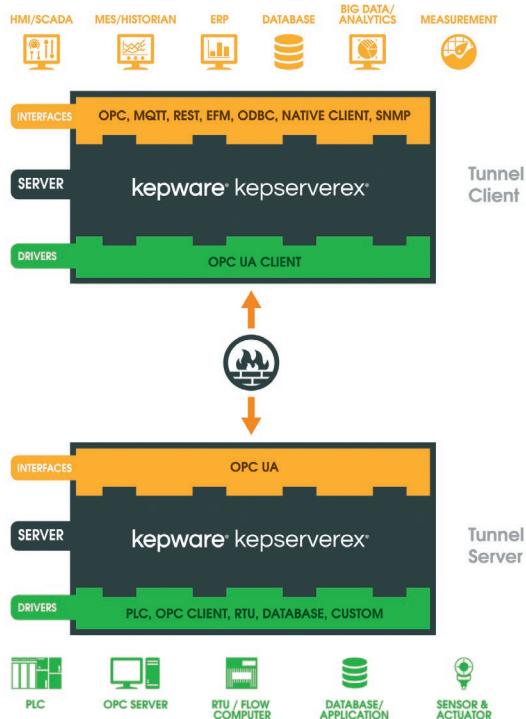


OPC UA – Bezpieczna komunikacja i drzwi do Przemysłu 4.0

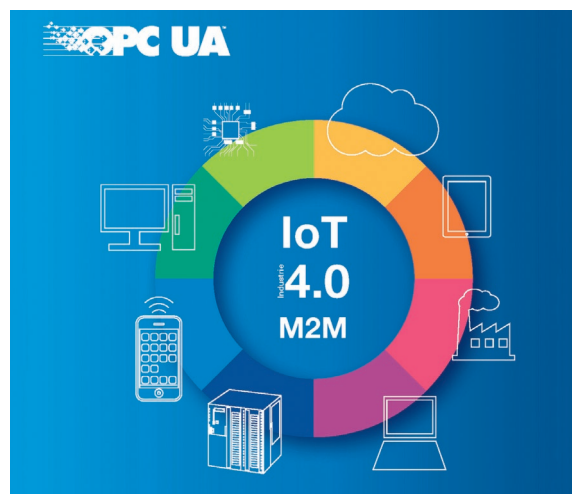
Przemysł 4.0, IoT, M2M, chmura obliczeniowa – te i pokrewne im terminy już na dobre zagościły w opisach produktów przemysłowych oraz wszelkich treściach marketingowych pojawiających się w przemyśle. Jeśli wciąż budzą one u Ciebie obawy i niepokój, ten artykuł jest doskonałą okazją by to zmienić. Przekonaj się co Ty i Twoja firma możecie osiągnąć na wdrożeniu OPC UA.

CZYM JEST OPC UA?

OPC UA (Unified Architecture) to najnowsza wersja standardu komunikacyjnego OPC (OLE for process control), który od samego początku miał służyć i służy do komunikacji aplikacji komputerowych z urządzeniami automatyki przemysłowej. Początkowo, (w architekturze OPC DA) bazowano na technologiach COM/DCOM firmy Microsoft, które z biegiem czasu zostały wyparte przez Web Services oraz SOA (Service Oriented Architecture). Poza tym korzystanie z tych technologii ograniczało komunikację do aplikacji dla systemów Windows. Z tego powodu (i kilku innych) postanowiono stworzyć nowy, bardziej otwarty standard, przy okazji skupiając się na poprawie bezpieczeństwa. Architektura OPC UA została oddana do użytku w 2008 roku, jednak dopiero w ostatnich kilku latach przeżywa prawdziwy rozkwit. Z pewnością, w dużej mierze zawdzięcza to popularyzacji idei Przemysłu 4.0 oraz IoT.



Przykład tunelowego połączenia 2 instancji serwera OPC firmy Kepware poprzez Firewall.



Rys. 1

OPC UA – szansa na jeden standard komunikacji w IoT, M2M i Przemysłu 4.0 (źródło: OPC Foundation)

OPC UA A PRZEMYSŁ 4.0

Niezależność od platformy systemowej oraz duża skalowalność standardu OPC UA sprawia, że jest on chętnie wykorzystywany do tworzenia i wdrażania rozwiązań, określanych mianem Przemysł 4.0 czy też smart factory. Multiplatformowość OPC UA pozwala instalować serwer OPC na komputerach z systemem Linux, czy np. Raspberry Pi. Dostępne są już także sterowniki PLC z wbudowanym serwerem OPC UA, np. SIMATIC S7-1500 czy urządzenia typu IoT Gateway, pobierające dane z czujników i elementów wykonawczych i udostępniające je poprzez OPC. To wszystko sprawia, że OPC UA może być podstawowym sposobem i standardem komunikacji urządzeń w Przemysłowym Internecie Rzeczy (IIoT) i tym samym w przemyśle w ogóle, a duże zaangażowanie największych firm z branży (m.in. Siemens, Beckhoff, B&R, Wago) potwierdza, że nie jest to tylko hipoteza, lecz dziejąca się na naszych oczach rewolucja.

BEZPIECZEŃSTWO I OTWARTOŚĆ

Niewątpliwie kluczem do sukcesu standardu OPC UA (i OPC w ogóle) jest jego otwartość. Podczas gdy przez długie dekady, producenci sprzętu próbując jak najmocniej przywiązać do siebie klientów tworzyli własne standardy komunikacji, OPC pozwalało właścicielom róż-

Rys. 2

nych urządzeń skomunikować je ze sobą. OPC UA poszło jeszcze o krok dalej i umożliwia wygodną komunikację pionową już od warstwy czujników, aż do systemów nadrzędnych (ERP, BI), także tych pracujących w chmurze oraz horyzontalną wymianę danych, np. pomiędzy dwoma sterownikami PLC różnych producentów. Jednak sama otwartość to za mało. Incydenty z wyciekiem danych z takich serwisów jak Google, Microsoft czy Yahoo! oraz inne podobne nie zachęcają do udostępniania danych, zwłaszcza tak newralgicznych, jak dane z bieżącej produkcji. Jednak przypomnijmy sobie atak na elektrownię atomową w Iranie, której infrastruktura produkcji była całkowicie odcięta od Internetu, a do której robak Stuxnet dostał się przeniesiony na pamięci USB. To pokazuje, że nie ma w pełni bezpiecznych instalacji przemysłowych. Zamykanie się na rozwój i nowe możliwości w obawie przed zagrożeniami w dłuższej perspektywie zawsze prowadzi do strat i choć otwartość na zmiany również może do nich doprowadzić, zdecydowana większość firm podejmuje ryzyko, nie chcąc pozostać w tyle za konkurencją. Oczywiście wszyscy chcą, żeby było ono jak najmniej, a OPC UA wydaje się zapewniać akceptowalny poziom bezpieczeństwa dla zakładów produkcyjnych. Najważniejszymi elementami są tutaj certyfikaty X.509 oraz szyfrowanie danych. Każdy produkt OPC otrzymuje certyfikat składający się z klucza prywatnego, klucza publicznego i danych identyfikacyjnych. Najpierw klient i serwer wymieniają się certyfikatami publicznymi. Obie strony muszą zaakceptować nowy certyfikat. Następnie tworzony jest bezpieczny kanał komunikacyjny. Klient podpisuje wiadomość kluczem publicznym serwera, co gwarantuje, że tylko ten serwer może odczytać wiadomość oraz swoim kluczem prywatnym, co pozwala serwerowi na identyfikację klienta. Sytuacja jest analogiczna, gdy serwer wysyła wiadomość do klienta.

JAK ZACZAĆ?

Jeśli jeszcze nie korzystasz z komunikacji OPC UA, najwyższa pora żeby to zmienić. Na początek proponujemy pobranie wersji demo serwera OPC (polecamy KEPServerEx firmy Kepware, grupa PTC) i zainstalowanie na dowolnym komputerze oraz wymianę danych pomiędzy sterownikiem PLC a klientem OPC. Może to być klient testowy lub np. oprogramowanie typu SCADA. W dalszej kolejności może zainteresować Cię wymiana danych z bazami danych czy systemami ERP, np. SAP. Dzięki wieloletniemu doświadczeniu w sprzedaży i wdrażaniu produktów OPC w firmie INEE szybko i sprawnie dobierzemy odpowiednie rozwiązanie do Twoich potrzeb, a jeżeli będzie taka potrzeba pomożemy Ci je wdrożyć. Zapraszamy również na organizowane przez nas regularnie szkolenia z zakresu komunikacji przemysłowej, w których główną rolę odgrywa właśnie komunikacja przez OPC.

Krzysztof Kuźniar

INEE Sp. z o.o.
tel. 32 235 45 69, www.inee.pl



DO MORE WITH YOUR DATA

Dane przemysłowe w czasie rzeczywistym
w chmurze firmowej z wykorzystaniem
platformy komunikacyjnej firmy Kepware



kepware®

Preferowany dystrybutor Kepware w Polsce



www.inee.pl
info@inee.pl
tel. 32 235 45 60



Kepware dostarcza szereg rozwiązań, które pomagają firmom łączyć różnorodne urządzenia automatyki wraz z wykorzystywanym oprogramowaniem pozwalając na integrację z przemysłowym internetem rzeczy (IoT). Firma powstała w 1995 roku i obecnie obejmuje ponad 100 krajów oferując oprogramowanie pomagające tysiącom przedsiębiorstw w ulepszeniu procesów.



KEPWARE.COM