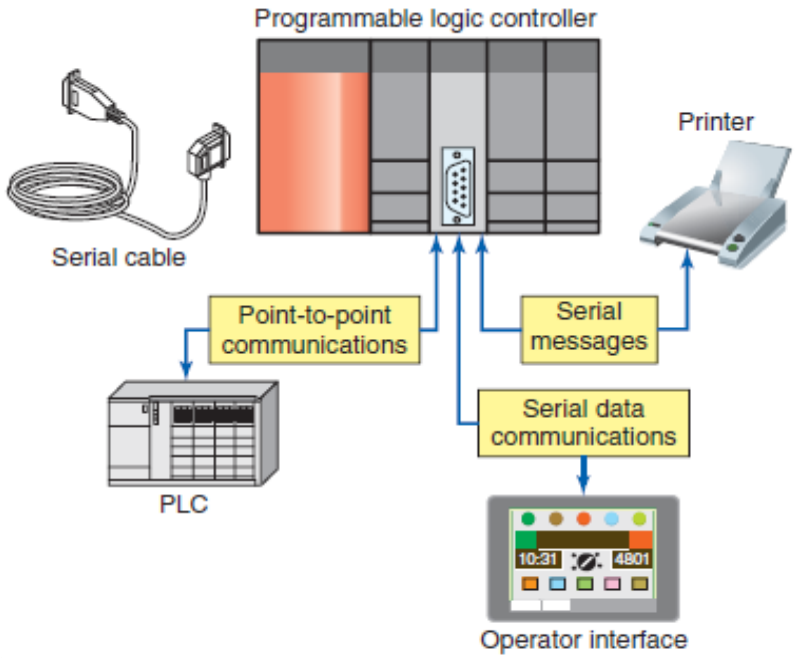
# Industrial Automation (ICE 3252)

## Industrial Communication Protocol Basics

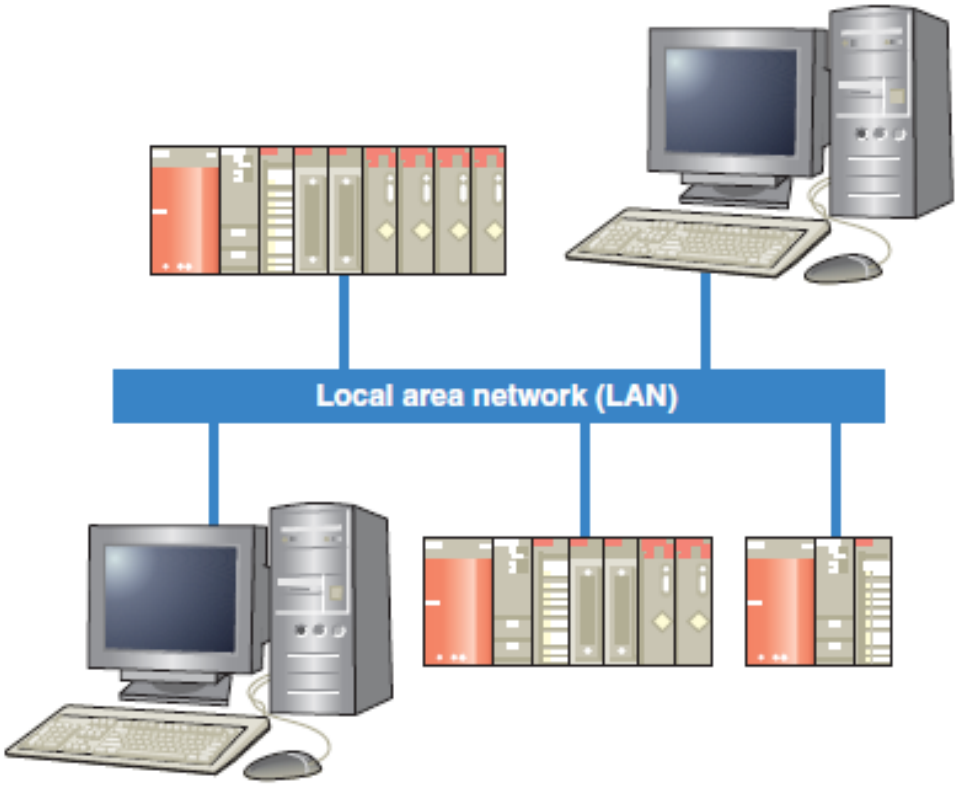
Bipin Krishna
Assistant Professor (Sr.)
ICE Department
Manipal Institute of Technology
MAHE, Karnataka, India

# Data Communications

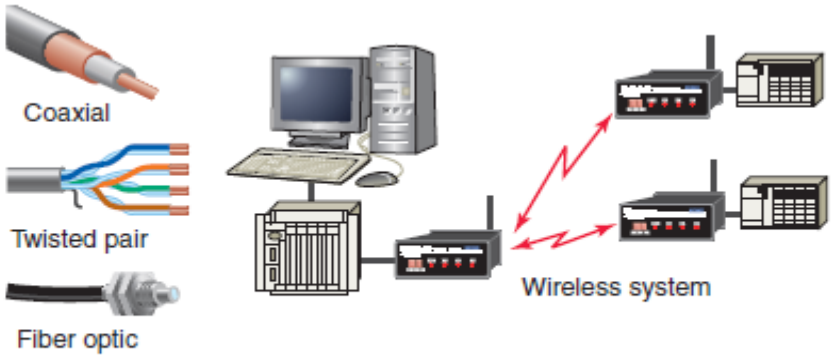
- *Data communications* refers to the different ways that PLC microprocessor-based systems talk to each other and to other devices.
- The two general types of communications links that can be established between the PLC and other devices are point-to-point links and network links.




Point-to-point serial communications link.

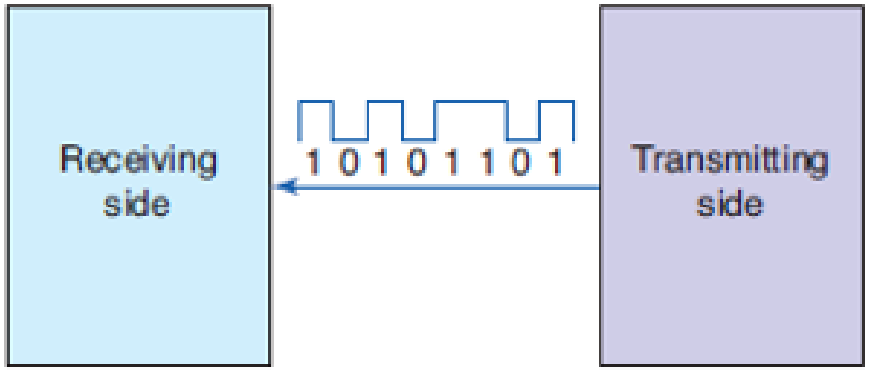



Local area network (LAN) communication link.

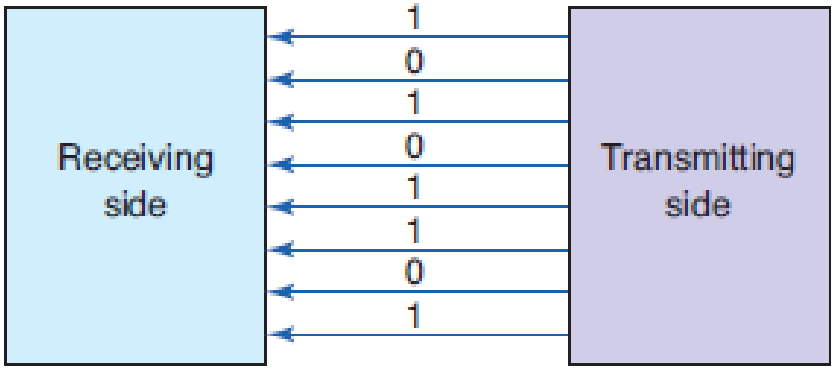



Transmission media.

# Serial Vs Parallel Communication




Serial data transmission.




Parallel data transmission.

# Industrial Communication

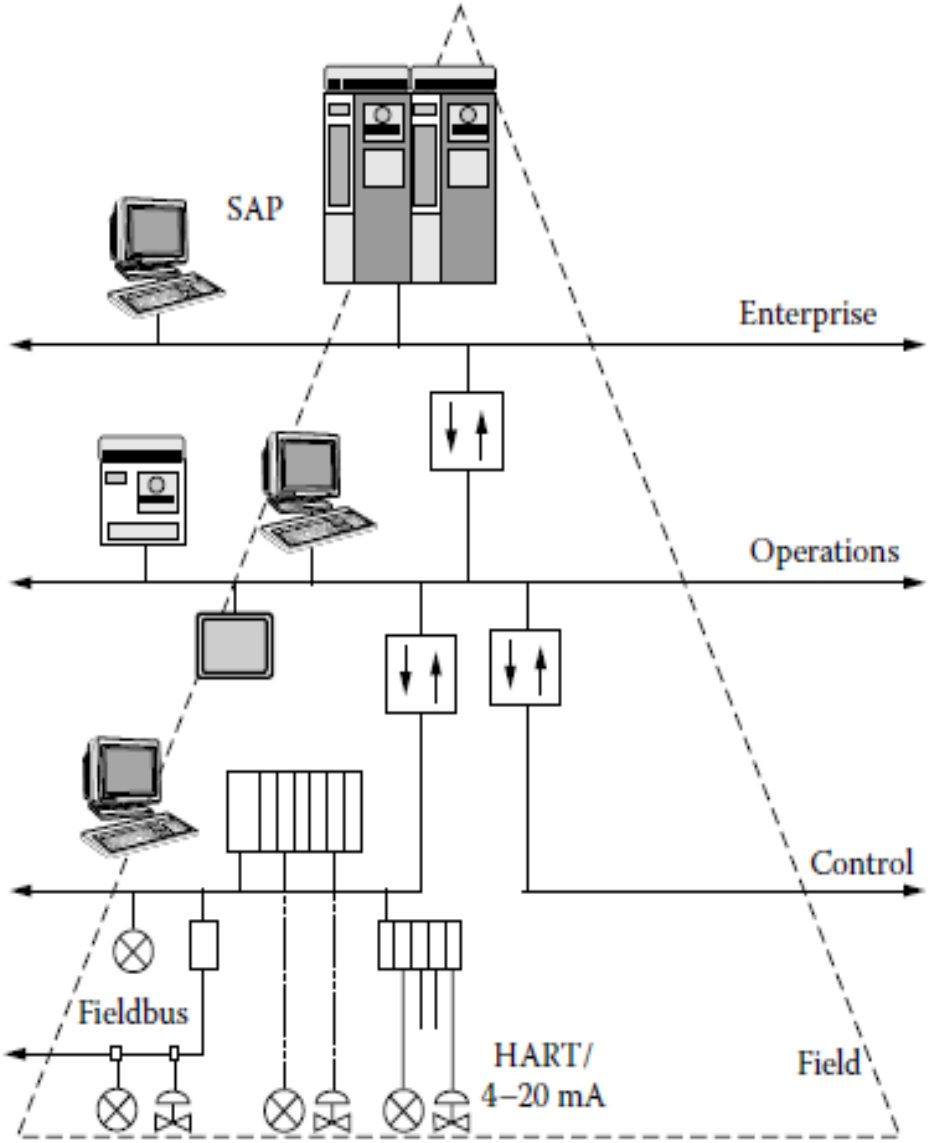
- The aim of industrial communication is the reliable transmission of data from the field through to the control level.
- Connect all sections of a plant in a single networked system, from the management level right down to the field level.
- Industrial network communication also allows all business units to be integrated, making it a central component for the availability of data in the **Industrial Internet of Things (IIoT).**
- An **industrial communication network** is a backbone for any automation system architecture as it has been providing a powerful means of data exchange, data controllability, and flexibility to connect various devices.

# What is an Industrial Communication Network?

- Data communication refers to the transformation of information or data, mostly in digital format from a transmitter to a receiver through a link (which can be copper wire, coaxial cable, optical fiber, or any other medium) connecting these two.
- Traditional communication networks are used to enable data communication between computers, computers and its peripherals and other devices.
- On the other hand, **industrial communication network** is a special type of network made to handle real-time control and data integrity in harsh environments over large installations.

# Communications Hierarchy

- Field level-sensors and actuators, limit switch signal or continuous signal
- Control level-PLC, PCS, DCS
- Operations level-SCADA, Asset management
- Enterprise level




*Automation pyramid.*

# Communication system requirements

- Transmission of control variables between LCUs in the system. This is a requirement for all applications in which the control strategy requires multiple interacting controllers. To minimize delays and maximize the security of transmission, the LCUs should be able to communicate directly with one another and not through an intermediary.
- Transmission of process variables, control variables, and alarm status information from the LCUs to the high-level human interfaces and to the low-level human interfaces in the system.
- Communication of set-point commands, operating modes, and control variables from the high-level computing devices and human interface devices to the LCUs for the purpose of supervisory control.

# Communication system requirements

- Downloading of control system configurations, tuning parameters, and user programs from the high-level human interfaces to the LCUs.
- Synchronization of real time among all of the elements in the distributed control system
- Transfer of large blocks of data, programs, or control configurations from one high level computing device or human interface to another.
- Transmission of information from the data I/O units to the high level computing devices for further purpose of data acquisition or transfer.

# Network topologies

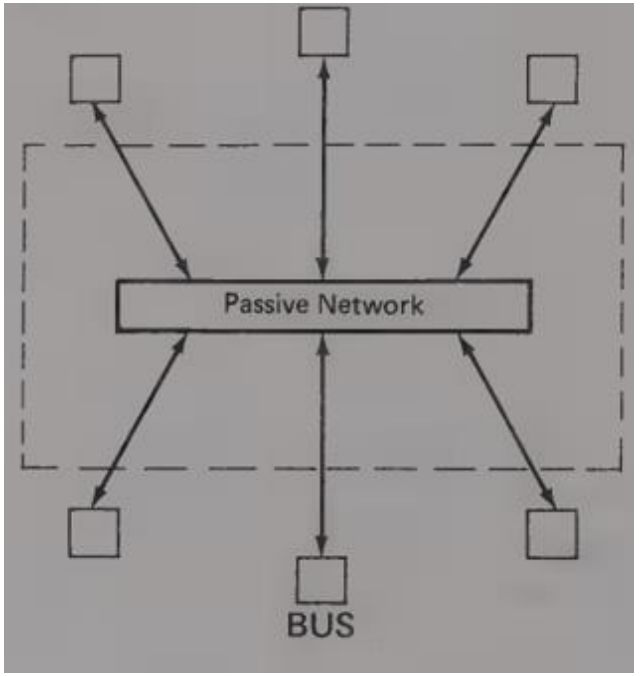
- The network topology describes the way in which the devices in the network are connected together.

Major network topologies

- **Star**
- **Bus**
- **Mesh**
- **ring**

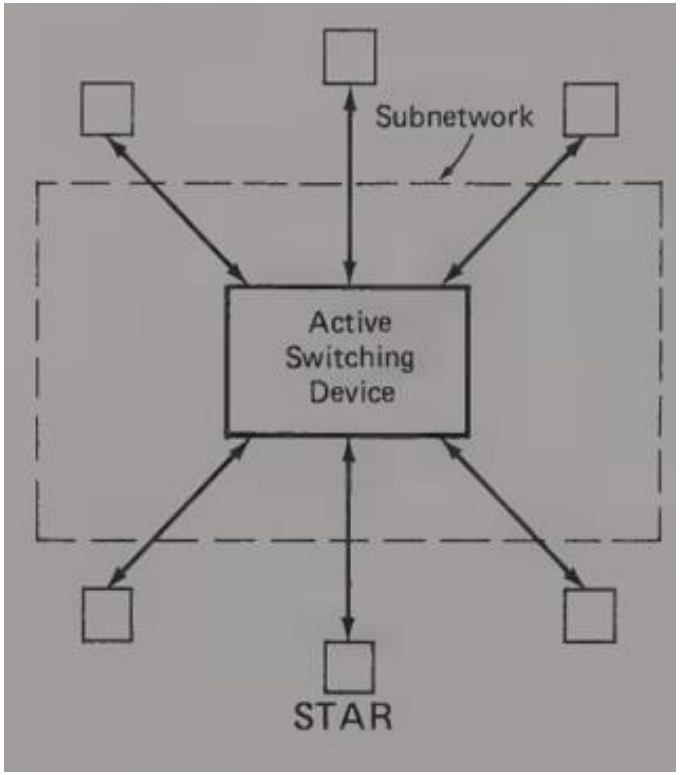
# Bus topology

- In case of Bus topology, all devices share single communication line or cable.
- Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue.
- It is one of the simple forms of networking where a failure of a device does not affect the other devices.
- But failure of the shared communication line can make all other devices stop functioning.



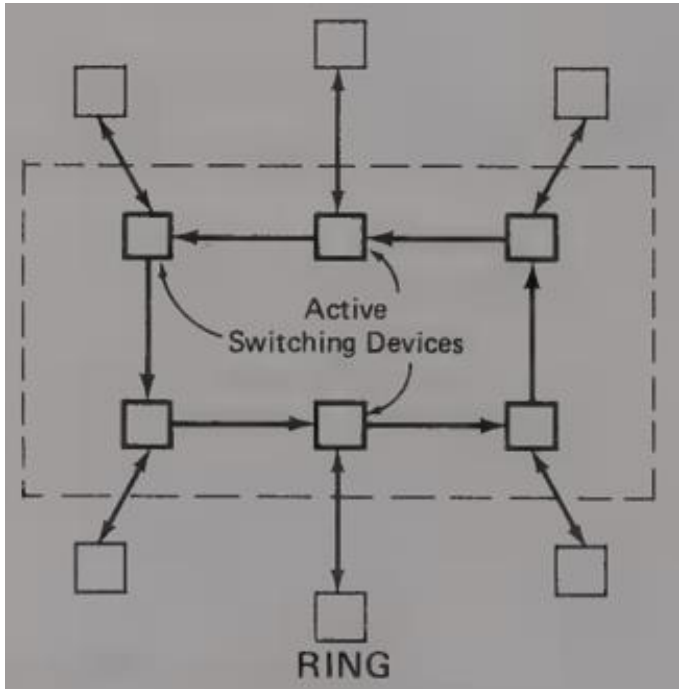
# Star topology

- All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub.
- As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails.
- Every communication between hosts, takes place through only the hub.
- Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.



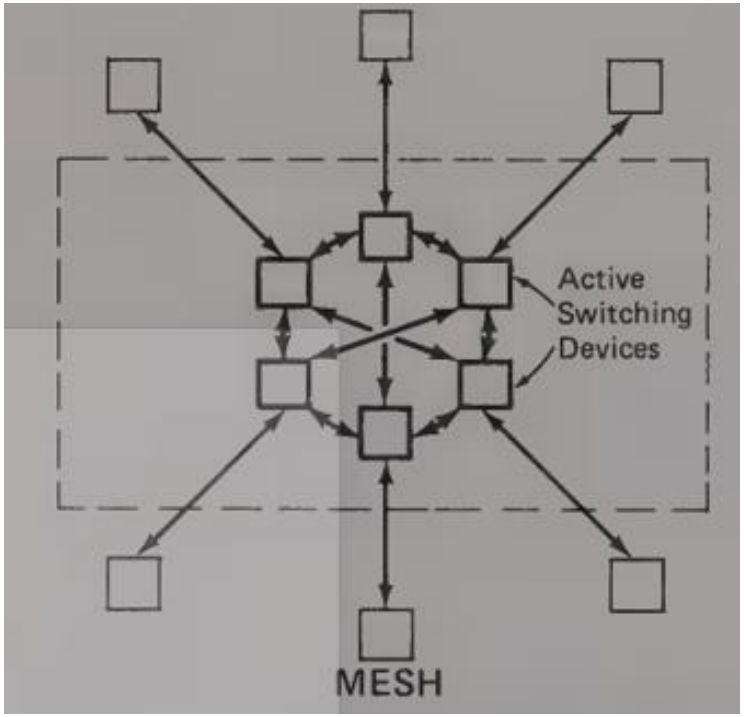
# Ring topology

- In ring topology, each host machine connects to exactly two other machines, creating a circular network structure.
- When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts.
- To connect one more host in the existing structure, the administrator may need only one more extra cable.
- Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.



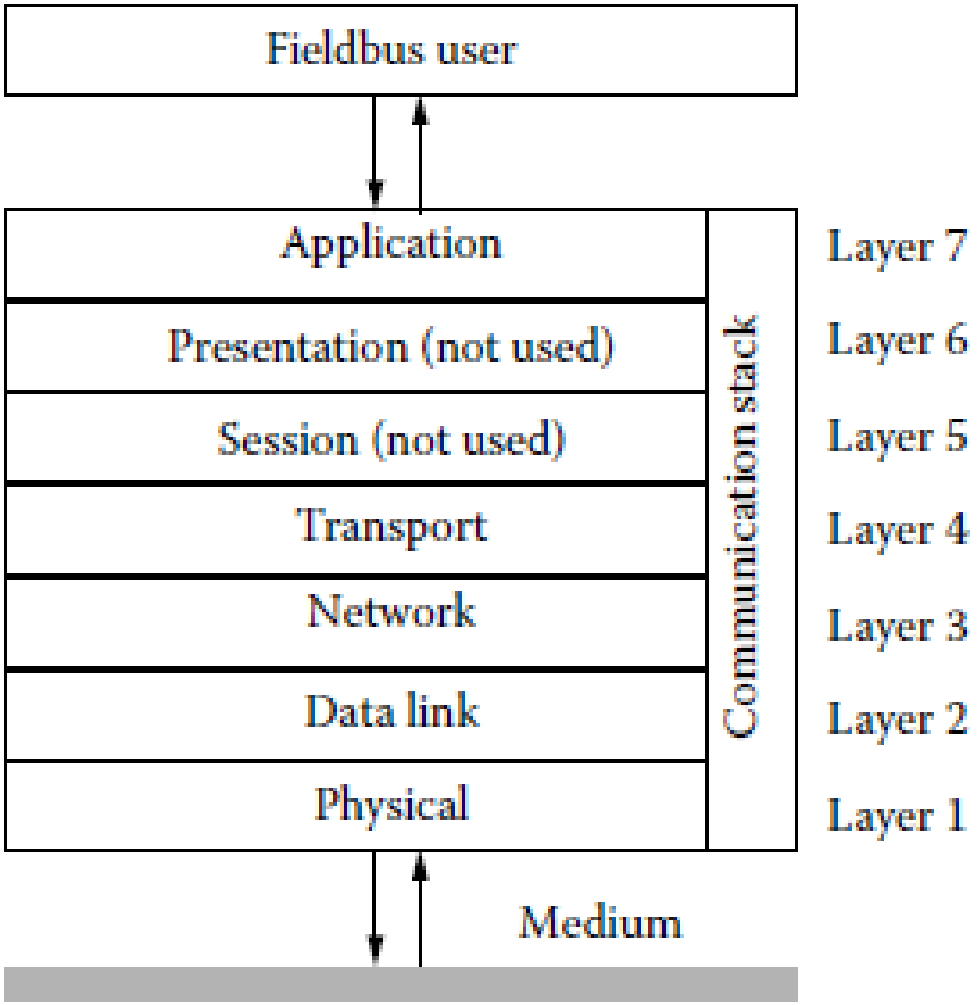
# Mesh topology

- In this type of topology, a host is connected to one or multiple hosts.
- This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.



# ISO/OSI Protocol Reference Model

- The Open Systems Interconnection Model was published in
- 1978 and aimed to bring uniformity and transparency into
- communication network standards.
- It defines a communication model that is applicable to all network devices, from mainframe computers operating at enterprise level to simple actuators in the field.
- It makes no physical specifications: rather, it provides a framework in which communications standards can be placed.
- The OSI model splits the communication process into seven functional levels or "layers,"




*ISO-OSI communications model.*

# Layers of OSI model

- **Physical layer:**
  - This layer defines the electrical and mechanical characteristics of the interface-between the physical communication medium and-the driver and receiver electronics like modems, network adapters, cables, hubs etc. These characteristics include voltage levels. Channel structure and the signalling or modulation technique used by the hardware to transmit the data:
- **Data link layer :**
  - The function of this layer is to determine which element has control-of the hardware at any given time. It also structure the transmission of messages from one element-to another at the bit level.
  - defines the error detection and error correction techniques used and sets up the conventions for defining the start and stop of each message
- **Network layer:**
  - This layer handles the routing of messages from one client to another. In a communication system consisting of multiple subnetworks, this layer handles the translation of addresses and routing of information from one subnetwork to another.

# Layers of OSI model

- **Transport layer**
  - Ensures the end-to-end message transmission
  - The services provided by the transport protocol layer include acknowledging messages, detecting end-to-end message errors and retransmitting the messages, prioritising messages and transferring messages to multiple receivers
- **Session layer**
  - This level of protocol schedules the starting and stopping of communication activity between two elements in the system.
  - It may also specify the quality of transport service required if multiple levels of service are available.
- **Presentation layer**
  - This layer translates the message formats in the communication system into the information formats required by the next higher layer, the application layer.
  - The presentation layer allows the application layer to properly interpret the data sent over the communication system and.

# Layers of OSI model

- **Application layer**
  - This layer is not strictly part of the communication protocol, structure; rather. it is the part of the application software or firmware that calls up the communication services at the lower layers.
  - In a high level language program, it might be a statement such as READ/COM or INPUT/COM that requests information from another system element over the communications facility.
  - In a function block logic structure, it would be an input block that requests a certain process variable to be read from another system clement over the communications facility .

# OSI layer protocols

| Layer | Name | Protocols |
|---|---|---|
| Layer 7 | Application | SMTP, HTTP, FTP, POP3, SNMP |
| Layer 6 | Presentation | MPEG, ASCH, SSL, TLS |
| Layer 5 | Session | NetBIOS, SAP |
| Layer 4 | Transport | TCP, UDP |
| Layer 3 | Network | IPV5, IPV6, ICMP, IPSEC, ARP, MPLS. |
| Layer 2 | Data Link | RAPA, PPP, Frame Relay, ATM, Fiber Cable, etc. |
| Layer 1 | Physical | RS232, 100BaseTX, ISDN, 11. |

# Types of Networks in Industry

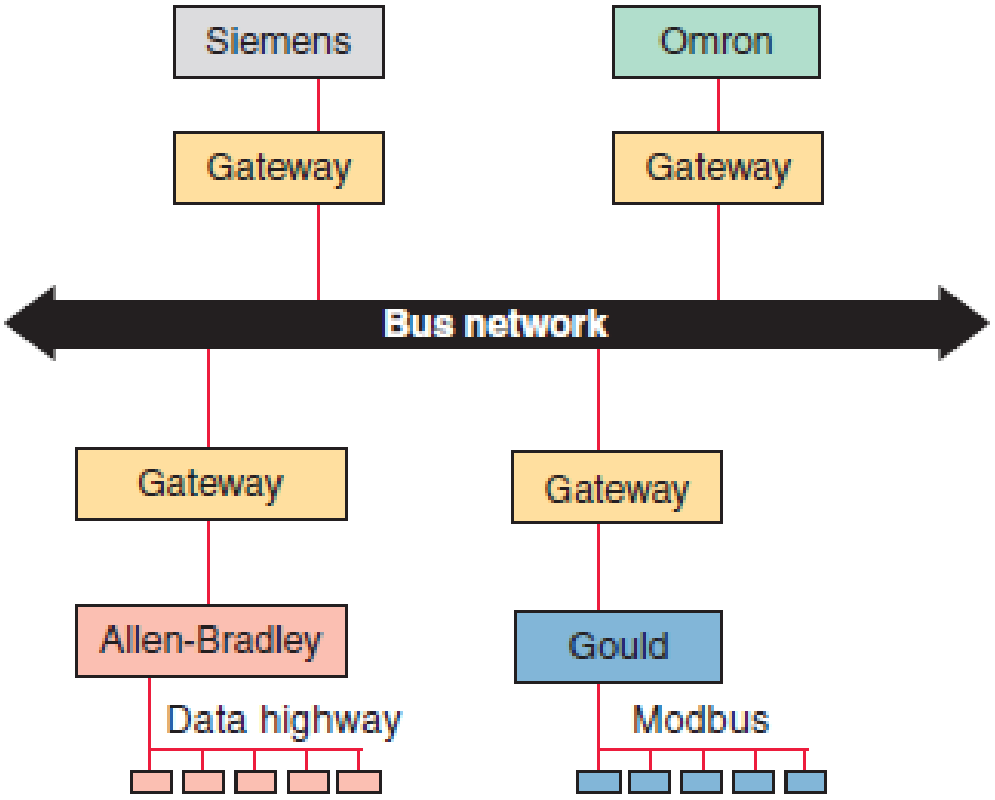
- I/O bus networks can be divided into two categories:
- Device bus networks and
- process bus networks.
- *Device bus networks* interface with low-level information devices such as pushbuttons and limit switches that primarily transmit data relating to the on/off state of the device and its operational status.
- Device bus networks can be further classified as
- bit-wide or byte-wide buses.

- Device bus networks that include discrete devices as well as small analog devices are called *byte-wide bus networks*.
- These networks can transfer 50 or more bytes of data at a time.
- Device bus networks that interface only with discrete devices are called *bit-wide bus networks*.
- Bit-wide networks transfer less than 8 bits of information to and from simple discrete devices.

# *Process bus networks*

- *Process bus networks* are capable of communicating several hundred bytes of data per transmission.
- The majority of devices used in process bus networks are analog, whereas most devices used in device bus networks are discrete.
- Process bus networks connect with high-level information devices such as smart process valves and flowmeters, which are typically used in process control applications.
- Process buses are slower because of their large data packet size.

# Gateways




Translating from one network-access scheme to another.

# *Gateways*

- *Gateways* make communication possible between different architectures and protocols.
- They repackage and convert data going from one network to another network so that the one can understand the other's application data.
- Gateways can change the format of a message so that it will conform to the application program at the receiving end of the transfer.
- If network access translation is their only function, the interfaces are known as *bridges*.
- If the interface also adjusts data formats or performs data transmission control, then it is called a *gateway*.

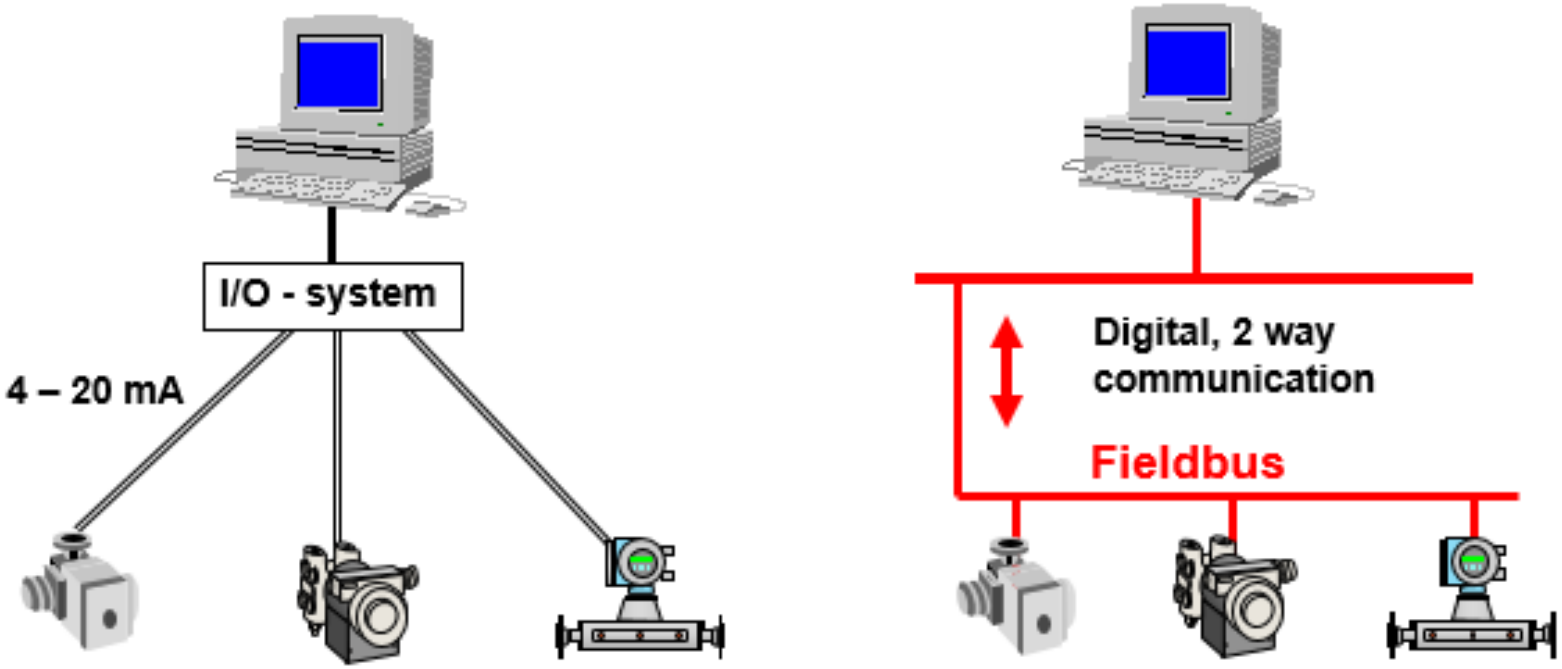
# Field Bus

- From the industry point of view the **Field** is an abstraction of the plant levels.
- As for the term **Bus** is a well-known word in computer science as a set of common line that electrically (or even optically) connects various units (circuits) in order to transfer the data among them.
- Fieldbus is an open, serial, two-way communications system that interconnects measurement and control equipment such as sensors, actuators, and controllers.
- At the base level in the hierarchy of plant networks, it serves as a network for field devices used in process control applications.

# Field Bus

- The origin of the fieldbus was to replace any point-to-point links between the field devices (Field Devices are simply the Sensors and Actuators of the plant) and their controllers (like **PLC**'s, **CNC**'s …etc.) by a digital single link on which all the information is transmitted serially and multiplexed in time.

# What is a fieldbus ?



# What is a fieldbus ?

- Fieldbus is a new digital communication network which will be used in industry to replace the existing 4 - 20mA analogue signal.

- The network is a digital, bi-directional, multidrop, serial-bus, communications network used to link isolated field devices, such as controllers, transducers, actuators and sensors.

- Each field device has low cost computing power installed in it, making each device a 'smart' device. Each device will be able to execute simple functions on it's own such as diagnostic, control, and maintenance functions as well as providing bi-directional communication capabilities.

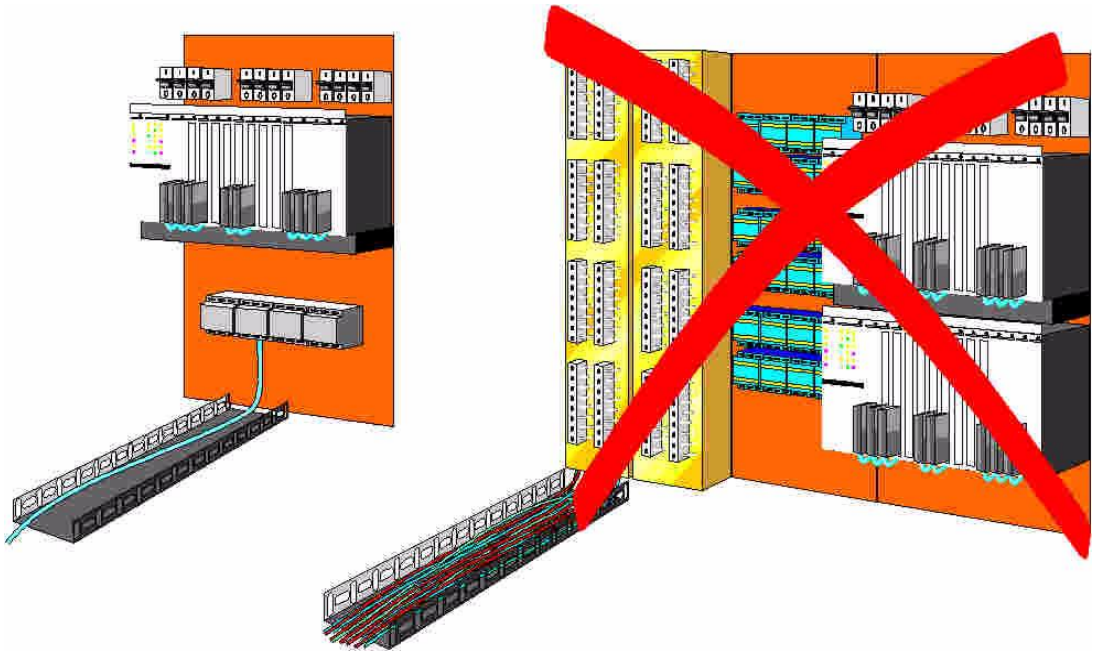
# What is a fieldbus ?

- In essence fieldbus will replace centralized control networks with distributed-control networks.

- Fieldbus is considered as a network that connects the field devices at the factory floor together with the controllers.

# What are the fieldbus Advantages?

- Reduced cabling
- Less hardware
- Simpler configuration
- Simpler maintenance
- Rreliability
- Flexibility
- More information from process to business level



# Fieldbus Advantages?

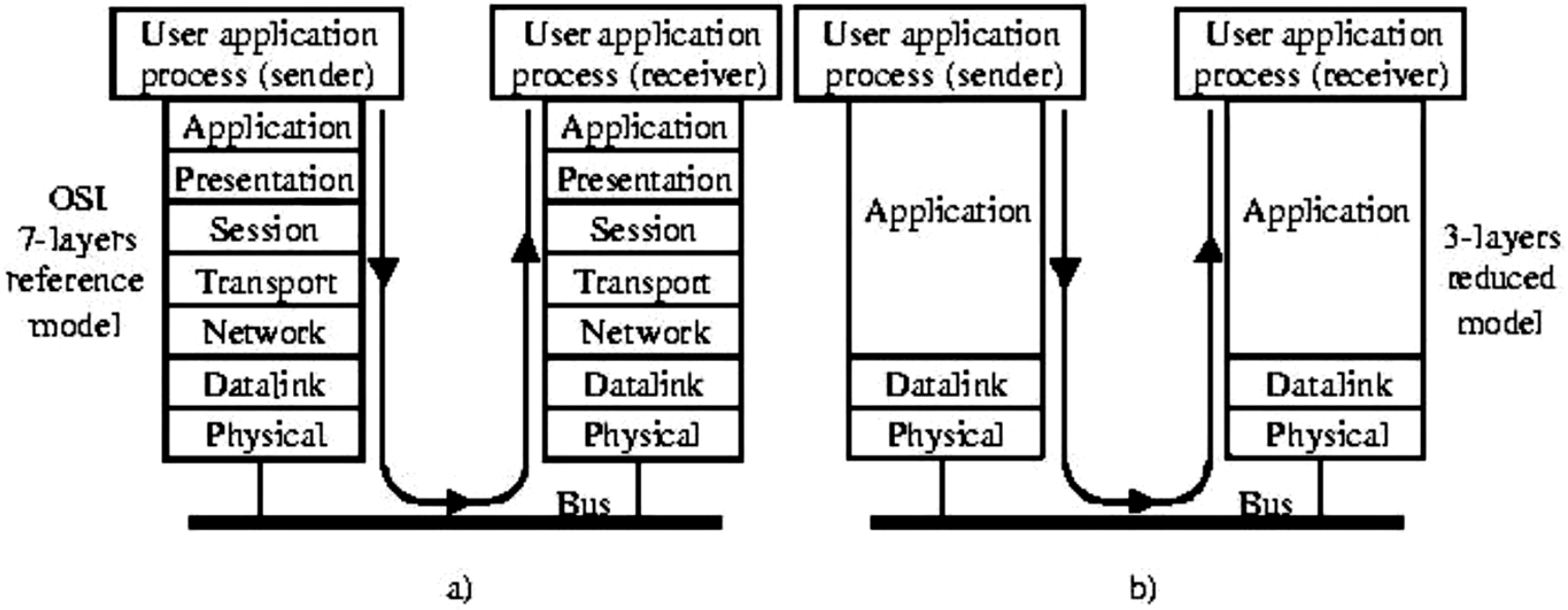
- The most obvious benefit from a fieldbus system is the reduction of cables. This means savings in cost and weight (important on e.g. ships and oil platforms) – and a tidier system without the mess that a multi-cabling system gives.

- Since all Digital/Analog or Analog/Digital transformations have to be done in the instruments, we will also see that fieldbus systems have less hardware components. So, even though a fieldbus instrument usually is more expensive than a traditional one, the overall hardware cost may be lower.

- Less components and less cables mean a system that can easier be configured and maintained. This means also a more reliable system. Fieldbus systems also have special configuration and documentation tools that will help further.

- Using a **standard, open** fieldbus will give high flexibility. Fieldbus instruments from different vendors can communicate directly on the same bus ( **interoperability** ), and a field instrument can easily be changed with another during run time (**interchangeability**).

# Fieldbus characteristic




**The OSI 7-layers reference model (a), and the reduced fieldbus 3-layer structure (b).**

# Fieldbus characteristic

- Fieldbus protocol are modeled according to the ISO/OSI model. Only layer 1, 2 and 7 based on OSI model are used.
- Only layer 1, 2 and 7 are used because that full seven layer stack requires too many resources and doesn't have an efficient implementation. It is a three layer structure consisting of physical layer, data link layer and application layer.
- But if the function of layer 3 and 4 as well as 5 and 6 still needed they are frequently included in layer 2 or 7.

# Fieldbus characteristic

- For example, the main function of the presentation layer, which is to support the interoperability between different equipment's, is done now by the application layer in the fieldbus.
- The assembling and disassembling of data packets which was the function of the transport layer is done now by the datalink layer in the fieldbus network.
- If routers to be used in some fieldbus networks, then the routing service, which was assigned to the network layer, is done by the application layer in most cases in the fieldbus.

# Communication paradigms

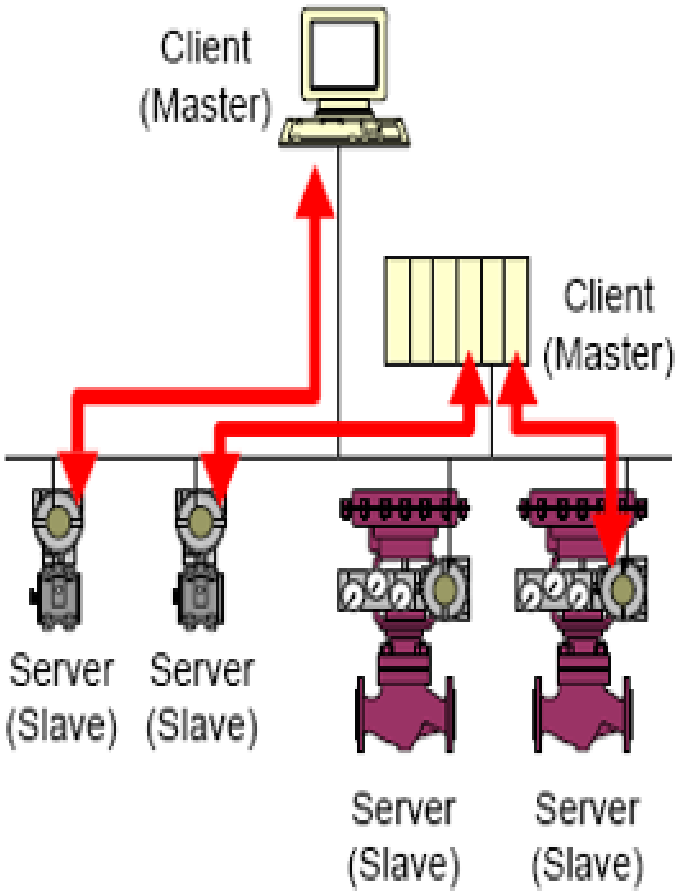
- There are 3 basic communication paradigms in Fieldbus namely
- Client-Server Model
- Producer-consumer Model
- Publisher-subscriber Model

# Client-server model

- A device such as a host workstation or PLC is the master that sends requests to read or write a value to other devices such as field instruments, which are called *slaves*. The slave that was addressed then responds to the request.

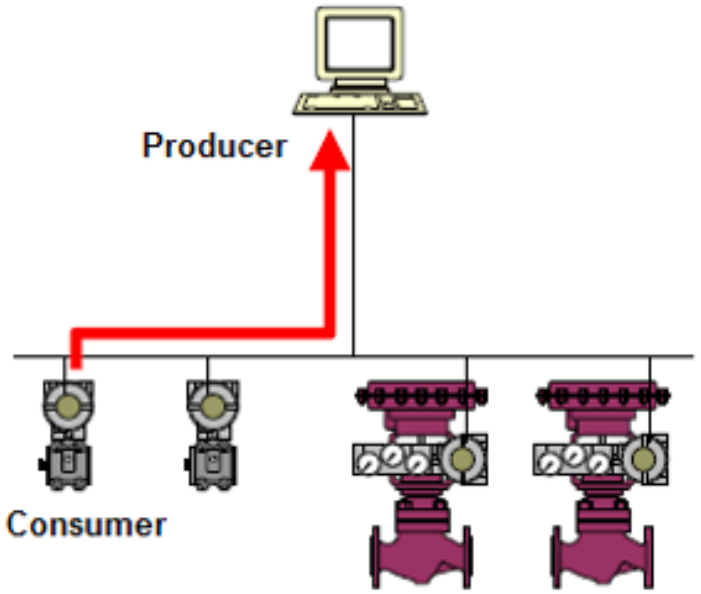
- A device (master) acting as a client requests, and the device (slaves) acting as server responds.

- An example of the client/server configuration is a master PLC reading a process value from a slave transmitter and then after executing a control algorithm writing the output to a slave positional.



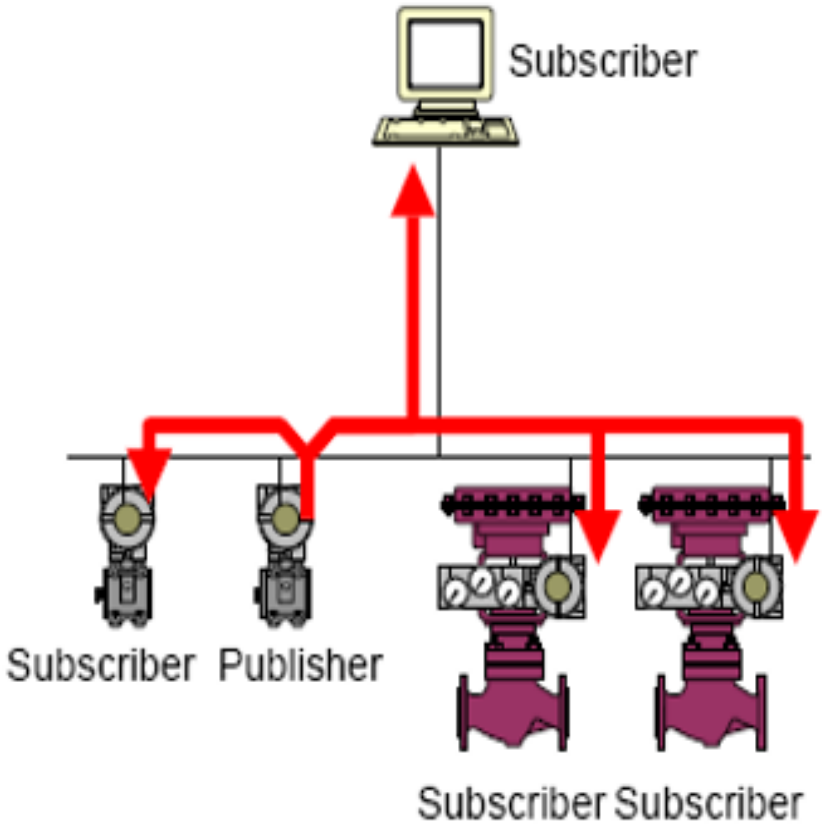
# Producer-consumer model

- A device acting as a "producer" transmits a message to a device acting as a "consumer" without the consumer having to solicit the data.
- While the state remains the same it is not communicated. The transmission is only made when there is a change of state sometimes called "report by exception", e.g. when an alarm occurs.
- This configuration is ideal for environments where operators want devices to report process alarms or fault events as they occur, while otherwise remaining silent.



# Publisher-subscriber model

- An ideal case for a cyclic communication
- A device acting as a "publisher" broadcasts a value that is then used by all interested devices, which act as "subscribers".
- This is very efficient because the value is transmitted directly from one field device to another in one single communication, reaching several subscribers at once.



# Properties of communication paradigms

| | Client–Server Model | Producer–Consumer Model | Publisher–Subscriber Model |
|---|---|---|---|
| Communication relation | Peer to peer | Broadcast | Multicast |
| Communication type | Connection oriented | Connectionless | Connectionless |
| Master–slave relation | Monomaster, multimaster | Multimaster | Multimaster |
| Communication service | Confirmed, unconfirmed, acknowledged | Unconfirmed, acknowledged | Unconfirmed, acknowledged |
| Application classes | Parameter transfer, cyclic communication | Event notification, alarms, error, synchronization | State changes, event-oriented signal sources (e.g., switches) |

# Fieldbuses and the IEC61158 standard

- International standardization organizations have worked for many years in order to get an agreement on a common fieldbus standard.
- But it seems that it is still a long way to go to get something comparable to the old 4 – 20 mA standard. Or – perhaps we never will get there.
- Among the existing fieldbuses some are better in one system, some other in another system.
- In year 2000 it came a document, the IECC 61158 standard, which includes 8 different fieldbuses in the same standard.
- The 8 fieldbuses included in this Octobus standard are:
  - ControlNet
  - FF – H1 (Foundation Fieldbus)
  - FF – HSE (Foundation Fieldbus)
  - Interbus
  - P-Net
  - PROFIBUS
  - SwiftNet
  - WorldFip

# PROFIBUS

- PROFIBUS-DP (where DP stands for Decentralized Periphery) is an open, international fieldbus communication standard that supports both analog and discrete signals.
- It is functionally comparable to DeviceNet.
- The physical media are defined via the RS-485 or fiberoptic transmission technologies.
- PROFIBUS-DP communicate at speeds up to 12 Mbps over distances up to 1200 meters.

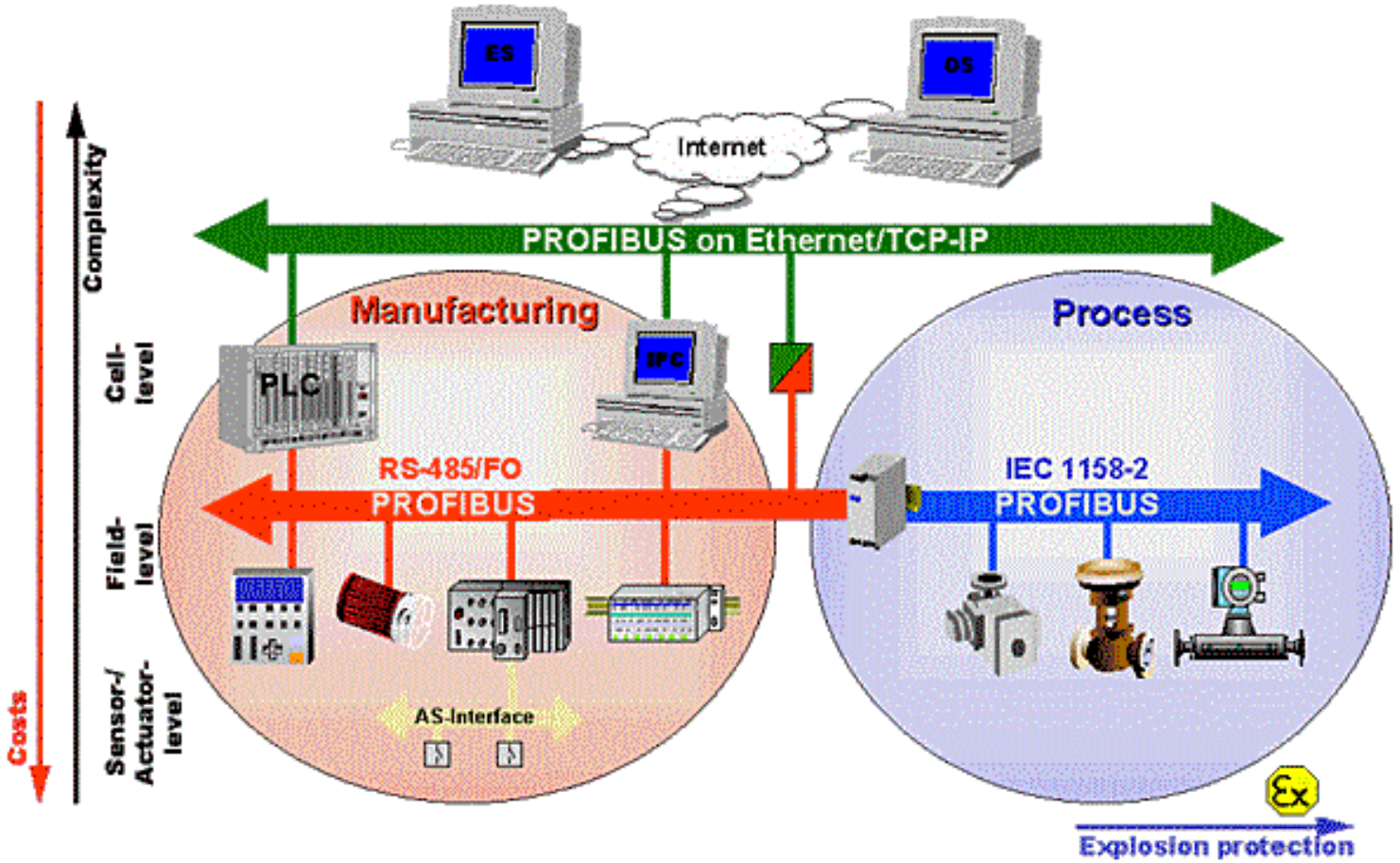
# ProfiBus

- PROFIBUS is a short form for PROcess FIeldBUS and is a vendor-independent, open fieldbus standard.

- It was developed in Germany as a joint project between several vendors. The most important ones : Siemens, Klöckner Möller (now Moeller Electric), and Bosch. The first specification was ready spring 1990. One year later it was taken in as a part of the german standard (DIN 19245) and became later a European standard (EN 50170).

- PROFIBUS is now part of the new international, Octobus standard IEC 61158.

- The PROFIBUS uses the IEC 1158-2, RS-485 or Fiber Optic technology. With the new PROFInet, the PROFIBUS will open up for the communication on Ethernet


ES
OS
Internet
PROFIBUS on Ethernet/TCP-IP
Manufacturing
Process
PLC
IPC
RS-485/FO
PROFIBUS
IEC 1158-2
PROFIBUS
AS-Interface
Complexity
Costs
Cell-level
Field-level
Sensor-/Actuator-level
Explosion protection

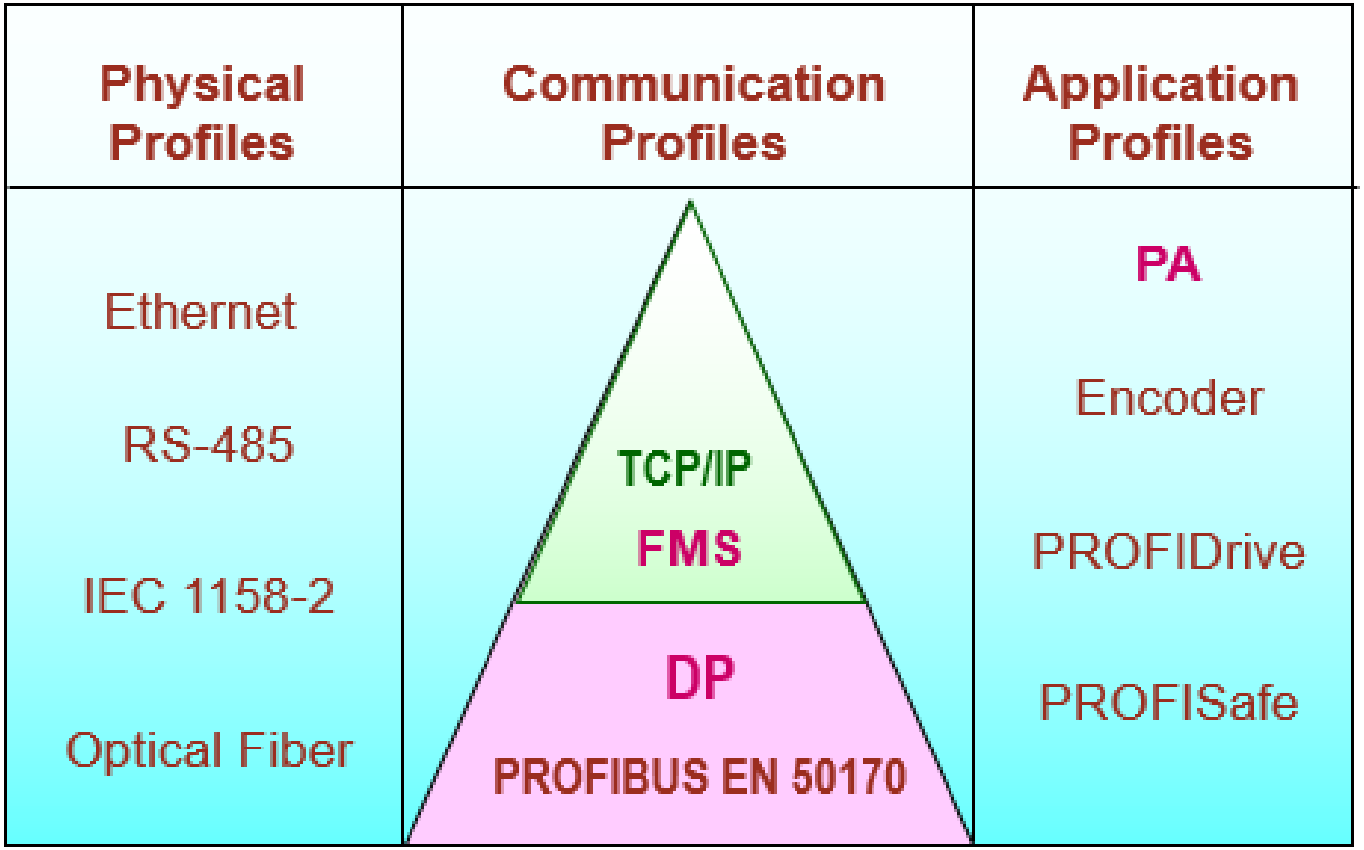
# Profibus

- In PROFIBUS we use the term **Profile** for different components :

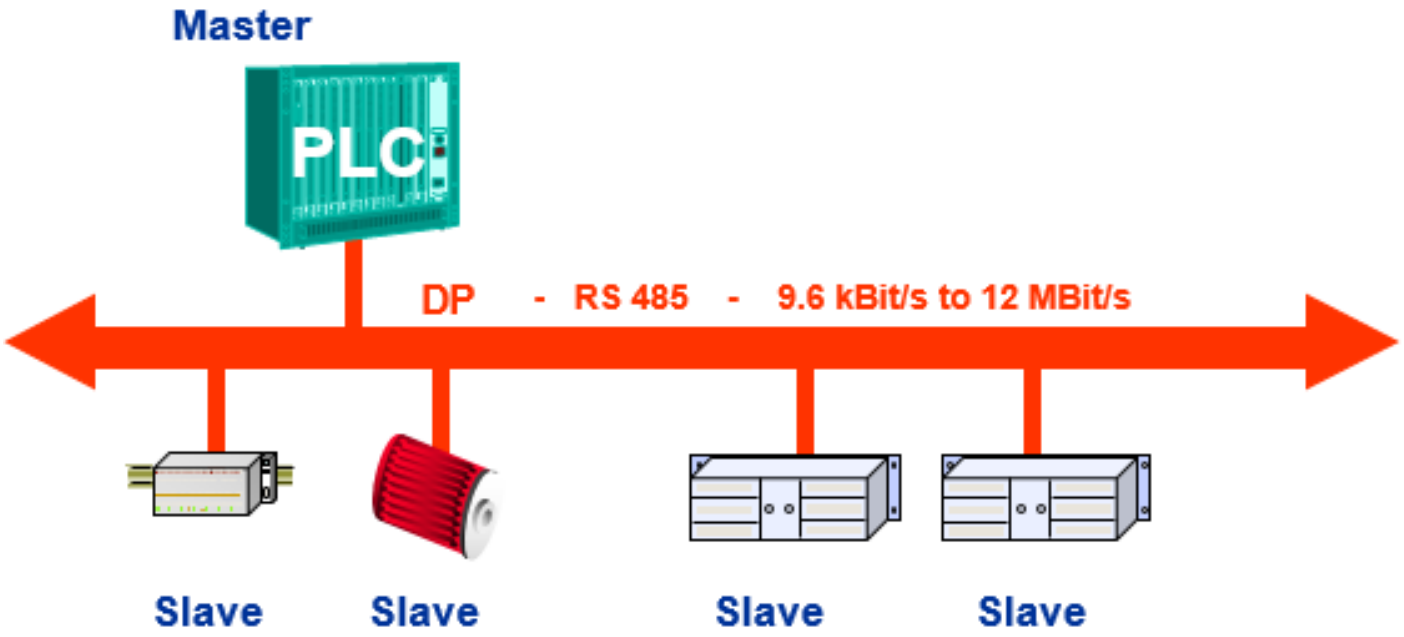
- ***Station types*** : ***Application Profiles*** (PA-devices, Encoders, Drivers, ..)
- ***Protocols*** : ***Communication Profiles*** ( DP, FMS, TCP/IP)
- ***Signal transmission: Physical Profiles*** (RS-485, IEC1158-2, O.F., Ethernet)

- This design philosophy enhances transparent communication both horizontally and vertically in a company. While PROFIBUS DP and PROFIBUS FMS are two compatible protocols, PROFIBUS PA is an application profile using the PROFIBUS DP protocol.

- PROFIBUS DP and PROFIBUS FMS use the same transmission technology, Fiberoptics or RS 485 (0 / 5V signals), but PROFIBUS PA, on the other hand, use the IEC 1158-2 transmission technology ( 0 / 20 mA).


Physical Profiles
Communication Profiles
Application Profiles
Ethernet
RS-485
IEC 1158-2
Optical Fiber
TCP/IP
FMS
DP
PROFIBUS EN 50170
PA
Encoder
PROFIDrive
PROFISafe

# DP : Distributed Peripherals



# DP : Distributed Peripherals

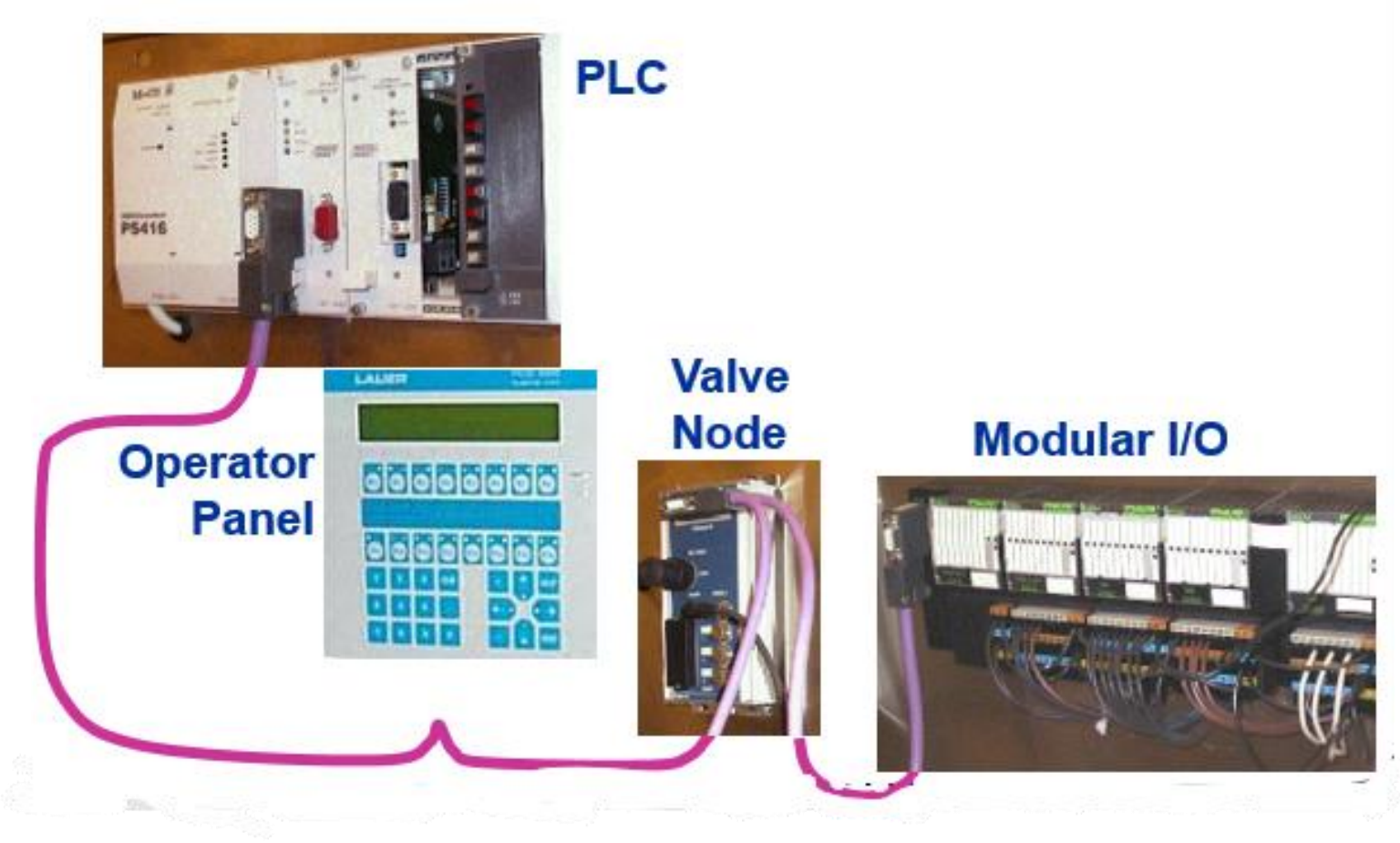
- The objective of PROFIBUS DP is fast and effective communication on the field level. It uses RS 485 (Voltage levels 0 and 5 V) or Fiber Optics. The baudrate can be chosen from 9.6 kBit/s to 12 Mbit/s. The cycle time will also depend on the amount of data to be transmitted.

- The communication is build on the master/slave principle, with typically a PLC or a PC as a master and several stations as slaves: Digtal I/O, Analogue I/O, AC or DC drives, Magnetic or pneumatic valves, panels, etc.

- The DP stations must be assigned a unique address, a number (0 to 126). One master can handle at most 126 slaves. Each station can send or receive a maximum of 244 bytes.

- In RS 485, the network needs a repeater for every 32 stations. A repeater is also needed if the cable distance is long (100m at 12 Mbit/s, 1200m at 9.6kBit/s). The total length of the network can not exceed 10 km.

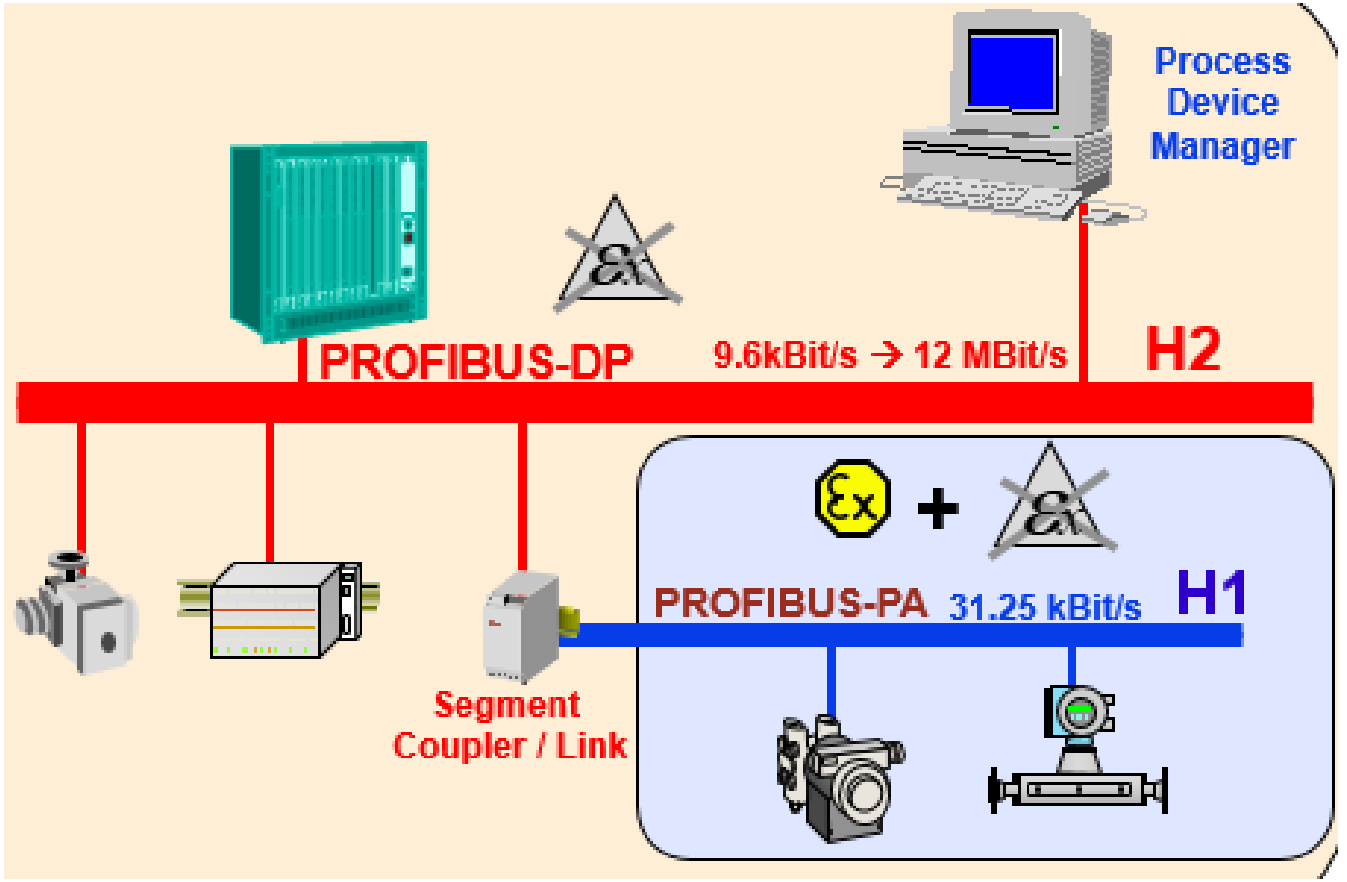
# DP - Example



# DP Example

- The picture above shows some of the instruments on production machine. It shows a PLC, a panel, a pneumatic valve node and a modular I/O station.
- The PLC is the master, the other three are slaves.
- The modular station is expandable with both analogue and digital I/O's .
- All the stations are connected to the same PROFIBUS cable

# PA : Process Automation



# PA : Process Automation

- The two main reasons for choosing a PA solution are :

**1. Intrinsically safety:**

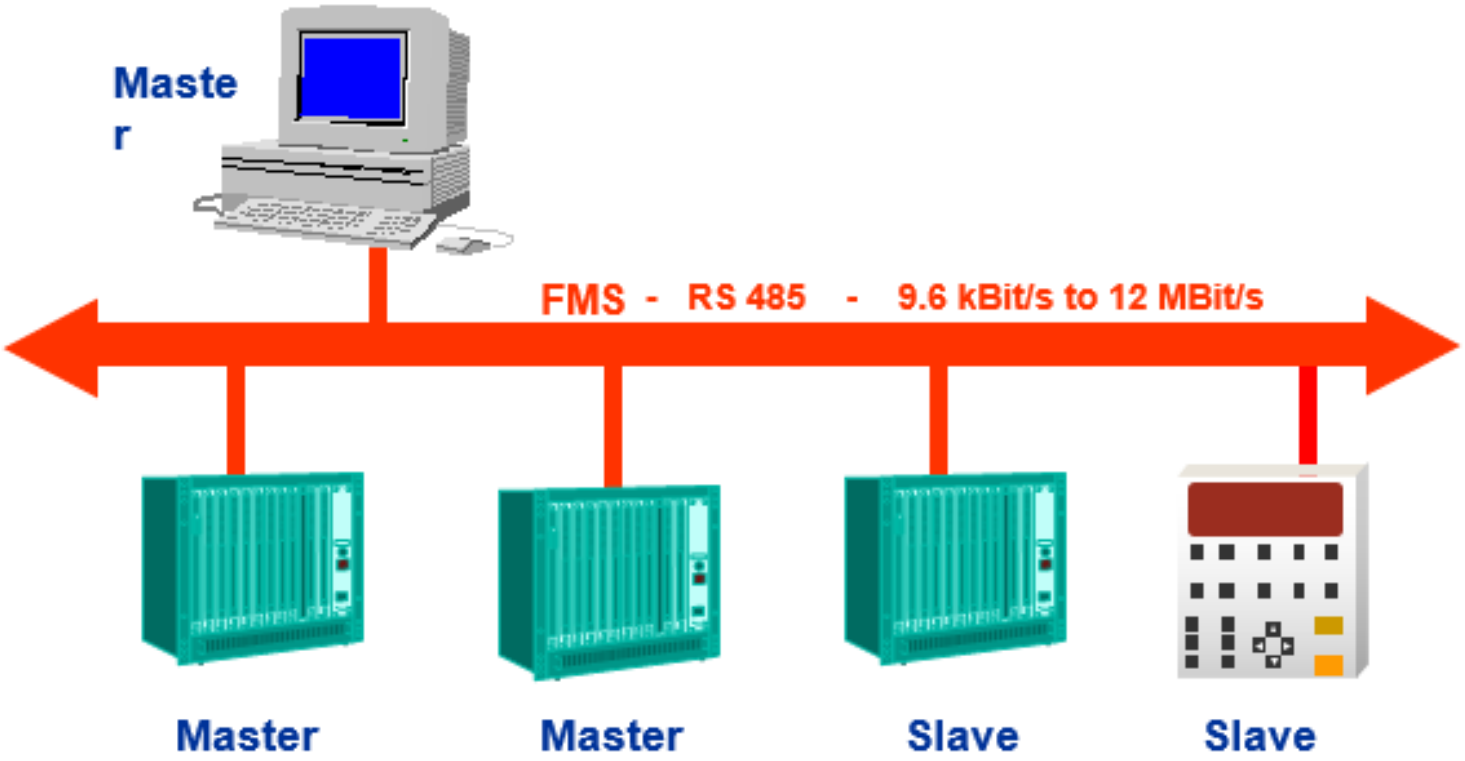
With PA it is possible to make intrinsically safe solutions.

**2. Powering over the bus**

The PA-instrument can get its power supply over the bus, on the same two wires as data is transmitted.

- PA uses the DP protocol, and it can not exist without a DP master. The PA network will be a part of a DP network.

# FMS : Fieldbus Message Specification

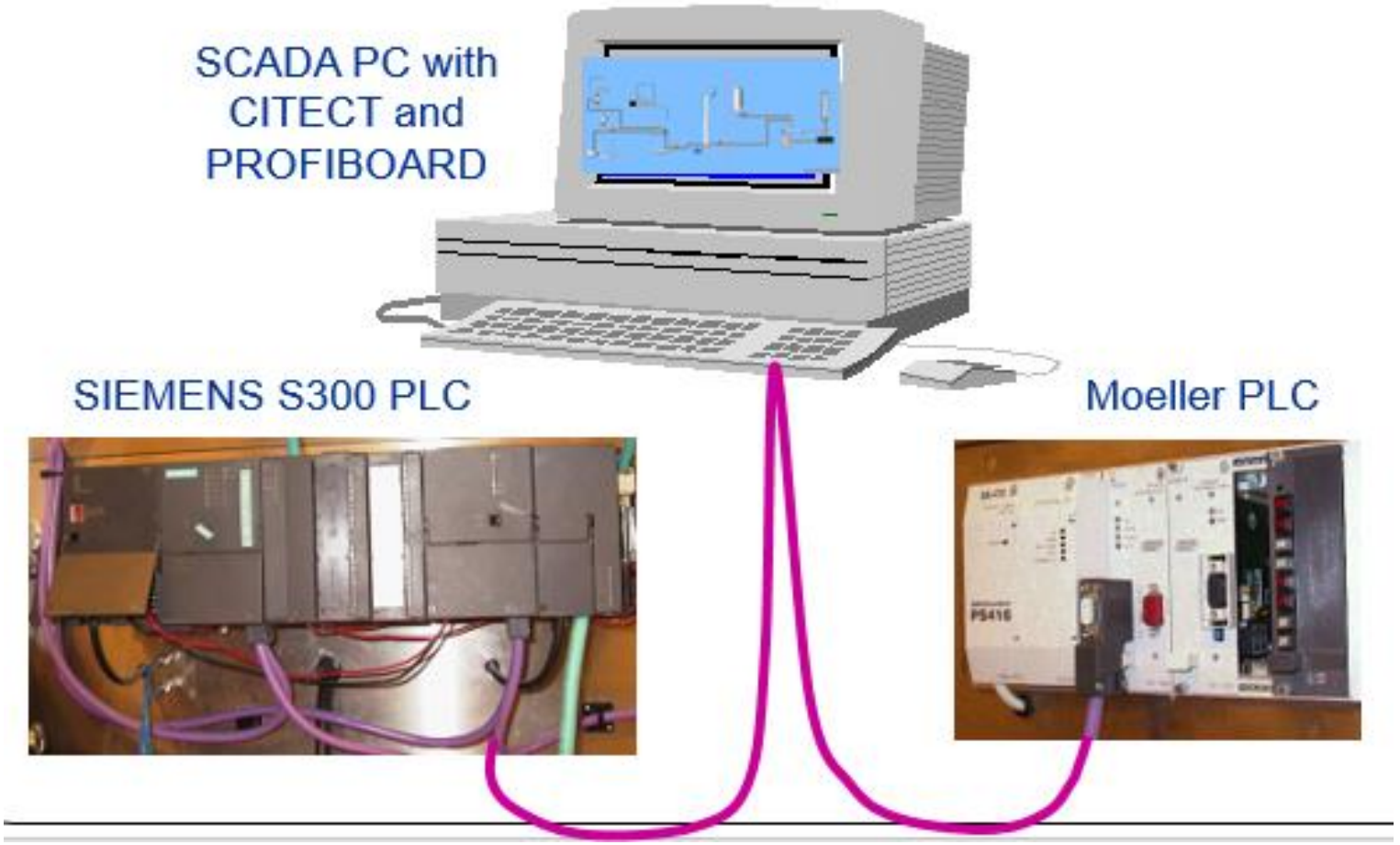


# FMS

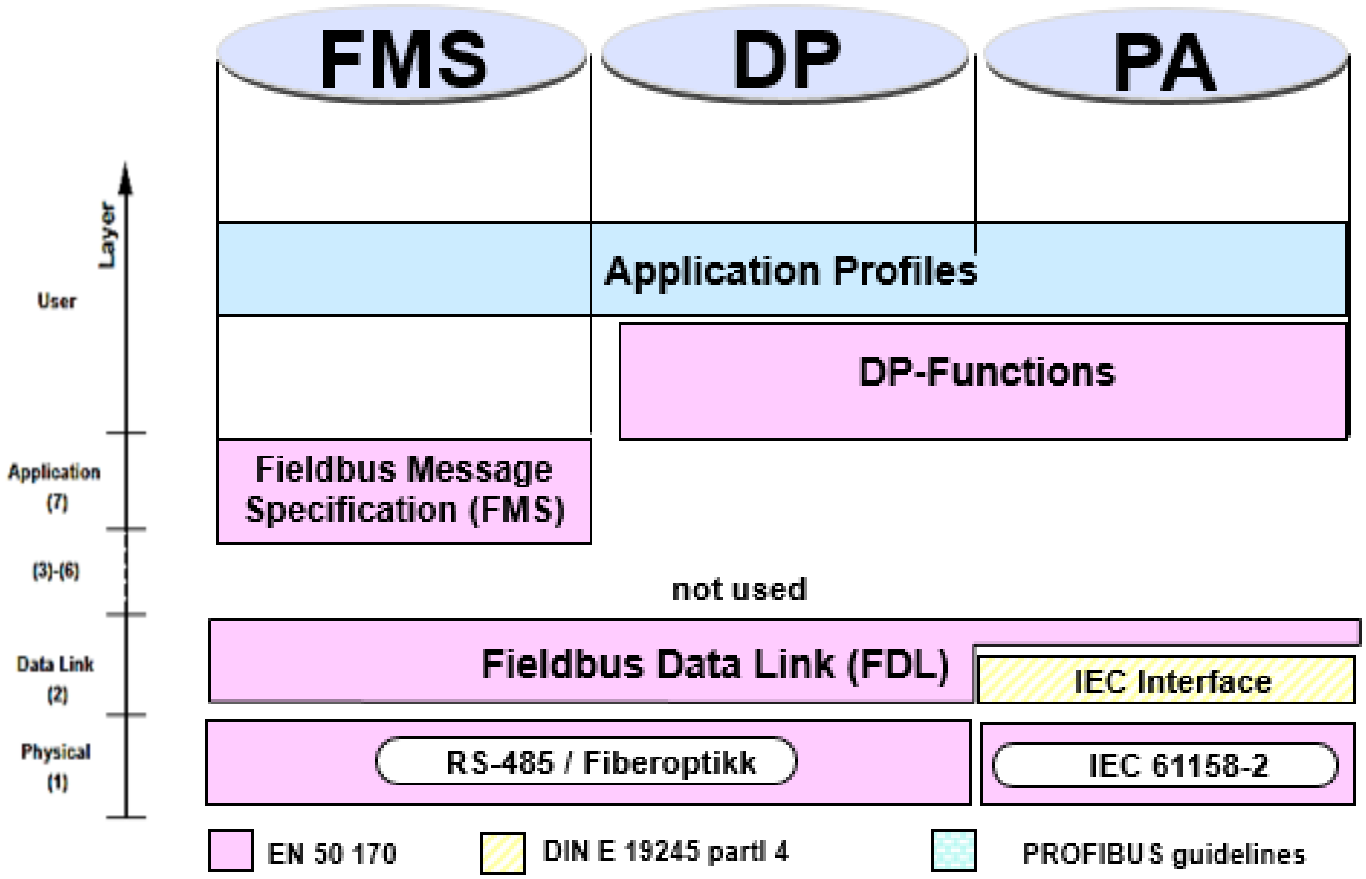
- The objective for FMS is multimaster communication at the cell level. It is better for the transmission of larger amounts of data like programs or data blocks. Typically we use FMS between PLCs and PCs.

- FMS uses the same signal transmission technology as DP: Fiber Optics or RS 485 with voltage signal levels. The baudrate of FMS is as for DP : 9.6 kBit/s to 12 Mbit/s.

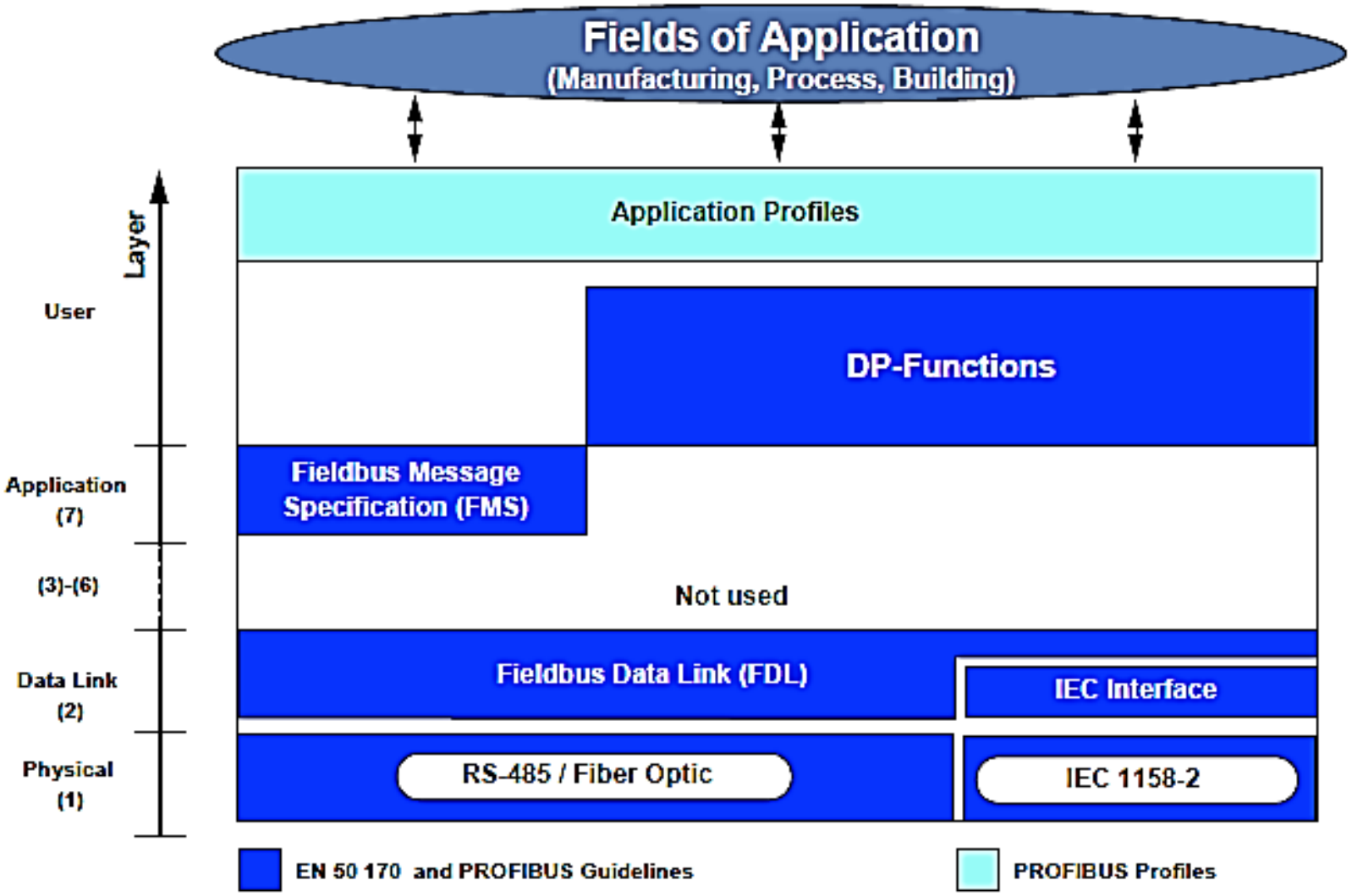
# FMS - Example


SCADA PC with
CITECT and
PROFIBOARD
SIEMENS S300 PLC
Moeller PLC

# The PROFIBUS protocols



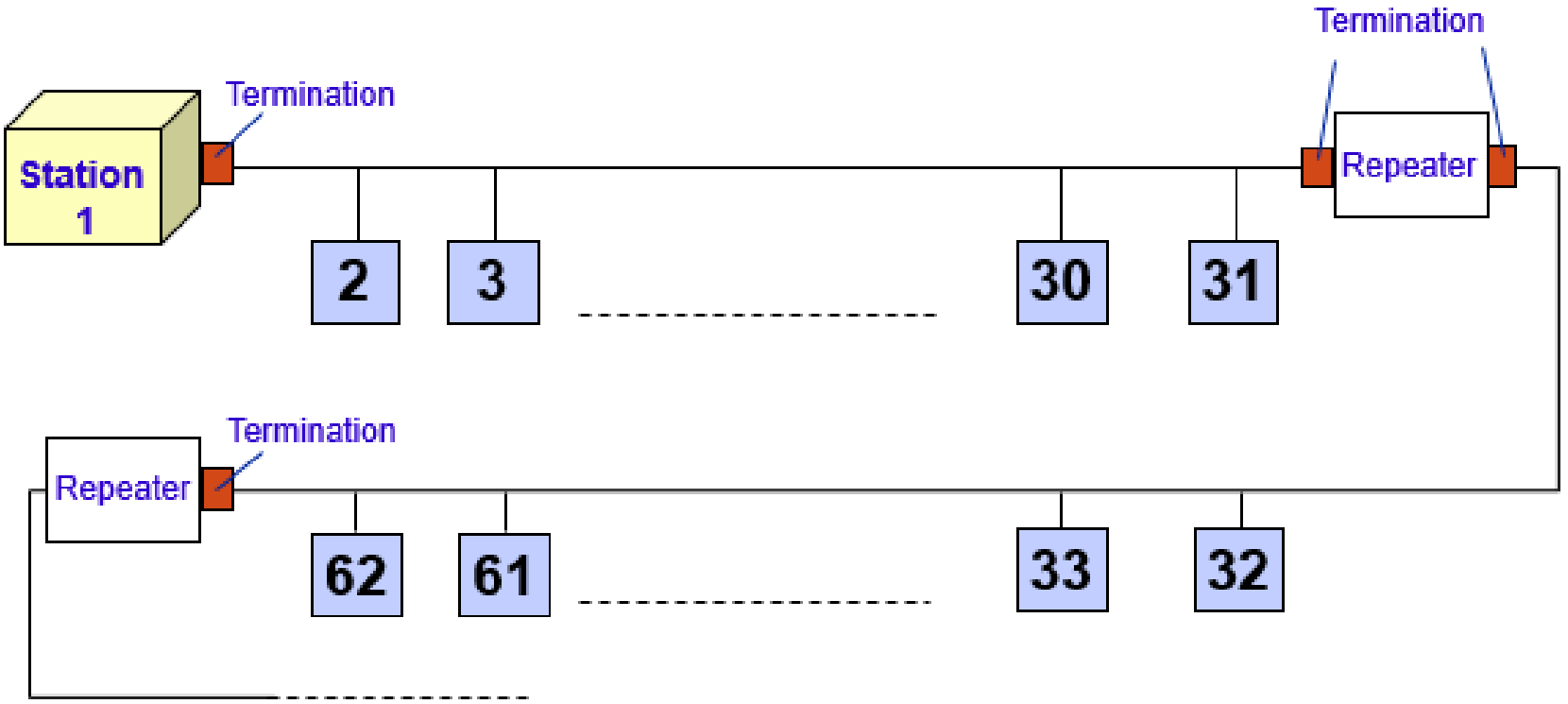
# The PROFIBUS protocols



# The PROFIBUS protocols

- The principles for the FMS, DP and PA protocols are shown above. FMS and DP use the same transmission technology. The physical layer for these two protocols follow the standard EN 50 170.
- The PA standard for this layer is IEC 61158-2.
- The next layer, the link layer, is equally described in all three protocols.
- At user level, DP and PA are equal and FMS is different.

# Stations, repeaters and segments



# Stations, repeaters and segments

- Each PROFIBUS station is given a unique address which should be a number between 0 and 126.
- This means that it can never be more than 127 stations in a network.
- If the cables are long or the number of stations exceeds 32, it is a need for repeaters.
- Each segment has to be terminated in each end as in the picture above.

# Reference


- Liptak, B.G., *Instrument engineers' handbook, volume two: Process control and optimization*, CRC press, 2018.
- Frank D. Petruzella, *Programmable Logic Controllers,* MGH, (2e), 1997.