



Stefan-Helmut Leitner, ABB Corporate Research Germany, Zukunft der Netze 2011, Hamburg

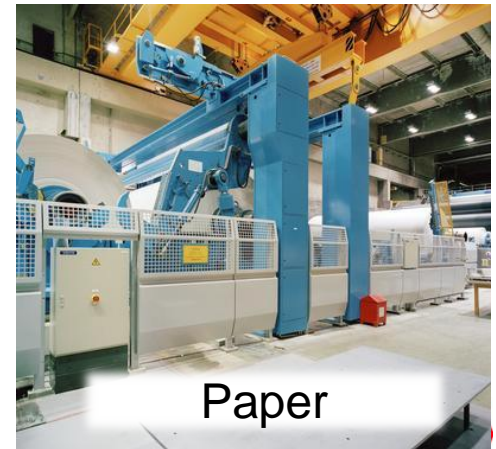
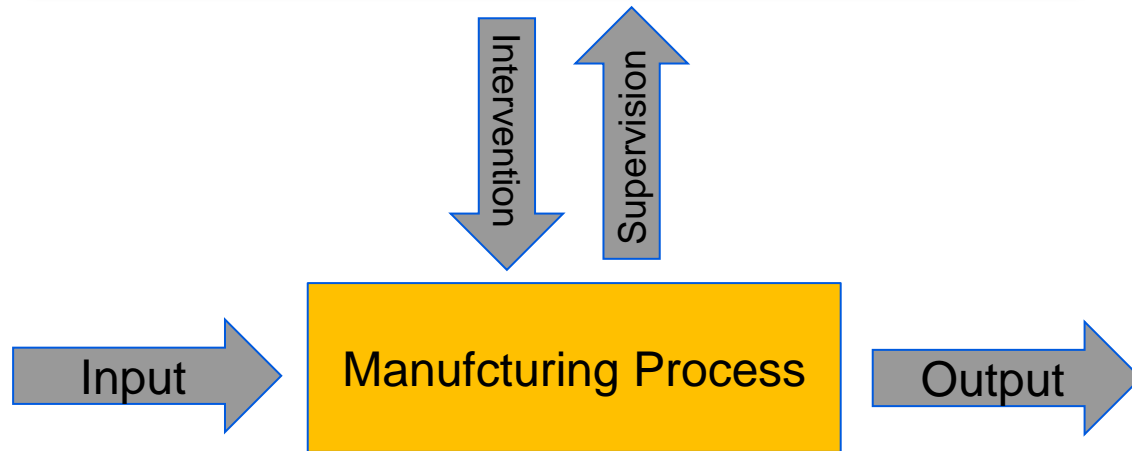
Secure Communication in Industrial Automation by Applying OPC UA

Agenda

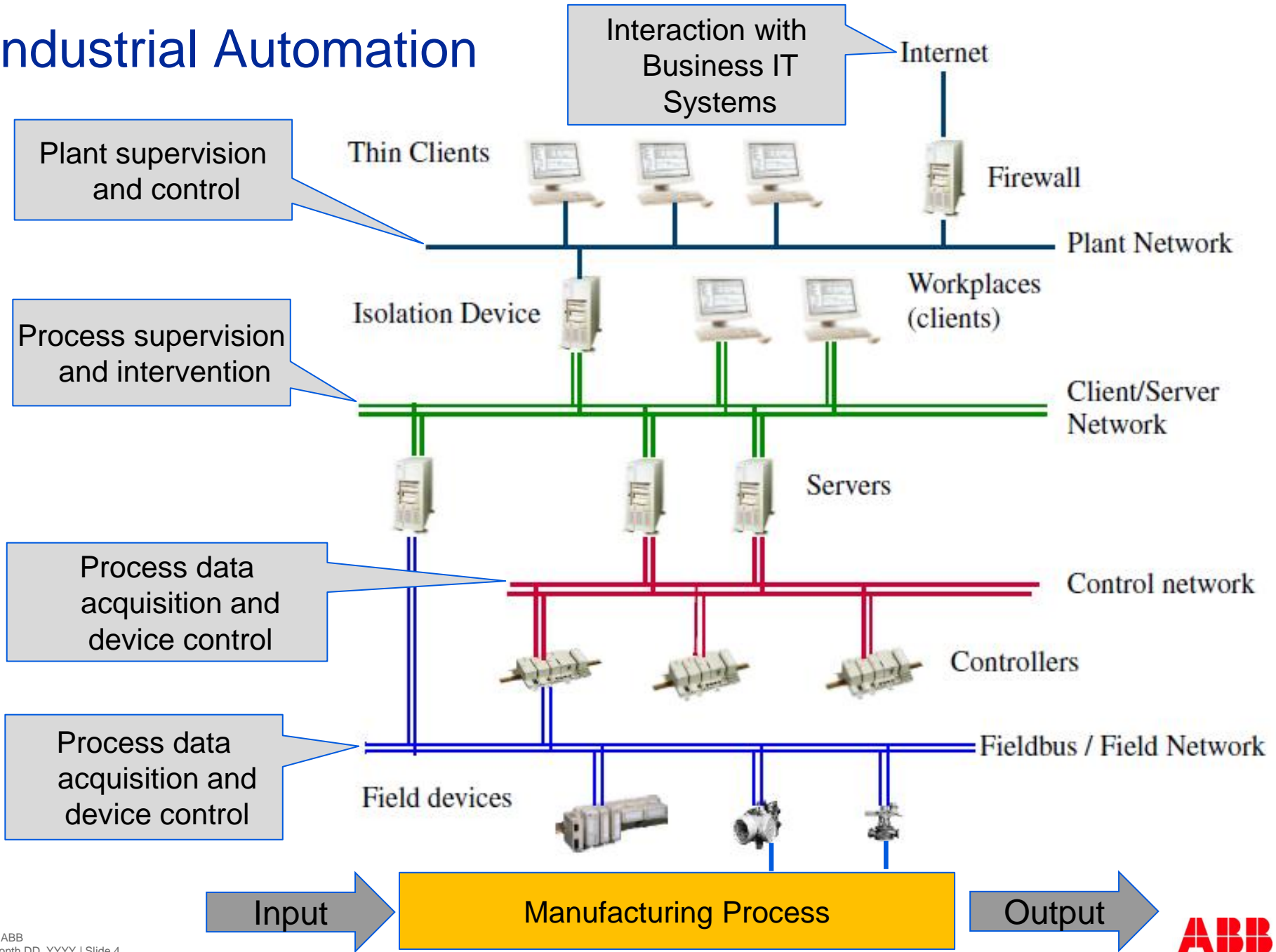
- Industrial Automation
- Classic OPC and OPC UA?
- All problems solved?
- Future?

Industrial Automation

Industrial Automation deals with automation of manufacturing processes



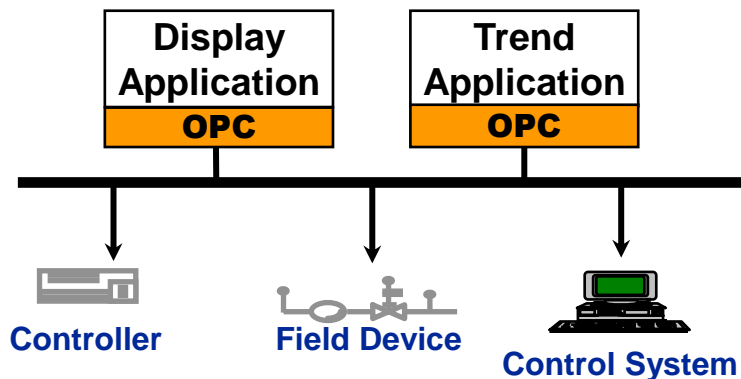
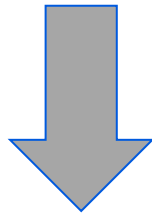
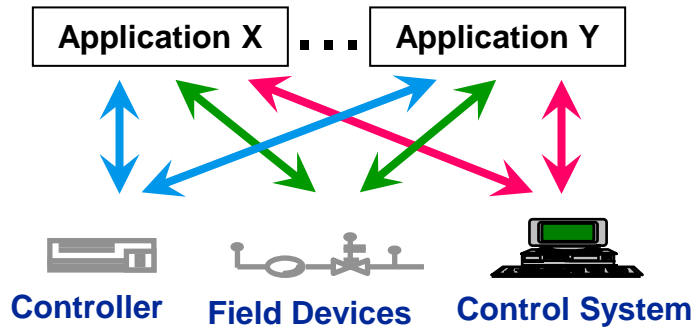
Industrial Automation



Industrial Automation

- Differences compared to Business IT
 - Availability has highest security goal
 - Safety is (often) more important than security
 - Long system lifetime (<20 years without interruption)
- Other Challenges
 - Increasing interconnectivity
 - Increasing usage of COTS and Open Source
 - Interoperability and standardization
 - Example: OPC

Classic OPC and OPC UA



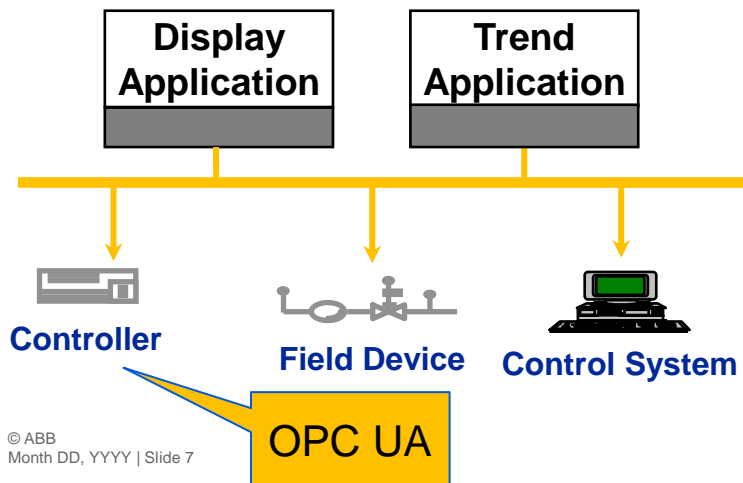
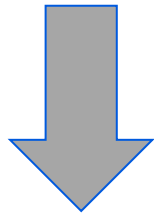
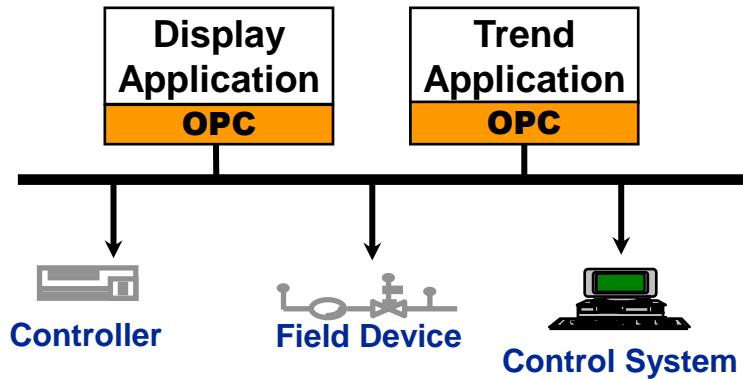
■ OPC

- Widely adopted industry standard
- Data exchange with process devices
- Pure interface specification
- Based on Microsoft COM/DCOM

■ Deficiencies

- Technology Dependency (COM/DCOM retires)
- Complicated security configuration
- Security not sufficiently considered in architecture

Classic OPC and OPC UA



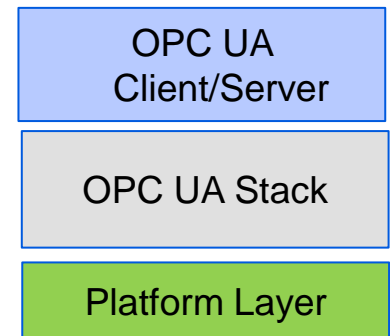
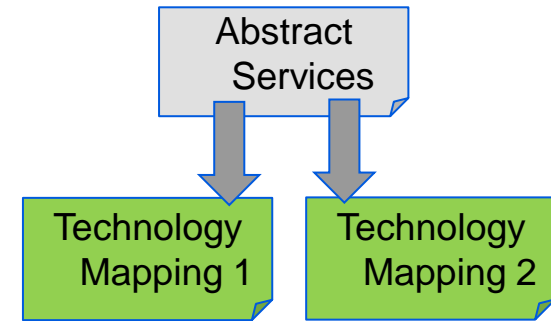
■ OPC UA

- Abstract protocol specification and concrete technology mappings
- Service-oriented Architecture
- More areas of applications incl. embedded systems
- Benefits compared to OPC
 - Reduced technology or vendor dependency
 - Security is inherent part of architecture and implementation
 - Simplified security onfiguration

Classic OPC and OPC UA

Reduced technology or vendor dependency

- Specification
 - Abstract service and technology mappings
 - *Allows adding new mappings in case of security vulnerabilities!*
- Protocol Stack Implementation
 - Minimal platform-dependent layer
 - *Allows replacing libraries in case of security vulnerabilities!*



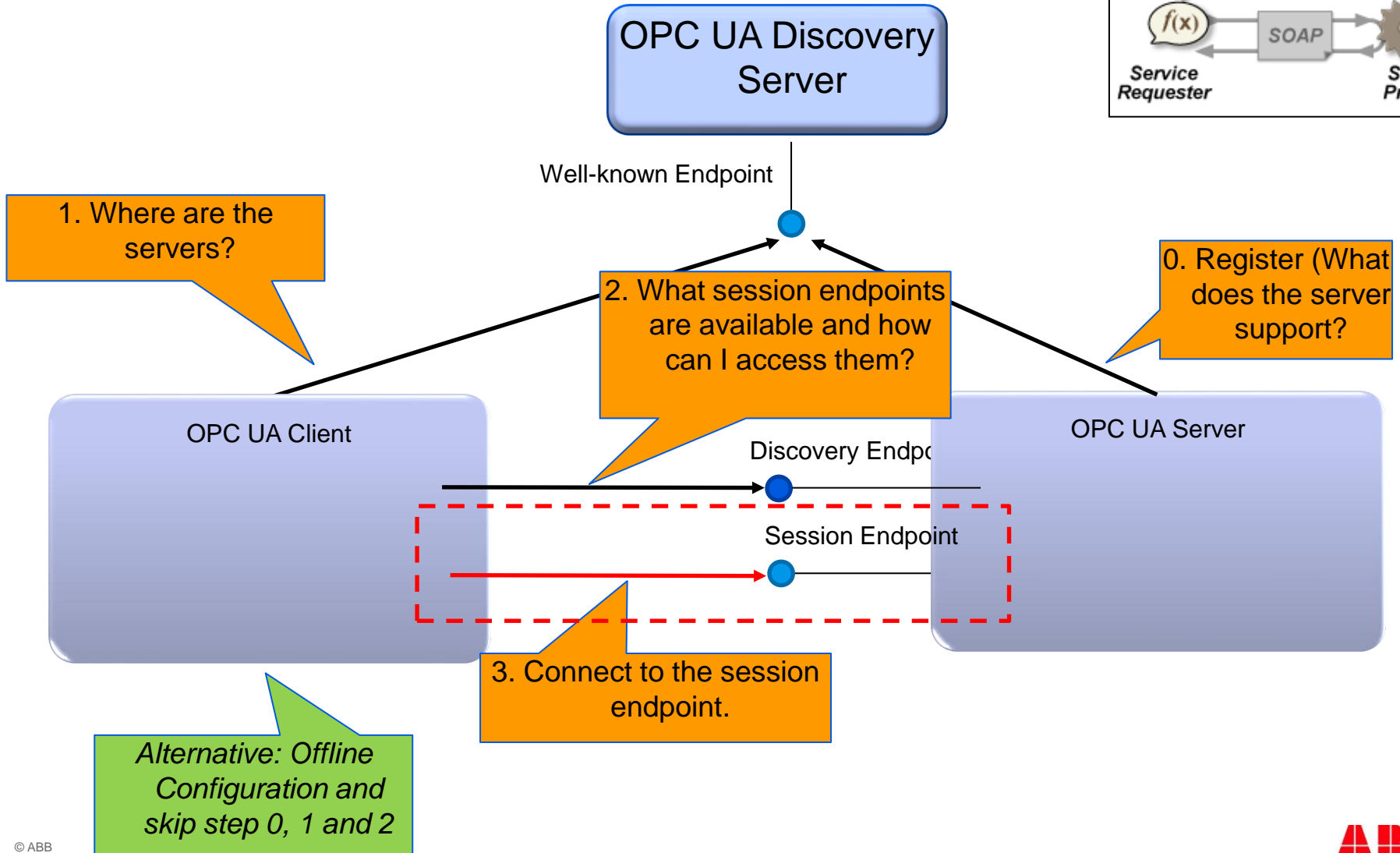
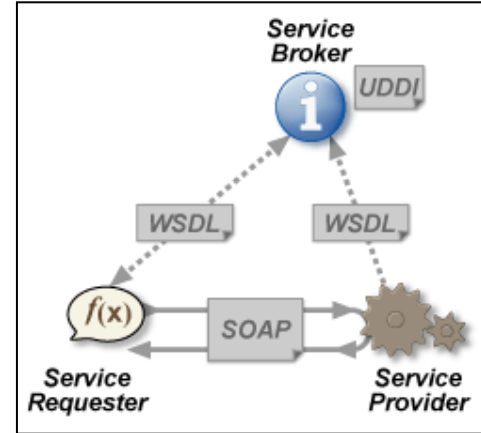
Classic OPC and OPC UA

Simplified security configuration

- Few well-defined security policies
 - Consistent set of security-related configuration for communication
 - Algorithms for encryption and digital signatures
 - Type of user credentials
 - ...
- Agreement of applied security can be done by
 - Pre-configuration by client
 - Selection after server discovery
 - Automatic negotiation between client and server

Classic OPC and OPC UA

Simplified security configuration



Classic OPC and OPC UA

...and where are remaining challenges?

- OPC UA requires up to three types of digital certificates for different purposes !
- Public Key Infrastructure required which requires significant efforts.
- Usage of digital certificates is quite new to automation
 - Learning curve is still required
- Dealing with certificates in controllers
 - Limited resources (processing power, memory)
 - Long lifetime without interruption (up to 10-20 years)
 - Poor entropy sources

All problems solved?

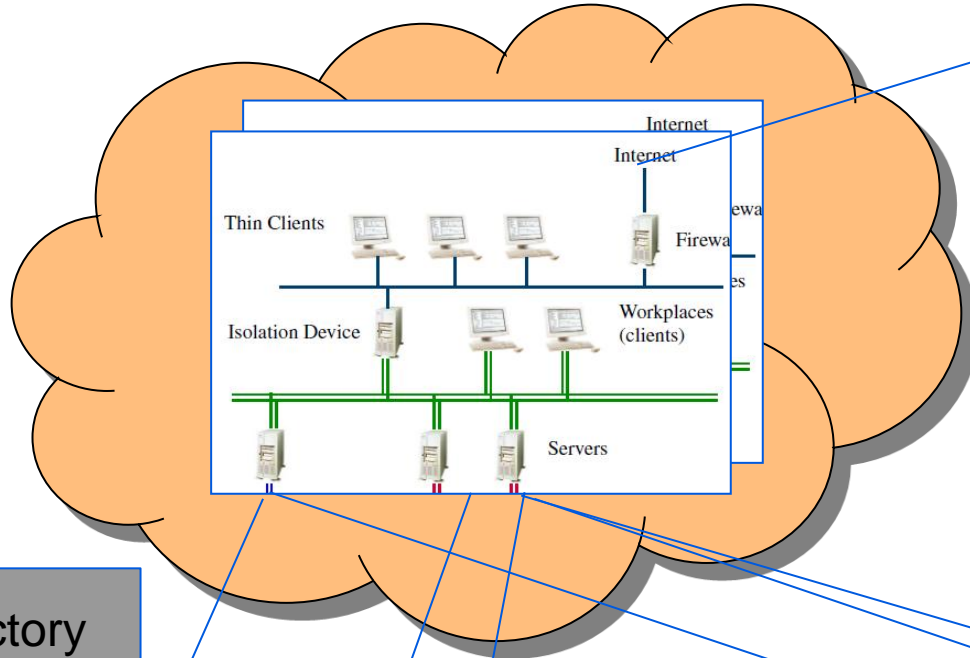
- Reduced technology dependency 😊
- Security is inherent part of architecture and implementation 😊
- Simplified security configuration 😞

Future?

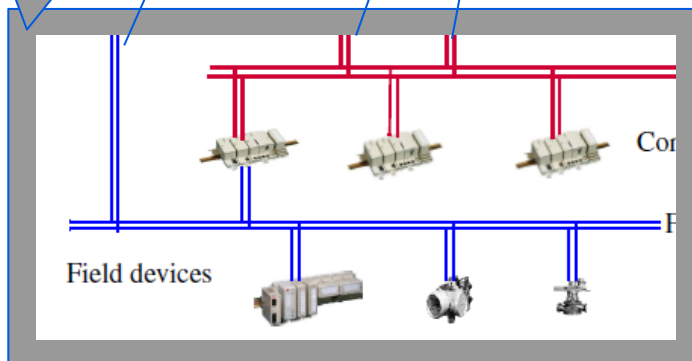
Security impact of Cloud Computing



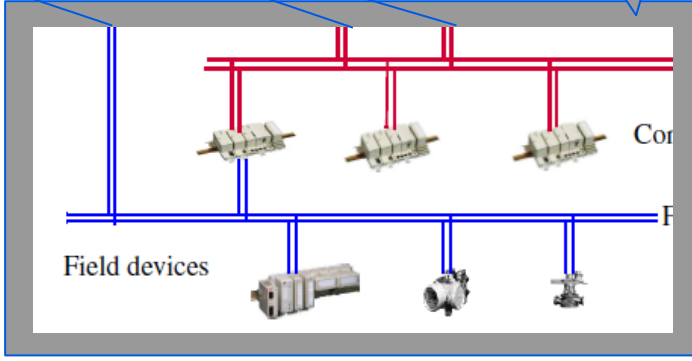
Headquarter



Factory



Factory



Power and productivity
for a better world™

