PLC e SCADA, Sect.4

Alessandra Flammini
alessandra.flammini@unibs.it
Ufficio 24 Dip. Ingegneria dell'Informazione
030-3715627 Lunedì 16:30-18:30

SCADA e OPC

SCADA: dove si colloca

Modello di riferimento Purdue (ISA95)

- Livello 4 (MANAGEMENT/AREA) **Business Logistic Systems**
  - Sistemi ERP di gestione degli ordini e della produzione (big data, giorno)

- Livello 3 (AREA/CELLA) **Manufactoring Operating Systems**
  - Sistemi MES ERP di gestione operativa del flusso di produzione e dei macchinari (big data, minuto/secondo)

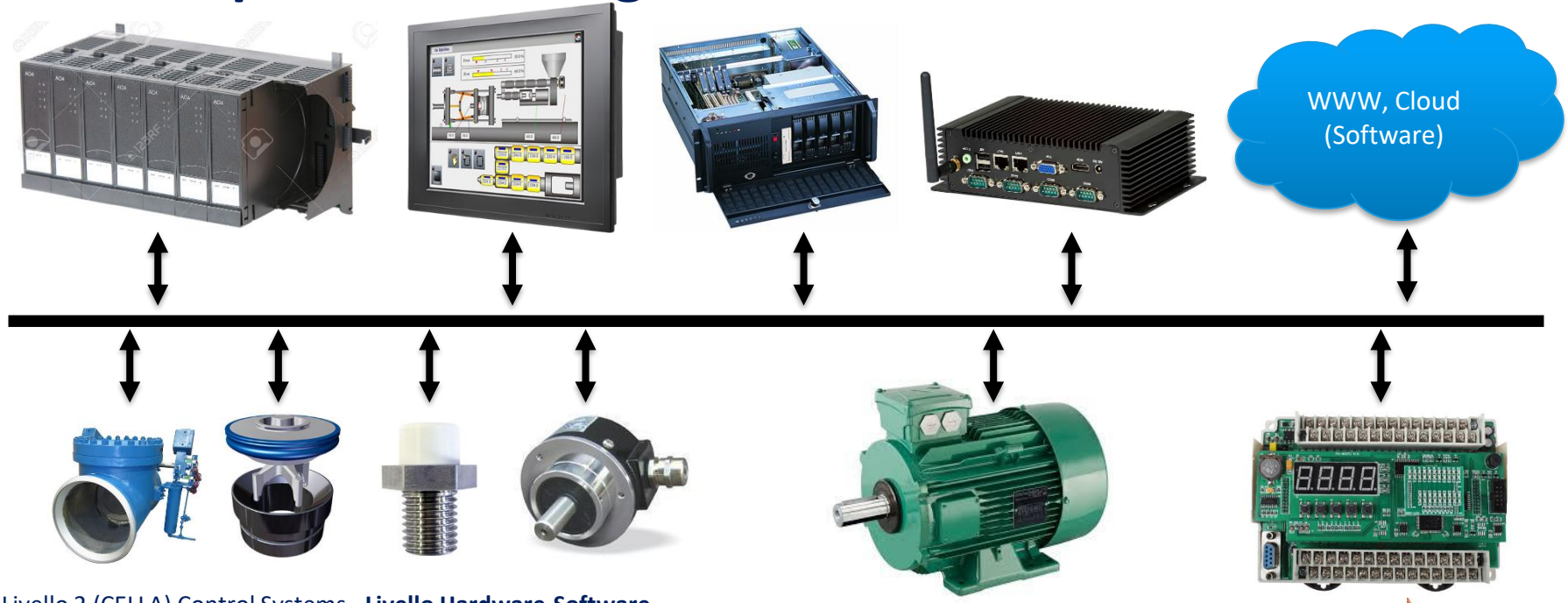
- Livello 2 (CELLA) **Control Systems**
  - Sistemi PLC (automazione di fabbrica), DCS (controllo di processo), SCADA per supervisione, monitoraggio, controllo statistico, interfaccia operatore (ms)

- Livello 1 (CELLA/CAMPO) **Intelligent Devices**
  - Sensori, attuatori, periferia (0,1ms)

- Livello 0 (CAMPO) **Physical Process**
  - Macchinari (motori, trasformatori, generatori, sistemi idraulici, veicoli,…(10ms)

SCADA: dove si colloca

Tutti i dispositivi, intelligenti e connessi, allo stesso livello



- Livello 2 (CELLA) Control Systems **- Livello Hardware-Software**
  - Sistemi PLC (automazione di fabbrica), DCS (controllo di processo),
    SCADA per supervisione, monitoraggio, controllo statistico, interfaccia operatore (ms)

- Livello 1 (CELLA/CAMPO) Intelligent Devices **- Livello Hardware**
  - Sensori, attuatori, periferia (0,1ms)

- Livello 0 (CAMPO) Physical Process **- Livello Meccanica-Hardware**
  - Macchinari (motori, trasformatori, generatori, sistemi idraulici, veicoli,…(10ms)

PLC e SOFT-PLC

Il controllore riceve le informazioni dai sensori e, secondo metodi noti a priori, agisce sugli attuatori «in tempo reale». Riferisce ad una cella di produzione

- Controllore (regolatore) di grandezza (temperatura, posizione e/o velocità di un motore)
  - Sensori e attuatori a informazione continua
  - Dato un riferimento, si misura e si valuta l'errore e si agisce azzerando l'errore e tenendo conto dei ritardi del sistema
  - Campionamento e regolazione a intervallo costante di tempo
  - Campionamento e regolazione solo se la grandezza è variata (approccio semi-discreto e a risparmio di tempo)

- Sequenza temporizzata di operazioni
  - Sensori e attuatori a informazione binaria
  - La regolazione mediante il tempo
    - Riempi fino a quando non è pieno continuando a misurare (regolatore classico)
    - Riempi per un certo tempo (impreciso, senza retroazione)
    - Riempi fino a metà, conta il tempo per arrivare a ¾ e riempi ancora per quel tempo (sensori discreti)

PLC e SOFT-PLC

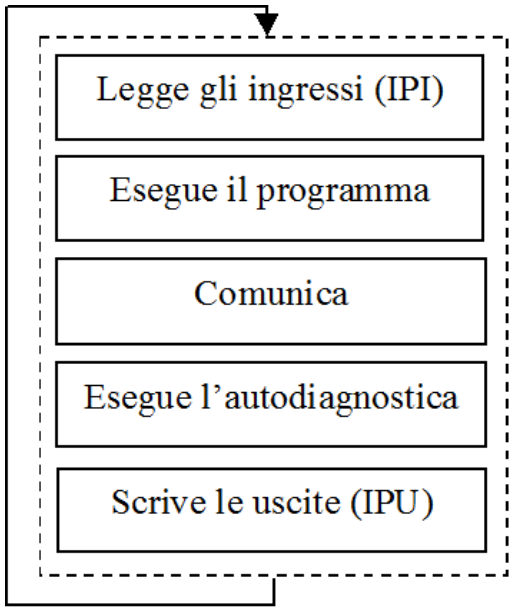
PLC = sistema logico programmabile in grado di realizzare un insieme ordinato di operazioni, definite da comandi facilmente modificabili, strutturate in modo ciclico

- Nasce negli anni 70 in sostituzione alle logiche a relais
  - E' facilmente riprogrammabile e consuma meno
  - Oltre a sequenze temporizzate svolge regolazione
  - Oltre a sequenze temporizzate scambia dati con altri sistemi (diagnostica)
- Il PLC ha struttura modulare (o compatta nei sistemi economici) e consta di:
  - Alimentatore, CPU
  - Ingressi e uscite digitali (gestione diretta sensori e attuatori discreti)
  - Ingressi e uscite analogici (gestione diretta sensori e attuatori continui)
  - Interfacce di comunicazione «semplice» (gestione diretta sensori e attuatori «smart»)
  - Moduli per compiti specifici (controllori di movimentazione, regolatori di temperatura,...)
  - Interfacce di comunicazione «standard» per programmazione, diagnostica scambio dati
- Il PLC non è un PC, ma un sistema dedicato alle applicazioni industriali in tempo reale

PLC e SOFT-PLC

Deve poter essere programmato in modo semplice

- Ha un «sistema operativo» diverso, in tempo reale
  - Organizzato in modo ciclico
  - Precedenza al programma utente
- Il programma è una sequenza di istruzioni
  - Le istruzioni sono tutte del tipo
    « SE condizione ALLORA azione ALTRIMENTI prosegui»
  - non vi sono attese, o salti all'indietro
  - L'ultima istruzione ha la priorità
- Linguaggi di programmazione «a contatti»
  - Facile negli anni '80 ma limitato
  - è cambiato il concetto di facile
  - nuovi linguaggi IEC61131 (5)
  - nuove esigenze (affidabilità, integrazione, sicurezza)
- Riprogrammare il PLC ha un costo elevato (costo del test)




```
|      C                  D
|-----]\[-------------( )    NOT
|
|      A                  C
|-----] [-----|-------( )    OR
|      B      |
|-----] [-----|
|
|      A     E          F
|-----] [---] [-------( )    AND
|
```

PLC e SOFT-PLC

Una scheda PC costa pochissimo e, con periferia di interfaccia per sensori e attuatori, e per applicazioni senza requisiti di determinismo, può ospitare PLC (Soft-PLC) e SCADA (macchine)

- Best effort o determinismo statistico (soft real-time)
  - Ritardo richiesta-risposta (latenza) < Tnoto al 99%
- Determinismo (real-time)
  - Ritardo richiesta-risposta (latenza) < Tnoto sempre
- Determinismo (hard real-time)
  - Ritardo richiesta-risposta (latenza) < Tnoto < 1ms
- Isocronia
  - Latenza fissa e nota (= Tnoto a meno del jitter)

Raspberry Pi3, Linux, WiFi, BLE, 35€

- **RTOS (Real-Time Operative System, es. WxWorks by WindRiver) e sistema di comunicazione «real-time» tra PLC e Periferia**

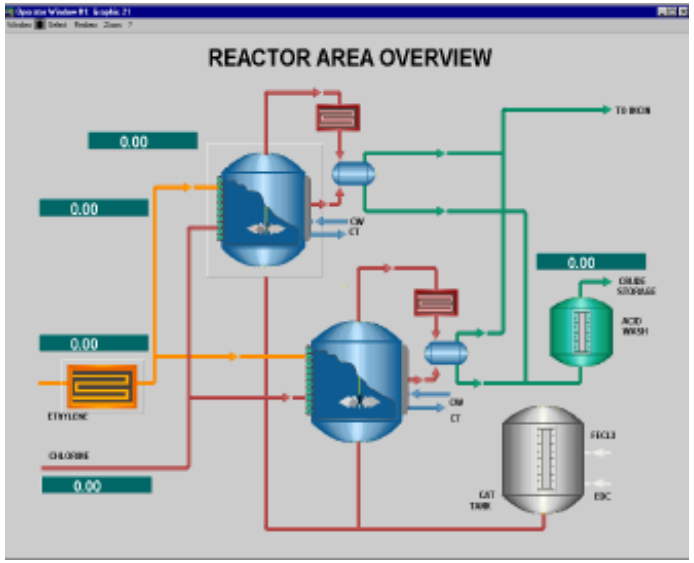
SCADA

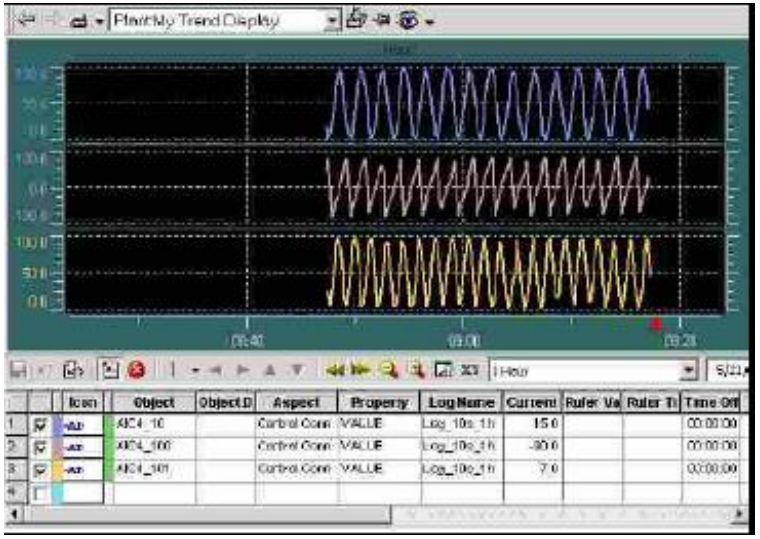
Il PLC non ha interfaccia utente e non gestisce strutture dati, ma si interfaccia ad un sistema (PC+software) che può coordinare più celle, detto SCADA, Supervisory Control And Data Acquisition

- Lo SCADA è un software basato su un database per la gestione e l'interfaccia operatore di sistemi di controllo distribuiti (uno o più PLC). Principali funzionalità:
  - Database e storico
  - Interfaccia operatore (anche decentrato, tablet) e sistema di supporto alle decisioni
  - Gestione ricette, manutenzione, trend e rapporti
  - Controllo di processo (lento), Allarmi
- Il PLC ha un'interfaccia di rete (seriale, Ethernet) per
  - Programmazione, Diagnostica
  - Scambio dati con sistemi SCADA di gestione della cella o dell'area di produzione
- Il PLC comunica con lo SCADA mediante un meccanismo Client-Server detto OPC

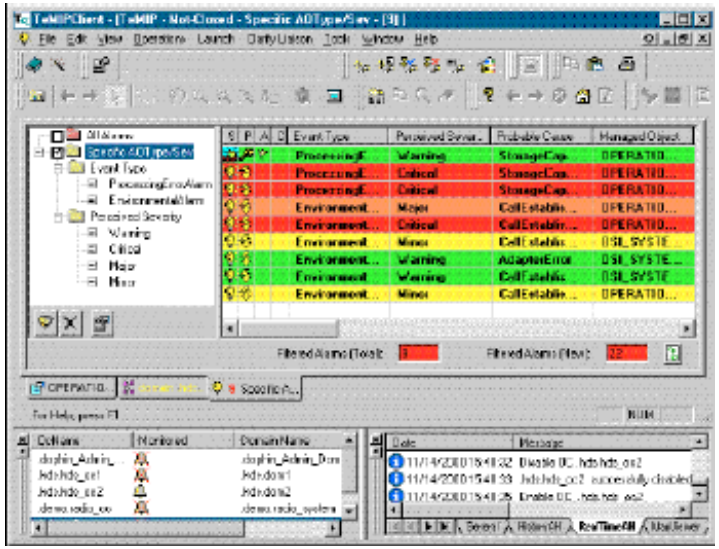
SCADA is monitoring

Trends & History





Current state



Alarms and events

SCADA is also control

Not critical, not real-time control, but control -> security

Today SCADA are connected

-Web-Based SCADA systems

- -Connecting SCADA system to Internet
- -Gives more functionality to our system
- -Security issues should be covered

-Using Instant Messaging to report systems status

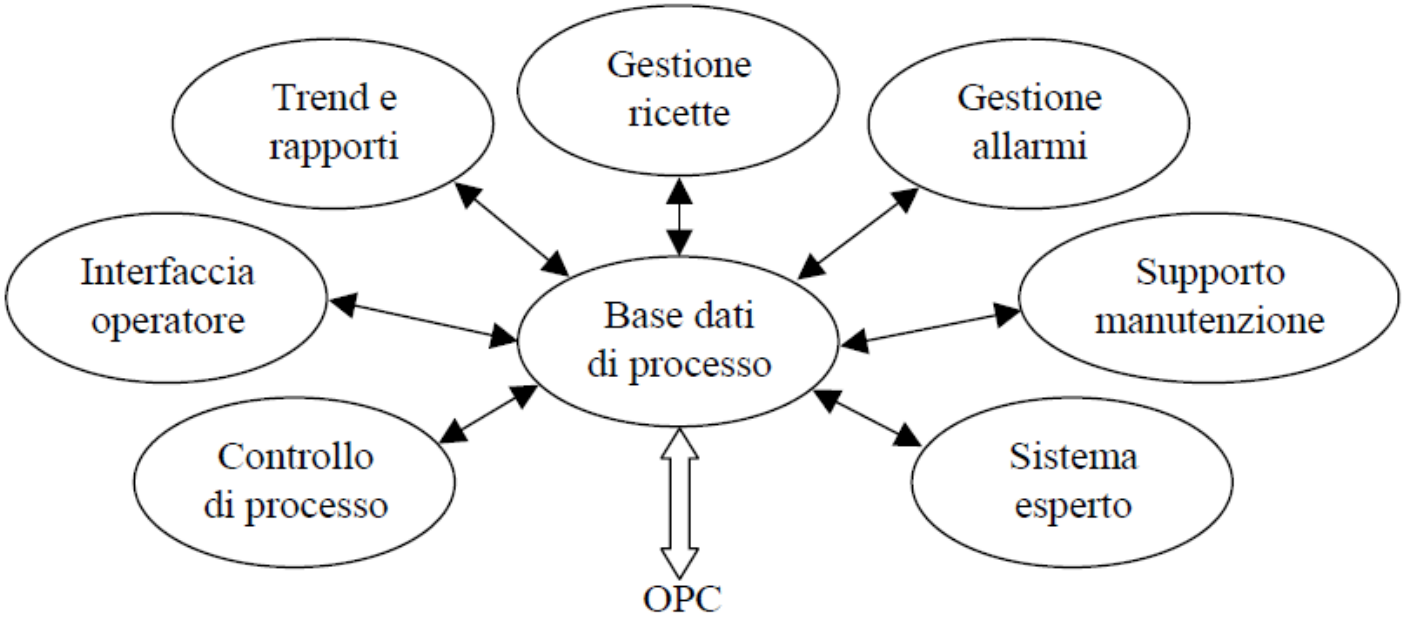
- -Giving more functionality
- -Using a reliable instant messaging service

-Using Short Message Service to report critical situations

- -A kind of instant messaging, using Mobile Telecommunication network
- -Using SMS Server, connecting a cell to PC, setting up a web server and using WAP Current state

SCADA

- **SCADA = Supervisory Control And Data Acquisition**
  - **Sistema centralizzato di supervisione e controllo di sistemi distribuiti**
  - **Si basa su un Host computer (PC o Workstation) e supporta linguaggi visuali**
  - **Si collega (LAN) ai sistemi ERP (OPC server) e mediante bus di cella ai PLC**
  - **Architettura SCADA = più stazioni client che utilizzano un unico server come gestore di database e funzioni centralizzate**



OPC (OLE for Process Control)

OPC è un'interfaccia di programmazione standard, indipendente dal produttore, attraverso la quale un client (applicativo di automazione), come un'interfaccia oumo-macchina, può accedere ai dati dell'impianto provenienti da dispositivi remoti, quali controllori logici programmabili, dispositivi fieldbus o database in tempo reale.

A tale scopo, il produttore di dispositivi di automazione o fornisce di un'interfaccia OPC-server i suoi dispositivi, oppure fornisce un server OPC che gira su un PC, che comunica con i suoi dispositivi tramite un protocollo proprietario. Un server OPC può gestire diversi dispositivi dello stesso tipo. Diversi server possono essere eseguiti in parallelo e ciascun server può essere utilizzato da diversi client, che vengono eseguiti sullo stesso PC o nella stessa rete. Tutti i server OPC presentano le variabili di processo nello stesso formato ai loro clienti come un'interfaccia uniforme.

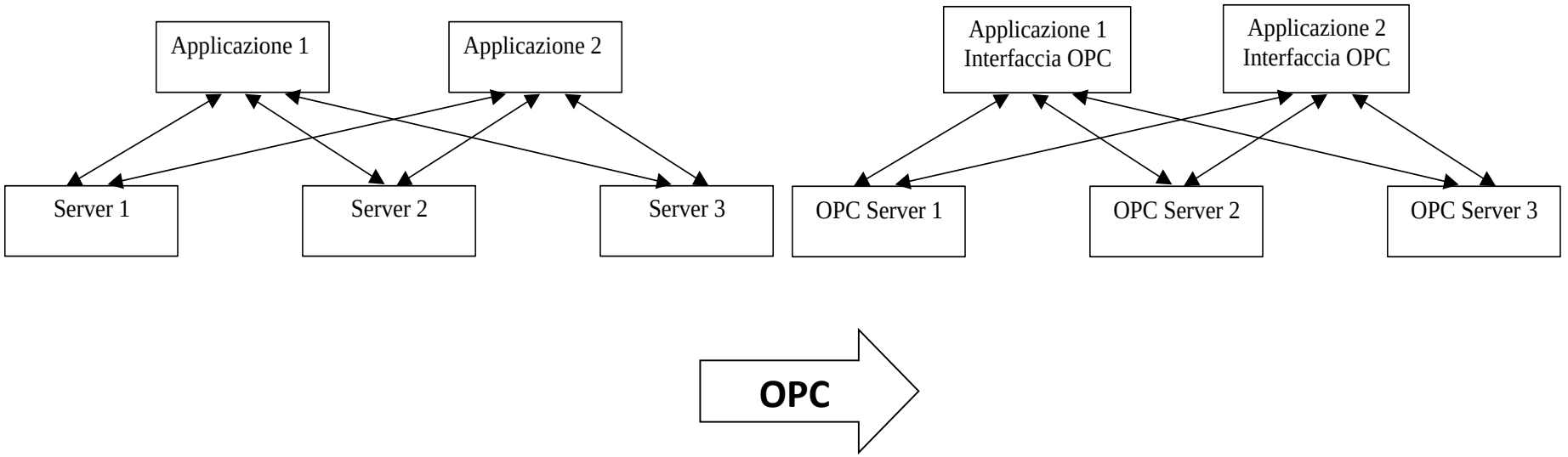
OPC (OLE for Process Control)

Il PLC ha un'interfaccia TCP/IP come lo SCADA, ma serve un meccanismo di scambio dati tra le diverse applicazioni

- OLE = Object Linking and Embedding (trasferimento e condivisione di dati tra processi diversi.

Esempio: edit di un foglio excel in un documento word).

- OLE Automation = Possibilità di accedere alle funzionalità di un software da un programma esterno (Es. programmazione automatica di una CNC



OPC (OLE for Process Control)

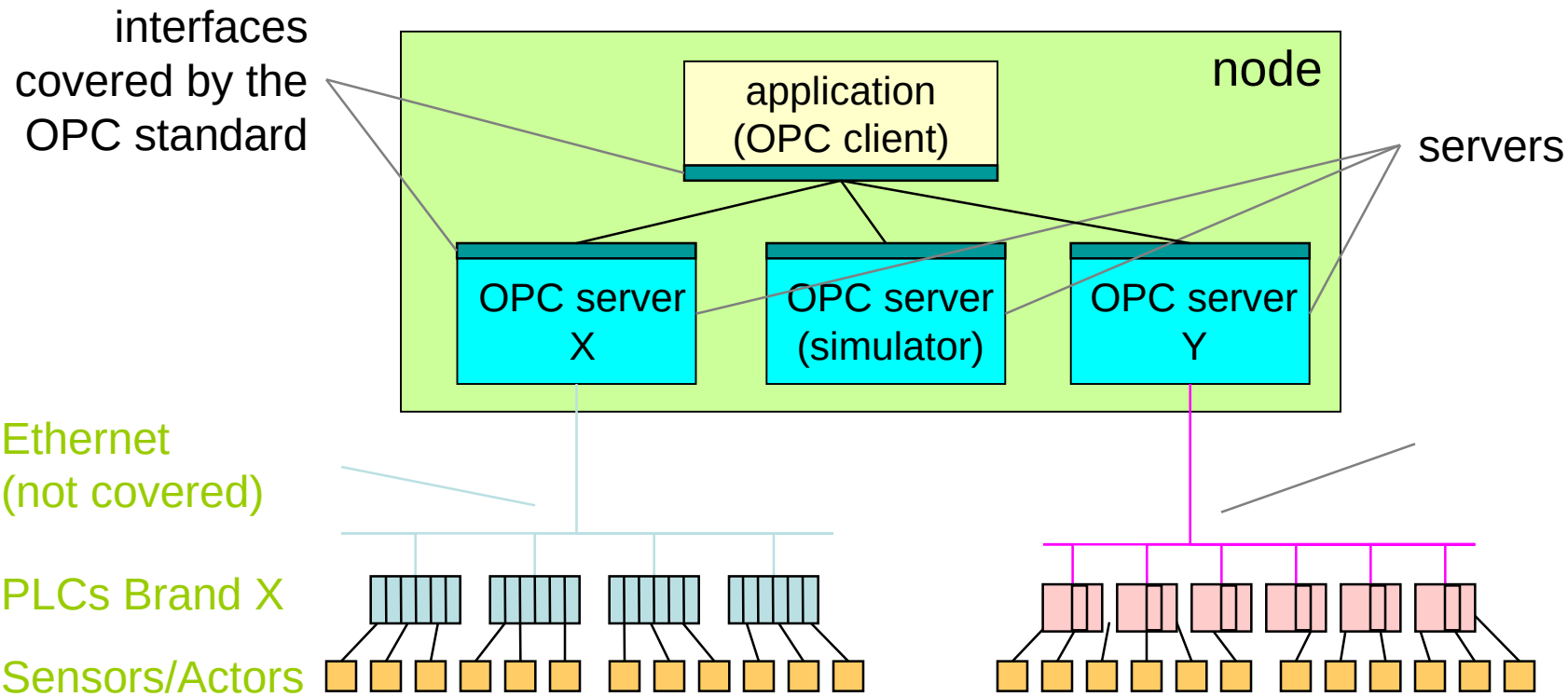
Un'interfaccia OPC consiste in un insieme di comandi raccolti in una libreria software (DLL) che può essere chiamata dalle applicazioni client scritte in Visual Basic, C # o altri linguaggi di programmazione Microsoft (anche Excel) e che accedono ai server OPC.

La libreria OPC consente in particolare di leggere e scrivere variabili di processo, leggere allarmi ed eventi e riconoscere allarmi e recuperare dati storici da basi di dati in base a diversi criteri.

OPC (oggi OPC-UA) è il metodo di connettività preferito da PLC, SCADA, DCS e MES di quasi tutti i costruttori ed è supportato da oltre il 50% dei produttori di software ERP

OPC (OLE for Process Control)

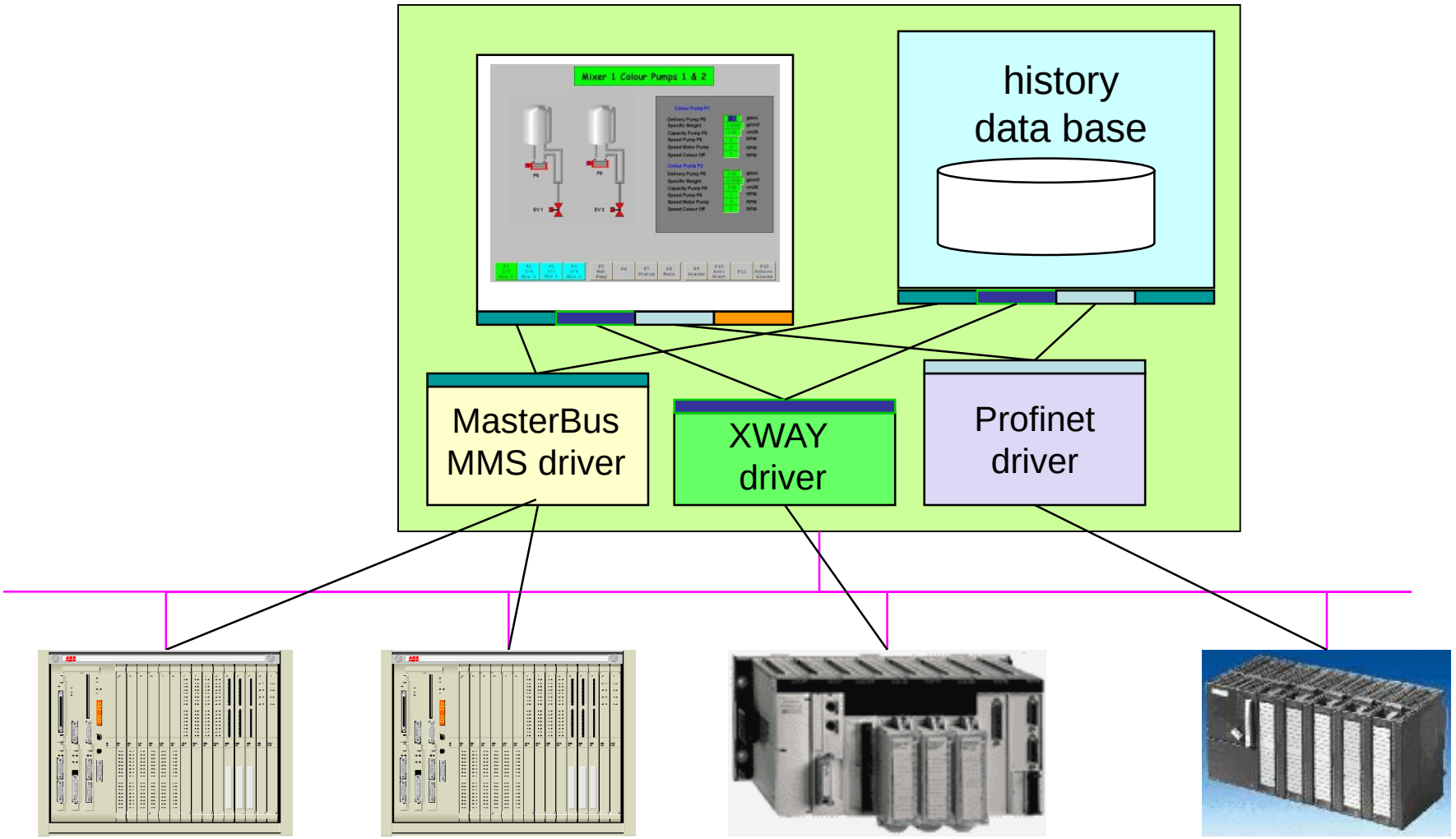
OPC (formerly: "OLE[1] for Process Control", now: "Open Process Control") is an industry standard set up by the *OPC Foundation (http://www.opcfoundation.org/)* specifying the software interface (objects, methods) to a server that collects data produced by field devices and programmable logic controllers.



1) OLE (Object Linking and Embedding) is a Microsoft technology for connecting software components. It has since been extended by the COM / DCOM technology. It corresponds to Java Beans.

Courtesy of Prof. Kirmann - EFPL

Before OPC



Courtesy of Prof. Kirmann - EFPL

With OPC (ABB application)

application software is written independently from the type of controller

the drivers still exist, but the clients do not see them anymore

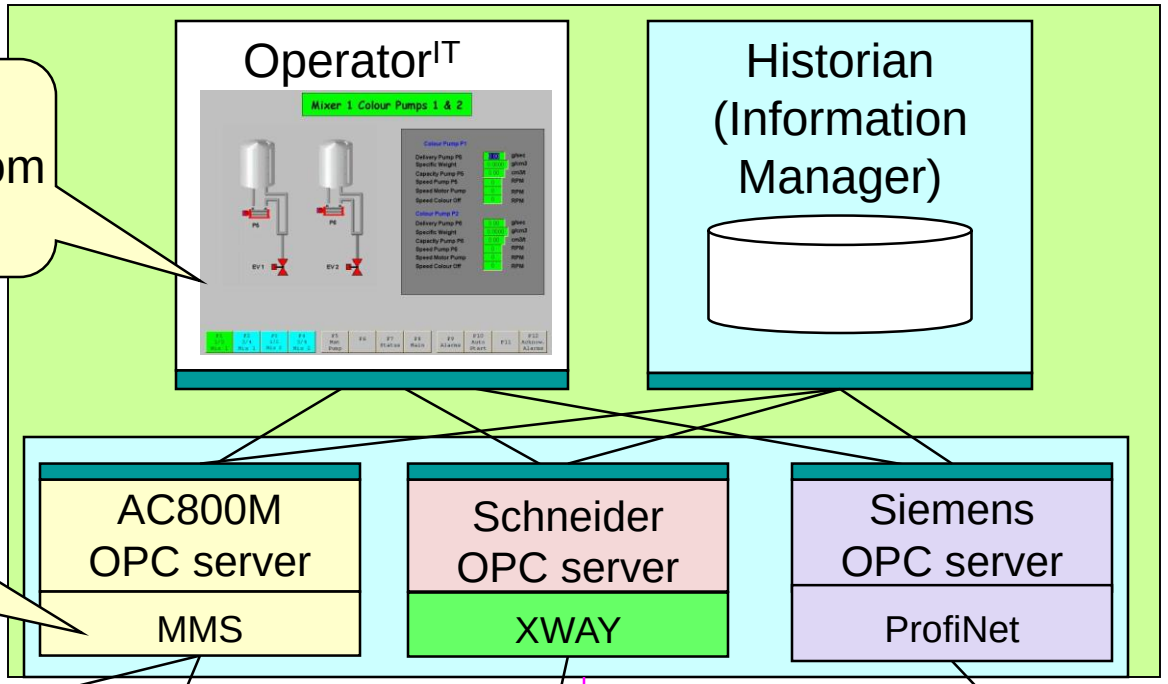
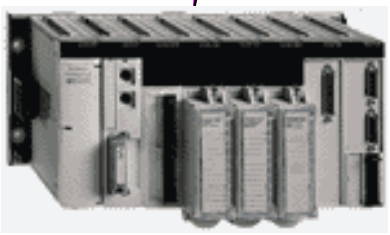


ABB AC800M

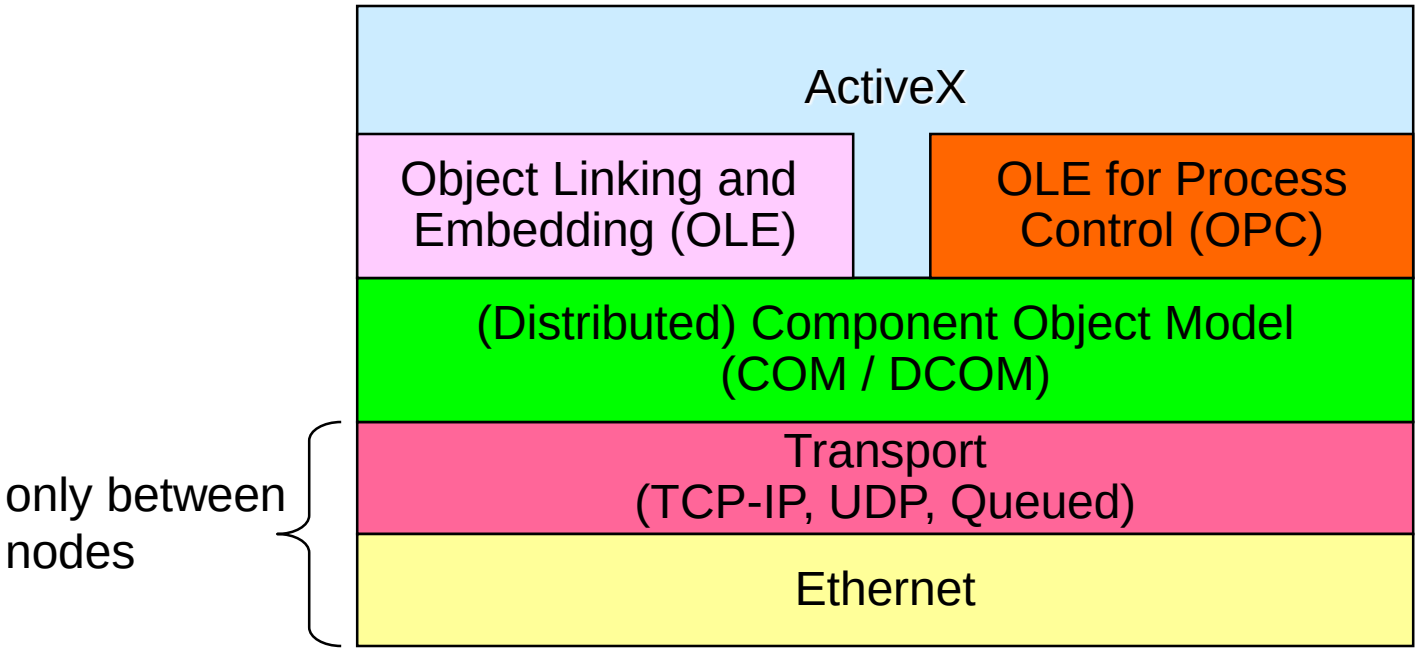


Télémécanique TSX

Siemens S7

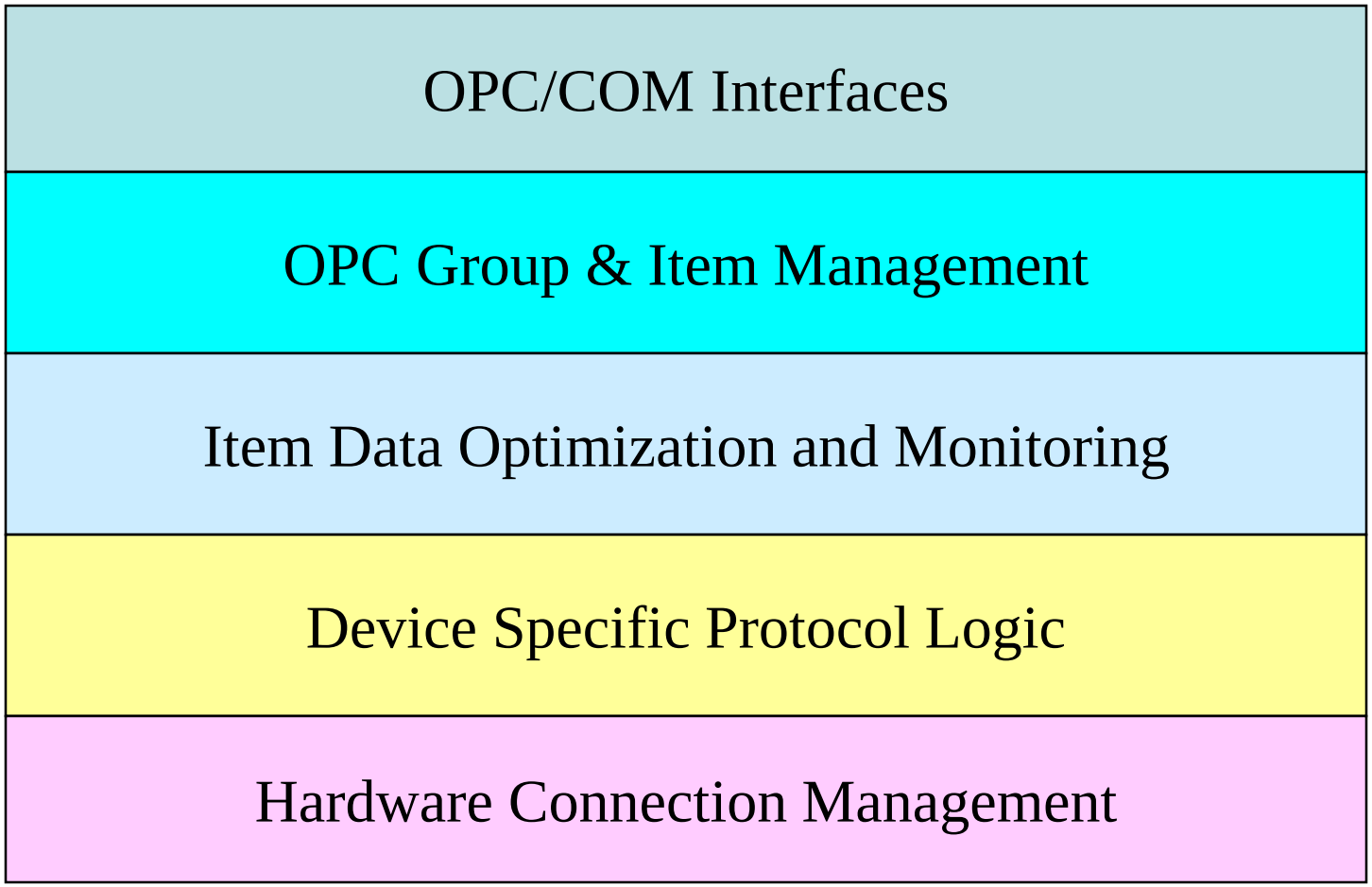
Courtesy of Prof. Kirmann - EFPL

OPC (Windows technology, abandoned)



Courtesy of Prof. Kirmann - EFPL

OPC server



Courtesy of Prof. Kirmann - EFPL

OPC, "Custom" and "Automation" Client

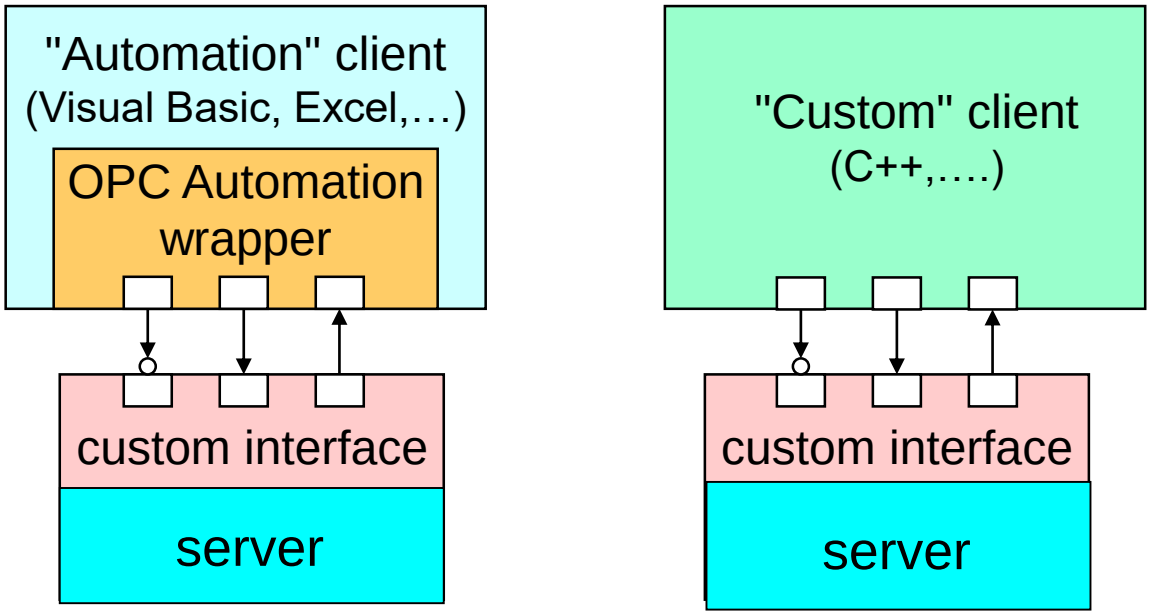
The OPC specifications define two interfaces: "custom" and "automation".

“custom” is the native C++ interface of COM.

“automation” is the interface offered in Visual Basic, used in Word, Excel,…..

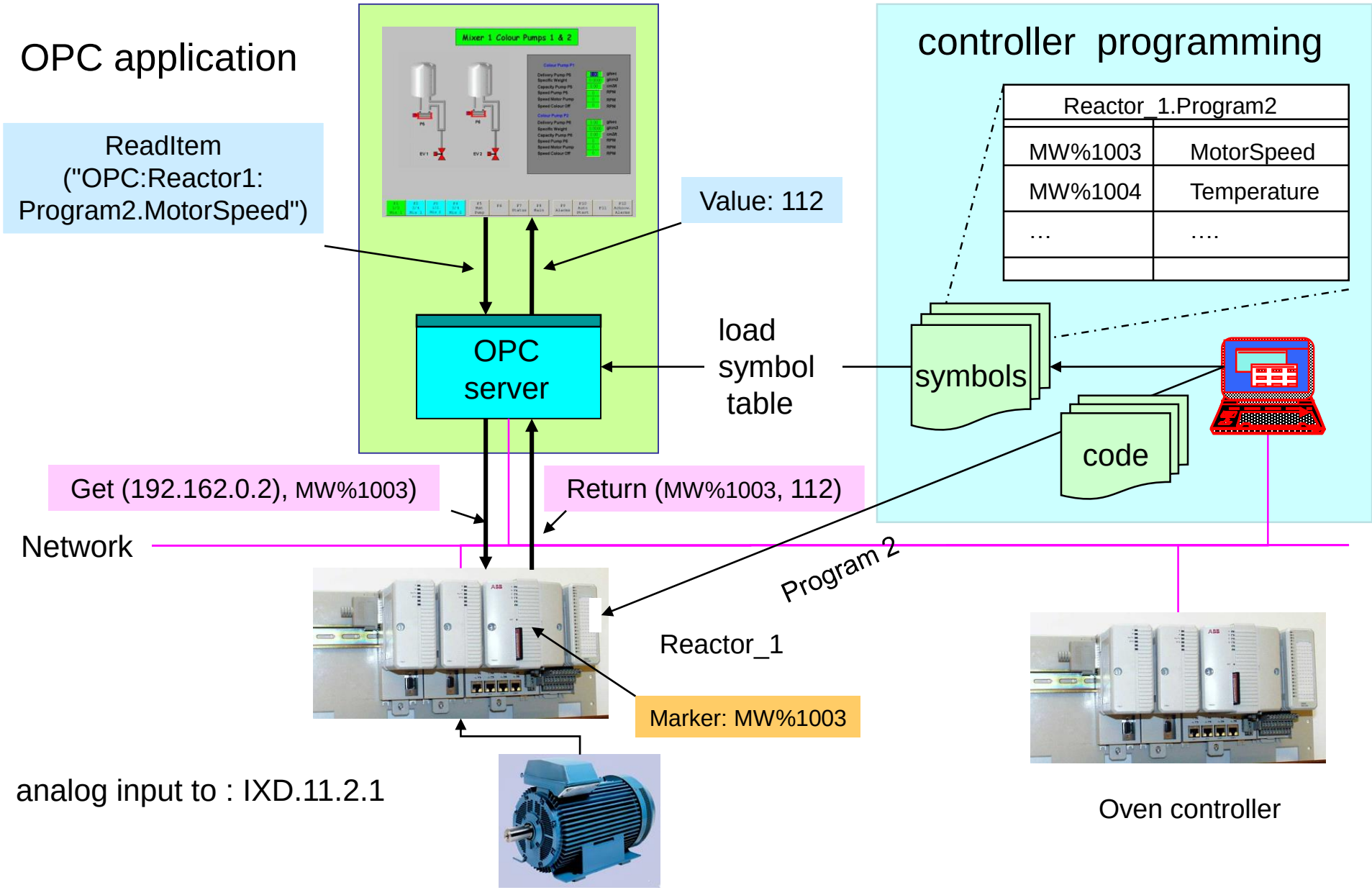
The interface is defined by a Type Library (distributed by the OPC Foundation)

Functionality is roughly the same in both models, “automation” is easier to use, but "custom" gives a more extended control.



Courtesy of Prof. Kirmann - EFPL

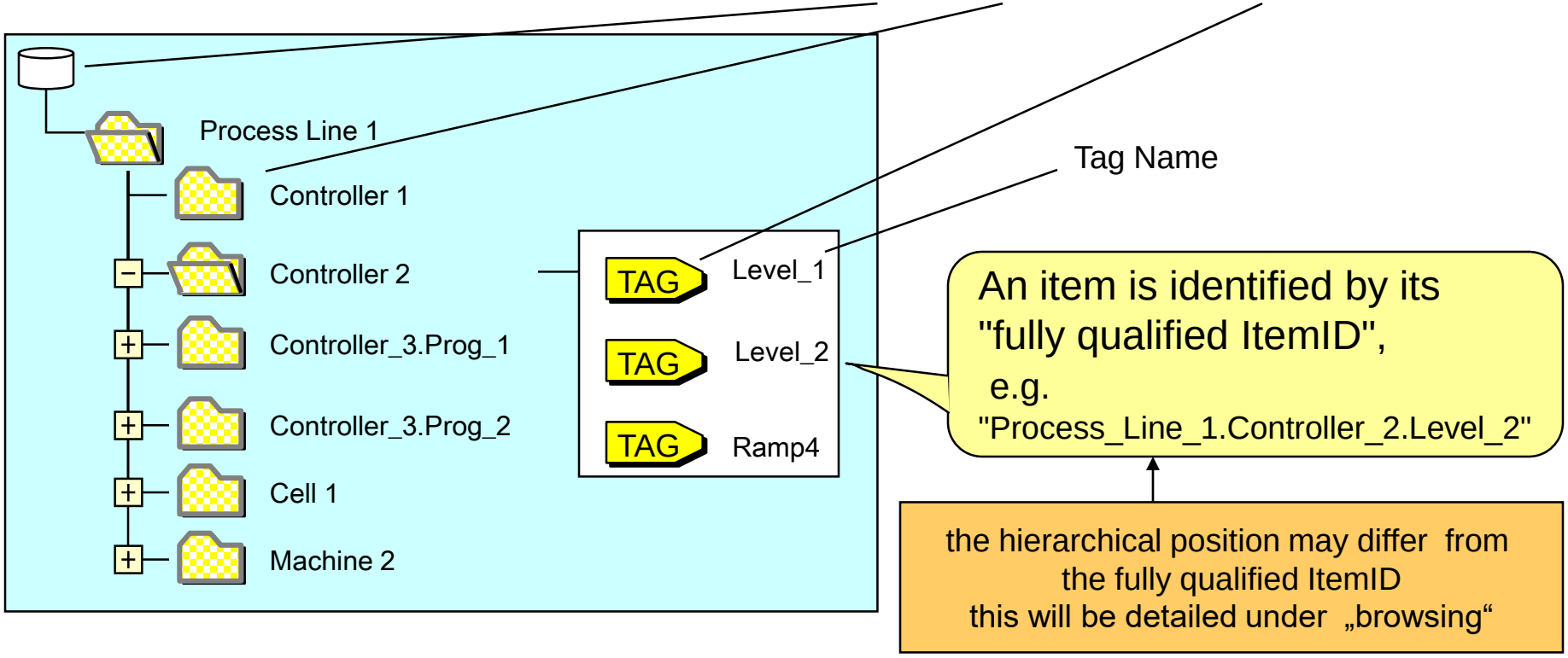
OPC Data Access: access to a variable



Courtesy of Prof. Kirmann - EFPL

OPC Data Access: access to a variable

An OPC server is structured as a directory with root, branches and leaves (items)



Branches may contain other branches and items
The structure may also be flat instead of hierarchical
This structure is defined during engineering of the attached devices and sensor/actors.
(Intelligent servers could configure themselves by reading the attached devices)

Courtesy of Prof. Kirmann - EFPL

OPC: item

The process data are represented by three dynamic properties of an item:

Value V: numerical or text

time-stamp T: the time at which this data was transmitted from the PLC to the server
this time is UTC (Greenwich Winter time), not local time.

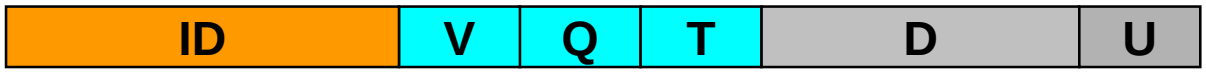
Quality Q: validity of the reading (not readable, dubious data, o.k.)

and two optional static property:

Description D: a text string describing the use and of the variable (optional)

engineering unit U: the unit in which the variable is expressed (optional)

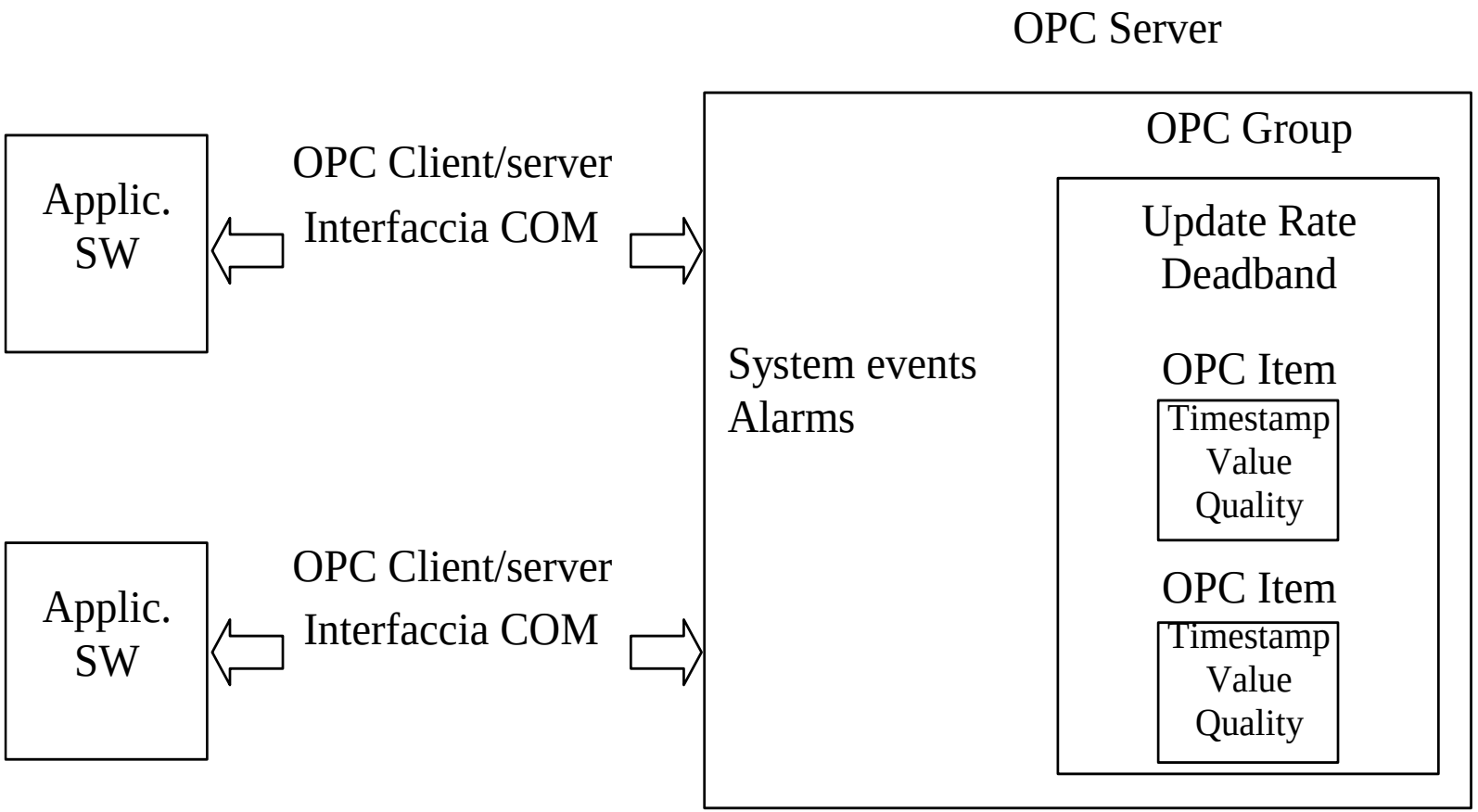
(when writing, only the value is used)



Courtesy of Prof. Kirmann - EFPL

OPC SERVER (es. PLC, SCADA vs ERP-MES)

Item = riferimento del dato = {valore | qualità | timestamps}



Da OPC a OPC-UA

OPC (Microsoft Windows-only COM/DCOM) è diventato uno standard de facto fino al 2005, poi OPC Foundation ha rilasciato OPC-UA (Unified Architecture)

- Piattaforma aperta e non legata ad un sistema operativo o ad un linguaggio di programmazione
  - Comunicazione Machine to Machine (M2M)
- Architettura Service-oriented
- Maggior sicurezza
- Modello dati sofisticato e completo
- **OPC UA è un modo di organizzare i dati e renderli fruibili alle applicazioni senza interventi di programmazione o configurazione**
  - Vedo quali servizi sono disponibili e sottoscrivo quelli che mi interessano