Koncepcje automatyki przemysłowej w środowisku Industry 4.0

Concepts of industrial automation products for Industry 4.0

PIOTR SZULEWSKI*

DOI: 10.17814/mechanik.2016.7.221

Omówiono zaprezentowane na targach Hannover Messe 2016 **innowacyjne koncepcje programowo-sprzętowe związane z wprowadzaniem idei Industry 4.0 w praktykę przemysłową: nowe środowiska programowe wspierające sieci przemysłowe, systemy cyber-fizyczne, Internet rzeczy, komunikację** maszyna–maszyna. Przeanalizowano sens inteligentnego **zakładu, bezpieczeństwo transmisji i wymianę danych OPC.**
SŁOWA KLUCZOWE: Hannover Messe 2016, Industry 4.0, sterowniki PLC, inteligentna fabryka, Internet rzeczy, sieci przemysłowe

The paper illuminates innovations of software and hardware associated with the introduction of the Industry 4.0 concept in practice, presented at Hannover Messe 2016: the new industrial network systems, cyber-physical systems, Internet of things and machine to machine communication. The idea of intelligent, Smart Factory, transmission security and exchange OPC data are also presented.
KEYWORDS: Hannover Messe 2016, Industry 4.0, PLC controllers, IoT, M2M, Smart Factory, field communication

W dniach 25÷29 kwietnia 2016 r. odbyła się kolejna już edycja targów w Hanowerze. Zgromadziły one ponad 5200 wystawców maszyn, urządzeń technologicznych i komponentów automatyki przemysłowej. W tym roku partnerem strategicznym wydarzenia były Stany Zjednoczone. Ekspozycje odwiedziło ponad 190 000 osób, z czego 50 000 to goście z zagranicy. Zorganizowanych zostało 1500 wykładów, konferencji oraz pokazów – co wyraźnie sugeruje, że poza przedsięwzięciem typowo biznesowym istotnym aspektem targów są działania edukacyjne. W opinii organizatorów tegoroczne Hannover Messe dowodzą ostatecznego triumfu koncepcji „Industry 4.0". Wsparciem dla tej tezy była niewątpliwie prezentacja ponad 400 urządzeń i systemów komputerowych wpisujących się w promowaną ideę zgodnie z hasłem przewodnim: „Zintegrowany przemysł to odkrycie nowych rozwiązań". Wystawcy koncentrowali się na prezentowaniu koncepcji inteligentnych fabryk (Smart Factory), które są przyszłością przemysłu wytwórczego, ponieważ tylko „Cyfrowa fabryka zwiększa elastyczność wytwarzania".

Interfejsy komunikacyjne stały się już standardem we współczesnych urządzeniach automatyki. Coraz trudniej znaleźć „samotną wyspę automatyzacji". Środowiska sterowania rozproszonego zadomowiły się w praktyce przemysłowej. Podejmowane przez producentów działania koncentrują się przede wszystkim na rozwoju zaawansowanego oprogramowania, które stanowi klucz do sukcesu, czyli obniżenia kosztów wytwarzania, uelastycznienia produkcji, skrócenia czasu dostawy i znacznego poszerzenia asortymentu – zgodnie z rosnącymi wymaganiami rynku.

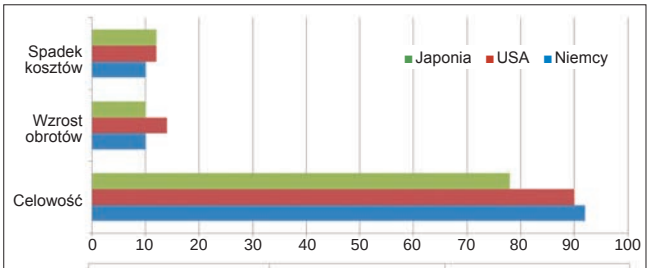
* Dr inż. Piotr Szulewski (maxer@cim.pw.edu.pl) – Instytut Technik Wytwarzania, Wydział Inżynierii Produkcji Politechniki Warszawskiej

Industry 4.0

Wprowadzenie idei Industry 4.0 jest związane z oczekiwanym intensywnym rozwojem różnych dziedzin działalności przemysłowej. Według badań Instytutu Fraunhofera przeprowadzonych w oparciu o analizy firm niemieckich w okresie 2014÷2025 należy się spodziewać wzrostu zysku (brutto) w przemyśle maszynowym z poziomu 76,8 do 99,8 mld euro (o ok. 30%), a w przemyśle wytwarzającym komponenty elektryczne i automatykę z 40,3 do 52,4 mld euro (również o ok. 30%). Należy zauważyć, że przewidywana korzystna koniunktura będzie dotyczyć praktycznie wszystkich działów gospodarki. Przykładowo w rolnictwie i leśnictwie estymowany jest wzrost o co najmniej 15%. To właśnie z tego powodu wiele firm już teraz proponuje szeroką gamę rozwiązań zgodnych z ideą Industry 4.0.

Ponieważ wprowadzenie pełnej „cyfryzacji" produkcji jest – jak każde nowe działanie – obarczone niezerowym ryzykiem, dlatego warto zacytować wyniki sondy przeprowadzonej w roku 2016 w 300 przedsiębiorstwach z USA, Niemiec i Japonii. Pytano o spodziewany sukces przedsięwzięcia, wzrost obrotów firmy oraz oczekiwane oszczędności w nakładach na produkcję. Na rys. 1 zestawiono przewidywane efekty modernizacji. Zdecydowanie ponad 75% przedsiębiorstw widzi celowość wprowadzenia idei cyfrowej fabryki. Wiąże się z tym planowany, co najmniej dziesięcioprocentowy wzrost obrotów i dodatkowy dziesięcioprocentowy spadek kosztów produkcji. Oznacza to, że przedsiębiorstwa widzą ekonomiczną celowość podejmowania takich działań.

Kluczowe jest uzyskanie bardzo krótkiego czasu pomiędzy powstaniem koncepcji nowego produktu a dostawą finalnego wyrobu. Sukcesem będzie sytuacja, kiedy już pierwszy wykonany prototyp będzie miał pełną funkcjonalność gotowego wyrobu i będzie mógł być zaoferowany klientowi. Jest to możliwe jedynie w przypadku, gdy już od samego początku, w trakcie rozwoju produktu, powstanie jego w pełni cyfrowy model. Na jego podstawie można szczegółowo określić sposób działania, cechy funkcjonalne, wprowadzić konieczne zmiany, a nawet oszacować zadowolenie przyszłego użytkownika.



	Celowość	Wzrost obrotów	Spadek kosztów
Japonia	78	10	12
USA	90	14	12
Niemcy	92	10	10

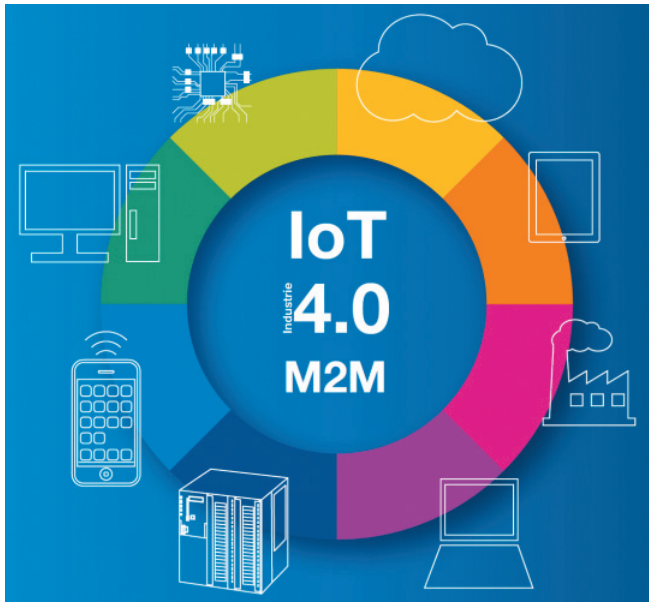
Rys. 1. Przyczyny popularności idei Industry 4.0

Według specjalistów proces wprowadzania technologii cyfrowych do wytwarzania rozpoczął się już bardzo dawno. Takie koncepcje pojawiały się od lat osiemdziesiątych ubiegłego wieku (CAD, CIM, CAM). Problemem były niezbyt duże moce obliczeniowe stosowanych wówczas mikroprocesorów i bardzo mała wydajność sieci komputerowych oscylująca wokół wartości 56 kbit/s (takie parametry osiągały modemy pracujące z wykorzystaniem linii telefonicznych). Obecnie podstawowe wymagania dla systemu komunikacji w koncepcji cyfrowej fabryki (Industry 4.0) to przede wszystkim:

- Całkowita niezależność stosowanej w zakładzie technologii komunikacji od producenta, rodzaju systemu operacyjnego czy środowiska programistycznego itp.
- Pełna skalowalność zintegrowanej sieci pozwalająca na aktywną współpracę podstawowych czujników i elementów wykonawczych, wbudowanych sterowników PLC, PAC i NC, tabletów, smartfonów, komputerów i stacji roboczych, systemów klasy *main-frame* oraz aplikacji działających w chmurach obliczeniowych.
- Zapewnienie swobodnego przepływu danych zarówno w pionie, jak i w poziomie hierarchicznej struktury informatycznej zakładu.
- Maksymalne bezpieczeństwo transferu danych oraz uwierzytelnianie na poziomie użytkownika i w aplikacji.
- Wspieranie architektury zorientowanej na usługi SOA (*service oriented architecture*), wykorzystywanie w warstwie transportowej (model ISO/OSI) tylko znanych i utwierdzonych standardów (np. TCP/IP).
- Zapewnienie możliwości przesyłania danych bieżących (aktualnych) i historycznych, transmisji swobodnych komunikatów, rozkazów i odpowiedzi.
- Tworzenie danych zagregowanych (zespolonych), umożliwiających wydajne modelowanie wirtualnych przedmiotów służących do skutecznego odtwarzania rzeczywistych produktów i ich detali lub określania stanu realizacji produkcji.
- Szybkie i bezproblemowe tworzenie połączeń, także tych nieplanowanych lub okazjonalnych, wspieranie samoczynnych konfiguracji dołączonego sprzętu sieciowego, inteligentnego tworzenia struktury sieci i automatycznego rozpoczynania komunikacji w przypadku pojawienia się nowych obiektów.
- Otwartość wymiany danych także dla systemów komputerowego wspierania działań inżynierskich i swoboda kształtowania współpracy z innymi standardami, nawet przy braku zgodności semantycznej sieci i transmitowanych komunikatów.
- Wymaganie potwierdzenia przez niezależną instytucję/organizację opisu i szczegółów standardu wymiany danych w celu zachowania daleko idącej niezależności i otwartości (laboratoria certyfikujące).

IoT, CPS, M2M

Kolejna faza rewolucji przemysłowej jest bezpośrednio związana z wprowadzaniem nowego modelu produkcji realizowanego w tworzonych obecnie inteligentnych fabrykach. Na rys. 2 przedstawiono przykład znaku identyfikującego tę ideę. Istotnym elementem jest dążenie do pozyskania precyzyjnego, w pełni cyfrowego opisu produktu, technologii i urządzeń biorących udział w wytwarzaniu. Model informatyczny ma stanowić podstawę do projektowania przedmiotu, modelowania, przetwarzania, a w rezultacie sterowania wszystkimi obrabiarkami biorącymi udział w produkcji – koncepcję tę można określić skrótowo jako cyfrowe przetwarzanie materii – aczkolwiek produkt finalny ma mieć jak najbardziej rzeczywisty (materialny) charakter. Wymagana wobec tego całkowita „digitalizacja" procesu produkcji musi korzystać z nowych źródeł danych i informacji, które wzbogacą i uzupełnią tradycyjny model fizyczny.



Rys. 2. Koncepcja Industry 4.0 (źródło: https://opcfoundation.org/resources/brochures/)

Proponowane są dwa główne kierunki: systemy cybernetyczno-fizyczne (*cyber-physical system*) oraz Internet rzeczy – IoT (Internet of Things). Pod pojęciem systemów cyber-fizycznych zwykło się rozumieć urządzenia składające się ze zintegrowanej struktury informacyjno-technicznej, w których wbudowany (*embeded*) mikroprocesor (mikrokontroler) stanowi część urządzenia wytwórczego. Przykładem może być popularny sterownik programowalny PLC. Do tej kategorii można także zaliczyć rozbudowane czujniki i układy wykonawcze realizujące zadania autonomiczne, sieci przemysłowe i magistrale komunikacyjne łącznie z Internetem.

Internet rzeczy jest związany z koncepcją tworzenia jednoznacznie identyfikowalnych (np. RFID) przedmiotów, które za pośrednictwem systemów komunikacji (sieci przewodowych i bezprzewodowych) mogą wymieniać między sobą dane celem wzajemnego współdziałania. W przypadku automatyki przemysłowej dobrym przykładem jest komunikacja pomiędzy obrabiarkami i maszynami technologicznymi, nazywana M2M (Machine to Machine). W szerszym pojęciu są to dowolne urządzenia (np. artykuły gospodarstwa domowego, komputery noszone), które mogą pośrednio albo bezpośrednio gromadzić, przetwarzać lub wymieniać informacje. Sumarycznie możemy zatem stwierdzić, że Industry 4.0 to cyfryzacja materii wytwórczej, sterowanej systemami cyber-fizycznymi w środowisku Internetu rzeczy, gdzie obserwujemy płynne i bezkolizyjne przenikanie się świata realnego z rzeczywistością wirtualną.

Podstawą sukcesu implementacji koncepcji Industry 4.0 jest pozyskiwanie dużych ilości precyzyjnych informacji o kondycji obrabiarki, procesu lub urządzenia biorącego udział w wytwarzaniu. Aby uzyskać te dane, konieczne jest stosowanie różnego rodzaju czujników pozwalających na wnikliwe badanie wielu parametrów i zmiennych. Niektórzy producenci nazywają sensory (czujniki) współczesnymi organami percepcji systemów sterowania produkcją i, rozumiejąc ich wagę oraz skomplikowanie zadań,

proponują oparte na takich właśnie danych, coraz bardziej wyrafinowane modele maszyn, wytwarzania i produkcji.

Potencjał rynku Internetu rzeczy jest na tyle duży, że wiele firm zaczyna oferować gotowe rozwiązania specjalizowanych modułów komunikacyjnych możliwych do zabudowania w dowolnych układach automatyki. Są to elementy elektroniczne wykonywane w technice jednoukładowej. W skład takiego elementu wchodzą: mikroprocesor lub mikrokontroler (zazwyczaj 32-bitowy), zestaw interfejsów sprzętowych (UART, USB, I^2C, SPI) oraz gotowe moduły komunikacyjne (IrDA, Ethernet, CAN, ASI, Profibus, Profinet, Modus, EtherCat i inne). Moduły sieciowe zawierają całe konieczne oprogramowanie stosu komunikacyjnego danego standardu wymiany danych. Nie jest konieczne samodzielne programowanie nieraz bardzo skomplikowanych procedur utrzymania łączności. Warto podkreślić, że układy te są tak projektowane, aby możliwe było ich zastosowanie w aplikacjach mobilnych, gdzie zasilanie jest realizowane przez wbudowane baterie lub akumulatory. Niewielki pobór prądu z zachowaniem pełnej funkcjonalności zapewnia długotrwałą pracę. Przykładem tego typu rozwiązań mogą być produkty firmy Renesans (głównie w obszarze sieci Internetu przemysłowego) lub Texas Instruments (praktycznie wszystkie liczące się standardy sieci).

Podobne urządzenia oferuje firma Altera. Aby zapewnić skuteczną implementację Internetu rzeczy, proponowane jest zastosowanie mikrokontrolera jednoukładowego – gotowego do natychmiastowego użycia w całkowicie nowych lub istniejących elementach automatyki (rys. 3). Pod kontrolą systemu operacyjnego Linux (RTOS) działają różnorakie interfejsy umożliwiające szybkie dołączenie do sieci Profinet, EtherCat, EtherNet/IP, zwykłego Internetu lub Ethernetu IEEE 802.1 TSN (*Time-Sensitive Networking*). W strukturze sprzętowej układu są także zabudowane kontrolery czytnika znaczników RFID oraz sterownik napędów z możliwością realizacji ruchów robota. W sferze programowej jest zaimplementowany serwer HTML5 do bezpośredniej wizualizacji stanu układu i procesu, a także klient/serwer standardu OPC-UA.

Rys. 3. Internet rzeczy według firmy Altera (źródło: Intel, www.intel.com)

Zastosowanie koncepcji Internetu rzeczy może być bardzo efektywne w przypadku gromadzenia danych związanych z predykcyjną konserwacją PdM (*Predictive Maintenance*). Wyposażenie maszyny lub obrabiarki w zabudowane w jej istotnych podzespołach mikrokontrolery z czujnikami pozwala na prowadzenie ciągłego monitorowania kondycji urządzenia. Analizując pozyskiwane dane, można kontrolować stan poszczególnych zespołów i podejmować działania uprzedzające wystąpienie uszkodzenia lub stanu awaryjnego. Według firmy Dell zastosowanie tej technologii przynosi policzalne korzyści. Można się spodziewać trzynastoprocentowej redukcji kosztów utrzymania wraz ze zmniejszeniem nakładów czasu pracy i wynagrodzenia personelu, podniesienia współczynnika wykorzystania posiadanego sprzętu o 89%, powiększenia stopy zwrotu aktywów o 24% oraz skrócenia nieplanowanych przestojów posiadanego parku maszynowego o 3,5%.

Inteligentna fabryka (Smart Factory)

Tradycyjny model wytwarzania opiera się na łańcuchach technologicznych, których wynikiem jest stosowanie linii produkcyjnych. Poszukiwanie większej elastyczności wytwarzania bezwzględnie musi być związane ze zmianą dotychczasowego podejścia – co nie jest łatwym zadaniem. Według propozycji Instytutu Fraunhofera mogą to być samodzielne centra zadaniowe, grupy obrabiarek, systemy agentowe, holistyczne i inne działające bez sztywnych, niezmiennych planów, a pozwalające na adaptacyjne dostosowywanie się do bieżących wymagań produkcyjnych. W propagowanej obecnie idei cyfrowej fabryki (*digital enterprise*) można określić pięć głównych etapów nazywanych tradycyjnie: rozwój produktu, planowanie produkcji, inżynieria produkcji, realizacja produkcji oraz usługi posprzedażowe (np. serwis gwarancyjny). Jednak w odróżnieniu od dotychczasowego podejścia etapy te są postrzegane holistycznie, tzn. że traktujemy je jako w pełni zintegrowany system, a nie łańcuch procesów następujących w kolejności chronologicznej (gr. *holos* – oznacza całość, według tej koncepcji wszelkie zjawiska tworzą wyłącznie układy całościowe). Wszystkie istotne dane są pozyskiwane, przesyłane i analizowane na każdym etapie oraz we wszystkich interakcjach pomiędzy etapami, dając najpełniejszy obraz podejmowanych działań.

Wprowadzenie koncepcji Smart Factory wiąże się z koniecznością zapewnienia możliwości szybkiej i efektywnej wymiany danych pomiędzy różnego rodzaju modułami, urządzeniami i sterownikami. Mnogość występujących na rynku rozwiązań i propozycji sieciowych systemów komunikacyjnych utrudnia to zadanie. Pojawiają się więc koncepcje ujednolicenia i ustandaryzowania tej problematyki. Ich celem jest maksymalizacja dostępności danych pochodzących ze wszystkich urządzeń, uzyskanie jak największej przepustowości linii transmisyjnych z zachowaniem minimalnych czasów zwłoki w dostępie do danych oraz ułatwienie operatorom korzystania z informacji i efektywne wspieranie ich działań. Jedną z takich koncepcji jest inicjatywa Smart Factory stawiająca sobie za cel opracowanie niezależnego od producenta standardu wymiany danych w fabryce przyszłości, począwszy od interfejsów pomiarowych aż po wydajne protokoły łączące poszczególne fragmenty modułowej fabryki. Podstawowe składniki tej koncepcji to:

- Zapewnienie modułowej (elastycznej) struktury linii produkcyjnych.
- Uniwersalne (*plug-in*) połączenie mediów (powietrza, zasilania, hydrauliki, sterowania), sieci przemysłowych (*industrial ethernet*) i systemów bezpieczeństwa.
- Inteligentne nadzorowanie każdego etapu produkcji i każdego obrabianego przedmiotu za pomocą bezprzewodowych, ustandaryzowanych znaczników RFID.
- Powszechne stosowanie w trakcie obróbki komponentów klasy *plug & produce* – np. modułów pozycjonowania osi, aktywnego przeciwdziałania wibracjom.

- Łatwa obsługa infrastruktury informatycznej będąca wynikiem stosowania dokładnie udokumentowanych modułów i interfejsów.
- Zuniformizowana struktura elementów mechanicznych, elektromechanicznych i informatycznych pozwalająca na tworzenie niezależnych od producentów urządzeń składających się z modułów wyposażanych w indywidualne cechy obróbkowe, ale tworzących wspólnie sterowalną i zarządzaną całość.

W skład konsorcjum wchodzą różni znani producenci układów automatyki – m.in. Festo, Hirschmann, Cisco, IBM, SAP, Bosch Rexroth. Pojawiają się już pierwsze, przykładowe implementacje – na razie na skalę laboratoryjną (rys. 4). Według firmy Bosch Rexroth dobrym kierunkiem działań jest wprowadzanie modułowości do przestrzeni produkcyjnej. Zaproponowano linię montażową składającą się z szeregu stanowisk roboczych (do rozładowywania, załadowywania, dokręcania, składania, kontroli itp.), połączoną informatycznie „w pionie i poziomie" za pomocą otwartych interfejsów pozwalających na monitorowanie wszystkich istotnych informacji w czasie rzeczywistym. Są one bezproblemowo udostępniane nadrzędnym systemom informatycznym, w tym systemom znajdującym się w chmurze.

Rys. 4. Inteligentna fabryka (Smart Factory) według firmy Bosch Rexroth (źródło: www.boschrexroth.com/smartfactory)

OPC UA

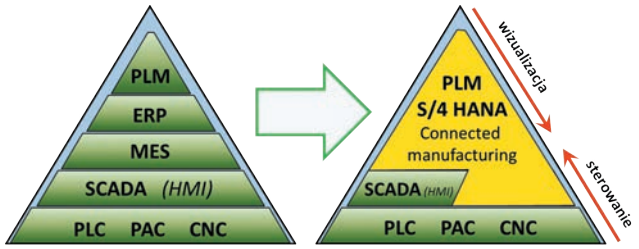
Aby ułatwić komunikację pomiędzy różnymi typami urządzeń automatyki pochodzącymi od rozmaitych producentów, we wrześniu 1996 r. powołano do życia OPC Foundation, która koordynuje działania mające na celu rozwijanie, utrzymywanie i publikowanie nowych specyfikacji OPC (rys. 5). Aktualnie fundacja liczy ponad 450 członków (są to: producenci, użytkownicy, organizacje, instytuty badawcze). Produkty spełniające wymagania są dostarczane przez ponad 4200 wytwórców, a na rynku dostępnych jest ok. 35 000 różnych wyrobów stosowanych we wszystkich gałęziach przemysłu. Pod sformułowaniem OPC należy rozumieć praktycznie otwarty standard przemysłowy komunikacji; najczęściej stosowany jest w informatyce oraz automatyce przemysłowej. Pozwala on na prowadzenie bezpiecznej, szybkiej i efektywnej wymiany danych pomiędzy urządzeniami automatyki (pochodzącymi od różnych dostawców) i komputerami klasy PC, na których mogą być uruchamiane (pod kontrolą różnych systemów operacyjnych) programy do wspomagania zarządzania przedsiębiorstwem.

Dostępne są różnorakie funkcjonalności zwane interfejsami. Są to: Data Acces (OPC DA), Alarms & Events (OPC AE), Batch, Security, Historical Data Acces (OPC HDA). Najbardziej zaawansowana i rozwijana obecnie struktura OPC – UA (*United Architecture*) ma stanowić

Rys. 5. Logo standardu OPC (źródło: http://opcfoundation/org)

bazę wymiany danych w środowiskach Internetu rzeczy, komunikacji pomiędzy maszynami i wymiany danych w cyfrowej fabryce. Serwer OPC to tak naprawdę aplikacja, która powinna być traktowana jako pośrednik pomiędzy skomplikowanym protokołem komunikacji natywnej danego producenta (np. sterownikiem PLC lub sterownikiem PAC) a źródłem danych. Aplikacja może pobierać dane ze źródła i je zapisywać. Źródłem może być urządzenie fizyczne lub inny program uruchomiony na komputerze. Elastyczność, wielowymiarowość i rozpowszechnienie tej koncepcji jest już tak duże, że zaproponowano przekształcenie tradycyjnej piramidy informacyjnej, w jakiej przedstawiany jest zazwyczaj system informatyczny zakładu w nową koncepcję mającą na celu znaczne uproszczenie wymiany danych, a co za tym idzie przyspieszenie ich cyrkulacji i zmniejszenie obciążenia magistral przesyłowych.

Na rys. 6 przedstawiono proponowaną zmianę. Wydzielono dwie podstawowe warstwy zadaniowe: „sterowanie" oraz „wizualizację". Zmniejszenie liczby pośredniczących w wymianie informacji warstw wpłynie także korzystnie na niezawodność komunikacji. Jest to istotne zwłaszcza w aspekcie przewidywanego lawinowego wzrostu transmitowanych danych przy wprowadzaniu koncepcji Industry 4.0 oraz IoT.



Rys. 6. Nowa piramida informacyjna zakładu przemysłowego

Standard OPC UA otrzymał w marcu 2016 r. certyfikację bezpieczeństwa wydaną przez niemieckie Federalne Biuro Bezpieczeństwa Informacji (BSI). Certyfikat dotyczy specyfikacji protokołu i jego fizycznej implementacji. Jest to obecnie jedyny standard komunikacji dla przemysłu oferujący tak zaawansowane i zintegrowane funkcje bezpieczeństwa. Współpraca z organizacją W3 ma na celu opracowanie skutecznych metod integracji w pionie i poziomie struktury informacyjnej zakładu. Warto wspomnieć także o inicjatywie OpenFog Consortium stawiającej sobie za cel utworzenie i rozpowszechnienie standardu architektury definiującej dystrybucję, przetwarzanie, sterowanie i utrzymanie stałej łączności pomiędzy chmurą obliczeniową a układami wykonawczymi i czujnikami jako Internetem rzeczy.

Praktycznie wszyscy producenci elementów i układów automatyki wyposażają je w funkcje i oprogramowanie współpracujące ze standardem OPC UA. Oprogramowanie OPC można także samodzielnie tworzyć w ogólnie dostępnych środowiskach programistycznych, takich jak: C++, C#, .Net, VB. W skład konsorcjum OPC weszli ostatnio bardzo znani producenci, m.in. Microsoft, SAP, Cisco oraz Intel.

Koncepcja *open source*

Coraz powszechniejsze wykorzystywanie narzędzi informatycznych w przemyśle jest również związane z koniecznością ponoszenia różnorakich opłat licencyjnych na rzecz producentów programów, środowisk i systemów. Nie są to kwoty błahe, zwłaszcza w przypadku rozbudowanych przedsiębiorstw. Naturalnym kierunkiem działań jest poszukiwanie możliwości minimalizowania lub wręcz rezygnowania z tych niemałych obciążeń. Jedną z obiecujących i coraz bardziej popularnych metod jest stosowanie oprogramowania dystrybuowanego na zasadzie otwartego kodu (*open source*). Koncepcja ta opiera się na czterech cechach – oprogramowanie *open source* powinno:

- pozwalać na swobodne jego użytkowanie,
- umożliwiać analizowanie kodu,
- zezwalać na poprawianie i modyfikowanie kodu,
- nie nakładać ograniczeń na dystrybuowanie oryginalnego i zmodyfikowanego kodu.

Zainteresowanie producentów systemów automatyki programami opartymi na bezpłatnych licencjach *open source* jest coraz większe. Zwłaszcza że popularna staje się idea Internetu rzeczy polegająca na nieskrępowanym komunikowaniu się przeróżnych urządzeń za pośrednictwem sieci komputerowych. Jednym z poważnych problemów tej koncepcji jest dopuszczenie swobodnej aktualizacji nowych wersji oprogramowania, aby można było adaptować je do zmieniających się wymagań, usuwać dostrzeżone błędy, rozszerzać funkcjonalność komunikacji. W celu ułatwienia wymiany pomysłów w 2005 r. powołano w Niemczech specjalną organizację wytwórców, badaczy oraz użytkowników – The Open Source Automation Development Lab (OSADL). Wśród jej członków znaleźli się wiodący producenci systemów automatyki, m.in.: Sick, Sercos, Phoenix, Moxa i Festo.

Bezpieczeństwo informatyczne

Powszechna cyfryzacja produkcji jest ściśle związana z tworzeniem, gromadzeniem, przetwarzaniem i przesyłaniem bardzo wielu danych. Praktycznie każda informacja jest obecnie istotna i nie powinna być dostępna dla firm oraz osób trzecich, gdyż może stanowić całkiem realne zagrożenie. Dlatego wielu użytkowników zwraca uwagę na problem bezpieczeństwa danych jako często kluczowy w efektywnej implementacji koncepcji Industry 4.0 w warunkach przemysłowych. Należy być świadomym, że współczesne systemy informatyczne wykorzystywane w zakładach mogą być podatne na ataki cyberprzestępców. Potencjalne cele/przyczyny takiego ataku to zazwyczaj:

- Bardzo popularne biurowe systemy operacyjne klasy Windows, w tym również te niewspierane już przez producenta (np. XP, NT, Vista) – często wykorzystywane także przez producentów obrabiarek a instalowane w sterownikach CNC.
- Powszechne niestosowanie w warunkach przemysłowych systemów antywirusowych – zwykle instalacja dodatkowego oprogramowania zabezpieczającego źle wpływa na efektywność pracy sterowników itp.
- Bardzo długi czas pracy (żywotności) środowisk programowych w zakładach przemysłowych (priorytetem jest ciągłość wytwarzania, a nie bezpieczeństwo) – okazjonalne odnawianie programów lub co najwyżej instalacja ważnych poprawek.
- Praktycznie w każdym przypadku instalacja poprawek do oprogramowania wymaga dostępu do publicznego Internetu.
- Zazwyczaj dość wiekowe i nieunowocześniane oprogramowanie komunikacyjne (moduły) w wykorzystywanych w zakładach sterownikach PLC i NC.
- Przypadki przetwarzania poufnych i wrażliwych danych w ogólnie dostępnych chmurach obliczeniowych.

Jak się wydaje, konieczne jest wprowadzenie zaleceń i regulacji zmniejszających wydatnie problemy związane z bezpieczeństwem użytkowania systemów informatycznych – szczególnie w ramach koncepcji Industry 4.0. Jako podstawowy warunek należy przyjąć bezpieczny zdalny dostęp w celu umożliwienia monitorowania i zarządzania z zachowaniem optymalizacji wydajności. Wszelkie dane udostępniane (wysyłane) w sieci muszą być bezwzględnie szyfrowane za pomocą sprawdzonych, wydajnych i odpornych algorytmów. Dotyczy to zwłaszcza wsparcia technicznego sterowników i jest związane z usługami klasy *teleservice* (awaria, analiza błędów, wskazówki techniczne). Powinny być wymagane zarówno skuteczne zarządzanie oprogramowaniem, jak i jego aktualizacja we wszystkich komponentach systemu informatycznego zakładu. Przykładowo: firma Siemens proponuje kompleksowe podejście do zagadnienia zabezpieczeń przed tego rodzaju cyberatakami w postaci środowiska SPSS (Siemens Plant Security Service) składającego się z trzech głównych działań:

- **oceny bezpieczeństwa** (przeprowadzane są audyty w trybie oceny kompetencji pod kątem norm IEC 62443, ISO 27001, SIMATIC PCS 7 & WinCC oraz ocen ryzyka i wrażliwości/podatności na atak),
- **zarządzania zabezpieczeniami** (monitorowanie informatycznego bezpieczeństwa zakładu, zdalna obsługa sytuacji kryzysowych/incydentów, zarządzanie systemami zapór internetowych/*firewall*, prowadzenie polityki antywirusowej, centralne zarządzanie odnawianiem oprogramowania i instalacjami wszelkich poprawek, skuteczne monitorowanie informacji o pojawiających się lub dostrzeżonych błędach systemów operacyjnych i właściwym sposobie postępowania),
- **wdrażania bezpieczeństwa** (prowadzenie szkoleń podnoszących świadomość zagrożeń, konsultowanie online polityki bezpieczeństwa w zakładzie, wspieranie monitorowania sieci, prowadzenie centralnego systemu kopii bezpieczeństwa, instalacja i aktualizacja programów antywirusowych i odpowiednich baz danych, zautomatyzowana instalacja poprawek do systemów Windows).

* * *

Następne targi Hannover Messe odbędą się w dniach 24÷28 kwietnia 2017 r., a krajem partnerskim będzie tym razem Polska.

* * *

Badania realizowane w ramach Projektu „Zaawansowane techniki wytwarzania przekładni lotniczych”, Nr umowy Innolot/I/10/NCBR/2014 – INNOGEAR, współfinansowanego przez Narodowe Centrum Badań i Rozwoju.