

Budowa i oprogramowanie komputerowych systemów sterowania

Wykład 11

OPC

OPC - Wprowadzenie

- OPC jest przemysłowym standardem komunikacji stworzonym przez producentów sprzętu i oprogramowania.
- Utworzyli oni organizację OPC Foundation, której zadaniem jest rozwijanie tego standardu.
- W chwili jej członkami jest ponad trzysta firm, wśród nich: CAS, Microsoft, GE, Siemens, Rockwell, ABB.
- Standard OPC definiuje sposoby komunikacji między urządzeniami przemysłowymi, przez co pozwala uniezależnić oprogramowanie monitorujące i sterujące od producentów sprzętu.

OPC - zalety

- Do zalet technologii OPC można zaliczyć m.in.:
 - standaryzację komunikacji i wymiany danych przemysłowych,
 - dużą uniwersalność i skalowalność rozwiązań,
 - znaczne obniżenie kosztów integracji dużych systemów przemysłowych.

OPC - Rozwój

- Brak standardu, jakim jest OPC, powodował konieczność stosowania sterowników dedykowanych.
- Każdy twórca oprogramowania musiał stworzyć własne sterowniki do wszystkich urządzeń, z którym dany program miał współpracować.
- Wynikało z tego wiele problemów – wybór oprogramowania dla danego sprzętu był bardzo ograniczony, a jego tworzenie wymagało większych nakładów czasu i pracy.
- Wprowadzenie standardu stało się koniecznością.

OPC - Rozwój

- Dynamiczny rozwój systemów z rodziny Windows umożliwił powstawanie technologii pozwalających na komunikację komponentów programowych za pośrednictwem standardowych interfejsów.
- Pierwszym krokiem była technologia DDE (Dynamic Data Exchange), która pojawiła się na przełomie lat 80. i 90.
- Dzięki niej wymiana danych między aplikacjami stała się łatwiejszą, częściowo uniezależniając oprogramowanie od sprzętu.
- Szybko okazało się jednak, że DDE to za mało.
- Przede wszystkim technologia była mało wydajna, nie oferowała też komunikacji za pośrednictwem sieci.
- W efekcie opracowane zostały różne rozszerzenia dla DDE (np. NetDDE, FastDDE autorstwa Wonderware, czy AdvanceDDE autorstwa Rockwell Software).
- Nie były one jednak standardem, a jedynie kolejnymi rozwiązaniami autorskimi.

OPC - Rozwój

- W 1992 roku wprowadzono technologię OLE 2.0, która miała z czasem zastąpić większość zastosowań DDE.
- W tym samym czasie działalność rozpoczęła grupa WinSEM (Windows in Science, Engineering and Manufacturing), zainteresowana wykorzystaniem OLE w systemach przemysłowych czasu rzeczywistego.
- Mimo przedstawienia paru ciekawych propozycji, nie udało się jej jednak wypracować standardu.
- W 1995r. uformowała się grupa OPC Task Force, w skład której weszły firmy: Fisher-Rosemount, Intellution, Intuitive Technology, Opto22, Rockwell i Siemens AG.
- Po intensywnych pracach, w sierpniu 1996 roku opublikowano pierwszą specyfikację OPC.
- We wrześniu 1996r. powołano do życia OPC Foundation, która od tamtego czasu koordynuje działania mające na celu utrzymywanie i publikowanie nowych specyfikacji OPC.

OPC - Rozwój

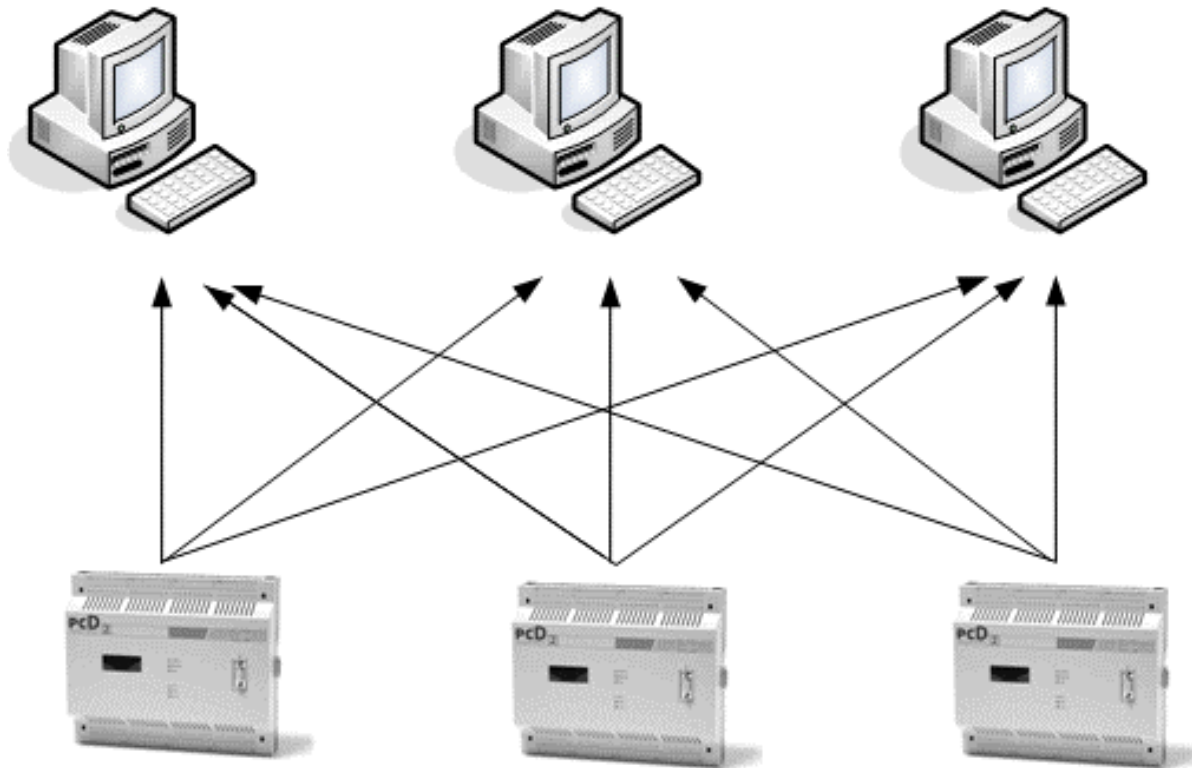
- W styczniu 2004 roku OPC Foundation stworzyła grupę roboczą, której zadaniem było przygotowanie nowej architektury, zapewniającej dalszy rozwój technologii OPC przez przynajmniej 10 kolejnych lat.
- Nowa „wersja” OPC została nazwana „OPC Unified Architecture”.
- Pierwsze części jej specyfikacji zostały opublikowane w czerwcu 2006r.; praca nad dokończeniem specyfikacji trwa nadal.
- Nowa architektura ma bazować na usługach internetowych, łączyć w sobie zalety wszystkich dostępnych aktualnie specyfikacji i odejść od interfejsu opartego o DCOM (przez co stanie się łatwiejsza do implementacji na innych platformach niż MS Windows).

Architektura OPC

- OPC zostało zbudowane w oparciu o architekturę klient-serwer.
- Aplikacja wymagająca dostępu do określonego urządzenia, komunikuje się przez wbudowanego w nią klienta OPC z serwerem OPC, który jest odpowiedzialny za bezpośrednią komunikację z urządzeniem.
- Bez OPC każdy klient musiałby posiadać sterownik odpowiedni do komunikacji z danym urządzeniem.
- Przykładowo, jeśli mamy 3 różne urządzenia i chcemy, aby trzech różnych klientów pobierało z nich dane, musimy dla każdego klienta zaimplementować sterownik właściwy dla protokołu komunikacji z każdym urządzeniem.
- Ponadto, jeśli trzech klientów będzie potrzebowało tych samych danych, każde urządzenie wyśle dane wielokrotnie.

Architektura OPC

- System bez OPC

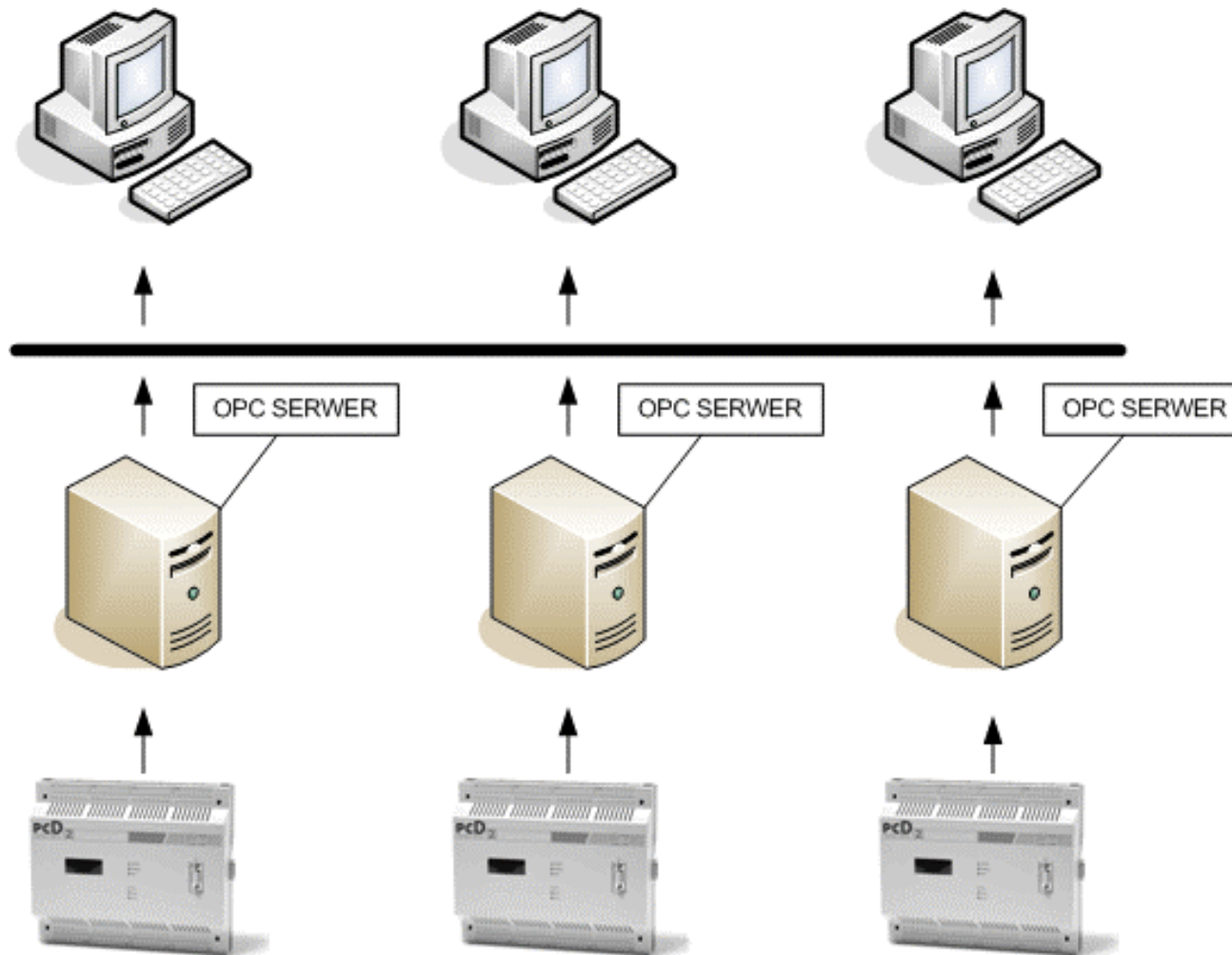


Architektura OPC

- OPC likwiduje ten problem oddzielając warstwę klienta od urządzenia.
- W wymianie danych pośredniczy serwer OPC.
- Nie ma konieczności pisania osobnych sterowników dla każdego klienta, znika też problem wielokrotnego wysyłania danych przez urządzenie, które może korzystać z dowolnego protokołu, np. MODBUS.

Architektura OPC

- System z serwerem OPC



OPC – Podsumowanie cech

- Reasumując, z zastosowania standardu OPC płyną następujące korzyści:
 - Zmniejszenie obciążenia urządzeń
 - Zwiększenie żywotności urządzeń
 - Zwiększenie skalowalności systemów
 - Serwery OPC mogą przechowywać dane w pamięci podręcznej
 - Klienci OPC nie muszą korzystać ze sterowników urządzeń
 - Standaryzacja

OPC - Specyfikacje

- W ramach projektu zajmującego się standaryzacją OPC powstały różne specyfikacje, z których każda definiuje odrębną funkcjonalność.
- Wśród istniejących specyfikacji możemy wyróżnić:
 - OPC Data Access (OPC DA)
 - OPC Historical Data Access (OPC HDA)
 - OPC Alarms & Events (OPC A&E)
 - OPC Security
 - OPC BatchOPC
 - OPC XML DA
 - Unified Architecture (OPC UA)

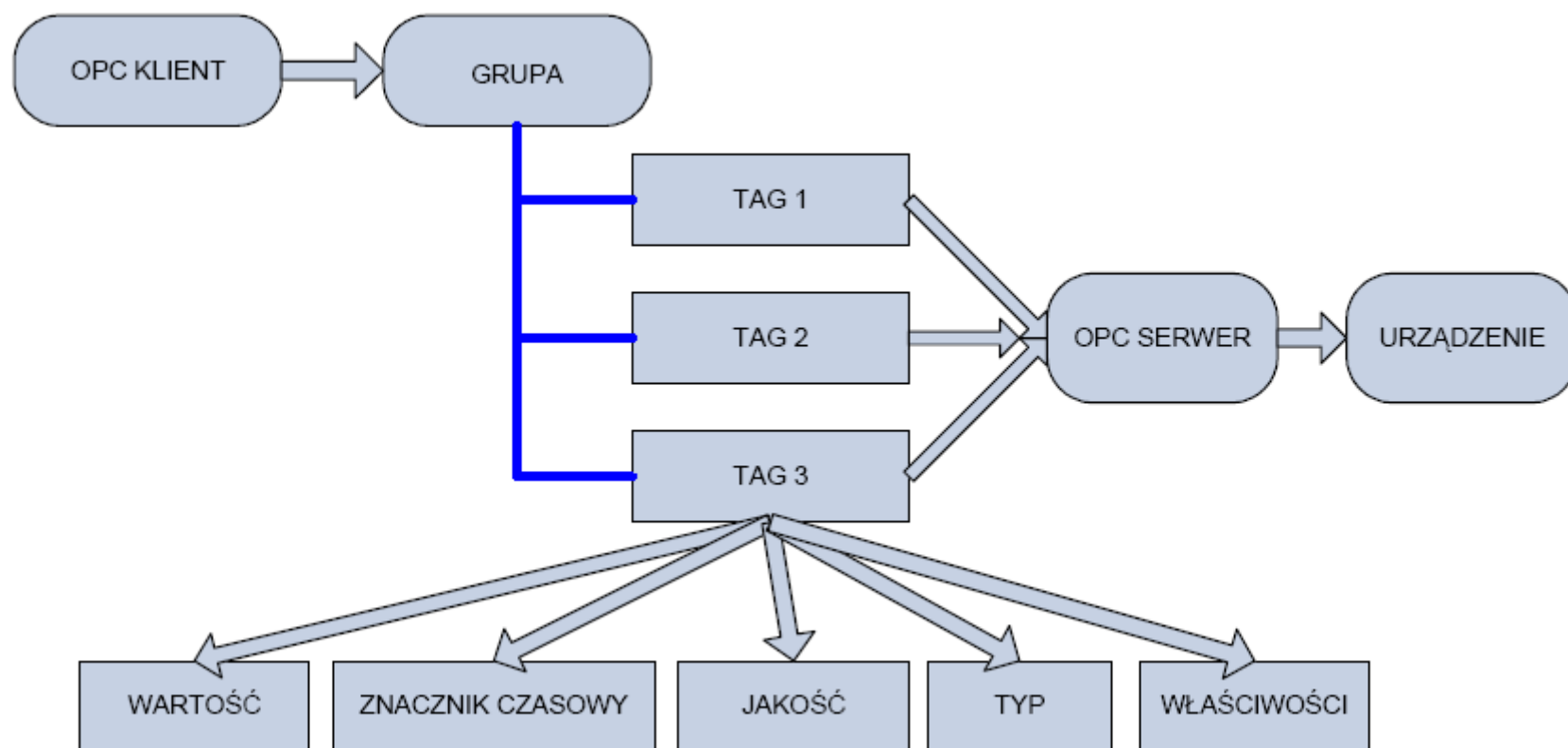
OPC Data Access (OPC DA)

- OPC Data Access umożliwia dostęp do aktualnych danych generowanych w czasie rzeczywistym.
- Przy pomocy OPC DA do serwera OPC kierowane są zapytania o aktualne wartości zmiennych procesowych - temperatur, ciśnień itp.
- Komunikacja z każdym serwerem odbywa się w taki sam sposób, z wykorzystaniem tego samego formatu.
- Klient nie musi wiedzieć, w jaki sposób serwer komunikuje się z urządzeniem.
- Wielu klientów może korzystać jednocześnie z tych samych danych udostępnianych przez serwer.
- OPC DA daje dostęp (możliwość odczytu lub zapisu) do pojedynczych elementów (tagów), z których każdy posiada wartość, znacznik czasowy, typ i jakość.
- Znacznik czasowy może być generowany przez urządzenie lub przez serwer OPC (jeżeli dane urządzenie nie generuje znacznika).
- Przy pomocy OPC DA nie jest możliwe przeglądanie wartości wcześniejszych, a jedynie aktualnych.

OPC Data Access (OPC DA)

- Klient OPC może logicznie podzielić odczytywane dane na grupy, charakteryzujące się np. różnymi czasami skanowania (czasem pomiędzy dwoma kolejnymi odczytami), trybem odczytu, itp.
- Charakterystyczną cechą grupy jest jej odczyt w jednej transakcji.
- W zależności od wersji OPC DA możliwe są dwa tryby odczytu danych:
 - synchroniczny – odczyt występuje zawsze w jednakowych odstępach czasowych,
 - asynchroniczny – odczyt występuje wtedy, gdy pewne dane ulegną zmianie – możliwa jest definicja progów, po przekroczeniu których powinien nastąpić odczyt.

OPC Data Access (OPC DA)



OPC Data Access (OPC DA)

- Dostęp do danych przy pomocy OPC DA może odbywać się na trzy sposoby:
 - z wykorzystaniem COM/DCOM,
 - z wykorzystaniem XML (eXtensible Markup Language) i protokołu SOAP (Simple Object Access Protocol),
 - za pośrednictwem technologii .NET Remoting, posiadającej szersze możliwości niż DCOM (obsługa różnych formatów i protokołów komunikacji, łatwa komunikacja za pośrednictwem Internetu).
- OPC DA występuje w wielu wersjach, z których najnowszą jest wersja 3.0. (każda wersja zapewnia inny zestaw interfejsów, jednak powinna być zachowana kompatybilność wsteczna).

OPC Historical Data Access (OPC HDA)

- OPC HDA umożliwia przeglądanie i analizę zgromadzonych danych historycznych, np. w celu oceny wydajności systemu, bądź przewidywania błędów.
- Klient uzyskuje dostęp do zarchiwizowanych danych (odczytów jakiegoś urządzenia itp.) poprzez zgłaszanie zapytań do serwera OPC HDA.
- Specyfikacja OPC HDA zakłada dwa typy serwerów:
 - Prosty serwer trendów - zapewniający implementację interfejsów koniecznych do dostępu do surowych (nieprzetworzonych) danych pomiarowych.
 - Zaawansowany serwer analiz – zapewniający operacje analizy danych (takich jak liczenie średnich, wartości minimalne, maksymalne), odtwarzanie danych, adnotacje, historię odczytów i zmian danych.

OPC Historical Data Access (OPC HDA)

- Specyfikacja zapewnia dostęp do następujących operacji:
 - Odczyt – Klient odczytuje dane i informacje z serwera.
 - Zapis/Aktualizacja – Klient zapisuje dane lub informacje do serwera.
 - Adnotacje – Klient odczytuje lub zapisuje adnotacje do danych w serwerze.
 - Odtwarzanie (Playback) – Klient otrzymuje odtwarzane dane historyczne.

OPC Alarms & Events (OPC A&E)

- OPC A&E służy do informowania o występujących w systemie zdarzeniach i zgłaszanych alarmach.
- Przez alarm rozumiany jest nienormalny stan jakiegoś obiektu, wymagający szczególnej uwagi.
- Zdarzenie może być związane ze stanem, jak np. zdarzenie przejścia danej wartości do poziomu alarmowego lub niezwiązane ze stanem, jak zmiany konfiguracji, czy błędy systemowe.
- Serwery OPC A&E mogą pobierać dane bezpośrednio z urządzenia lub z serwera OPC DA.
- Serwer OPC A&E może być samodzielnym modułem lub też wchodzić w skład serwera OPC DA.

OPC Alarms & Events (OPC A&E)

- Specyfikacja definiuje zdarzenie, którego wystąpienie jest rejestrowane (do zdarzeń mogą np. należeć: awaria urządzenia, przekroczenie wartości granicznej dla pewnej zmiennej procesowej, akcja operatora).
- Różne zdarzenia mogą być przypisywane to pewnej zmiennej, mogą być definiowane różne wartości progowe.
- Specyfikacja zapewnia możliwość tworzenia warunków i podwarunków wystąpienia zdarzenia.

OPC Alarms & Events (OPC A&E)

- Serwer OPC A&E powinien zapewniać następujące typy zdarzeń:
 - Zdarzenia zorientowane warunkowo (condition-related events) – klient jest informowany o wystąpieniu zdarzenia. Warunki mogą być aktywowane i dezaktywowane. Serwer implementuje również mechanizm potwierdzania zdarzeń.
 - Zdarzenia śledzone (tracking-related events) – są wykorzystywane w celu zapewnienia informacji o wystąpieniach danego zdarzenia (np. interwencji operatora).
 - Zdarzenia proste (simple events) – używane w celu powiadomienia klienta o wystąpieniu zdarzenia (np. awarii urządzenia).

OPC Security

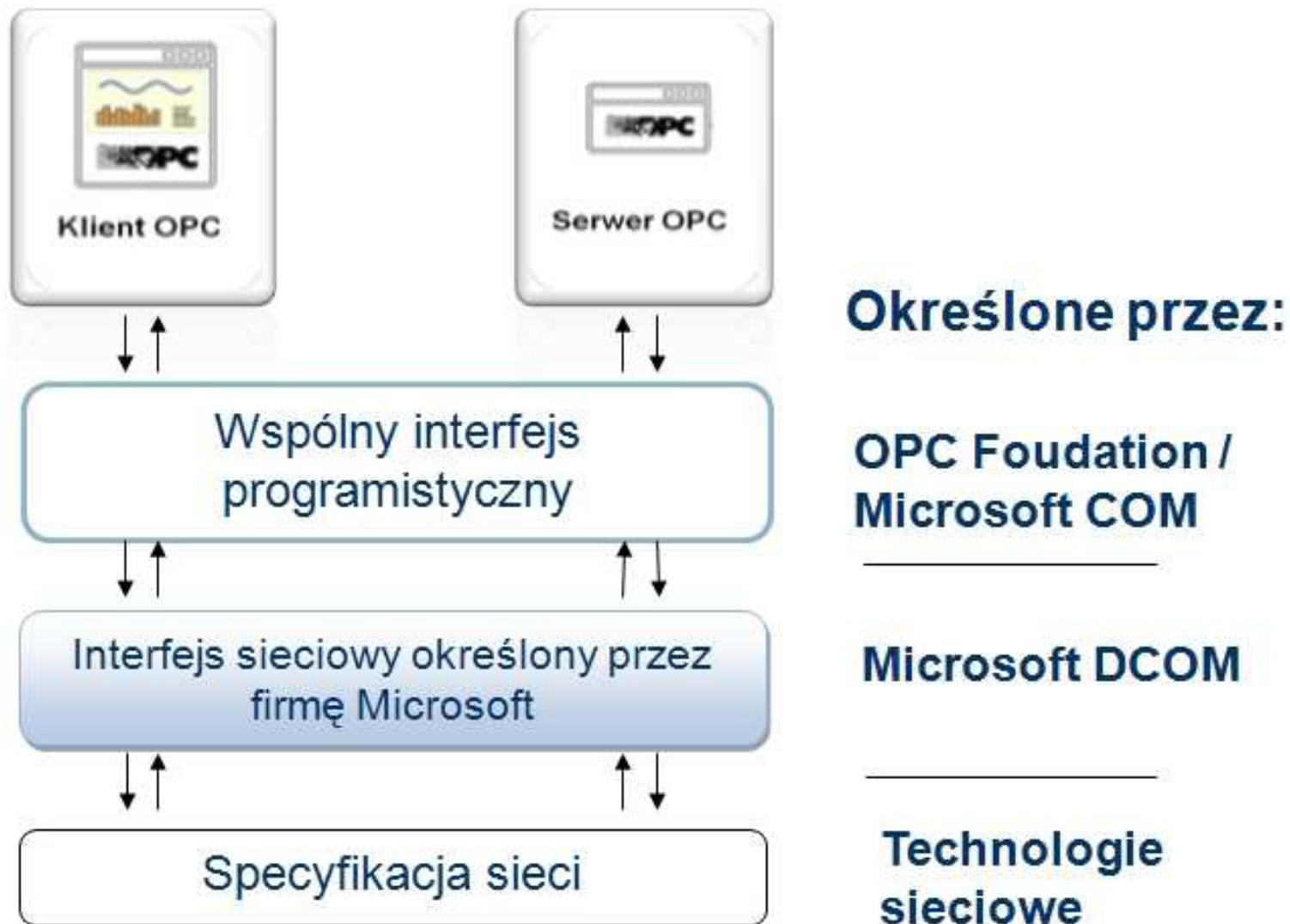
- Specyfikacja OPC Security ma służyć zapewnieniu bezpieczeństwa dostępu do danych oferowanych przez serwery OPC.
- Umożliwia poprawną weryfikację klienta, który chce uzyskać dostęp i weryfikację poprawności transmisji (czy dane nie zostały zmienione).
- Specyfikacja określa trzy poziomy bezpieczeństwa:
 - Disabled security – Zabezpieczenia są wyłączone, każdy posiada prawo dostępu.
 - DCOM Security – Ustawienie domyślne. Działają jedynie zabezpieczenia DCOM, określające, kto ma prawo dostępu i do jakich aplikacji. Nie ma kontroli nad dostępem do poszczególnych obiektów na serwerze.
 - OPC Security – Serwer OPC kontroluje dostęp do poszczególnych obiektów.

OPC XML DA

- Poprzednie wersje specyfikacji OPC bazowały na modelu COM/DCOM, co praktycznie uniemożliwiało komunikację pomiędzy różnymi platformami.
- OPC Foundation zdecydowała, że XML może zostać użyty do definiowania wiadomości przesyłanych pomiędzy klientem a serwerem.
- W rezultacie OPC Foundation rozpoczęła pracę nad nową wersją specyfikacji OPC DA nazwaną OPC XML DA.
- XML stał się językiem szeroko stosowanym w Internecie i właśnie o ten standard został oparty protokół komunikacyjny SOAP, który bardzo szybko upowszechnił się wśród producentów oprogramowania.
- Nowa strategia rozwoju OPC została oparta właśnie o język XML i protokół SOAP.

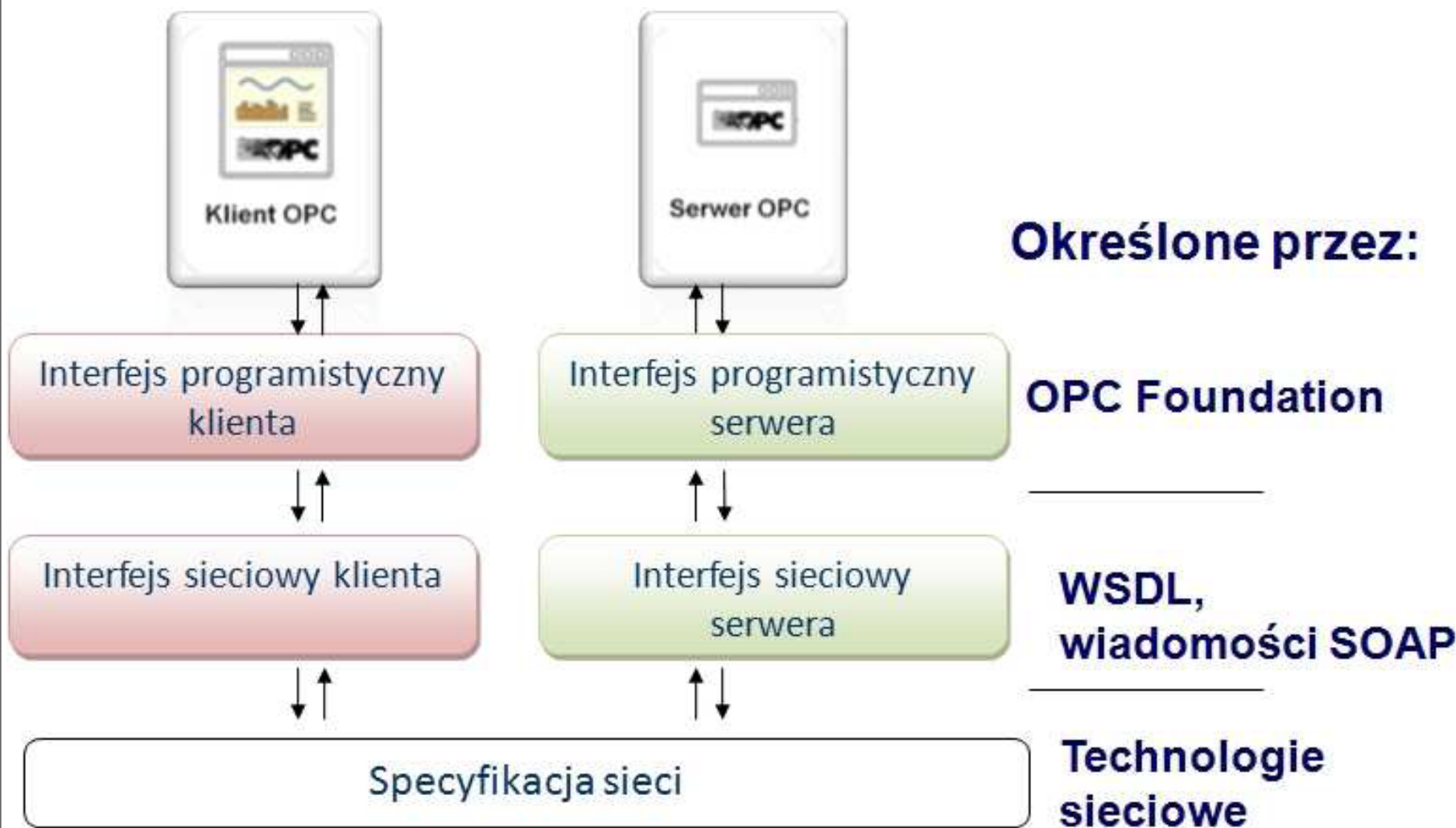
OPC Architektura COM/DCOM

- Architektura z wykorzystaniem COM/DCOM



OPC Unified Architecture (OPC UA)

Architektura OPC UA



OPC Unified Architecture (OPC UA)

- OPC Unified Architecture jest nowym niezależnym od platformy systemowej standardem, który pozwala na komunikację pomiędzy różnymi typami systemów i urządzeń poprzez wysyłanie wiadomości pomiędzy klientem a serwerem.
- Dzięki zastosowaniu ogólnie przyjętych standardów sieciowych serwer OPC i klienci OPC mogą działać na różnych platformach.
- Standard OPC Unified Architecture, bazuje na ogólnie przyjętych protokołach komunikacyjnych, takich jak TCP/IP, HTTP, SOAP, co zapewnia bardzo dużą skalowalność rozwiązań implementowanych w oparciu o tę technologię.
- OPC Unified Architecture umożliwia przesyłanie danych za pośrednictwem różnych formatów m.in. formatu opartego o XML i formatu binarnego.

OPC Unified Architecture (OPC UA)

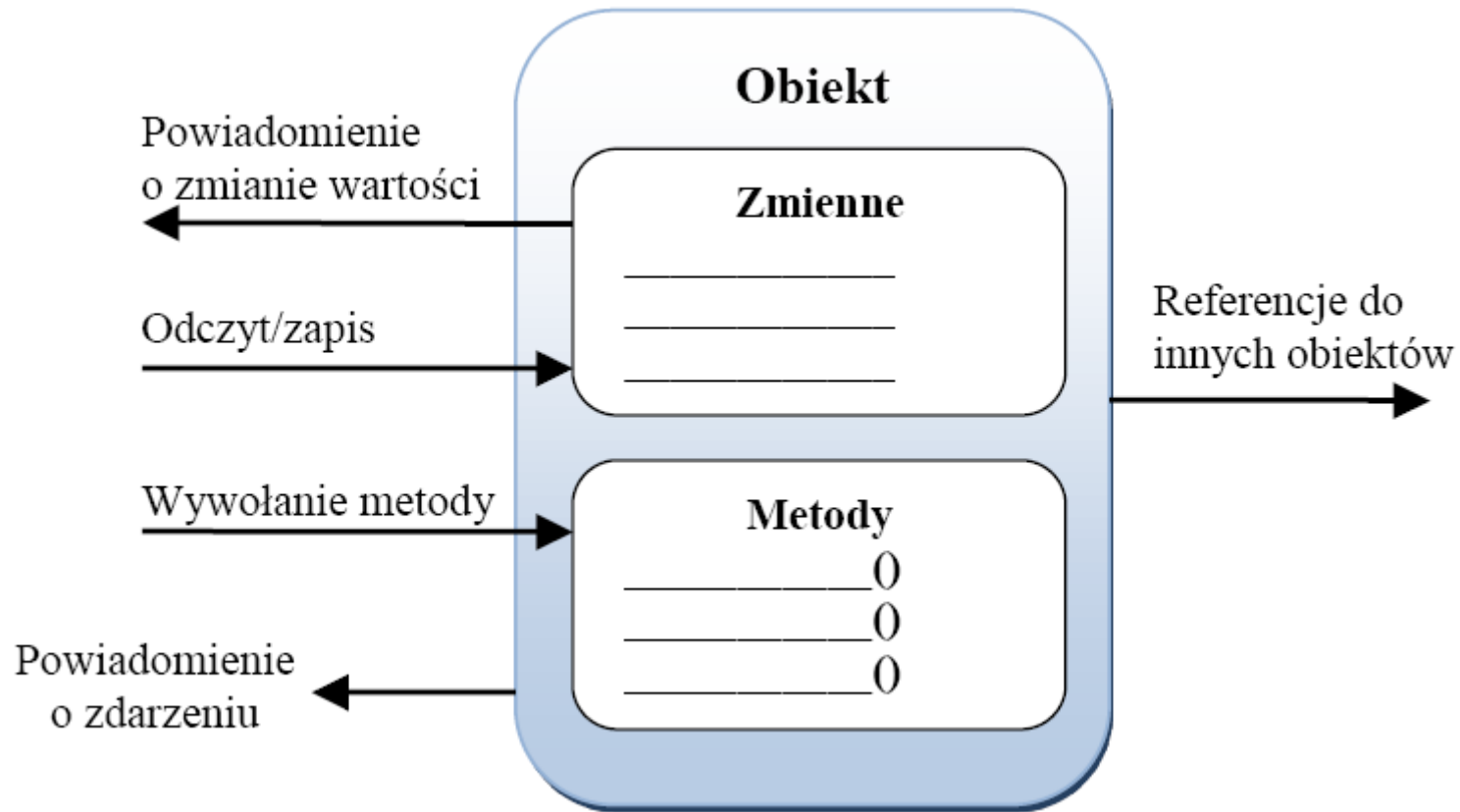
- OPC Unified Architecture jest nowym niezależnym od platformy systemowej standardem, który pozwala na komunikację pomiędzy różnymi typami systemów i urządzeń poprzez wysyłanie wiadomości pomiędzy klientem a serwerem.
- Dzięki zastosowaniu ogólnie przyjętych standardów sieciowych serwer OPC i klienci OPC mogą działać na różnych platformach.
- Standard OPC Unified Architecture, bazuje na ogólnie przyjętych protokołach komunikacyjnych, takich jak TCP/IP, HTTP, SOAP, co zapewnia bardzo dużą skalowalność rozwiązań implementowanych w oparciu o tę technologię.

OPC Unified Architecture (OPC UA)

- OPC Unified Architecture umożliwia przesyłanie danych za pośrednictwem różnych formatów m.in. formatu opartego o XML i formatu binarnego.
- Serwer OPC zbudowany w oparciu o Unified Architecture definiuje swoim klientom zestaw usług, jakie oferuje oraz format danych procesowych za pośrednictwem, którego ma odbywać się komunikacja.

OPC Unified Architecture (OPC UA)

- Model obiektowy OPC UA definiuje obiekty jako zmienne i metody, jak również pozwala na utworzenie relacji pomiędzy obiektami OPC.

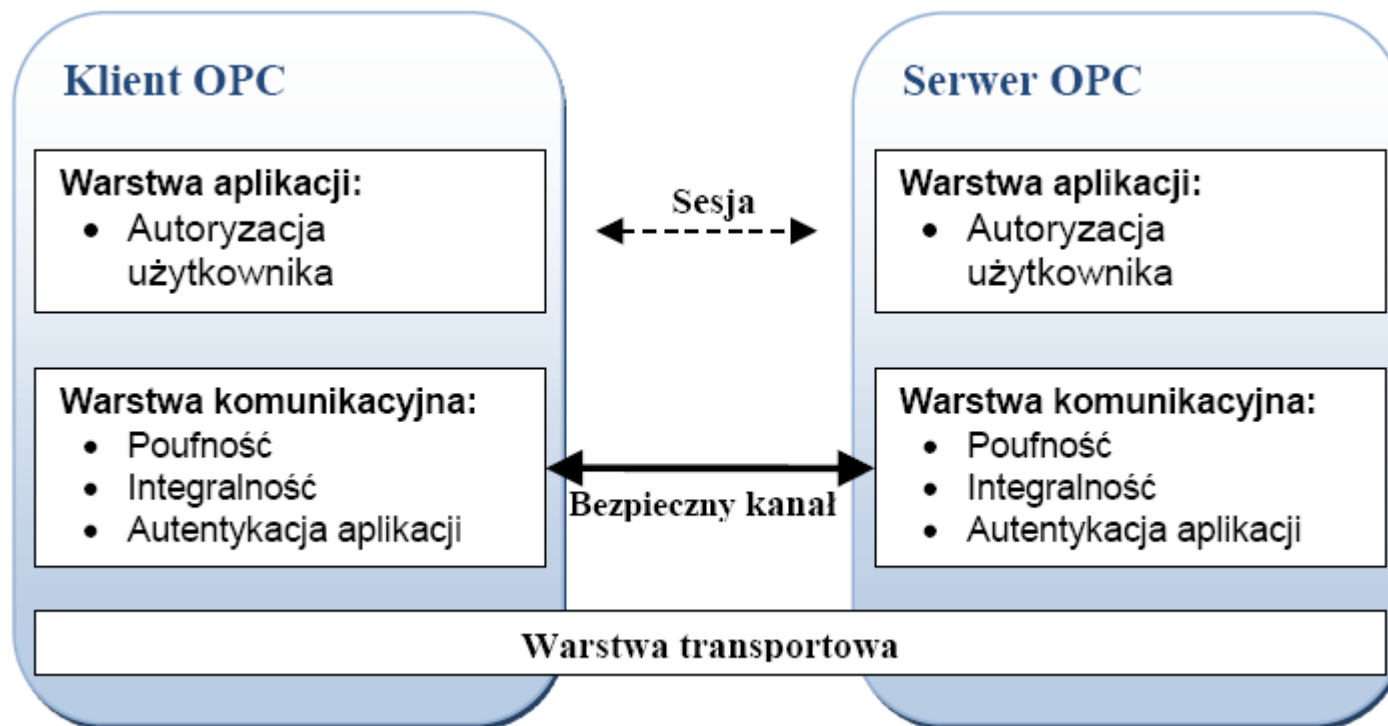


OPC UA - Bezpieczeństwo

- Podczas tworzenia specyfikacji OPC UA położono szczególny nacisk na bezpieczeństwo.
- Specyfikacja nowej technologii opracowanej przez OPC Foundation jest zgodna ze specyfikacjami: WS-Security, WS-Trust, WS-Policy, WS-Secure Conversation.
- Architektura bezpieczeństwa OPC UA dostarcza rozwiązań pozwalających na implementację rozwiązań zgodnych z następującymi wymaganiami bezpieczeństwa:
 - Przesyłane dane są widoczne tylko dla autoryzowanych użytkowników.
 - Dane procesowe mogą zostać zmienione tylko przez autoryzowanych użytkowników.
 - Poufność.
 - Śledzenie ruchu.
 - Odporność na ataki typu DoS (ang. denial of service).

OPC UA - Bezpieczeństwo

- Mechanizmy bezpieczeństwa OPC UA umieszczone są w warstwie aplikacji i w warstwie komunikacyjnej, na szczycie warstwy transportowej



OPC UA - Bezpieczeństwo

- Zarządzanie sesją użytkownika odbywa się w warstwie aplikacji.
- W warstwie tej działają mechanizmy bezpieczeństwa odpowiedzialne za uwierzytelnianie i autoryzację użytkowników.
- Sesja w warstwie aplikacji jest realizowana poprzez bezpieczny kanał transportowy, który działa w warstwie komunikacji i zapewnia bezpieczną komunikację pomiędzy klientem a serwerem.
- Wszystkie dane dotyczące sesji są przekazywane do warstwy komunikacyjnej, gdzie są przetwarzane.
- Warstwa komunikacji dostarcza mechanizmy bezpieczeństwa, które zapewniają poufność, integralność realizowaną poprzez podpisy i autentykację aplikacji dzięki certyfikatom.
- Dane zabezpieczone w warstwie aplikacji są następnie przesyłane poprzez warstwę transportową, która jest odpowiedzialna za transmisję danych pomiędzy klientem a serwerem.