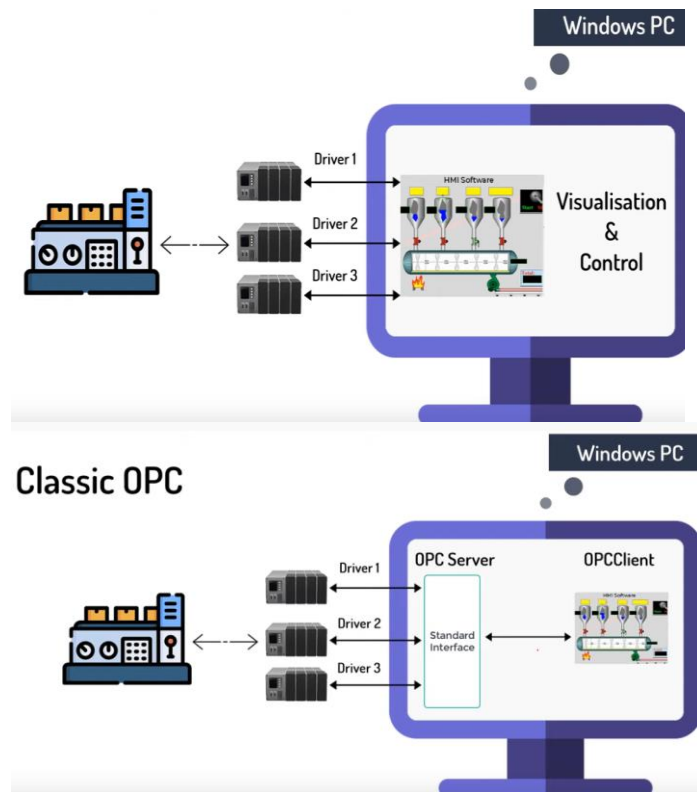


## Die Geschichte von OPC UA

Der erste Schritt hin zu OPC UA wurde in den 90er Jahren getan. Jeder Hersteller musste für seine Steuerungen einen eigenen Treiber zur Verfügung stellen, um z. B. die Daten mit einer SCADA-Software auszutauschen. Unterschiedliche Hersteller von Steuerungen taten sich also zusammen und vereinbarten ein **Standard-Interface**. Sowohl die Steuerungen als auch die SCADA-Software kommunizierten nun über eine standardisierte Schnittstelle.

**OPC Classic** war geboren. Die Steuerungen kommunizieren im oben stehenden Beispiel über das Standard Interface, das als Server agiert, mit der SCADA Software, die einen sogenannten OPC-Client darstellt. Nun war es also leichter möglich Daten auszutauschen und diese auch an höhere Ebenen der „Automatisierungspyramide“ weiterzugeben.



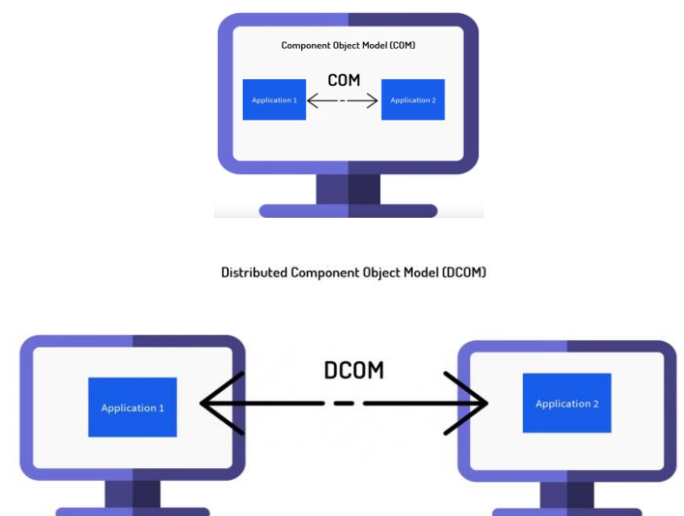
## COM/DCOM von Microsoft

### Client-Server-Kommunikation

Basis für die Kommunikation zwischen den OPC-Client und Server bilden diese beiden Modelle oder Frameworks.

Das COM (Component Objekt Modell) stellt über DLLs Funktionen für Kommunikation von Programmen zur Verfügung. Z. B. kann damit Programm1 mit Programm 2 auf demselben PC kommunizieren.

DCOM (Distributed COM) ermöglicht es COM-Objekten miteinander über ein Netzwerk zu kommunizieren. DCOM ist also die Basis für die OPC UA-Client –Server-Kommunikation



## Classic OPC Daten

Neben den einfachen Maschinen- oder Daten, die eine Steuerung zeitnah liefert (OPC DA → Data Access) können z. B. längere Zeitverläufe (OPC HA → Historical Access) und auch Alarmer und Events zwischen den OPC Server und OPC Client ausgetauscht werden.

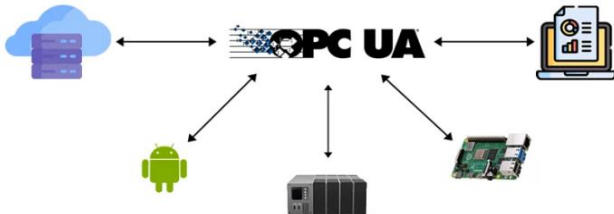


## Weiterhin bestehende Probleme bei Classic OPC bis ins Jahr 2008:

Die Kommunikationssoftware ist abhängig von einem Microsoft-Betriebssystem und eine Kommunikation über das Internet ist nur bedingt möglich.

## Die vier wichtigsten „Kern-Kompetenzen“ von OPC UA (ab 2008)

### 1. Cross Platform & Internet Ready



#### Beschreibung:

.....

.....

.....

.....

.....

### 2. Complex Information Model

OPC UA



Units

Pressure Setpoints

Type of Pressure Sensor

Instrument Config Parameters

Hierarchical Position

Related Components

#### Beschreibung:

.....

.....

.....

.....

**Hinweis:** OPC UA unterstützt auch weiterhin die klassischen einfachen Datenformate OPC DA/HA/A&E.

### 3. Service Oriented Architecture



Maschinen kommunizierten bisher mit schwer verständlichen Bits und Bytes. Bei der Service Orientierten Architektur (SOA) jedoch werden standardisierte, einfach verständliche Module oder Methoden (z.B. „FindServer()“, ...) verwendet. Wer also Anfragen (requests → „FindServer()“) erhält, bearbeitet dies und schickt die Ergebnisse mit der Antwort (response) zurück.

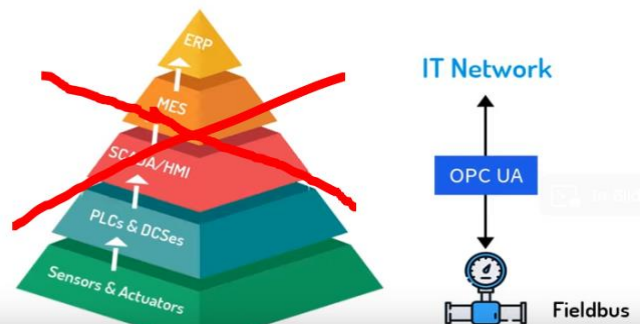
#### Vorteile von SOA:

.....

.....

.....

### 4. Simplified IT Integration



OPC UA ermöglicht eine Kommunikation, ohne alle Ebenen der Automatisierungspyramide durchlaufen zu müssen. Ein OPC UA-fähiger Sensor mit Netzanschluss kann ohne Steuerung Daten an eine beliebige Ebene oder auch über das Internet an Externe weitergeben. Weitere Beispiele: Automatische Benachrichtigung der Wartungsfirma bei 20000 Betriebsstunden einer Maschine.

#### Vor- und Nachteile:

.....

.....

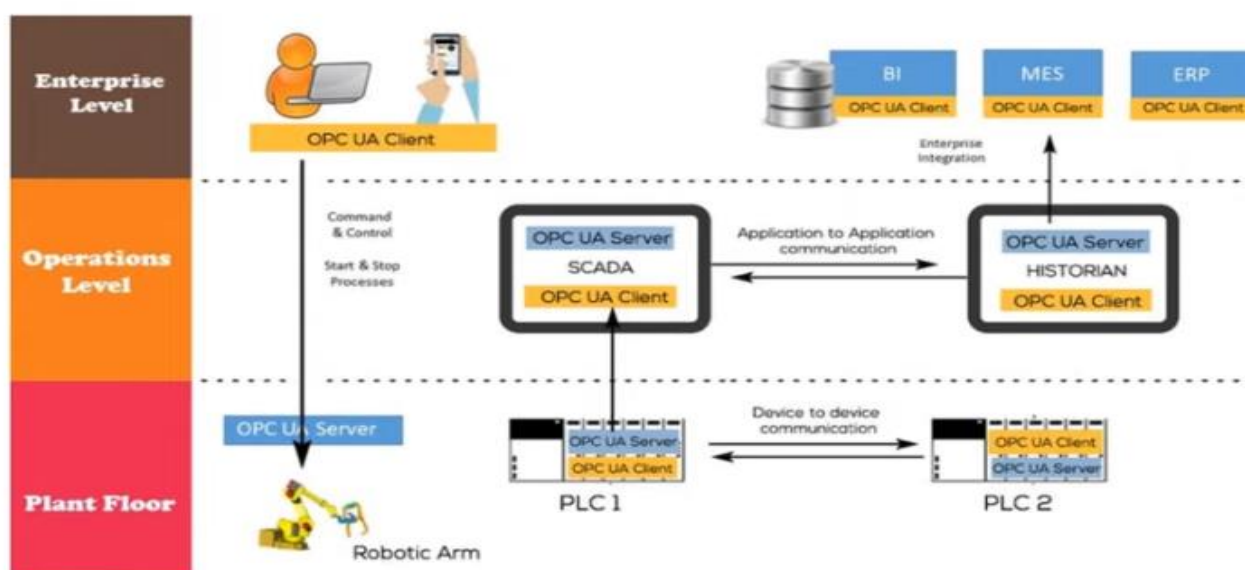
.....

### Weitere Information zu „1. Cross Platform & Internet Ready“:

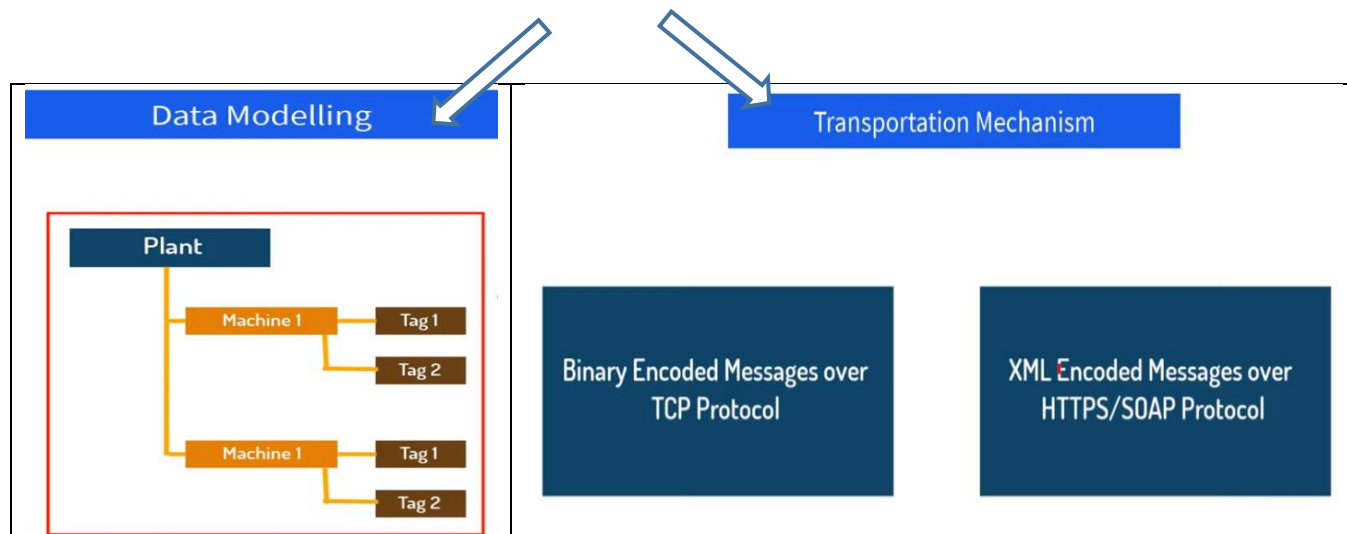
OPC UA verwendet ein TCP-basiertes, optimiertes, binäres Protokoll für den Datenaustausch über den bei der IANA (Internet Assigned Numbers Authority) eingetragenen Port 4840. Webservice und HTTP werden optional zusätzlich unterstützt. Es ist ausreichend einen einzigen Port in der Firewall frei zu schalten. Integrierte Verschlüsselungsmethoden sorgen für sichere Kommunikation über das Internet.

## Zu 4. Simplified IT Integration → Vertikale Kommunikation bei OPC UA

Da OPC UA nicht mehr alle Ebenen der klassischen Automatisierung durchlaufen muss, hat sich bei der vertikalen Kommunikation eine Einteilung in drei Ebenen etabliert. Die unterste Ebene der **Shopfloor (OT)**, gelegentlich „Plantfloor“ zu Deutsch „Werkhalle“ genannt, beinhaltet neben den Sensoren und Steuerungen nun auch OPC UA-Server oder Clients. Diese kommunizieren nun mit anderen OPC UA-Servern und Clients auf der mittleren Ebene (**IT oder nun Operations Level**). Hier werden die komplexen Prozesse überwacht und angepasst. Diese Ebene kann man als die Zusammenfassung der Prozess- und Betriebsleitebene der klassischen Automatisierungspyramide ansehen. Auf der obersten Ebene (**Enterprise Level, Unternehmensebene oder auch Cloud-Ebene**) werden die Daten über OPC UA-Clients gesammelt, aufwendig analysiert und strategische und unternehmerische Entscheidungen getroffen. Hier findet sich auch die Unternehmensleitebene (Enterprise Level) wieder.



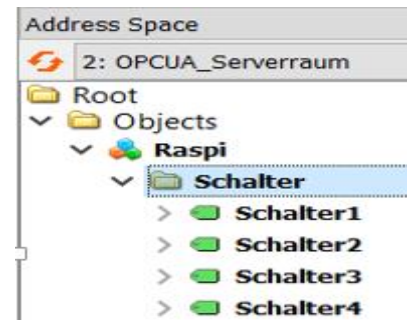
## Die zwei Säulen von OPC UA



Die Möglichkeit, ein komplexes und strukturiertes OPC UA-Datenmodell selbst zu erstellen und Transportmechanismen zu haben, die über „normales TCP“ hinausgehen, sind die beiden wichtigsten Eigenschaften (Säulen) von OPC UA. Dies unterscheidet OPC UA wesentlich von anderen Kommunikationsprotokollen.

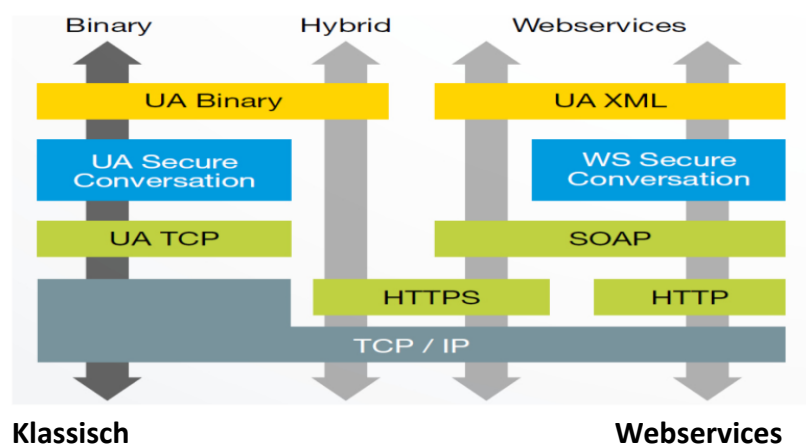
## →Hinweise zu „Data Modelling“

An anderer Stelle wird immer noch intensiver auf die erste Säule „Datenmodell in OPC UA“ eingegangen. Sie werden das Werkstattorprogramm OPC UA fähig erleben und auf die vier Schließer über das Netzwerk (TCP/IP) zugreifen und die Daten verarbeiten.



## →Hinweise zu „Transport Mechanism“

Neben den klassischen transportorientierten Mechanismen (UA TCP) ist OPC UA auch für Webservices konzipiert. Durch den Austausch von XML-Dokumenten können unterschiedlichste „Information Items“, die bei Webservices Anwendung finden, übertragen werden.



Auch Sie werden über OPC UA Daten in Webservices, z. B. in eine cloudbasierte NoSQL-Datenbank ablegen und erfragen.

## Security bei OPC UA

OPC-UA Technologie verwendet bewährte Sicherheitskonzepte, die Schutz vor unerlaubtem Zugriff bieten genauso wie Schutz vor Sabotage und Modifikation von Prozessdaten sowie Schutz vor unachtsamer Bedienung. Die OPC UA Sicherheitskonzepte beinhalten Anwenderauthentifizierung, die Signierung von Nachrichten und die Verschlüsselung der übertragenen Daten selbst. Die eingesetzten Zertifikate dienen der Identifikation von Benutzern, Computern und Geräten. OPC UA-Sicherheit basiert also auf anerkannten Standards, die auch für sichere Kommunikation im Internet verwendet werden, wie beispielsweise SSL, TLS und AES. Die Sicherheitsmechanismen sind Teil des Standards und verpflichtend für die Hersteller. Der Anwender darf die verschiedenen Sicherheitsfunktionen entsprechend seines Use-Cases frei kombinieren, somit entsteht skalierbare Sicherheit in Abhängigkeit der spezifischen Anwendung.

### Quellen:

[www.youtube.com/watch?v=vRk42W\\_4R0o](https://www.youtube.com/watch?v=vRk42W_4R0o)