwarantuje większe cyberbezpieczeństwo i optymalizuje pracę w czasie rzeczywistym. Przełączniki sieciowe warstwy 2 modelu ISO/OSI obsługują przepływ danych w granicach sieci VLAN, podczas gdy przełączniki i routery warstwy 3 kierują przepływem danych przez różne sieci VLAN.

Współpraca między działami IT a OT w sprawach sieci

Współpraca między działami IT a OT w firmach przemysłowych jest kluczem do połączenia każdego środowiska w strategicznej sieci szkieletowej z wykorzystaniem praktycznych, cyberbezpiecznych i niezawodnych sposobów, które oferują mocne strony i spełniają stawiane im wymagania. Ta współpraca może dostarczyć „to, co najlepsze z obydwu światów" w celu ułatwienia kompleksowej cyfryzacji, wymaganej dla zwiększenia efektywności operacyjnej, widoczności, elastyczności i cyberbezpieczeństwa. W pełni zdigitalizowane przedsiębiorstwa cyfrowe, wspierane przez dobrze współpracujące ze sobą działy IT i OT, uzyskają korzyści z dynamicznych przepływów danych podczas realizowania operacji.

Pracownicy działów IT przedsiębiorstw będą mogli szybciej realizować strategie biznesowe, szybciej uzyskiwać informacje zwrotne oraz praktyczne informacje dotyczące funkcjonowania zakładu, szybciej reagować na zmiany, wymagania i okazje tworzące się na rynku oraz skracać czas wprowadzania nowych wyrobów i usług na ten rynek. Natomiast pracownicy działów produkcyjnych (OT) poprawią niezawodność, widoczność i cyberbezpieczeństwo, co zwiększy dyspozycyjność i wykorzystanie maszyn.

Skuteczna współpraca pomiędzy działami IT a OT pomaga firmom w uzyskaniu przewagi nad konkurencją, która jeszcze w wielu przypadkach nie traktuje sieci informatycznych jako zasobów strategicznych.

Donald Mannon *jest specjalistą ds. rozwoju rynku przemysłowego w firmie Siemens Industry Inc.* ■

Konferencja i Wystawa

Smary & oleje

Smarowanie • Konserwacja • Tribologia

18 lutego 2020 | Hotel Ibis we Wrocławiu

ZAGADNIENIA PORUSZANE NA KONFERENCJI OBEJMUJĄ:

- Monitorowanie warunków – Online • On-Site • Offline
- Smary – Najnowsze osiągnięcia
- Zarządzanie cieczami – Innowacyjność i zrównoważony rozwój
- Smary – od projektu do aplikacji
- Tribologia – Badania ukierunkowane na doświadczenie
- Smary w specjalnych środowiskach
- Ciecze funkcjonalne – nie tylko smary
- Smary przy obróbce i formowaniu metali

Zarejestruj się już dziś na stronie:

www.smaryioleje.eu

Organizator:

INŻYNIERIA & UTRZYMANIE RUCHU

Bariery fizyczne i osłony na straży bezpieczeństwa

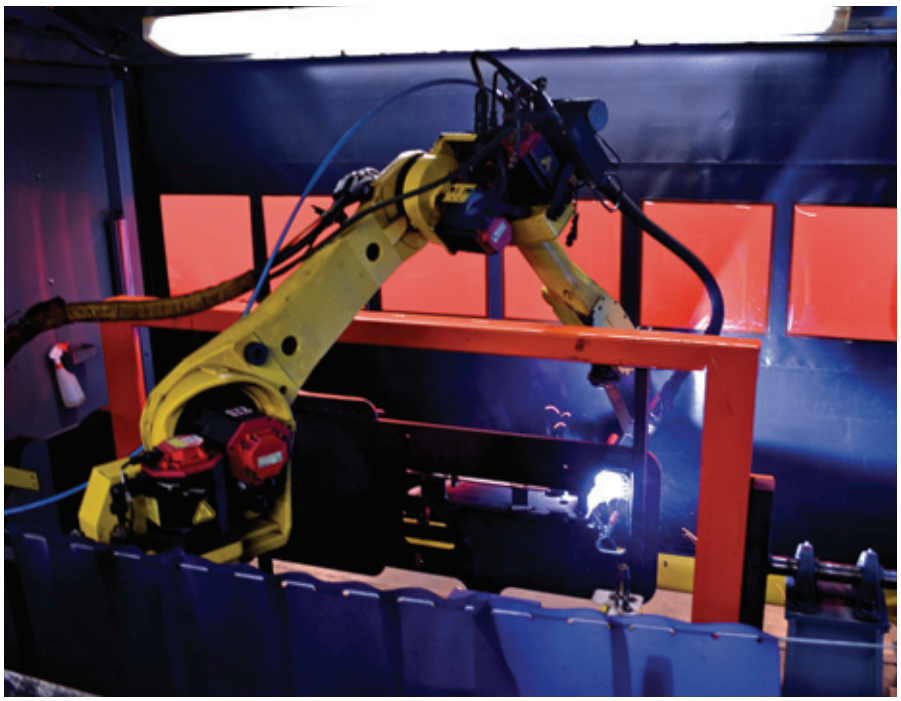
Bariery fizyczne, stanowiące istotny element zabezpieczenia pracowników w wielu aplikacjach przemysłowych, są często najlepszym wyborem po dokonaniu oceny ryzyka w miejscach, gdzie ludzie stykają się i współpracują bezpośrednio z maszynami.

John Ritter

Zawsze gdy praca ręczna może być automatyzowana, warto to robić ze względu na możliwy wzrost wydajności operacyjnej zakładu przemysłowego. Jednak należy pamiętać, że brak zastosowania odpowiednich zabezpieczeń dla pracowników może spowodować zagrożenia prowadzące do naruszenia przepisów i zasad BHP. Ponieważ we współczesnych warunkach rynkowych realizacja zamówień wymaga coraz krótszego czasu, co jest związane m.in. ze spełnianiem rosnących wymagań klientów dokonujących zakupów w sklepach internetowych, dyrektorzy zakładów przemysłowych poszukują każdego dostępnego rozwiązania, które pomoże im rozwiązać ten problem.

Maszyny mogą wykonywać żmudne i monotonne zadania, jak np. pakowanie w folię termokurczliwą, znacznie szybciej i zwykle z większą precyzją niż ludzie. Biorąc pod uwagę, że na całym świecie w przemyśle pracuje ponad 1,5 mln robotów przemysłowych, trudno wyobrazić sobie sprawne funkcjonowanie produkcji bez tych rozwiązań.

Niestety, istnieje zwiększone ryzyko zagrożeń w przypadkach, gdy maszyny i pracownicy koegzystują ze sobą, w szczególności na tych samych stanowiskach roboczych. Personel kierowniczy fabryk, który nadzoruje instalowanie nowego sprzętu, musi być świadomy tych zagrożeń i pomyśleć o zabezpieczeniach dla swoich pracowników. Nie jest to tylko najlepsza praktyka, ale konieczność wynikająca z przepisów prawnych.



Źródło: Rite-Hite

↖ Ryzyko może wzrosnąć wtedy, gdy maszyny i pracownicy koegzystują ze sobą na stanowiskach. Personel kierowniczy fabryk musi być świadomy tych zagrożeń i zatroszczyć się o odpowiednie zabezpieczenia dla swoich pracowników.

Zrozumienie regulacji i przepisów

Punkt interakcji (*point-of-interaction* – POI) pomiędzy robotami a pracownikami, podobnie jak w przypadku obsługiwania działających maszyn, występuje tam, gdzie często istnieje jednocześnie naj-

Źródło: Rite-Hite

Fizyczne bariery – osłony – ograniczają dostęp do procesu i zabezpieczają przed zagrożeniami wtórnymi, takimi jak dym, iskry, opary lub odpryski, związanymi ze zautomatyzowanymi operacjami spawalniczymi.

większe ryzyko oraz brak jednoznaczności przepisów normujących zasady pracy i jej bezpieczeństwa.

Najlepiej więc rozpocząć działania od zapoznania się z regulacjami w tym zakresie. W przypadku rynku amerykańskiego są to przepisy opracowywane przez OSHA (amerykańska Agencja Bezpieczeństwa i Zdrowia w Pracy). Według dyrektywy OSHA 29 CFR 1910.212(a)(3)(ii), „Wymagania ogólne dla wszystkich maszyn" (*General Requirements of All Machines*) procesy realizowane w kluczowych punktach interakcji muszą być zabezpieczane za pomocą osłon lub innych środków w celu zabezpieczania pracowników przed zranieniem. W Europie kwestie te reguluje norma EN ISO 14120, w Polsce wprowadzona norma PN-EN ISO 14120 „Bezpieczeństwo – Osłony – Ogólne wymagania dotyczące projektowania i budowy osłon stałych i ruchomych".

Przepisy dyrektywy OSHA stwierdzają: „Punkt obsługi maszyn, w którym pracownik jest narażony na zranienie, powinien być zabezpieczony. Urządzenie zabezpieczające powinno być zatem zgodne ze wszystkimi mającymi zastosowanie normami lub, w przypadku braku mających zastosowanie szczegółowych norm i standardów, powinno być tak zaprojektowane i skonstruowane, aby chroniło operatora przed dostaniem się jakiejkolwiek części jego ciała do strefy niebezpiecznej podczas cyklu operacyjnego".

W klauzuli OSHA: Obowiązki Ogólne, sekcja 5 podano:

a) Każdy pracodawca
   1. Musi zapewnić każdemu pracownikowi takie miejsce i warunki pracy, które są wolne od rozpoznanych zagrożeń, które powodują lub mogą spowodować śmierć albo poważne uszkodzenie ciała.
   2. Musi przestrzegać standardów BHP, podanych w niniejszym akcie.

Te regulacje OSHA wskazują wyraźnie, że bezpieczeństwa w pracy nie można ignorować. Jednak, ponieważ procesy realizowane w zakładach ciągle są modernizowane i ulepszane, a opracowane niemal 50 lat temu przez OSHA przepisy nie nadążają za postępami technologicznymi, obecnie są opracowywane nowe wytyczne bazujące na najlepszych praktykach.

Stowarzyszenie Przemysłu Robotycznego (*Robotics Industries Association* – RIA) opracowało dla rynku amerykańskiego normę ANSI/R15.06 Bezpieczeństwo Robotów Przemysłowych (*Industrial Robot Safety*). Odnosi się ona do norm obowiązujących również w Polsce: PN-EN ISO 10218-1 „Roboty i urządzenia dla robotyki – Wymagania bezpieczeństwa dla robotów przemysłowych – Część 1: Roboty" oraz ISO 10218-2: „Część 2: System robotowy i integracja". Normy te odnoszą się do robotów, systemów robotowych (robotycznych) oraz integracji. Norma amerykańska RIA 15.06 została napisana w celu zharmonizowania norm już obowiązujących w Europie. W swojej istocie norma ta wymaga lepszej identyfikacji zagrożeń, uwzględniania ruchu robo-

tów oraz specyficznych zadań, które one wykonują. Zgodnie z jej zapisami można zaprogramować bezpieczny ruch robota przy użyciu oprogramowania, które kontroluje obszar operacyjny robota i prędkość, z jaką może się on poruszać.

W pierwszej kolejności należy wykonać ocenę ryzyka

Norma RIA R15.06 wymaga wykonania oceny ryzyka. Wymienione wcześniej zabezpieczenia stanowisk obsługi maszyn są być może najtrudniejszym aspektem tej regulacji. Dotyczy to bowiem zarówno oddzielenia człowieka od maszyny, jak i zwiększenia bezpieczeństwa oraz efektywności prac.

Podczas dokonywania analizy należy wziąć pod uwagę wiele szczegółów. Niektóre z nich to układ albo projekt procesu, ograniczenia systemu oraz prawidłowe zidentyfikowanie wszystkich związanych z tym zagrożeń, opracowanie metod eliminacji zagrożeń i zmniejszenia ryzyka.

W wytycznych OSHA podano następujący wzór na obliczenie najlepszej odległości zabezpieczenia od maszyny:

$$DS = K \cdot T + DPF$$

gdzie **DS** oznacza bezpieczną odległość (*safety distance*), **K** – maksymalną prędkość, z jaką człowiek może się zbliżyć do źródła zagrożenia, **T** (*time*) – całkowity czas do zatrzymania niebezpiecznego ruchu, **DPF** (*depth penetration factor*) – współczynnik penetracji głębi urządzenia zabezpieczającego (określa odległość, jaką pokona pracownik, zanim zostanie wykryty przez to urządzenie, np. kurtynę świetlną).

Na podstawie tego wzoru zabezpieczenie ma zaleconą lokalizację, wyznaczoną w oparciu o pewną liczbę czynników, w tym zagrożenia wtórne, które mogą wyrządzić szkodę operatorowi maszyny. Wzór ma duże znaczenie dla określania, które z zabezpieczeń powinno zostać zastosowane i gdzie w danej fabryce.

Bezpieczeństwo w punkcie interakcji

Najbardziej podstawowymi urządzeniami stosowanymi do zabezpieczania pracowników realizujących operacje związane z produkcją przemysłową są: kurtyny świetlne, skanery laserowe oraz inne urządzenia wykrywające obecność. Po przerwaniu wiązki światła podczerwonego tych urządzeń następuje zatrzymanie zautomatyzowanego procesu.

W wielu przypadkach urządzenia te zapewniają akceptowalny poziom bezpieczeństwa. Jednak nie zawsze są one najlepszym wyborem do wszystkich aplikacji, szczególnie po wykonaniu oceny ryzyka. Jednym z największych problemów jest to, że pracownicy muszą przestrzegać reguły trzymania się od maszyn w pewnej odległości, wyznaczonej ze wzoru podanego przez OSHA, aby zmniejszyć ryzyko zranienia. Może to doprowadzić do konieczności budowania większych gniazd produkcyjnych, co z kolei pociąga za sobą dodatkowy czas, który potrzebny będzie pracownikom na pokonanie dystansu pomiędzy maszyną a obszarem bezpiecznym, gdy maszyna pracuje. W praktyce często pracownicy omijają ten system za pomocą skrótów, narażając się na niebezpieczeństwo. Ponadto pracownik, który wchodzi do gniazda produkcyjnego, może nadal być narażony na niebezpieczeństwo zranienia, gdy części maszyny po jej wyłączeniu jeszcze obracają się na skutek bezwładności.

Zautomatyzowane drzwi-bariery ochronne

Szybko działające drzwi-bariery ochronne lub zwijane kurtyny są często najlepszym wyborem, ponieważ każde z tych zabezpieczeń może wyeliminować zarówno narażenie na niebezpieczne ruchome części maszyn, jak i zagrożenia wtórne, których źródłem jest proces technologiczny/produkcji, potencjalnie eliminując ryzyko oraz stopień narażenia na niebezpieczeństwo.

W połączeniu z blokadami bezpieczeństwa (do poziomu zapewnienia bezpieczeństwa PLe, Kategorii 4 wg PN-EN ISO 13849-1 „Bezpieczeństwo maszyn – Elementy systemów sterowania związane z bezpieczeństwem – Część 1: Ogólne zasady projektowania" zautomatyzowane drzwi-bariery i kurtyny rozwijane oferują zwiększony poziom ochrony dla zabezpieczania punktu obsługi.

Ograniczają one dostęp do procesu i zabezpieczają przed zagrożeniami wtórnymi, takimi jak dym, iskry, opary lub odpryski, związanymi ze zautomatyzowanymi operacjami spawalniczymi, przez umieszczenie bariery pomiędzy operatorami maszyn a poruszającymi się częściami maszyn. Te typy zabezpieczeń w wielu sytuacjach są idealną alternatywą dla kurtyn świetlnych oraz innych urządzeń wykrywających obecność.

Bezpieczniejsza i bardziej efektywna automatyka

Wzór OSHA na bezpieczną odległość nie ma zastosowania dla zautomatyzowanych drzwi-barier z blokadą, ponieważ nie ma tam konieczności uwzględniania współczynnika penetracji głębi, co pozwala na umieszczenie zabezpieczenia znacznie bliżej obszaru niebezpiecznego. To koreluje z mniejszą przestrzenią przeznaczoną na „strefę bezpieczeństwa" i daje w wyniku końcowym zmniejszenie objętości gniazda produkcyjnego.

Eliminowanie przypadkowych wejść do gniazda produkcyjnego jest dodatkową korzyścią wynikającą ze stosowania zautomatyzowanych drzwi-barier z blokadą. W odróżnieniu od niewidzialnych wiązek podczerwieni w urządzeniach wykrywających obecność, bariery i osłony stanowią zabezpieczenie, które można zobaczyć. Fizyczna separacja, jaką realizują, jest wyraźnym wskaźnikiem optycznym, że operator maszyny wykonuje jakieś zadanie.

Prawidłowe zabezpieczanie operacji realizowanych przez maszyny

Personel kierowniczy musi zawsze poszukiwać nowej technologii, która może przyśpieszyć operacje realizowane w zakładzie przemysłowym. Jednak musi on także mieć przede wszystkim na uwadze przepisy BHP i uwzględniać je przed podjęciem każdej decyzji w tej sprawie. Ocena ryzyka w celu określenia najlepszego zabezpieczenia dla pracowników obsługujących maszynę jest tu pierwszym krokiem. Po sprecyzowaniu wyborów na podstawie wymagań przepisów BHP należy przeanalizować taką opcję zabezpieczeń, która najmniej wpływa na wydajność produkcji – zabezpieczenie fizyczne w postaci zautomatyzowanych drzwi-barier.

***John Ritter** jest menedżerem produktu w firmie Rite-Hite Doors.* ■

Obsługa nowoczesnych systemów bezpieczeństwa

Po zainstalowaniu złożonych systemów bezpieczeństwa procesowego sporym wyzwaniem okazuje się ich serwis i konserwacja. Pracownicy operacyjni i zajmujący się konserwacją muszą dobrze poznać i zrozumieć stan pracy systemu, wiedzieć, kiedy wprowadzono zmiany, sprawdzać je okresowo oraz mieć poczucie, że są odpowiednio przeszkoleni do pracy przy tych systemach. Efektywny program obsługi może przyczynić się do uniknięcia niepotrzebnego zadziałania zabezpieczeń oraz zbędnych wyłączeń.

Johan School

Aby zwiększyć efektywność produkcji i sprostać wymaganiom konkurencyjnego rynku, współczesne fabryki i zakłady przemysłowe zbliżają się sukcesywnie do swoich ograniczeń operacyjnych, co stwarza większe zagrożenia dla bezpieczeństwa pracy ludzi i maszyn. Ponadto coraz bardziej rygorystyczne przepisy dotyczące bezpieczeństwa mogą zwiększyć konieczny zakres aplikacji bezpieczeństwa w jednostkach operacyjnych. Natomiast dokonane za pomocą złośliwego oprogramowania (*malware*) ataki na systemy bezpieczeństwa w przemyśle mogą z kolei prowadzić do zwiększenia obaw związanych z cyberbezpieczeństwem zautomatyzowanych i zdigitalizowanych fabryk.

Rola przyrządowego systemu bezpieczeństwa

W operacjach realizowanych w przemyśle procesowym, przy klasycznym podejściu organizacyjnym struktur systemów wsparcia produkcji, rozproszony system sterowania (*distributed control system* – DCS) zarządza normalną pracą urządzeń w fabrykach, podczas gdy przyrządowy system bezpieczeństwa (*safety instrumented system* – SIS) chroni pracowników, środowisko oraz monitorowany sprzęt. System SIS składa się z czujników, jednostek logicznych sterowników bezpieczeństwa (*logic solver*) oraz końcowych elementów sterujących. Jego zadaniem jest sprowadzenie realizowanego procesu technologicznego/produkcji do stanu bezpiecznego, jeżeli wystąpią warunki, parametry pracy urządzeń i inne, przekraczające określone ograniczenia. Celem tych działań jest uniknięcie w fabrykach i otaczających je obszarach takich zdarzeń, jak pożary, eksplozje i uszkodzenia sprzętu.

Konwencjonalny SIS jest systemem wielopłaszczyznowym, wymagającym od personelu zakładowego wykonywania pracochłonnych procesów w celu utrzymania integralności bezpieczeństwa w całym okresie eksploatacji tej fabryki. Prace te są często utrudniane przez:

- problemy z konserwacją systemu spowodowane ograniczoną widocznością stanu technicznego zasobów,
- niezdolność do analizowania działania systemu podczas realizowania operacji w fabryce,
- potrzebę kompleksowego szkolenia w celu zrozumienia funkcjonalności bezpieczeństwa,
- trudność w interpretowaniu zapisów zdarzeń i alarmów z przeszłości,
- brak zrozumienia celów systemu SIS,
- problemy z zarządzaniem i zapisywaniem historycznych danych dotyczących bezpieczeństwa.

Z punktu widzenia utrzymania ruchu ważną normą jest IEC 61511, wprowadzoną w Polsce normą PN-EN 61511 – „Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego", ponieważ określa ona wytyczne na temat regularnej konserwacji/walidacji i weryfikacji systemu bezpieczeństwa, dokonywanej przez przeszkolony personel.

Strategia zabezpieczania zasobów

Organizacje przemysłowe doświadczają rosnących kosztów wdrażania skutecznych rozwiązań systemów bezpieczeństwa. Muszą także rozwiązywać problem braku fachowców lub mniejszej ilości dostępnych zasobów ludzkich. Z tego powodu stosowane przez nie systemy bezpieczeństwa muszą być łatwe do zrozumienia i konserwacji oraz wystarczająco elastyczne, aby mogły być wykorzystywane w wielu różnych aplikacjach bezpieczeństwa.

Najlepszym rozwiązaniem systemu bezpieczeństwa w przemyśle jest takie, które zapobiega problemom, zanim wystąpią. Niestety, starzejąca się zainstalowana baza systemów bezpieczeństwa procesowego jest zwykle duża, złożona i trudna do utrzymania przez tych samych ludzi, dla których zostały one kiedyś zaprojektowane i zainstalowane.

Infrastruktura SIS wymaga wykonywania starannej konserwacji zapobiegawczej i naprawczej w celu zapewnienia, że oczekiwany poziom bezpieczeń-

stwa jest realizowany i utrzymywany. Aby firma pozostała konkurencyjna i funkcjonowała zgodnie z przepisami, operatorzy w zakładzie muszą zadbać o to, by sprzęt zabezpieczający cały czas działał zgodnie z wymaganiami i z najwyższą wydajnością. Ważne jest, aby system zaprojektowany do pracy na poziomie nienaruszalności bezpieczeństwa SIL 3 (*safety integrity level*) rzeczywiście realizował wytyczne opisujące poziom zabezpieczeń SIL 3 i nie uległ degradacji do niższego poziomu bez wiedzy pracowników działu operacyjnego fabryki.

Wymagane są różne działania konserwacyjne, w których dokonuje się próbnego zadziałania zabezpieczeń systemu w celu zagwarantowania jego poprawnego działania, zgodnie ze zdefiniowaną specyfikacją wymagań dotyczących bezpieczeństwa. Fizyczna inspekcja systemu bezpieczeństwa może obejmować standardową konserwację obudów, w tym wymianę filtrów wlotowych powietrza, sprawdzenie parametrów zasilania i stanu baterii itd.

W przypadku wykrycia awarii w obiekcie lub w rzeczywistym systemie bezpieczeństwa wymagana będzie poprawna konserwacja. Awaria może być związana ze sprzętem, oprogramowaniem lub sprzętem i okablowaniem obiektowym.

Wyzwania dotyczące obsługi systemu

Ponieważ zasoby systemów bezpieczeństwa starzeją się, a doświadczony personel odchodzi na emeryturę, to wiedza na temat procedur prawidłowego i bezpiecznego utrzymania ruchu w firmie przemysłowej może zostać utracona. W niektórych przypadkach sprzęt nigdy nie był wymieniany na nowocześniejszy, a zatem nowe procedury muszą być w pełni zrozumiane, aby uniknąć nieplanowanych opóźnień lub poważnych zagrożeń dla bezpieczeństwa.

Problemy z obsługą systemu bezpieczeństwa są następujące:

- brak kompetencji personelu,
- złożoność aplikacji,
- różni producenci systemów,
- skalowalność platform.

Brak kompetencji personelu. Kompetencje personelu związanego z utrzymaniem systemu bezpieczeństwa są opisane w normie PN-EN 61511. Norma ta podaje w szczegółach wymagania dotyczące kompetencji osób zajmujących się konserwacją i obsługą systemu SIS w ciągu jego okresu eksploatacji. Wykonywane przez te osoby prace obejmują: testy kontrolne, inspekcje, zarządzanie zmianami, analizę oddziaływania, zarządzanie omijaniem procedur oraz zapisywanie danych dotyczących utrzymania ruchu w celu dokumentowania dowodów na to, że komponenty i podsystemy są odpowiednie do wykorzystania w systemie SIS.

Złożoność aplikacji. Im bardziej złożony jest system bezpieczeństwa oraz im większa jest liczba producentów tych systemów, tym bardziej skomplikowane stają się wymagania dotyczące szkoleń dla pracowników firm przemysłowych. Nowoczesne systemy o uproszczonych architekturach i ulepszonej diagnostyce umożliwiają ich obsługę i utrzymanie przez mniej wyspecjalizowany personel.

Praktyka wykazała, że posiadanie systemów bezpieczeństwa zainstalowanych w odległych lokalizacjach, takich jak rurociągi, odwierty oraz platformy wiertnicze, zwiększa koszty obsługi, ponieważ do czynności konserwacyjnych takich instalacji wymagani są technicy o wysokich umiejętnościach. Zaawansowana technologia bezpieczeństwa z możliwością dokonywania zdalnej diagnostyki pomaga w łagodzeniu tego problemu oraz zmniejsza wydatki operacyjne (OPEX).

Różni producenci systemów. Wykorzystywanie wielu platform bezpieczeństwa stwarza problem dla personelu utrzymania ruchu z powodu nieczęstych interakcji z systemem bezpieczeństwa, co może prowadzić do niepotrzebnych opóźnień, gdy wymagane jest rozwiązywanie problemów. Ponadto wymagane są wtedy większe inwestycje w narzędzia inżynierskie i części zamienne.

Skalowalność platform. Innym problemem użytkowników końcowych jest wybór takiego systemu bezpieczeństwa, który spełnia ich specyficzne wymagania dotyczące wielkości, dostępności i kosztów systemu. Zakłady przemysłowe poszukują takiej platformy bezpieczeństwa, która może być skalowana dla różnych aplikacji, od małych do dużych, co pozwala na wykorzystanie jednej wspólnej platformy w całym przedsiębiorstwie.

Postępy w technologii bezpieczeństwa

Organizacje przemysłowe zdają sobie sprawę z zalet standaryzowania architektury pojedynczego systemu bezpieczeństwa oraz wykorzystywania go w różnych aplikacjach w całej fabryce czy przedsiębiorstwie. Organizacje te czerpią ponadto korzyści z rozwiązań zintegrowanego bezpieczeństwa i rozproszonych systemów sterowania oraz prostoty współpracy partnerskiej z jednym tylko dostawcą rozwiązań dla wszystkich swoich potrzeb.

Nowa generacja zaawansowanych rozwiązań systemów bezpieczeństwa wykorzystujących modułową i skalowalną konstrukcję może funkcjonować jako pojedyncza platforma dla wszystkich aplikacji bezpieczeństwa w przedsiębiorstwie, pozwalając właścicielom fabryk, którzy często wykorzystują wiele różnych platform systemów bezpieczeństwa, skonsolidować i zredukować koszty szkoleń dla pracowników oraz zatrudniania wyspecjalizowanych inżynierów, a także zmniejszyć zapasy części zamiennych.

Najnowsze rozwiązania bezpieczeństwa wykorzystują uniwersalną technologię wejść/wyjść (We/Wy, I/O), co pozwala na indywidualną konfigurację każdego kanału dla różnych typów We/Wy (wejście analogowe AI, wyjście analogowe AO, wejście cyfrowe DI lub wyjście cyfrowe DO). Ponadto wykorzystanie wirtualizacji w trybie offline i technologii chmury obliczeniowej umożliwia odseparowanie konstrukcji fizycznej od funkcjonalnej, co pozwala na równoległe przepływy robocze i standaryzowane konfiguracje oraz wykonywanie prac inżynierskich i przeprowadzanie testów z każdego miejsca na świecie.

Zaawansowane rozwiązania bezpieczeństwa, wykorzystujące inteligentne oprogramowanie i bardziej solidny sprzęt, wymagają mniej testów kontrolnych i weryfikacji funkcjonalności. Wymagania dotyczące częstotliwości przeprowadzania testów mogą być zredukowane do 1 na 10 lub nawet 20 lat w niektórych przypadkach, co w sposób kolosalny zmniejsza koszty operacyjne.

Zaawansowane rozwiązania systemów bezpieczeństwa pomagają ponadto w zastąpieniu wiedzy pracowników odchodzących na emeryturę. Dzięki implementowanym funkcjom samodiagnostyki rozwiązania te są w stanie poin-

formować personel utrzymania ruchu, że wymagane jest przeprowadzenie prac konserwacyjnych i jaki typ prac jest konieczny do realizacji. To może pozwolić na pominięcie zaplanowanych w harmonogramie prac konserwacyjnych lub odłożenie ich na najbardziej dogodny termin.

Dzięki ścisłej kontroli oraz integracji systemu bezpieczeństwa zakłady mogą uzyskać takie korzyści, jak: zmniejszona liczba baz danych, łatwy dostęp do danych historycznych oraz raporty z kompleksowych analiz. Informacje na temat problemów związanych z bezpieczeństwem albo awariami sprzętu mogą być udostępniane operatorom systemu sterowania DCS, zaś problemy te mogą być rozwiązywane bez konieczności wyjazdów pracowników w teren w celu zdiagnozowania problemu i dokonania naprawy.

Najnowszy, usprawniony system SIS wykorzystuje tyko kilka komponentów, co odróżnia go od istniejących w zakładach przemysłowych starszych systemów, składających się z niezliczonej liczby pojedynczych komponentów i części. Tak więc jest on łatwiejszy w utrzymaniu oraz diagnozowaniu awarii. Wykorzystanie koncepcji uniwersalnych kanałów We/Wy zapewnia optymalne gabaryty i niższe całkowite koszty instalacji (TIC). Inżynierowie mogą teraz konfigurować wszystkie odmiany systemu za pomocą tego samego modułu We/Wy, podczas gdy przedtem musieli dysponować wieloma typami modułów We/Wy, aby osiągnąć ten sam wynik. Ponadto dzięki mniejszej liczbie komponentów fabryki nie muszą mieć w magazynie większej ilości części zamiennych. Dodatkowo płynna integracja takiego systemu z fabrycznym systemem sterowania DCS, zaawansowanymi aplikacjami i narzędziami inżynierskimi dostarcza personelowi działów operacyjnych i utrzymania ruchu kluczowych informacji na temat działania i statusu systemu.

Modułowe i skalowalne rozwiązania systemu SIS są łatwe w konfiguracji, tak więc stanowią małe i duże rozproszone aplikacje bezpieczeństwa, dotyczące zmiennych poziomów redundancji. Można odnotować kilka kluczowych zalet wykorzystania odległych modułów wejść/wyjść oraz szaf sterowniczych znajdujących się w niebezpiecznych lokalizacjach. Obejmują one uproszczoną konstrukcję, w której sterowniki i układy We/Wy są dobrane technicznie do obszaru procesowego. Ponadto istnieją tam warstwy redundancji ze sterownikami i układami We/Wy zainstalowanymi na każdym sprzęcie.

Korzyści dla operatorów

Innowacje w technologii systemów bezpieczeństwa, obejmujące metodologię Lean w realizacji projektów, uniwersalną technologię We/Wy, zaawansowaną diagnostykę, integrację z systemami DCS oraz zmniejszoną liczbę narzędzi/aplikacji programowych dzięki wykorzystaniu technologii chmury obliczeniowej do wykonywania prac inżynierskich i walidacji, co może pomóc w optymalizacji operacji oraz zwiększeniu bezpieczeństwa zakładów przemysłu procesowego.

Te nowoczesne rozwiązania uprościły konstrukcję systemu oraz związane z nim prace inżynierskie, rozwojowe i testowanie, jednocześnie redukując czas i koszty potrzebne na szkolenia dla pracowników i prace inżynierskie. Ponadto zminimalizowały wymagania dotyczące konserwacji i posiadania personelu technicznego o wysokich kwalifikacjach. Ostatnio systemy te są zabezpieczane przed cyberatakami, co jest potwierdzone przez certyfikaty amerykańskiego instytutu ISA Secure.

Dzięki zintegrowanemu podejściu do sterowania i bezpieczeństwa zakłady przemysłu procesowego mogą osiągnąć takie korzyści, jak:

- zmniejszona liczba baz danych i narzędzi inżynierskich,
- integracja alarmów i zdarzeń,
- lepsza obsługa sterowania procesami oraz alarmami systemu bezpieczeństwa,
- zautomatyzowane śledzenie, zapisywanie i zatwierdzanie systemów bezpieczeństwa oraz elementów końcowych w całym okresie eksploatacji systemu bezpieczeństwa,
- rozszerzone zbieranie i zapisywanie informacji dotyczących sekwencji zdarzeń (SOE),
- rozszerzony widok danych dotyczący stanu technicznego zasobów systemu,
- bezpieczna integracja z podsystemami w fabryce, np. pożarowymi i gazowymi, cyberzabezpieczeniami itd.

Dzięki optymalizacji kosztów i działania systemu SIS w okresie jego eksploatacji organizacje przemysłowe są w stanie:

- minimalizować przerwy i zakłócenia w realizacji procesów, co ogranicza przestoje,
- zmaksymalizować efektywne i wydajne wykorzystanie zasobów systemu bezpieczeństwa,
- zmniejszyć wymagania dotyczące testowania i konserwacji,
- przekazywać operatorom praktyczne i niezawodne dane oraz wiedzę na temat bezpieczeństwa.

Możliwość obsługiwania różnorodnych aplikacji bezpieczeństwa przez jedną wspólną platformę zmniejsza zapotrzebowanie zakładów przemysłowych na fachowców oraz upraszcza zarządzanie częściami zamiennymi. W przypadku najnowszych rozwiązań systemów SIS dzięki wykorzystaniu uniwersalnych modułów We/Wy istnieje tylko „garstka" komponentów do zarządzania na początku pracy z nowym systemem.

Podsumowanie

Organizacje przemysłowe, które dokonują migracji swoich starzejących się platform SIS do platform wykorzystujących zaawansowaną technologię komunikacji danych i integracji, mogą wykorzystać wiele funkcji, które upraszczają diagnostykę i konserwację systemu bezpieczeństwa. Rozwiązania te mogą udostępniać dane systemom DCS, zaawansowanym aplikacjom oraz narzędziom inżynierskim bezpieczeństwa, co pomaga pracownikom działów operacyjnych i utrzymania ruchu w zrozumieniu warunków pracy systemu w czasie rzeczywistym, danych historycznych dotyczących jego pracy oraz wymagań dotyczących konserwacji.

Dzięki wdrożeniu nowoczesnego rozwiązania systemu bezpieczeństwa, wyposażonego w innowacyjne funkcje i możliwości, menedżerowie i operatorzy w zakładach mogą efektywnie rozwiązywać problemy związane z konserwacją takiego systemu przy braku wyspecjalizowanych fachowców, a także ograniczać złożoność tematyki szkoleń i wsparcia oraz obniżać koszty posiadania części zamiennych.

Johan School *jest menedżerem produktu specjalizującym się w systemach bezpieczeństwa. Pracuje w Centrum Doskonałości Bezpieczeństwa firmy Honeywell w Hertogenbosch w Holandii.* ■

Jak zbudować
kulturę bezpieczeństwa w zakładzie

Podstawą w budowaniu bezpiecznego środowiska pracy jest standaryzacja wymagań w zakresie bezpieczeństwa. Program, który pozwala osiągać cele takiej standaryzacji wymagań, powinien bazować na audytach wewnętrznych, spójnej i skutecznej komunikacji oraz strategii Lean manufacturing.

Bill D'Amico

Zakłady przemysłowe od dziesięcioleci skupiają się na eliminacji ryzyka wypadków i związanych z nimi zranień pracowników. Inwestują czas i zasoby w celu opracowania wspólnych zasad, praktyk i postaw w zakresie bezpiecznej pracy. Dla wielu organizacji idea bezpieczeństwa jest nawet sposobem na prowadzenie biznesu. To swego rodzaju nowa kultura osiągnięć kierowanych potrzebą zapewnienia bezpieczeństwa w miejscu pracy, która jest procesem ewolucyjnym, zachodzącym już od dłuższego czasu. Nie pojawiła się ona z dnia na dzień ani też przypadkowo.

Trzeba mieć świadomość, że nawet jeśli firma dokonała znacznego postępu w tworzeniu nowej kultury w zakresie bezpieczeństwa, to przed nią jeszcze długa droga związana z jej wdrożeniem. Co więcej, zawsze będą zachodzić zmiany w przepływach roboczych, konieczne adaptacje do nowych technologii oraz będzie

↘ Standaryzacja wymagań w zakresie bezpieczeństwa jest podstawą w budowaniu bezpiecznego środowiska pracy.

Źródło: Victaulic

istniała potrzeba zatrudniania i szkolenia nowych pracowników, którzy następnie będą musieli być zaznajomieni z tymi nowymi zagadnieniami i wdrożeniami. Ulepszenia, poprawki i szkolenia są niezbędne do utrzymania kultury bezpieczeństwa w miarę upływu czasu.

Bezpieczeństwo rozpoczyna się od standardów

Standaryzacja wymagań bezpieczeństwa to ogromna wartość. Ustalone kryteria bezpieczeństwa, które zostały potwierdzone przez stronę trzecią, mogą pozwolić na dokonanie istotnych zmian w zabezpieczeniach pracowników, polegających na odejściu od rozwiązań bazujących na subiektywnych ocenach zagrożeń i sposobie ich eliminacji, na korzyść rozwiązań dedykowanych i bardziej wymiernych.

Jednym z najbardziej użytecznych narzędzi do przeprowadzania kompleksowego audytu wewnętrznego jest lista kontrolna, która określa wszystkie elementy programu bezpieczeństwa. Taka lista sprawia, że firmie znacznie łatwiej jest kontrolować każdy swój zakład, stosując jednolite kryteria.

Statystyki ilustrują wpływ standaryzacji procedur i środków bezpieczeństwa w miejscu pracy. Przed utworzeniem OSHA (Agencji Bezpieczeństwa i Zdrowia w Pracy) w USA 46 lat temu szacowano, że każdego roku w pracy ginęło 14 tys. osób, czyli 38 dziennie. Dziś miejsca pracy są znacznie bardziej bezpieczne, co potwierdzają statystyki OSHA. Mimo zauważalnego postępu, nadal jest wiele do zrobienia. Nawet jeden śmiertelny wypadek przy pracy, to o jeden za dużo.

Ujednolicenie i standaryzacja wymagań w zakresie bezpieczeństwa jest więc podstawą w tworzeniu bezpiecznego i wolnego od wypadków środowiska pracy. Sukcesy wynikające ze stosowania znormalizowanych praktyk są wskaźnikiem ogromnego wpływu procesów ujednolicania i standaryzacji na zmniejszanie się liczby wypadków przy pracy. Opracowanie i wdrożenie podstawowych wytycznych pomaga w optymalizacji niezawodności i jakości procesów realizowanych w zakładach, zwiększając w ten sposób prawdopodobieństwo stworzenia bezpiecznego miejsca pracy. Jednak zbudowanie tego typu kultury, w której jednolitość jest sprawą pierwszoplanową, wiąże się z licznymi wyzwaniami.

Konfrontacja ze zmianami

Zanim firmy zaczną wdrażać systematyczny program bezpieczeństwa, muszą przemyśleć swoje już funkcjonujące procedury i działania, aby ustalić, czy istnieją zachowania, które mogłyby stać na drodze do osiągnięcia najważniejszych celów.

Dokonywanie zmian zwykle nie jest procesem łatwym. W firmach często istnieje skłonność do zachowywania pozorów. I w tym tkwi zasadniczy problem. Trzymanie się kultury korporacyjnej, która nie została zbudowana na uregulowanych celach programu zarządzania bezpieczeństwem, jest przeszkodą we wdrożeniu standaryzacji wymagań w zakresie bezpieczeństwa do organizmu i struktur korporacji.

Przejęcia jednych firm przez inne stanowią kolejny problem. Dwie firmy rzadko mają to samo podejście do bezpieczeństwa lub bazują na podobnej kulturze działań w tym obszarze. Gdy duża grupa pracowników jest poddawana procesowi asymilacji, to często okazuje się, że pracownicy ci mają różne podejścia do kwestii bezpieczeństwa, często niezgodne z polityką korporacyjną.

Nawet wtedy, gdy firma dąży do poprawy kultury bezpieczeństwa, personel kierowniczy często przekonuje się, że wdrożenie zmian jest trudne. Nie jest czymś niezwykłym, że kierownicy produkcji, którzy są przyzwyczajeni do wykonywania swoich zadań w pewien ustalony już nawykami sposób, mają trudności z przystosowaniem się do jednolitego zbioru praktyk, które wydają się „zaburzać" realizowane w zakładach operacje. Zapewnienie, że pracownicy będą rzeczywiście zainteresowani realizacją celów bezpieczeństwa, wymaga czasu, cierpliwości, komunikacji i szkoleń.

↘ Zmiana w kulturze bezpieczeństwa następuje wtedy, gdy pracownicy zaczynają czuć się odpowiedzialni za swoje bezpieczeństwo w miejscu pracy.

Inna sytuacja, być może najbardziej złożona w zarządzaniu, występuje wtedy, gdy inne procesy, które bezpośrednio wpływają na produkcję, zyski i operacje, mają wyższy priorytet niż ustandaryzowane kwestie bezpieczeństwa. W takich przypadkach, gdy bezpieczeństwo może nie mieć najwyższego priorytetu, należy poświęcić czas na określenie, w jaki sposób ujednolicone i ustandaryzowane inicjatywy w zakresie zapewnienia bezpieczeństwa mogą być pogodzone z innymi celami biznesowymi firmy.

Jak przeprowadzić ten proces

Cel ulepszenia procesów bezpieczeństwa jest wart czasu i pracy, która musi być włożona w jego planowanie, wdroże-

nie oraz realizację. Skuteczny plan musi obejmować przeprowadzenie audytów wewnętrznych, spójną i efektywną komunikację oraz program wdrożenia strategii Lean manufacturing.

Jednym z najbardziej użytecznych narzędzi do przeprowadzania kompleksowego audytu wewnętrznego jest lista kontrolna, która określa wszystkie elementy programu bezpieczeństwa. Posiadanie listy kontrolnej sprawia, że firmie znacznie łatwiej jest kontrolować każdy swój zakład przy wykorzystaniu tych samych kryteriów.

Większość list kontrolnych zawiera takie elementy, jak:

- szkolenia,
- wdrażanie nowych pracowników,
- stosowanie w miejscu pracy środków ochrony indywidualnej (*personal protective equipment* – PPE),
- stosowanie osłon maszyn i narzędzi,
- przeprowadzanie prac konserwacyjnych (podnośniki i dźwigi),
- przechowywanie butli gazowych i prawidłowe obchodzenie się z nimi,
- obsługa wózków widłowych,
- identyfikacja i eliminacja zagrożeń,
- określenie praw i obowiązków pracowników,
- opracowanie procedur JSA (*Job Safety Analysis* – analiza bezpieczeństwa pracy) oraz LOTO (*lockout/tagout*),
- prowadzenie dochodzeń po wypadkach przy pracy,
- utrzymanie porządku (metoda 5S),
- zarządzanie kontrahentami/wykonawcami,
- wytyczne dla odwiedzających zakład oraz gotowość na wystąpienie sytuacji awaryjnych,
- świadomość zagrożeń i przekazywanie informacji o zagrożeniach (*Hazard Communications* – HazCom).

Wykonywanie analiz wewnętrznych nie tylko pozwala firmie określić, czy wszystkie jej zakłady spełniają wymagania przepisów dotyczących bezpieczeństwa, ale także umożliwia śledzenie, w jaki sposób wdrażane są plany standaryzacji wymagań w zakresie bezpieczeństwa i gdzie wymagane jest wprowadzanie ulepszeń. Audyt pokazuje prawdziwą naturę pracy i sposób jej wykonywania.

Gdy organizacja zmienia swój program bezpieczeństwa, sprawą kluczową jest, aby pracownicy każdego szczebla rozumieli swoją w nim rolę i przyczyny dokonywania zmiany. Nie ma bardziej wartościowego narzędzia do osiągnięcia tego celu niż efektywna komunikacja. Skuteczny plan komunikacyjny pozwala na jasne wyrażanie swoich oczekiwań, umacnia korporacyjną politykę bezpieczeństwa oraz zapewnia, że warunki programu są spełnione.

Organizowane co miesiąc telekonferencje, w których uczestniczą wszyscy kierownicy ds. bezpieczeństwa, pomagają w rozpowszechnianiu informacji w firmie, co ułatwia wprowadzanie zmian. Wykorzystanie szablonu raportu do zarządzania tymi zebraniami tworzy ramy spotkania, dzięki czemu jego uczestnicy są skoncentrowani na istotnych informacjach, realizując przede wszystkim elementy strategii wdrożenia i poprawy zasad BHP i usprawniając procedury raportowania skupiające się na najważniejszych kwestiach. Poza spotkaniami miesięcznymi ważne jest komunikowanie się co tydzień za pomocą e-maili. Wiadomości te mogą pomóc w zaakcentowaniu znaczenia zmian w polityce bezpieczeństwa, wzmacnianiu inicjatyw oraz określaniu priorytetowych zadań dla liderów grup. Cotygodniowa komunikacja działa jak narzędzie częstego monitorowania, które przypomina, że cele związane z dążeniem do standaryzacji procedur i zasad bezpieczeństwa są stale na pierwszym planie.

Ważnym elementem tej układanki jest także komunikacja twarzą w twarz. Wizyty w poszczególnych zakładach, niezależne od corocznego audytu, stwarzają okazję do dyskusji nad problemami, które są właściwe dla danego zakładu, dzielenia się pomysłami na temat zmian we wdrażaniu oraz ułatwiają przeprowadzanie rozmów na temat nowych inicjatyw.

Ważne są także coroczne zebrania liderów grup. Organizowanie takich spotkań

Źródło: Victaulic

↙ Gdy bezpieczeństwo zostaje włączone do programu Lean, zostaje ono przekazane w ręce dyrekcji fabryki i nie jest już postrzegane wyłącznie jako odpowiedzialność zakładowego specjalisty ds. BHP.

stanowi swego rodzaju forum, na którym można wyłonić najlepiej funkcjonujące zakłady oraz wymienić z zespołem informacje na temat najlepszych praktyk. Spotkania te zachęcają do pracy zespołowej i koleżeństwa oraz ułatwiają zamianę pomysłów na realne usprawnienia. Wszystko to jest nieocenione przy tworzeniu silnej organizacji oraz trwałego programu zarządzania bezpieczeństwem.

Strategia Lean manufacturing jest trzecim elementem skutecznego planu zarządzania bezpieczeństwem. Mówiąc najprościej, proces Lean w sposób ciągły identyfikuje i eliminuje marnotrawstwo.

Zasady Lean w przeszłości były wykorzystywane jako siła napędowa usprawnień procesów oraz zwiększania satysfakcji klienta. Zwykle dotyczyły one:

- standardowego przepływu roboczego,
- jakości,
- sprzętu,
- łańcucha dostaw,
- pracy zespołowej (bezpieczeństwa),
- utrzymywania porządku (metoda 5S).

Lista kontrolna dla każdego z tych obszarów funkcjonalnych pozwala mierzyć postępy na drodze do osiągnięcia celów firmy. Przedsiębiorstwa osiągające sukcesy uwzględniają bezpieczeństwo jako część swojego formalnego programu Lean, dzięki czemu jest ono integralnym elementem pomiaru wydajności.

Najskuteczniejsze programy Lean mają 3 lub więcej rosnących poziomów trudności (często określane jako: brązowe, srebrne, złote i platynowe) w każdym obszarze funkcjonalnym w celu napędzania ciągłych ulepszeń. Dzięki jasno zdefiniowanym kryteriom na każdym poziomie pracownicy wiedzą, jakie jest ich miejsce i co musi być zrobione, aby przejść na następny poziom.

Zachęcanie do pracy zespołowej pozwala organizacji sformalizować takie sprawy, jak szkolenia w zakresie bezpieczeństwa, utrzymywanie porządku w miejscu pracy, przeprowadzanie dochodzeń w sprawie wypadków przy pracy oraz zarządzanie umowami – postrzeganymi jako kryteria obowiązkowe. Gdy bezpieczeństwo zostaje włączone do programu Lean, tym samym zostaje ono przekazane w ręce dyrekcji fabryki i nie jest już postrzegane wyłącznie jako odpowiedzialność zakładowego specjalisty ds. BHP.

Prawdziwa zmiana w kulturze bezpieczeństwa nastąpi wtedy, gdy organizacja osiągnie punkt zwrotny, w którym bezpieczeństwo stanie się osobistym celem każdego pracownika.

Podsumowanie

Przed faktycznym rozpoczęciem działań na drodze do standaryzacji wymagań w zakresie bezpieczeństwa organizacja musi ocenić obecne warunki i zrozumieć, gdzie należy wprowadzić ulepszenia. Pierwszym etapem tego procesu jest określenie mocnych i słabych stron firmy poprzez przeprowadzenie analizy rozbieżności. Po zdefiniowaniu i zrozumieniu słabych punktów możliwe jest z kolei wytyczenie drogi oraz wskazanie kamieni milowych, które będą oznaczać osiągane na tej drodze sukcesy.

Dzięki udziałowi kierownictwa w programie, który bazuje na audytach wewnętrznych, efektywnej komunikacji oraz założeniach strategii Lean manufacturing, firmy mogą osiągnąć cele standaryzacji wymagań w zakresie bezpieczeństwa, a w efekcie stworzyć środowisko pracy, które jest bezpieczniejsze i bardziej efektywnie zarządzane.

Budowa takiej kultury bezpieczeństwa w zakładzie wymaga zasobów, wysiłku i czasu, ale jest niezaprzeczalnie warta tego wysiłku.

Bill D'Amico *– globalny dyrektor ds. bezpieczeństwa, zdrowia i ochrony środowiska w firmie Victaulic.* ■

AnterSystem

WYPOSAŻAMY PRZESTRZEŃ
NAJBEZPIECZNIEJ

ANTER SYSTEM POLSKA SP. Z O.O.
ul. Krakowska 52/6
50-425 Wrocław
DZIAŁ HANDLOWY
e-mail: info@antersystem.pl
tel.: +48 32 32 31 696
+48 606 116 171

WWW.ANTERSYSTEM.PL

NAJPEWNIEJSZA OCHRONA
TWOICH PRACOWNIKÓW

PRODUKT POLSKI

BARIERY PRZEMYSŁOWE • SŁUPY OCHRONNE • ODBOJNICE PRZEMYSŁOWE
• OCHRONA MASZYN, ŚCIAN, BRAM, KOLUMN • WYGRODZENIA TYMCZASOWE
ZABEZPIECZENIE DOKÓW PRZEŁADUNKOWYCH • POPRAWA BEZPIECZEŃSTWA W TWOIM ZAKŁADZIE

URZĄD DOZORU TECHNICZNEGO

eUDT – PORTAL INTERNETOWY URZĘDU DOZORU TECHNICZNEGO

Załóż konto na portalu eUDT, wypełniając formularz rejestracyjny dostępny na eudt.gov.pl i korzystaj z usług oferowanych przez UDT on-line!

- Wygodny i szybki dostęp do informacji o Twoich urządzeniach, terminach badań i rozliczeniach finansowych z UDT
- Darmowy dostęp do portalu **24/7/365**
- Łatwiejsze i prostsze śledzenie zdarzeń związanych z Twoimi urządzeniami - możliwość definiowania własnego kalendarza wydarzeń oraz alertów
- Możliwość wyświetlania i pobierania dokumentów UDT, w tym także e-decyzje i e-protokoły
- Elektroniczna korespondencja z UDT, rosnąca liczba spraw, które załatwisz on-line
- Możliwość składania elektronicznych wniosków

KONTAKT

W razie dodatkowych pytań skontaktuj się z wybranym oddziałem/biurem UDT

eudt.gov.pl