25.05.2023

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Niemcy
http://www.pilz.com

Komunikat prasowy

Thomas Pilz: Ochrona i bezpieczeństwo w ramach cyfrowej automatyzacji

Ostfildern, 25.05.2023 - **(Obowiązuje wersja wygłoszona).**

Thomas Pilz

Bezpieczeństwo: Branże przemysłowa i technologiczna będą się musiały podporządkować nowym przepisom

Trwa właśnie rewolucja w świecie norm i przepisów dotyczących bezpieczeństwa w środowisku przemysłowym. Siłą napędową transformacji są wyzwania związane z bezpieczeństwem i rozwojem sztucznej inteligencji (AI). Przed branżami przemysłową i technologiczną stoją wyzwania związane z trzema nowymi aktami prawnymi dotyczącymi bezpieczeństwa: dyrektywą UE NIS 2, nowym rozporządzeniem w sprawie maszyn oraz Cyber Resilience Act.

Podobnie jak na ostatniej dorocznej konferencji prasowej skupię się na zagadnieniach bezpieczeństwa i chciałbym dziś omówić spodziewane długofalowe skutki dla całej branży.

NIS 2: Więcej obowiązków i więcej sankcji dla większej liczby firm

NIS (Network and Information Security) to dyrektywa Unii Europejskiej mająca na celu wzmocnienie cyberbezpieczeństwa. Obowiązuje od 2016 r. i do tej pory dotyczyła dostawców infrastruktury krytycznej, w tym energii, ruchu, banków i finansów, zdrowia, zaopatrzenia w wodę pitną i jej dystrybucji oraz infrastruktury cyfrowej. Dostawcy w tych branżach musieli wdrożyć „odpowiednie zabezpieczenia" i zgłaszać wszelkie poważne incydenty związane z cyberbezpieczeństwem. Dotychczasowe przepisy zastępuje dyrektywa NIS 2, która weszła w życie na początku 2023 r., ale musi jeszcze zostać wdrożona do prawa krajowego przez państwa członkowskie UE do jesieni 2024 r. Nowa dyrektywa ma również zastosowanie do branż technologicznej i motoryzacyjnej, między innymi do firm zatrudniających ponad 50 osób lub osiągających roczny obrót przekraczający 10 mln euro. Według Związku Niemieckich Producentów Maszyn i Urządzeń (VDMA) dotyczy to około 9000 firm w całej Europie. W przyszłości firmy te będą musiały udowodnić, że podjęły środki techniczne, operacyjne i organizacyjne w celu ochrony przed incydentami zagrażającymi bezpieczeństwu. Po pierwsze wymaga to przeprowadzenia analizy ryzyka istniejących systemów, w tym w środowiskach produkcyjnych, czyli szeroko rozumianej technologii operacyjnej (OT). Następnie konieczne jest opracowanie i wdrożenie określonych procesów i środków, takich jak ochrona hasłem lub szyfrowanie, a także zapewnienie programu szkoleń dla pracowników. Incydenty związane z cyberbezpieczeństwem muszą być zgłaszane odpowiednim władzom w ciągu 24 godzin. Nowością jest również wyraźne włączenie łańcuchów dostaw. Podsumowując: dyrektywa NIS 2 dotyczy teraz większej liczby firm, rozszerza obowiązki i przewiduje surowsze sankcje. Firmom, które nie podejmą oczekiwanych działań, grożą surowe kary.

Cyber Resilience Act – bezpieczeństwo w całym cyklu życia produktu

We wrześniu 2022 r. Komisja Europejska przedstawiła projekt rozporządzenia, którego celem jest zwiększenie cyberbezpieczeństwa produktów. Przepisy te są skierowane do producentów produktów zawierających składniki cyfrowe. Oznacza to zarówno sprzęt, jak i oprogramowanie (np. oprogramowanie układowe). Rozporządzenie odnosi się zarówno do produktów konsumpcyjnych, jak i do wyrobów przemysłowych, takich jak na przykład sterowniki do maszyn. Zgodnie z Cyber Resilience Act na rynek mogą trafiać wyłącznie produkty gwarantujące odpowiedni poziom cyberbezpieczeństwa. Producenci są również zobowiązani do informowania klientów o stwierdzonych lukach w zabezpieczeniach oraz do jak najszybszego ich usuwania. Tym samym przepisy te mają zastosowanie w całym cyklu życia produktu. Oznacza to, że producenci muszą teraz oferować aktualizacje oprogramowania poza zwykłym okresem gwarancyjnym, tak aby możliwe było odpieranie przyszłych zagrożeń. Zakładamy, że przepisy zostaną przyjęte pod koniec 2024 r.

Nowe rozporządzenie w sprawie maszyn – obowiązkowe cyberbezpieczeństwo

Trzecim źródłem nowego prawodawstwa dotyczącego bezpieczeństwa jest unijne rozporządzenie w sprawie maszyn. Jego publikacja ma nastąpić niebawem. Ponieważ przepisy mają formę rozporządzenia, nie muszą zostać przetransponowane do prawa krajowego. Producenci maszyn będą mieli 42 miesiące na dostosowanie się do nowych wymagań. Rozporządzenie w sprawie maszyn zastępuje istniejącą dyrektywę maszynową i wprowadza dodatkowy wymóg dotyczący zapewnienia cyberbezpieczeństwa. Podczas gdy dyrektywa maszynowa dotyczyła jedynie bezpieczeństwa, nowe rozporządzenie uwzględnia cel ochrony bezpieczeństwa wyrażony w „Zasadniczych wymaganiach w zakresie zdrowia i bezpieczeństwa", w części „Ochrona przed naruszeniem integralności": Funkcje ochrony maszyny nie mogą ulec pogorszeniu w wyniku naruszenia integralności – czy to zamierzonego, czy przypadkowego. Jak na razie wiadomo, że spełnienie wymagań Cyber Resilience Act jest równoznaczne z domniemaniem zgodności z postanowieniami rozporządzenia w sprawie maszyn.

A teraz: Kto powinien się na czym skupić?

Co niosą ze sobą nowe przepisy? Potencjalny wpływ można zobrazować na przykładzie sektora energetycznego: Dotychczas dyrektywa NIS obowiązywała tylko dostawców energii. Zgodnie z treścią dyrektywy NIS 2 nowym wymogom będą musieli w przyszłości sprostać także konstruktorzy maszyn, np. producenci instalacji energetycznych (np. turbin wiatrowych). Z kolei producenci turbin wiatrowych potrzebują automatyki, sterowników czy czujników, np. dostarczanych przez firmę Pilz. Od określonej wielkości przedsiębiorstwa producenci podzespołów elektrycznych również podlegają dyrektywie NIS 2. A ponieważ zapisy dyrektywy NIS 2 uwzględniają także dostawców, firmy, takie jak Pilz, muszą również zatroszczyć się o bezpieczne łańcuchy dostaw i postawić wymagania swoim dostawcom. Jak widać, wymogi dyrektywy NIS 2 rozciągają się na cały łańcuch dostaw.

Aby sprzedawać maszyny w Europie, konstruktorzy musieli dotąd przejść procedurę oceny zgodności zakończoną przyznaniem znaku CE.
Obecnie, w ramach nowego rozporządzenia w sprawie maszyn, konstruktorzy maszyn muszą udowodnić, że ich wyroby są także chronione przed manipulacją. I wreszcie: producenci podzespołów elektrycznych będą w przyszłości podlegać wymogom planowanych przepisów o cyberodporności.

Podsumowując: decyzja o tym, czy i w jakim stopniu zająć się kwestiami bezpieczeństwa, nie leży już w gestii firmy. Zostało to uregulowane w prawie. Firmy powinny jak najszybciej przygotować się na wejście w życie dyrektywy NIS 2 i przeprowadzić kompleksową ocenę bezpieczeństwa firmy. Obejmuje to na przykład opracowanie systemu zarządzania bezpieczeństwem informacji (ISMS) zgodnie z normą dotyczącą bezpieczeństwa informacji ISO 27001.

W branży przemysłowej, bezpieczeństwo przemysłowe nie jest wyłącznie domeną działu IT, lecz stanowi integralny element projektowania i budowy. Wdrożenie bezpieczeństwa w ramach doposażenia jest zawsze skomplikowane i zwykle oznacza pogorszenie łatwości obsługi, funkcjonalności i produktywności. Ocena ryzyka obejmuje teraz zarówno bezpieczeństwo, jak i ochronę. Bez bezpieczeństwa nie ma oznakowania CE!

W przypadku producentów wyrobów zawierających składniki cyfrowe wytyczne stanowi seria norm IEC 62443, która przedstawia wymagania dotyczące „bezpiecznego procesu planowania cyklu życia”.

UE szybko zareagowała na wymogi dotyczące bezpieczeństwa – w Europie obowiązywać będą najsurowsze na świecie wymagania. Jednak ze względu na obowiązujące umowy z innymi krajami tam też zostaną wprowadzone podobne przepisy. Na przykład Australia prowadzi obecnie rozmowy z UE i prawdopodobnie będzie przestrzegać europejskich norm. Należy zatem spodziewać się globalnej harmonizacji wymogów dotyczących bezpieczeństwa przemysłowego.

Thomas Pilz

Otwarte standardy komunikacji jako historyczna misja

W firmie Pilz otwartość i łatwość obsługi to kluczowe cechy oferowanych produktów. Chcemy dostarczać klientom najnowocześniejsze produkty, które pozostają łatwe w użytkowaniu i można je włączyć do dowolnej architektury automatyki.

W oparciu o SafetyBUS p, pierwszy bezpieczny system Fieldbus, oraz zapewniający komunikację w czasie rzeczywistym system Ethernet SafetyNET p, udało nam się wpłynąć na rozwój bezpiecznej komunikacji przemysłowej. Jednak czasy zastrzeżonych rozwiązań biznesowych już minęły. Zależy nam na tworzeniu standardów branżowych. To nasza historyczna misja!

OPC UA

Branża uznała przydatność architektury OPC UA (Open Platform Communications Unified Architecture) jako sposobu na budowę bezpiecznej sieci opartej na rozwiązaniach różnych producentów. Jest to protokół komunikacyjny, który oferuje zestandaryzowany (IEC 62541) interfejs na potrzeby komunikacji między różnymi źródłami danych. Działając w ramach Fundacji OPC, pracownicy firmy Pilz są aktywni zarówno w komitecie sterującym, jak i technicznych grupach roboczych poświęconych inicjatywie Field Level Communication (FLC). Nasz uwaga skupia się na grupie roboczej poświęconej bezpieczeństwu (Safety over OPC UA),

gdzie szczególnie przydatna jest nasza wiedza w zakresie wykorzystania technologii Publisher/Subscriber (Pub/Sub) w powiązaniu z wymaganiami funkcjonalnie bezpiecznych protokołów Fieldbus. W porównaniu z klasyczną architekturą Master/Slave w technologii Pub/Sub dane mogą być wymieniane bezpośrednio pomiędzy subskrybentami. Dzięki temu architektura OPC UA może być również wykorzystywana z wymagającymi, rozproszonymi zadaniami automatyzacji. Możemy pochwalić się szczególnie szerokim doświadczeniem w tym obszarze, ponieważ nasz system SafetyNET p jest jedynym systemem Fieldbus opartym na sieci Ethernet, który od początku obsługuje technologię Pub/Sub.

Prace nad zagadnieniami bezpieczeństwa funkcjonalnego wyraźnie postępują. Grupa blisko współpracuje z organami kontrolnymi nad specyfikacją i testami, a także nad certyfikacją stosów komunikacyjnych w kontekście protokołu OPC UA Safety. Wersja 1.05 została już opublikowana.

IO-Link Safety
Na poziomie czujników automatyzacja zrobiła już duży krok naprzód pod względem otwartości. Protokół komunikacyjny IO-Link Safety będzie wkrótce dostępny na rynku. Bezpośrednia komunikacja między punktami oferuje wiele korzyści, takich jak prostsza instalacja (np. dzięki standardowemu okablowaniu oraz ze względu na brak okablowania równoległego), zautomatyzowana, wspomagana narzędziami parametryzacja oraz zaawansowane opcje diagnostyczne.

Aby standard IO-Link mógł być wykorzystywany w automatyzacji również do zadań związanych z bezpieczeństwem, działając w ramach grupy IO-Link firma Pilz intensywnie pracowała nad odpowiednim rozwiązaniem. Nasi eksperci kierują obiema grupami roboczymi ds. protokołu IO-Link Safety (w zakresie marketingu i technologii).

Pierwsze gotowe do wprowadzenia na rynek czujniki przedstawimy podczas targów SPS w listopadzie br. Podejście firmy Pilz polega na oferowaniu kompletnego systemu, tj. czujników, aktuatorów oraz modułów nadrzędnych. Upraszcza to tworzenie rozwiązania u klienta i zwiększa jego wydajność.

Jesteśmy przekonani, że przyszłe rozwiązania w zakresie automatyzacji będą wyróżniać się jeszcze bardziej pod względem funkcjonalności: jakości interfejsów użytkownika, prostej obsługi czy dodatkowych korzyści. Stoi za tym wiele innowacji, co wiąże się z ogromnym potencjałem w kontekście nowych zastosowań.

Thomas Pilz

Przyszłość bezpieczeństwa nie jest jeszcze rozstrzygnięta

Co z punktu widzenia ochrony ludzi i maszyn oznacza dalsza cyfryzacja? Które technologie spełniają wymagania w zakresie bezpieczeństwa ? Jaką rolę odgrywają ludzie? Dziś również chcemy spojrzeć w przyszłość. Najpierw dobra wiadomość: w centrum uwagi pozostaje człowiek, którego rola zostanie jeszcze wzmocniona.

Człowiek jako aktywny podmiot kształtujący otoczenie

Jak na przykład w projekcie „płynnej produkcji" w ramach programu Arena 2036. Firma Pilz wraz z partnerami pracuje nad opracowaniem i wdrożeniem skoncentrowanej na człowieku cyberfizycznej koncepcji produkcji dedykowanej branży motoryzacyjnej. Zakłada ona rozbicie zakładów produkcyjnych na elastyczne lokalizacyjnie moduły, tak aby tworzyć i rozwiązywać jednostki w dynamiczny sposób stosownie do potrzeb. Moduły są projektowane z naciskiem na rolę człowieka jako aktywnego podmiotu kształtującego środowisko produkcyjne.

Z tych wymagań wynika rosnące zapotrzebowanie na ochronę dynamiczną, tj. możliwość bardziej elastycznego dostosowania funkcji bezpieczeństwa do zmieniających się procesów produkcyjnych i związanych z tym wymagań w zakresie bezpieczeństwa. Na przykład: zamiast natychmiastowego zatrzymania przewiduje się możliwość kontynuowania pracy przez roboty lub platformy mobilne ze zmniejszoną (a przez to bezpieczniejszą) prędkością w trakcie przebywania osoby w obszarze roboczym lub – jeszcze lepiej – wdrożenie bezpiecznych strategii unikania zagrożeń. Inteligentne czujniki i aktuatory w systemach rozproszonych będą przejmować od sterowników coraz więcej funkcji, co przełoży się na lepsze współdziałanie pomiędzy poszczególnymi modułami maszyn, a także między człowiekiem i maszyną.

Bezpieczeństwo w czasie rzeczywistym
W kontekście bezpieczeństwa ważne jest, aby dynamicznie zmieniająca się sytuacja w przyszłym środowisku produkcyjnym była nadzorowana w czasie rzeczywistym, tak aby przez cały czas zapewnić ochronę ludzi i maszyn. Wyrażeniem kluczowym jest tutaj „bezpieczeństwo w czasie rzeczywistym”. W przyszłości można sobie wyobrazić, że różne maszyny lub – ogólnie – zasoby będą miały wspólne zabezpieczenia. To właśnie „współdzieloną ochronę” testujemy w zakładzie SmartFactory KL. W ramach tak rozumianej ochrony wykluczone jest klasyczne oznakowanie CE jako wynik procedury analogowej oceny zgodności. Informacje o wszystkich zaangażowanych zasobach muszą być dostępne w czasie pracy; w tym kontekście słowami kluczowymi są: „cyfrowa tabliczka znamionowa” i „powłoka administracyjna”.

W ramach wspomnianego wcześniej projektu „płynnej produkcji” skupiamy się na innych zagadnieniach, takich jak identyfikacja (a co za tym idzie – rozróżnianie) ludzi i przedmiotów. Będzie to przydatne w przypadku wykorzystania sztucznej inteligencji. Zagrożenia będą wtedy mogły być identyfikowane i oceniane w oparciu o adaptacyjne algorytmy sztucznej inteligencji. W tym przypadku „analogowy” znak CE zapewnia podstawową ochronę. Można jednak wprowadzić dodatkowe środki redukcji ryzyka, które uczynią ochronę jeszcze bardziej elastyczną i przełożą się na jeszcze większą produktywność.

Podpis:

Teksty i zdjęcia dostępne są również do pobrania na stronie www.pilz.com. Aby uzyskać bezpośredni dostęp do odpowiedniej strony w naszym centrum prasowym , wpisz kod web w wyszukiwarce na stronie głównej.: **237512**

Grupa Pilz

Grupa Pilz jest globalnym dostawcą produktów, systemów i usług dla technologii automatyzacji. Ta rodzinna firma z siedzibą w Ostfildern koło Stuttgartu zatrudnia około 2500 osób. Dzięki 42 oddziałom na całym świecie dostarcza bezpieczne rozwiązania dla ludzi, maszyn i środowiska. Oferuje kompletne rozwiązania w zakresie automatyzacji obejmujące czujniki bezpieczeństwa oraz technologię sterowania i napędu - w tym systemy komunikacji przemysłowej, diagnostyki i wizualizacji. Konsulting, inżynieria i szkolenia uzupełniają międzynarodową ofertę usług. Oprócz maszyn i urządzeń, rozwiązania firmy Pilz są stosowane w wielu sektorach, takich jak energetyka wiatrowa, technologia kolejowa i robotyka.

www.pilz.com

Pilz w mediach społecznościowych

Na naszych profilach w portalach społecznościowych dostępne są informacje na temat firmy i jej pracowników oraz najświeższe informacje o aktualnych zdobyczach technologii automatyzacji.

https://www.facebook.com/pilzINT

https://twitter.com/Pilz_INT

https://www.youtube.com/user/PilzINT

https://www.xing.com/companies/pilzgmbh%26co.kg

https://www.linkedin.com/company/pilz

Dane kontaktowe dla mediów

Martin Kurth
Prasa korporacyjna i techniczna
+49 711 3409 - 158
publicrelations@pilz.com

Sabine Skaletz-Karrer
Prasa techniczna
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de