Industrie 4.0 – bezpiecznie i inteligentnie

PILZ
THE SPIRIT OF SAFETY

Biała księga

Zastrzeżenia prawne

Nasza Biała księga została sporządzona z najwyższą starannością. Zawiera ona informacje o naszej spółce oraz naszych produktach. Cała jej treść odpowiada aktualnemu stanowi technologii i powstała zgodnie z naszą najlepszą wiedzą oraz przekonaniem. Mimo że uczyniliśmy wszystko, aby uczynić zamieszczone informacje wyczerpującymi, nie odpowiadamy za ich kompletność i dokładność, z wyjątkiem rażących nieścisłości. Należy przede wszystkim zauważyć, że użyte stwierdzenia nie mają mocy prawnej. Prosimy o zgłaszanie wszelkich opinii dotyczących niniejszej treści.

Informacje o prawach autorskich

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern

Spis treści

1. O inicjatywie Industry 4.0

Industry 4.0 jest czymś więcej niż wizją przyszłości. Inteligentne sieci są ogromną szansą dla przemysłu. Elastyczna produkcja może pomóc w optymalizacji eksploatacji instalacji przemysłowych. Zwiększając wydajność instalacji, w warunkach produkcji masowej można wytwarzać produkty o indywidualnych cechach. Mimo tych wszystkich zalet wiele przedsiębiorstw wciąż waha się przed wdrożeniem Industry 4.0 w swoich własnych zakładach produkcyjnych. Zgodnie z badaniem przeprowadzonym przez Instytut McKinsey „Industry 4.0 – jak kierować cyfryzacją w przemyśle wytwórczym, 2015”[1] tylko sześć na dziesięć przedsiębiorstw w Niemczech gotowych jest na Industry 4.0, mimo że 91% zauważa, że cyfryzacja produkcji przemysłowej jest okazją do wzrostu. Pragniemy zmienić ten stan rzeczy i zaoferować rozwiązania oraz produkty dla Industry 4.0 przedsiębiorstwom na całym świecie. Ponieważ tematyka Industry 4.0 staje się punktem coraz baczniejszej uwagi również w skali międzynarodowej, trwający proces globalizacji czyni tym bardziej koniecznym przygotowanie sposobu integracji poprzez cyfryzację procesów produkcyjnych wzdłuż całego łańcucha nadawania wartości dodanej.

1.1. Historia i tło – od silnika parowego do inteligentnej fabryki

Pierwsza rewolucja przemysłowa polegała na mechanizacji z wykorzystaniem energii, wody i pary wodnej; po niej następowała kolejna rewolucja przemysłowa, która bazowała na przenośnikach i energii elektrycznej. Po nich przyszła rewolucja cyfrowa, kojarzoną również z nazwą „Industry 3.0”. Praca z wykorzystaniem komputera stała się normą, wprowadzono pierwszy programowalny logiczny układ sterowania.
Termin „Industry 4.0” oznacza czwartą rewolucję przemysłową, dopuszczającą stosowanie systemów cybernetyczno-fizycznych, Internet rzeczy, oraz inteligentną fabrykę. Jednak dla firmy Pilz Industry 4.0 oznacza bardziej ewolucję niż rewolucję, ponieważ jeśli wszystkie zainteresowane strony nie będą przygotowane na zmianę, wówczas rewolucja ta nie będzie realna.

Termin Industry 4.0 został po raz pierwszy wprowadzony do użycia podczas targów Hannover Messe 2011. W październiku 2012 grupa robocza Industry 4.0 wyłoniona z zespołu osób śledzących postęp w dziedzinie komunikacji, aktywnych w Research Alliance, przedstawiła zalecenia dla niemieckiego rządu dotyczące niezbędnych wdrożeń. Na targach Hannover Messe w kwietniu 2013 przedstawicielom rządu federalnego zaprezentowano raport końcowy sporządzony przez grupę roboczą Industry 4.0. Obecnie rozpoczęła prace platforma Industry 4.0 powołana przez trzy stowarzyszenia przemysłowe Bitkom[2], VDMA[3] i ZVEI[4]. Jej celem jest skoordynowanie działań w tym obszarze. Firma Pilz uczestniczy w tych działaniach od samego początku i wykorzystuje swoje wieloletnie doświadczenie w dziedzinie technologii automatyzacji do wspierania projektów.

[1] https://www.mckinsey.de/sites/mck_files/files/mck_industry_40_report.pdf
[2] Bitkom (Digitalverband Deutschlands/Niemieckie Stowarzyszenie Technologii Cyfrowej) https://www.bitkom.org/EN/index-EN.html
[3] VDMA (Verband Deutscher Maschinen- und Anlagenbau, Mechanical Engineering Industry Association) http://www.vdma.org/ueber-uns
[4] ZVEI (Zentralverband Elektrotechnik- und Elektronikindustrie e.V., Stowarzyszenie producentów przemysłu elektrycznego o elektronicznego) http://www.zvei.org/en/Pages/default.aspx

1.2. Smart Factory

Smart Factory jest to inteligentna fabryka przyszłości. Stanowi ona cel strategii rządu Niemiec w dziedzinie wysokiej technologii w ramach inicjatywy Industry 4.0[5]. Strategia ta obejmuje wizję środowiska produkcyjnego, w którym instalacje produkcyjne i systemy logistyczne w dużym stopniu same się organizują i optymalizują. Produkty wytwarzane w inteligentnej fabryce mają zarejestrowane informacje o miejscu, w którym się znajdują, znają swoją historię, aktualny stan i wymagane do zrealizowania etapy produkcji prowadzące do stania się produktem końcowym. W jaki sposób jest to możliwe?
Podstawą techniczną są systemy cybernetyczno-fizyczne, które[6] komunikują się ze sobą za pomocą Internetu rzeczy[7]. Komunikacja pomiędzy produktem (na przykład częścią) a linią produkcyjną stanowi element scenariusza na przyszłość: produkt niesie ze sobą informacje o jego wytwarzaniu w czytelnej dla maszyny formie, np. w postaci chipa RFID. Na podstawie tych danych kontrolowana jest ścieżka wiodąca poprzez linię produkcyjną i poszczególne etapy produkcji. Szkoły wyższe i instytuty badawcze pracują nad tematem Smart Factory w ramach tak zwanych fabryk modelowych.

1.2.1. Smart Factory^{KL}

SmartFactory^{KL} jest pionierem przyszłych inteligentnych fabryk. Jako wiodący ośrodek w dziedzinie doskonałości oraz niezależnej od producenta platformy demonstracyjno-badawczej, rozwija ona innowacyjne systemy wytwórcze, w których wizja Industry 4.0 staje się już rzeczywistością[8]. Jej celem jest utworzenie sieci wysoko rozwiniętych partnerów reprezentujących przemysł i ośrodki badawcze, które pracowałyby nad nowymi koncepcjami, normami i rozwiązaniami oraz zapewniły podstawę dla szeroko zróżnicowanej techniki automatyzacji. SmartFactory^{KL} dysponuje także pierwszą na świecie, niezależną od producenta instalacją w pełni zgodną z ideą Industry 4.0[9].
Firma Pilz jako pełnoprawny uczestnik tej inicjatywy, wspiera jej cel oraz śledzi rezultaty wspólnej pracy, a następnie wdraża je do swoich własnych produktów.
Dzięki swemu doświadczeniu w dziedzinie bezpieczeństwa maszyn przede wszystkim wspiera standaryzację i wspólne podejście do problemu bezpieczeństwa mającego dwa oblicza: bezpieczeństwo (bezpieczeństwo maszyn) i ochronę (zabezpieczenie IT), a także jest zaangażowana w zagadnienia modularyzacji. Budowa instalacji zgodnie z podejściem mechatronicznym umożliwia kompletną modułowość elementów maszyny. Funkcje sterowania można poddać standaryzacji i ponownie wykorzystywać je w całej serii modułów. Podstawą tej koncepcji są systemy sterowania, takie jak PSS 4000 firmy Pilz, które mogą dystrybuować różne funkcje sterowania. Taką koncepcję można testować w realizacjach Smart Factory. Od kilku lat platforma SmartFactory^{KL} prezentuje modułową linię produkcyjną, w której poszczególne moduły o różnej architekturze sterowania, wyprodukowane przez różnych producentów, współpracują ze sobą w sposób absolutnie bezkonfliktowy. Pilz rozbudowuje linię demonstracyjną Smart Factory^{KL} o inteligentny, zautomatyzowany moduł magazynowy.

[5] http://www.hightech-strategie.de/de/Industrie-4-0-59.php
[6] Definicja w Słowniku, strona 20f.
[7] Definicja w Słowniku, strona 20f.
s[8] http://www.smartfactory.de/
s[9] http://www.smartfactory.de/

Rysunek 1: SmartFactory^{KL} na targach Hannover Messe 2015

1.2.2. Linia demonstracyjna Smart Factory firmy Pilz

Linia demonstracyjna Smart Factory umożliwia zaprezentowanie, jak szybko, elastycznie i niedrogo można wytwarzać zindywidualizowane produkty. Modułowa linia produkcyjna ilustruje komunikację pomiędzy rozproszonymi systemami sterowania z wykorzystaniem aktuatorów i czujników. Realizujący ideę Industry 4.0 system sterowania PSS 4000 koordynuje etapy wszystkich połączonych w sieć elementów realizujących funkcje bezpieczeństwa i sterowania standardowego: od projektowania po wizualizację.
Zadaniem naszej inteligentnej linii produkcyjnej jest wytwarzanie spersonalizowanych etui na wizytówki i długopisów, a naszym celem jest utrzymywanie przejrzystego procesu produkcyjnego. Dzięki zastosowanym rozwiązaniom łatwo jest zrealizować złożoną instalację wykorzystującą skomplikowane funkcje, wymagane na przykład w cyfrowych systemach połączonych w sieć w ramach Industry 4.0.

Linia demonstracyjna składa się z trzech różnych modułów funkcjonalnych:
- Magazyn dla przenośników części
- Robot z magazynem części/stanowisko przekazywania produktu
- Stanowisko lasera

Za pośrednictwem komputera PC tworzony jest rekord danych klienta (dane kontaktowe, adres...), w którym klienci mogą wybrać pudełko na wizytówki lub długopis. Następnie mogą oni zamówić albo wydrukowanie na długopisie swego imienia, albo spersonalizowane etui na wizytówki.
Dane produkcyjne zapisywane są w sposób cyfrowy w chipie RFID umieszczonym na przenośniku części, co umożliwia zapisanie informacji w każdym module. W poszczególnych modułach żądana informacja jest odczytywana z chipa, w następstwie czego realizowany jest odpowiedni proces. Po wytworzeniu produktu, zawartość chipa jest kasowana na stanowisku wydawania produktu i możliwe jest zapisanie następnego rekordu danych.

Po wykasowaniu danych, przenośnik części zawierający chip RFID jest zawracany do magazynu, w przypadku braku dalszych rekordów danych przekazywany jest do kolejnego etapu cyklu produkcyjnego.

Rysunek 2: Instalacja demonstracyjna Smart Factory firmy Pilz na targach Hannover Messe 2016

1.3. Bezpieczeństwo i ochrona

Wraz z postępującym rozwojem automatyzacji zgodnie z ideą Industry 4.0 przedsiębiorstwa stają w obliczu nowych wymagań dotyczących bezpieczeństwa. Świat automatyzacji łączy się ze światem technologii informatycznej. Zaznaczają się wyraźne różnice w rozumieniu terminów: terminami stosowanymi na arenie międzynarodowej są „bezpieczeństwo” dla bezpieczeństwa maszynowego oraz „ochrona” dla informatyki i zabezpieczania danych; jest to pomocne w ich podstawowym rozróżnieniu.

Bezpieczeństwo wymaga, aby zagrożenia resztkowe związane z instalacja lub maszyną nie przekraczały akceptowalnych wartości. Dotyczy to zagrożeń dla otoczenia zakładu (np. szkody ponoszone przez środowisko), a także zagrożeń wewnątrz zakładu (np. wobec pracowników fabryki).

Ochrona zaś dotyczy zabezpieczenia instalacji lub maszyny przed nieuprawnionym dostępem z zewnątrz oraz zabezpieczenia wrażliwych danych przed sfałszowaniem, utratą lub nieuprawnionym dostępem od wewnątrz. Obejmuje to umyślne ataki oraz nieumyślne incydenty naruszające bezpieczeństwo.

Kompleksowa ochrona produkcji i związanych z bezpieczeństwem danych sterujących podczas przesyłania, przetwarzania i magazynowania musi objąć następujące aspekty:
- ochronę fizyczną i dyspozycyjność systemów IT,
- ochronę sieci,

- ochronę aplikacji programowych,
- ochronę danych,
- bezpieczeństwo operacyjne

1.4. Modułowe maszyny i decentralizacja

Już od kilku lat modułowość układów mechanicznych postrzegana jest jako klucz do większej elastyczności produkcji. Kompletna instalacja zawiera liczne niezależne moduły maszynowe. Każdy z tych modułów jest odzwierciedleniem jednego lub kilku standardowych etapów produkcji i można go połączyć z innymi modułami w celu utworzenia kompletnego procesu. Wymaga to dołączenia wszystkich modułów do szkieletu zaopatrującego każdy z nich w energię (prąd trójfazowy 400 V AC, powietrze sprężone...), a także w dane procesowe i dane potrzebne do sterowania. W przypadku konieczności zmiany metody produkcji lub zwiększenia jej wydajności można wymienić jeden lub więcej modułów lub dodać kolejne identyczne.

Modułowość i decentralizacja to dwa spośród najważniejszych czynników warunkujących odnoszenie sukcesu na drodze do automatyzacji przyszłości. Wymaga to stworzenia systemów sterowania zdolnych do zarządzania rozproszoną inteligencją w modułach maszyn, w sposób przyjazny dla użytkownika. Każdą instalację i maszynę można podzielić na sterowalne, niezależnie funkcjonujące jednostki.

Modułowa struktura instalacji i maszyn zgodna jest z podejściem mechatronicznym. Jej założeniem jest uniwersalne zintegrowanie wszystkich dyscyplin uczestniczących w procesie budowie maszyny: mechanicznej, elektrycznej i automatyzacji. W sposób powszechnie przyjęty określone jest współdziałanie pomiędzy różnymi indywidualnymi podzespołami z dziedziny automatyzacji i związanymi z nimi narzędziami programowymi w celu utworzenia rozwiązania automatyzacji. To uniwersalne podejście rozciąga się przez cztery poziomy piramidy automatyzacji (poziom zarządzania, poziom operacyjny, poziom kontroli i poziom instalacji). Zgodnie z podejściem mechatronicznym, nawet funkcje kontroli powinny umożliwiać ich wdrożenie w poszczególnych modułach mechatronicznych.
Jak do tej pory, w tym miejscu systemy spełniają swoje ograniczenia. Chociaż możliwe jest tworzenie modułów funkcjonalnych, które mają być wykonywane przez dysponujące dużą mocą centralne systemy sterowania, uruchamianie poszczególnych modułów, z powodu jego złożoności, szybko staje się pracochłonnym procesem. Kolejne zmiany w konfiguracji i programowaniu poszczególnych modułów funkcjonalnych w podobny sposób zwiększają obciążenie pracą.
Systemy zdecentralizowane sprawiają, że uruchamianie modułów stało się bardzo proste. Przyjazna dla użytkownika jest również konfiguracja, ponieważ może on wykorzystywać identyczne programy i podfunkcje kontrolne w odniesieniu do różnorodnych modułów.

Przyszłość należy do rozwiązań automatyzacji umożliwiających zastosowanie sterowania rozproszonego i zapewniających jednocześnie, że niezbędne połączenie w sieć szeregu systemów sterowania jest dla użytkownika łatwe w obsłudze. Firma Pilz oferuje takie rozwiązanie w postaci systemu sterowania PSS 4000.

2. Industry 4.0 i firma Pilz

2.1. Wkład firmy Pilz w tworzenie koncepcji Indystry 4.0

W roku 2010 Susanne Kunschert, Partner zarządzający firmy Pilz, została nominowana przez rząd niemiecki na stanowisko przedstawiciela małych i średnich przedsiębiorstw w Research Alliance. Research Alliance jest to centralny organ kreujący politykę innowacyjności, który doradza rządowi federalnemu w kwestiach wdrażania i rozwoju strategii dotyczących zaawansowanych technologii. Zadaniem Susanne Kunschert jest przedstawianie punktu widzenia innowacyjnych przedsiębiorstw małej i średniej wielkości.

Jako członek grupy instytucji promujących bezpieczeństwo, Susanne Kunschert zajmuje się poprawą skuteczności zabezpieczeń sieci komunikacyjnych oraz rozwojem rynku technologii bezpieczeństwa w Niemczech. Tam, gdzie zidentyfikowano określone potrzeby, Research Alliance opracował odpowiednie inicjatywy w ramach zespołów specjalistów. Jedną z najważniejszych jest właśnie Industry 4.0.

Firma Pilz czynnie wspierała pracę nowo powołanego biura administracyjnego Industry 4.0 w ramach różnych projektów realizowanych pod kierownictwem stowarzyszeń przemysłowych BITKOM, ZVEI i VDMA. Była również zaangażowana w opracowywanie wytycznych dotyczących dalszych działań. Zostały on przekazane Rządowi Federalnemu na targach Hannover Messe 2013.

Firma Pilz uczestniczy aktywnie w obszarach działalności takich jak:
- Współpraca w zakresie Platformy Industry 4.0;
- Współpraca w ramach Zespołu Zarządzającego Industry 4.0 w ZVEI;
- Współpraca z Federalną Siecią Mechatroniki w Badenii-Wirtembergii;
- Członkostwo w Komitecie Sterującym Stowarzyszenia Industry 4.0 w Badenii-Wirtembergii;
- Udział w niezależnej od producentów platformie demonstracyjno-badawczej Smart Factory^{KL}
- Członkostwo w ARENA2036 – Przyszłość przemysłu motoryzacyjnego

2.2. Industry 4.0 w produkcji realizowanej przez firmę Pilz

Wykraczając poza zaangażowanie w Research Alliance i platformę badawczą SmartFactory^{KL}, Industry 4.0 jest więcej niż tylko inicjatywą firmy Pilz; obecnie stała się ona integralną częścią jej procesu produkcyjnego.
Wraz z rosnącą integracją maszyn i infrastruktury, dzięki wykorzystaniu technologii informatycznej w produkcji, firma Pilz podkreśla również swój profil lidera technologicznego we własnych operacjach produkcyjnych. Zgodnie z założeniami inicjatywy Industry 4.0, stworzono infrastrukturę niezbędną dla inteligentnej produkcji i szybko wdrożono jej elementy.
W użyciu jest już opracowany w zakładzie inteligentny przenośnik części wykorzystywanych w produkcji. Przyspiesza on i upraszcza proces dostarczania płytek drukowanych oraz proces lutowania. Dzięki wbudowanemu chipowi RFID przenośniki części roboczych automatycznie przemieszczane są od linii lutowania do linii montażu.
W ciągu kilku następnych miesięcy Pilz planuje uruchomić inteligentną produkcję we własnym zakładzie produkcyjnym: dane o maszynach będą gromadzone i przetwarzane na potrzeby kontroli produkcji. Ocena tych danych dostarczy ważnych informacji o zmianach w stanie

maszyn i poziomach zużycia. Umożliwi to sprawne przeprowadzanie konserwacji zapobiegawczych. Ten typ konserwacji pozwala uniknąć nieprawidłowego działania i nieprzewidzianych przestojów.
Najnowsze wersje dokumentów roboczych będą również zapisywane w chmurze Pilz. Wszystkie dane i dokumenty będą wówczas dostępne w czasie rzeczywistym, zawsze w najbardziej aktualnej postaci i będzie można uzyskać do nich dostęp z urządzeń mobilnych, w dowolnym miejscu obszaru produkcyjnego.

2.2.1. Technologia informatyczna w zintegrowanej produkcji

Firma Pilz jest świadoma wyzwań związanych z zabezpieczeniem rozwiązań IT w przypadku w pełni zintegrowanego skonfigurowania produkcji. Właśnie dlatego inwestuje w rozbudowaną infrastrukturę zabezpieczeń do monitorowania całego przepływu danych. W tym celu powstało oddzielne centrum komputerowe będące odzwierciedleniem najnowszych standardów. Poprzez ciągłe analizowanie i zapisywanie w dziennikach wszystkich istotnych parametrów produkcji możliwe jest szybkie wykrywanie wszelkich niezgodności. Ponadto, w poszczególnych obszarach produkcyjnych zainstalowano różne systemy firewall, umożliwiające indywidualne określenie poziomu ochrony dla konkretnej strefy. Pozwala to zminimalizować przerwy w produkcji i zagrożenia dla bezpieczeństwa, a także chronić posiadane zasoby know-how.

2.2.2. „Pilz Think Tank 4.0”

Współpraca, w szczególności pomiędzy działami IT i produkcji, mająca tak istotne znaczenie dla inicjatywy Industry 4.0, jest kolejnym najwyższym priorytetem firmy Pilz. Specjalnie utworzony „Pilz Think Tank 4.0” skupia pracowników obszaru produkcyjnego i działu IT. Udostępnia im niezbędne zasoby do planowania oraz realizowania wspólnych projektów na rzecz inicjatywy Industry 4.0.

2.3. Obszar działania – Industry 4.0

Podstawową zasadą służącą zaakceptowaniu zrównoważonego rynku jest utworzenie standardowych mechanizmów w komunikacji pomiędzy maszynami i wewnątrz maszyn. Praktyczne rozwiązania akceptowalne dla użytkowników powstaną tylko wówczas, gdy zostaną uwzględnione wymagania obu dziedzin (automatyzacji i technologii informatycznej), co oznacza, że firma Pilz jest w pełni zaangażowana w tworzenie nowoczesnych rodzajów architektury sterowania w środowisku Industry 4.0.

Skupiamy się na następujących tematach:

- Bezpieczeństwo i ochrona:
  - Pomiędzy ochroną i bezpieczeństwem występują wyraźne podobieństwa z punktu widzenia normalizacji i procedury procesu technologicznego. Zależy nam na wykorzystaniu zgromadzonego doświadczenia w dziedzinie automatyzacji i bezpieczeństwa maszyn w celu przyspieszenia tego niezwykle ważnego procesu.
  - Wszystkie urządzenia i elementy automatyzacji, niezbędne do sprawowania funkcji kontroli, są bezpośrednio podłączane do internetu w celu wymiany danych procesowych i danych o parametrach na potrzeby diagnostyki i konserwacji (zdalnej). W rezultacie wzrasta popyt na wszystkie wymagane urządzenia automatyzacji dla zapewnienia bezpieczeństwa oraz wyposażenia w standardowe rodzaje diagnostycznych interfejsów i wyświetlaczy.

- Podejście modułowe:
  - Nasze nowoczesne funkcje sterowania projektowane są z naciskiem na obiekty będące elementami rozproszonymi – czujniki i elementy wykonawcze wyposażone są w sztuczną inteligencję. Tym samym Pilz powiela trend skierowany na mechatroniczne obiekty sterowania (podzespoły automatyzacji) w swoich produktach i odpowiednich narzędziach projektowych.

3. Obszar aktywności – bezpieczeństwo i ochrona

Warunkiem koniecznym dla funkcjonowania zakładów przemysłowych zgodnego z Industry 4.0 jest zapewnienie bezpieczeństwa i ochrony.

W przyszłości systemy zgodne z Industry 4.0 będą samodzielnie konfigurowane i optymalizowane – podczas pracy przez sam system – co wymaga ponownej oceny bezpieczeństwa i ochrony w trakcie pracy. Konieczne jest również zapewnienie, że w rezultacie pozostającego ryzyka resztkowego nie powstaną niedopuszczalnie wysokie zagrożenia dla bezpieczeństwa.

I ostatecznie, budowanie zaufania w tej dziedzinie należy wspierać wśród małych i średnich przedsiębiorstw jako najważniejszą podstawę produkcji w sieciach tworzonych specjalnie w tym celu. Przejrzystość, uczestnictwo i otwarta komunikacja są ważnymi i niezbędnymi warunkami w tej kwestii.

Rysunek 3: Wzajemne oddziaływanie bezpieczeństwa i ochrony

3.1. Bezpieczeństwo

Bezpieczeństwo maszyn wiąże się z koniecznością zabezpieczenia inwestycji oraz bezpieczeństwem prawnym. Wynika to częściowo z konieczności spełniania określonych norm i standardów.
Na przykład cała analiza ryzyka, ocena ryzyka i procesy wykonawcze są jednoznacznie zdefiniowane z wykorzystaniem klasyfikacji unormowanego w skali międzynarodowej poziomu nienaruszalności bezpieczeństwa (SIL), umożliwiając skuteczne w sensie prawnym porównywanie różnych rozwiązań.

3.1.1. Bezpieczeństwo – od statycznego do dynamicznego

Termin bezpieczeństwo oznacza funkcjonalne bezpieczeństwo maszyn lub, mówiąc inaczej, zabezpieczenie maszyn i ludzi i środowiska przed zagrożeniami, które mogą być stwarzane przez maszyny. Bezpieczeństwo wymaga, aby zagrożenia resztkowe związane z instalacja lub maszyną nie przekraczały akceptowalnych wartości. Dotyczy to zagrożeń dla otoczenia zakładu (np. szkody ponoszone przez środowisko), a także zagrożeń wewnątrz zakładu lub maszyny (np. wobec pracowników fabryki).
Jedną z opcji zabezpieczenia procesu jest natychmiastowe przerwanie zasilania w energię i sprowadzenie maszyny do nagłego zatrzymania. Tradycyjnym sposobem zapewnienia tej opcji jest wykorzystanie specjalnego okablowania bezpieczeństwa i takich elementów jak np. przekaźniki bezpieczeństwa. Jednak takie podejście jest w wysokim stopniu oparte na sprzęcie,

a tym samym statyczne, dlatego nie jest szczególnie odpowiednie dla inteligentnych procesów wytwarzania, w których występuje ciągła potrzeba zmiany konfiguracji instalacji. Definitywne zatrzymanie procesu wiąże się z dalszymi stratami, czy to wynikającymi z utraty wydajności, wydłużonych czasów przestoju spowodowanych bardziej złożonymi procedurami ponownego uruchomienia, czy też wiążącymi się z ograniczeniami obsługi i konserwacji maszyny.

Pojawiają się tu alternatywne koncepcje bezpieczeństwa dynamicznego oparte na zintegrowanym podglądzie zmieniających się procesów automatyzacji i wymagań bezpieczeństwa funkcjonalnego. Zmienia to pogląd na samo bezpieczeństwo; traktowane jest ono bardziej jako funkcja dotycząca cech wspólnych urządzeń niż jako charakterystyka sprzętu. Podejście to, opracowane przed nadejściem ery Industry 4.0, umożliwia obsługę procesów w sposób bezpiecznie kontrolowany, bez potrzeby przerywania ich natychmiast w przypadku każdorazowego wystąpienia usterki. Jednak podejście dynamiczne można wdrożyć skutecznie tylko wtedy, gdy bezpieczeństwo funkcjonalne jest wbudowane w projekt automatyzacji już od etapu jego planowania. Niespełnienie tego wymagania sprawia, że sekwencja poszczególnych etapów produkcji, lub całego procesu, może potrzebować wprowadzania zmian w sposób retrospektywny, co stanowi barierę do osiągnięcia optymalnego rozwiązania i pociąga za sobą również istotne koszty.
Podczas gdy bezpieczeństwo statyczne wymaga często przesyłania sygnałów binarnych (na przykład w celu zatrzymania maszyny po otwarciu drzwi ochronnych), to bezpieczeństwo dynamiczne wymaga bardziej rozbudowanej informacji. Przy takim podejściu istnieje wiele różnych trybów bezpiecznej pracy, które umożliwiają na przykład „pracę przy otwartych drzwiach ochronnych”. Jednakże tego typu informacja o bezpiecznym trybie pracy musi być obecna we wszystkich powiązanych podzespołach. W przykładzie dotyczącym drzwi ochronnych, w zależności od poziomu uprawnień użytkownika, takie działanie jak otwarcie drzwi ochronnych nie skutkuje już automatycznie wyłączeniem maszyny, lecz zamiast tego mechanizmy bezpieczeństwa monitorują, czy spełniony jest warunek zmniejszonej wartości granicznej prędkości lub generują i monitorują bezpieczną wartość nastawy osi obrotowej.

3.1.2. Safety 4.0 – od struktur monolitycznych do rozwiązań modułowych

Wizja inteligentnej fabryki pociąga za sobą konieczność szybkiego i elastycznego przekonfigurowania modułowej instalacji lub zmodyfikowanie jej jako całości. Zatem zatwierdzenie rozwiązania bezpieczeństwa musi umożliwiać dostosowanie się do (późniejszego) zwiększenia elastyczności. Ponieważ wszelkie konfiguracje, które nie zostały uwzględnione w procesie nadawania znaku CE, nie mogą być określane przez operatora.
Nie mamy tutaj do czynienia z prostą równością mówiącą, że
$CE_{moduł\ 1} + CE_{moduł\ 2} = CE_{kompletnej\ maszyny}$!
Funkcjonalna zaleta koncepcji maszyny modułowej jest tutaj oczywista. Wprowadza ona większą elastyczność do procesu produkcyjnego, zwiększając jednocześnie zakres standaryzacji na poziomie funkcjonalnym. Najwyższy potencjał standaryzacji można uzyskać, gdy granice różnych modułów charakteryzują się identyczną konfiguracją – niezależnie od tego, czy moduł obsługuje funkcję mechaniczną, elektryczną, sterowania, czy wizualizacji. Celem podejścia mechatronicznego jest tworzenie obiektów automatyzacji, które są w ten sposób unormowane.
Zalety podejścia modułowego są często unicestwiane przez sztywną koncepcję bezpieczeństwa, która może wciąż opierać się na niemodyfikowalnym okablowaniu. Również elektroniczne systemy kontroli bezpieczeństwa prawie zawsze naśladują bezpieczeństwo

oparte na sprzęcie – w postaci niezmiennych obwodów bezpieczeństwa – nawet jeśli produkt jest oferowany w wersji z dowolnie programowalną logiką obwodów.
W przeciwieństwie do tego podstawowa funkcja nowoczesnych typów architektury sterowania i kontroli polega na tym, że funkcjonuje ona w dużym stopniu bez narzucania jakichkolwiek reguł o charakterze systemowym. Celem jest umożliwienie użytkownikowi ich zoptymalizowania w sposób zależny tylko od niego, z zachowaniem ich stopnia modułowości. Usuwaj bariery tworzone przez różne poglądy na funkcje automatyzacji i bezpieczeństwa maszyn, co pozwoli Ci uzyskać podstawowe stopnie swobody.
PSS 4000 jest systemem sterowania obejmującym aspekty modułowości i podwyższonej elastyczności, będące jego podstawowymi funkcjami. Po raz pierwszy można obecnie zarządzać wszystkimi zmiennymi procesu – w tym również funkcjami bezpieczeństwa – używając metody symbolicznej, czyli bez jakichkolwiek uwarunkowań sprzętowych w systemie. Odzwierciedleniem tego jest udostępnienie wszystkich zmiennych procesu w całym systemie; dzięki architekturze o wielu podmiotach typu master zmienne te stają się automatycznie dostępne dla wszystkich systemów sterowania w systemie automatyzacji rozproszonej.

3.1.3. Certyfikacja modułów

Im więcej maszyn składa się z modułów, tym więcej podzespołów musi być połączonych w sposób zdecentralizowany. Modułowa konstrukcja maszyny, lub części maszyn cechuje się kilkoma znaczącymi zaletami. Moduły maszyn można ponownie łączyć i wymieniać. Można rozbudowywać maszyny lub na przykład dokonać wymiany narzędzia bez przerywania produkcji. Maszyny stają się bardziej elastyczne. Operator może wytwarzać większą liczbę produktów przy tej samej liczbie maszyn. Praca przy założeniu, że jest to korzyść dla operatora sprawia, że koncepcje kontroli stają się bardziej zdecentralizowane. W tym kontekście ważne są zagadnienia bezpieczeństwa i ochrony. Kluczową koncepcją jest modułowe certyfikowanie poszczególnych modułów instalacji. Obecnie maszyny są kontrolowane i dopuszczane do użytku przez jednostki certyfikujące jako kompletna całość. Nawet mała zmiana, taka jak np. zamiana dwóch modułów, może oznaczać, że wymagana będzie ponowna certyfikacja. Mimo że dyskutowane są różne rozwiązania, nie obowiązuje obecnie żadna standardowa praktyka. Jedno z takich podejść zakłada, że maszyna jest bezpieczna, jeśli bezpieczne są jej poszczególne moduły. Należy jednak uczulić przedsiębiorstwa i decydentów, że bez ram prawnych nie można wyobrazić sobie postępu w tej dziedzinie.

3.2. Ochrona

Wyzwaniem dla ochrony procesu jest – w przeciwieństwie do bezpieczeństwa funkcjonalnego – konieczność ciągłego dostosowywania mechanizmów ochrony do nowych zagrożeń. Może to być związane z wymaganymi aktualizacjami, ponieważ wirusy, robaki, Trojany itp. wciąż podlegają ewolucjom, a niedostateczne zabezpieczenie może w konsekwencji uniemożliwić produkcję, a także zablokować działanie wszystkich elementów funkcjonalnych.
Aby móc elastycznie odpowiedzieć na ewentualność wystąpienia istotnego zagrożenia, musi istnieć wszechstronna strategia bezpieczeństwa, zawierająca wiele warstw wspierających ochronę aplikacji dotyczących bezpieczeństwa: na pierwszym planie są podzespoły automatyzacji. Odnosi się to również do sieci, za pomocą których te podzespoły mogą komunikować się z innymi sieciami lub na przykład z systemem ERP. Najbardziej zewnętrzna warstwa jest odzwierciedleniem fabryki, którą chroni przed zewnętrznym światem specjalny system firewall, jest to tak zwana strefa zdemilitaryzowana.

Wymagania nakładane przez sfery technologii informatycznej i automatyzacji na ochronę istotnie się miedzy sobą różnią.
Podczas gdy poufność informacji ma najwyższy priorytet w środowisku biurowym, w sferze produkcyjnej najwyższe miejsce na tej liście zajmuje dostępność danych, ponieważ jest to najważniejszy warunek płynności procesu produkcyjnego. Aktualnie trwają prace nad stworzeniem międzynarodowej normy (IEC 62443), mającej na celu połączenie obu tych obszarów. Ponieważ zagrożenia pochodzące z cyber-świata są dynamiczne, bezpieczeństwo i ochrona będą stanowić dwa odrębne zagadnienia, które, mimo wszystko, są ściśle ze sobą związane.

Najważniejszy jest fakt, że opracowujemy metody i narzędzia, za pomocą których możemy analizować wpływ luk w ochronie na dodatkowe zagrożenia resztkowe dla bezpieczeństwa. Te metody i narzędzia powinno się bezwzględnie stosować podczas opracowywania systemów cybernetyczno-fizycznych (CPS), co możemy nazwać ochroną w fazie projektowej.

Należy uwzględnić następujące aspekty:
- zabezpieczenie interfejsów (sterowników PLC) przed wpływem z zewnątrz (internet, sieć firmowa…);
- ochronę systemów komunikacyjnych w instalacji i maszynach zależną od sposobów użytkowania (stała praca, zdalna konserwacja, zdalna diagnostyka, połączenia zależne od celu...).
- Ochrona stanowi tak zwany „ruchomy cel”; nie istnieje niezmienne rozwiązanie bezpieczeństwa.

3.2.1. Różne rozwiązania w dziedzinie ochrony

Jak rozwiązania bezpieczeństwa chronią przed zagrożeniami ze strony cyber-świata? Najkrótsza odpowiedź brzmi: tylko poprzez łączenie różnych metod i zaleceń ochrony, których wszystkie strony muszą konsekwentnie przestrzegać.
W przypadku łączenia w sieć receptą na sukces jest „głęboka obrona”. Jednym z podstawowych elementów, który przypomina sposób, w jaki budowano zamki średniowieczne, jest model ochrony typu „stref i kanałów”, który jest już zdefiniowany w normie IEC 62443. Rozpatruje on podział sieci automatyzacji na różne strefy, w których urządzenia mogą komunikować się między sobą. Wymiana danych z urządzeniami znajdującymi się w innych strefach możliwa jest wyłącznie poprzez pojedynczy kanał chroniony przez bezpieczny router lub system firewall, filtrujący dane zgodnie z określonymi regułami, blokując tym samym nieuprawniony dostęp. Nawet gdyby atakujący mógł wniknąć do jednej strefy, zagrożone byłyby urządzenia należące tylko do tej strefy, a inne pozostałyby bezpieczne.

3.2.2. Rozwiązania automatyzacji

Szereg norm dotyczących bezpieczeństwa technologii informatycznej w przemysłowych systemach sterowania (IEC 62443) określa siedem podstawowych wymagań ochrony rozwiązań automatyzacji:
- Kontrola identyfikacji i uwierzytelniania (IAC)
- Kontrola użytkowania (UC)
- Nienaruszalność danych (DI)
- Poufność danych (DC)
- Ograniczony przepływ danych (RDF)

- Natychmiastowa odpowiedź na zdarzenia (TRE)
- Dostępność zasobów (RA)

Każde z tych podstawowych wymagań można rozszerzyć na następujące elementy:

- identyfikacja i uwierzytelnianie,
- identyfikacja użytkownika-człowieka,
- wieloczynnikowe uwierzytelnianie w przypadku sieci niezaufanych;
- identyfikacja programu i urządzenia;
- jednoznaczna identyfikacja i uwierzytelnianie;
- moc uwierzytelniania z użyciem hasła;
- tworzenie haseł i ograniczenie na czas eksploatacji w przypadku użytkowników-ludzi.

Każdy z tych elementów dysponuje możliwymi do osiągnięcia czterema poziomami ochrony, bazującymi na pracy włożonej w projektowanie rozwiązań automatyzacji. Integrator systemów i operator instalacji muszą teraz określić poziomy ochrony odpowiednie dla aplikacji i związanego z nią modelu strefy. Bezsprzecznie najwyższy „Poziom 4” ochrony może wymagać ogromnej ilości pracy.

Nawet najlepsze techniczne środki ochrony są bezwartościowe, jeśli nie zostaną wdrożone w praktyce lub – co gorsza – gdy są celowo omijane, ponieważ ich przestrzeganie zajmuje zbyt wiele czasu albo wynikają z braku zrozumienia i nieznajomości. Środki techniczne muszą być wdrażane na równi z wytycznymi i zasadami organizacji. Jaki jest poziom bezpiecznych ustawień systemu firewall, jeśli zostaje wybrane hasło pochodzące z przykładu w instrukcji, lub jeśli łatwo jest ustalić związek między hasłem a urządzeniem? Poziom ochrony dla fragmentu instalacji jest rezultatem współdziałających zabiegów technicznych i organizacyjnych.

3.3. Wzajemne oddziaływanie bezpieczeństwa i ochrony

Holistyczne koncepcje ochrony nie tylko wymagają wzajemnego oddziaływania pomiędzy bezpieczeństwem a ochroną; ale także wykorzystania typów architektury systemu odnoszących się specyficznie do tego rodzaju koncepcji, opartych na otwartych standardach i dopuszczających stosowanie podzespołów pochodzących od różnych producentów. W odniesieniu do aspektów bezpieczeństwa konieczne jest sprawdzenie zakresu, w jakim zagadnienia ochrony wpływają na bezpieczeństwo funkcjonalne.
Najważniejsze z nich to wyraźny, bezpieczny dowód tożsamości produktów, procesów i maszyn, a także bezpieczna wymiana informacji na przestrzeni całego procesu produkcyjnego.

Potrzebne są również rozwiązania przyjazne dla użytkownika: konieczne jest zapewnienie stosunkowo łatwego wpływania na bezpieczeństwo i ochronę oraz uwzględnienie potrzeb użytkownika. Z ekonomicznego punktu widzenia bezpieczeństwo jest również siłą napędową innowacji; obejmuje ono łączenie struktury kosztów w odniesieniu do wydajności. Niezbędne jest zapewnienie możliwości ubezpieczenia się na wypadek szkód i dysponowanie wymaganymi metodami obliczeniowymi.
W odniesieniu natomiast do czynnika ludzkiego, ważnym zagadnieniem jest „możliwa do wykorzystania ochrona i prywatność”. Zadaniem jest utrzymywanie na minimalnym poziomie wysiłków rozłożonych w czasie i zrozumienie niezbędnych środków ochrony.

Istnieją tutaj analogie z bezpieczeństwem funkcjonalnym: środki ochrony nie mogą ujemnie wpływać na dyspozycyjność. Zasady związane z kategorią bezpieczeństwa można przenieść jednoznacznie na kategorię ochrony. Bezpieczeństwo wymaga podejścia holistycznego.

4. Obszar aktywności – podejście modułowe

Sukces w wyzwaniach średnio lub długoterminowych może zapewnić tylko ściśle interdyscyplinarne „myślenie modułowe". Główną rolę odgrywają tu wspomagające to podejście systemy sterowania.

4.1. Rozproszone systemy inteligentne – system sterowania PSS 4000

Realizację spójnego, mechatronicznego podejścia umożliwia firmie Pilz jej system sterowania PSS 4000. Koncepcja systemu PSS 4000 zakłada połączenie automatyzacji z bezpieczeństwem. Dane procesów lub sterowania, dane odporne na awarie oraz informacje o charakterze diagnostycznym są wymieniane i synchronizowane za pośrednictwem ethernetowego protokołu SafetyNET p. Z punktu widzenia funkcji sterowania nieistotne jest zatem miejsce wykonywania danej sekcji programu. Zamiast scentralizowanego systemu sterowania użytkownik ma do dyspozycji w ramach scentralizowanego projektu program o działaniu rozłożonym w czasie. Konfiguracji, programowania i diagnozowania wszystkich urządzeń podłączonych do sieci dokonuje się z poziomu takiego scentralizowanego projektu. Po zakończeniu konfigurowania projektu poszczególne komponenty programu przydzielane są pojedynczym aktywatorom. Osiąga się to na podstawie wyraźnej specyfikacji użytkownika dotyczącej podziału jednostek funkcjonalnych na grupy, co umożliwia prostą, unormowaną obsługę w ramach całego projektu. Zalety obejmują nie tylko tworzenie i standaryzację modułów, ale również bardziej elastyczne reagowanie na błędy, większą dyspozycyjność i wyższą wydajność dzięki krótszym czasom odpowiedzi dla całego systemu.

W odróżnieniu od klasycznych systemów automatyzacji, w których scentralizowany system monitoruje zakład lub maszyny oraz przetwarza wszystkie sygnały, PSS 4000 umożliwia modułowy podział funkcji sterowania. Mówiąc bardziej szczegółowo, system sterowania PSS 4000 składa się z komponentów sprzętowych, oprogramowania, sieci Ethernet czasu rzeczywistego SafetyNET p oraz zróżnicowanych edytorów oprogramowania opracowanych z myślą o różnych sektorach, a także z modułami funkcji podzielonymi pod względem zastosowań. Komponenty sprzętowe obejmują zróżnicowane systemy sterujące o różnych klasach wydajności. Dane dotyczące procesów lub sterowania, dane odporne na przekłamanie i informacje diagnostyczne są wymieniane i uzgadniane za pośrednictwem sieci Ethernet. To istotne połączenie funkcji bezpieczeństwa i sterowania standardowego zmniejsza stopień złożoności komunikacji, a także umożliwia optymalizację kosztów.

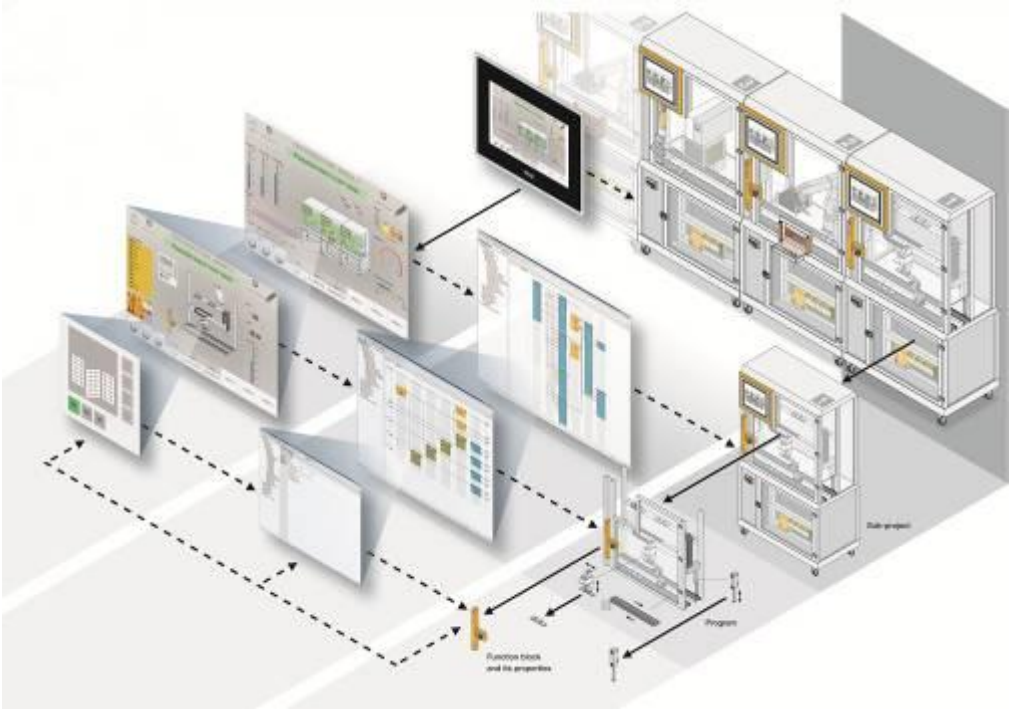
4.2. Narzędzia projektowe PAS4000

Zadaniem systemu sterowania PSS 4000 firmy Pilz jest uproszczenie decentralizacji funkcji sterowania z utrzymaniem przejrzystości działania. Platforma programowa PAS4000 pełni w tym kluczową rolę. Obejmuje ona szereg edytorów przeznaczonych do programowania

i konfigurowania sterowników PLC, jak również bloki programowe. W PAS4000 narzędzia do konfigurowania, programowania, uruchamiania i obsługi są ściśle ze sobą kompatybilne.

Platforma programowa PAS4000 obsługuje rozbicie funkcji instalacji/maszyny na jeszcze mniejsze moduły funkcyjne zgodnie z tą samą zasadą, która obowiązuje w przypadku określania granic pomiędzy jednostkami mechatronicznymi. Podstawowym aspektem jest modułowość: z funkcji podstawowych tworzone są elementy, które z kolei tworzą moduły, zaś moduły służą do budowania instalacji i maszyn – w sposób bardzo prosty, poprzez hierarchiczne zagnieżdżanie bloków. Podstawowe funkcje, elementy i moduły tworzą szkielet, wokół którego budowane jest oprogramowanie; nadają się one idealnie do ponownego wykorzystywania jako elementy programowe.

Platforma programowa PAS4000 udostępnia biblioteki programów zawierające najpowszechniejsze podstawowe funkcje i moduły. Wybór gotowych komponentów z bibliotek jako taki nie jest niczym nowym. Specjalną cechą PAS4000 jest przydzielenie tym komponentom „właściwości”. Umożliwia to dosyć łatwe ustawianie parametrów dla wymaganych funkcji, co stanowi szczególną korzyść w kategoriach standaryzacji funkcji.



Rysunek 4: Instalacje można dzielić na niezależnie funkcjonujące jednostki, którymi można zarządzać.

4.3. Wizualizacja PASvisu

Zgodnie z tą samą zasadą nawet programy do wizualizacji i sterowania można podzielić na mniejsze jednostki. Wspólna podstawa danych dla poszczególnych modułów sprawia, że moduły te mogą komunikować się między sobą. Dzięki jednolitej strukturze można łatwo ponownie wykorzystać dane konfiguracji projektu.

Oprogramowanie do wizualizacji umożliwia szybkie tworzenie i konfigurowanie projektów z wykorzystaniem programu PASvisu Builder.
Ponieważ w projekcie automatyzacji dostępne są wszystkie dane, w tym zmienne procesowe i obszary nazw OPC, nie ma już konieczności ręcznego wprowadzania i wpisywania zmiennych, co zawsze wiąże się z ryzykiem popełnienia błędu. Oznacza to, że obecnie można wywołać z systemu sterowania taką informację jak suma kontrolna projektu lub wersję oprogramowania firmowego dla jednostki głównej.

W inicjatywie Industry 4.0 rozważa się „wartość danych” – w tym przypadku danych dotyczących konfiguracji projektu. Ta podstawa wspólnych danych jest pomocna w zmniejszeniu źródeł potencjalnych błędów poprzez automatyczne przyjęcie danych „pasujących”, podczas gdy zautomatyzowane kontrole spójności skracają czasy projektowania: tworzenie jednolitych modułów na potrzeby sterowania i wizualizacji ułatwia ponowne wykorzystanie elementów maszyn i modułów.

Słownik

Inteligentny produkt
Inteligentny produkt ma swój numer identyfikacyjny lub jest oznakowany bezpośrednio z wykorzystaniem kluczowej informacji o jego wytwarzaniu, umożliwiając kontrolę jego procesu produkcyjnego. Jako obiekt inteligentny, stanowi on podstawę dla Internetu rzeczy.

Internet rzeczy
W Internecie rzeczy (IoT) inteligentne „rzeczy", elementy lub obiekty komunikują się z sobą za pośrednictwem uniwersalnej sieci cyfrowej. W coraz większym stopniu komputery jako indywidualne urządzenia zastępowane są przez „inteligentne rzeczy". Podłączone są one do internetu, co umożliwia ich niezależne komunikowanie się w celu wykonywania najróżniejszych zadań na rzecz właściciela.
W szczególności dzięki inteligentnej technologii lokalizacji polegającej na identyfikacji z wykorzystaniem częstotliwości radiowych (RFID) obiekty mogą teraz same się identyfikować i w rzeczywistości do pewnego stopnia się kontrolować. Obiekty te są nośnikami pewnych informacji zapowiadających przyszłe działania z ich udziałem.
Tak więc same produkty informują o sposobie ich traktowania w przyszłości lub o systemie produkcji w następnych etapach przetwarzania. Interwencja ludzka przestaje być niezbędna.

Systemy cybernetyczno-fizyczne (CPS)
Kluczowymi komponentami są mobilne i umożliwiające przemieszczanie instalacje, urządzenia i maszyny (w tym roboty), systemy zagnieżdżone i obiekty połączone w sieć (Internet rzeczy). Przesyłanie, wymiana, monitorowanie i kontrola ich charakterystycznych danych są realizowane w czasie rzeczywistym przez infrastrukturę taką jak internet.
Można je uaktywniać i dokonywać ich odczytu bez jakiegokolwiek bezpośredniego kontaktu i wykorzystywać ich inteligencję do niezależnego podejmowania decyzji. System cybernetyczno-fizyczny charakteryzuje się wysokim stopniem złożoności. Systemy cybernetyczno-fizyczne tworzone są przez integrowanie zagnieżdżonych systemów z wykorzystaniem przewodowych lub bezprzewodowych sieci komunikacyjnych.

Referencyjny model architektury (RAMI)
Wykorzystywaną automatyzację charakteryzuje struktura zorientowana sprzętowo (piramida automatyzacji). Taka struktura staje się obecnie przestarzała, gdyż automatyzacja może dotyczyć nie tylko połączonych urządzeń, ale również obejmuje połączenia z chmurą i połączenia danych. Ponadto, podobnie jak udostępnienie danych z produkcji w procesie, możliwe jest również uzyskanie dostępu do zewnętrznych danych sterujących. Dlatego też stworzono referencyjny model architektury (RAMI) będący zmodernizowaną piramidą automatyzacji. Stowarzyszenie ZVEI opracowało ideę i koncepcję przemysłu automatyzacji wspólnie z VDI/VDE-GMA, DKE oraz partnerami uczestniczącymi we wspólnej platformie Bitkom i VDMA realizującymi inicjatywę Industry 4.0.[10] Model ten łączy zasadnicze elementy inicjatywy Industry 4.0 po raz pierwszy w trójwymiarowym modelu warstwowym.[11] Dzięki takim ramom działalności inicjatywę Industry 4.0 można systematycznie klasyfikować i nadal rozwijać.

[10] http://www.zvei.org/Themen/Industrie40/Seiten/Das-Referenzarchitekturmodell-RAMI-40-und-die-Industrie-40-Komponente.aspx
[11] http://www.zvei.org/Downloads/Automation/ZVEI-Faktenblatt-Industrie4_0-RAMI-4_0.pdf

Model ten definiuje normy dla inicjatywy Industry 4.0. Taka standaryzacja jest niezbędna, ponieważ inicjatywa Industry 4.0 oznacza, że komponenty produkcji różnych firm muszą mieć możliwość komunikowania się ze sobą.

Jesteśmy obecni na arenie międzynarodowej. Więcej informacji znajduje
się na naszej stronie internetowej lub prosimy o kontakt z centralą naszej firmy.

Siedziba główna: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Niemcy
Telefon: +49 711 3409-0, Telefax: +49 711 3409-133, e-mail: info@pilz.com, Internet: www.pilz.com

PILZ

THE SPIRIT OF SAFETY