

# Lecture 11

## Industrial Networking

### - An Introduction

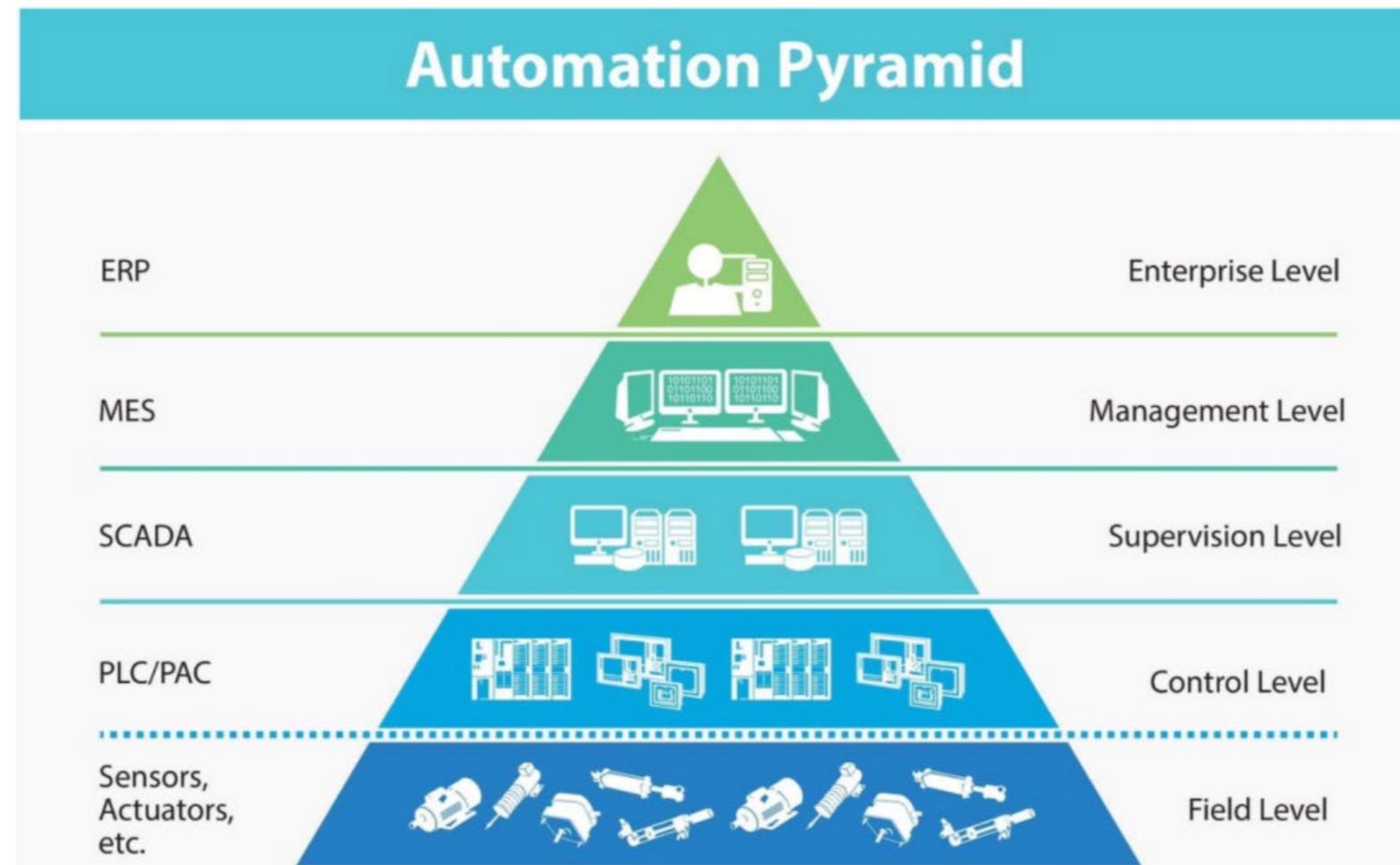
# Outline

- Industrial communication – Who is talking?
- Fieldbus, what and where?
- Computer networking – recap
- Modbus as an example
- Features/Properties of Fieldbuses
- CanOpen
- Ethernet as a basis
- PowerLink (CanOpen over Ethernet)
- Profinet
- Timeline

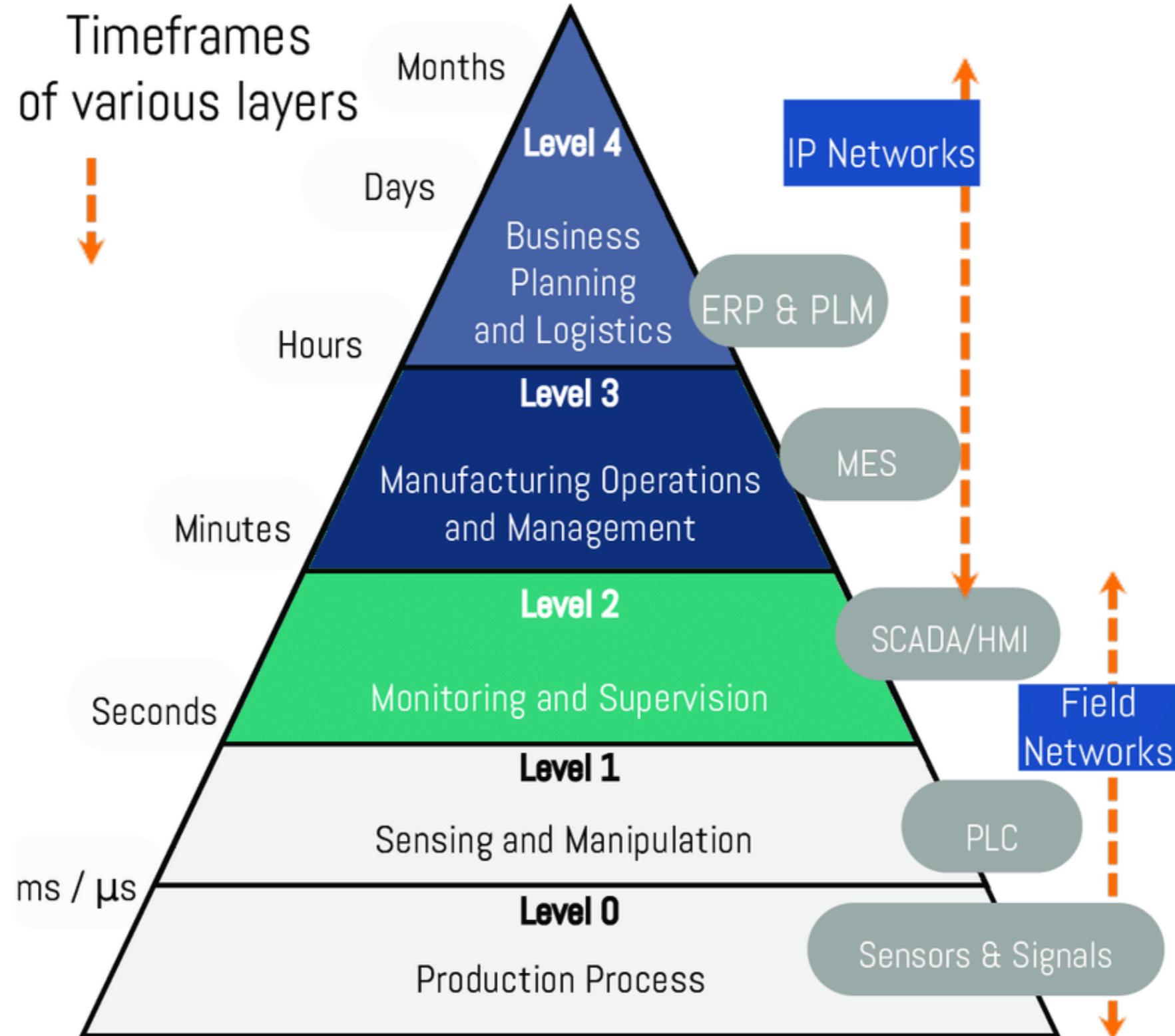
# Outline

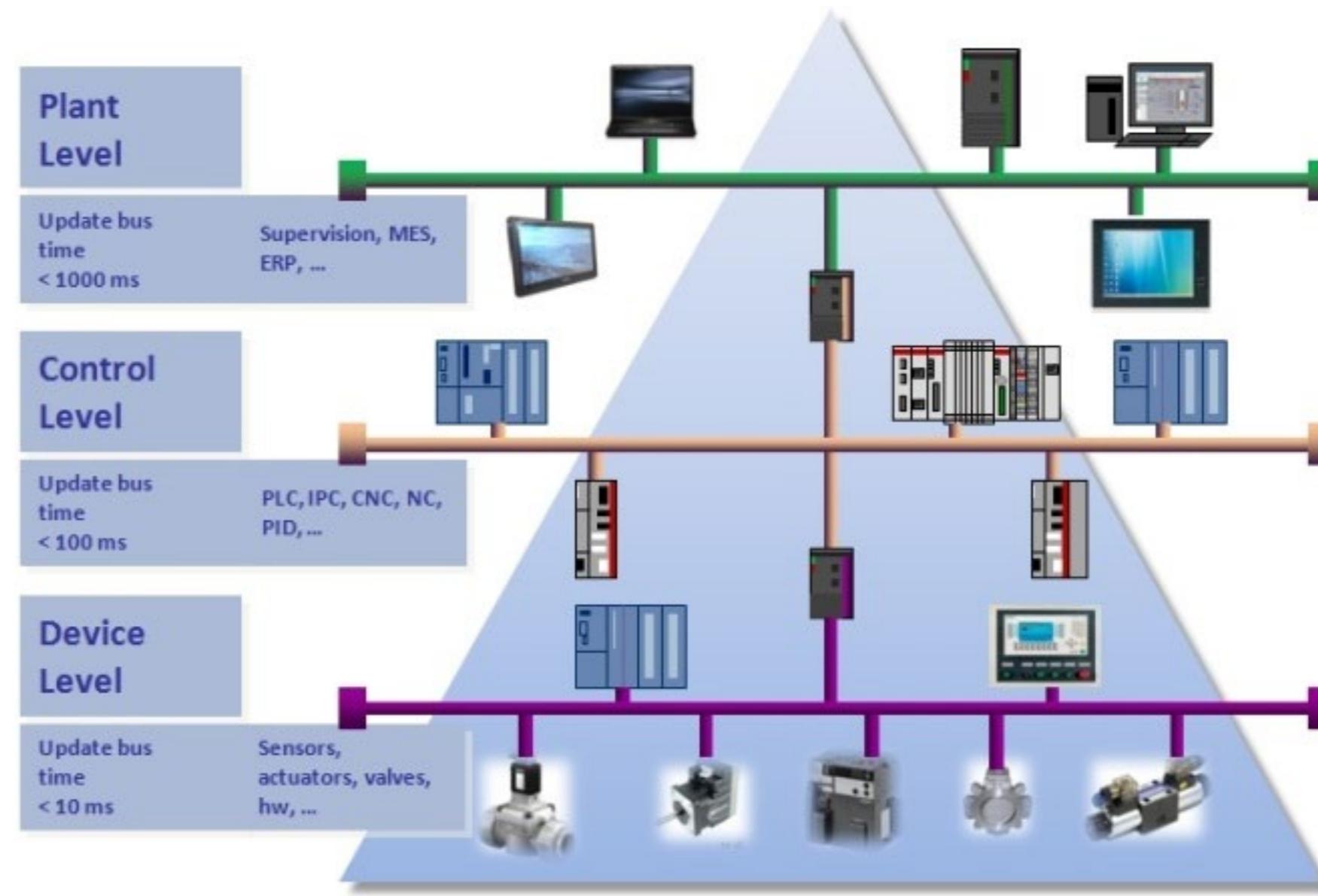
- Industrial communication – Who is talking?
- Fieldbus, what and where?
- Computer networking – recap
- Modbus as an example
- Features/Properties of Fieldbuses
- CanOpen
- Ethernet as a basis
- PowerLink (CanOpen over Ethernet)
- Profinet
- Timeline

# Automation pyramid



From: <https://integrated-controls.com/what-are-the-5-levels-of-automation/>



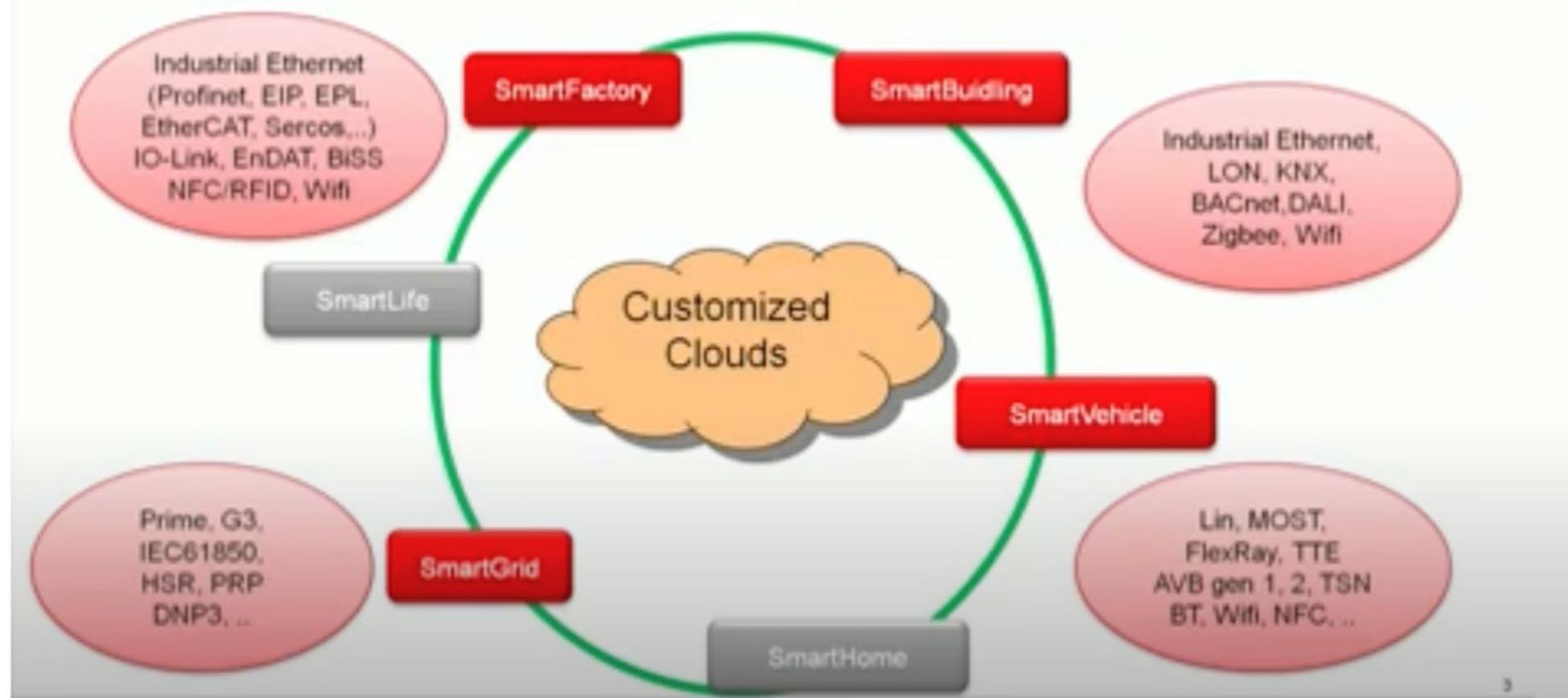


# What do we want to communicate?

- Digital values:
  - Motor running / stopped
  - Safety door open / closed
  - ...
- Integers / Floating points
  - Motor speed
  - Pressure
  - ...
- More complex / compounded data
- ...

# Domain /Industry

## The Industrial IoT has many Protocols



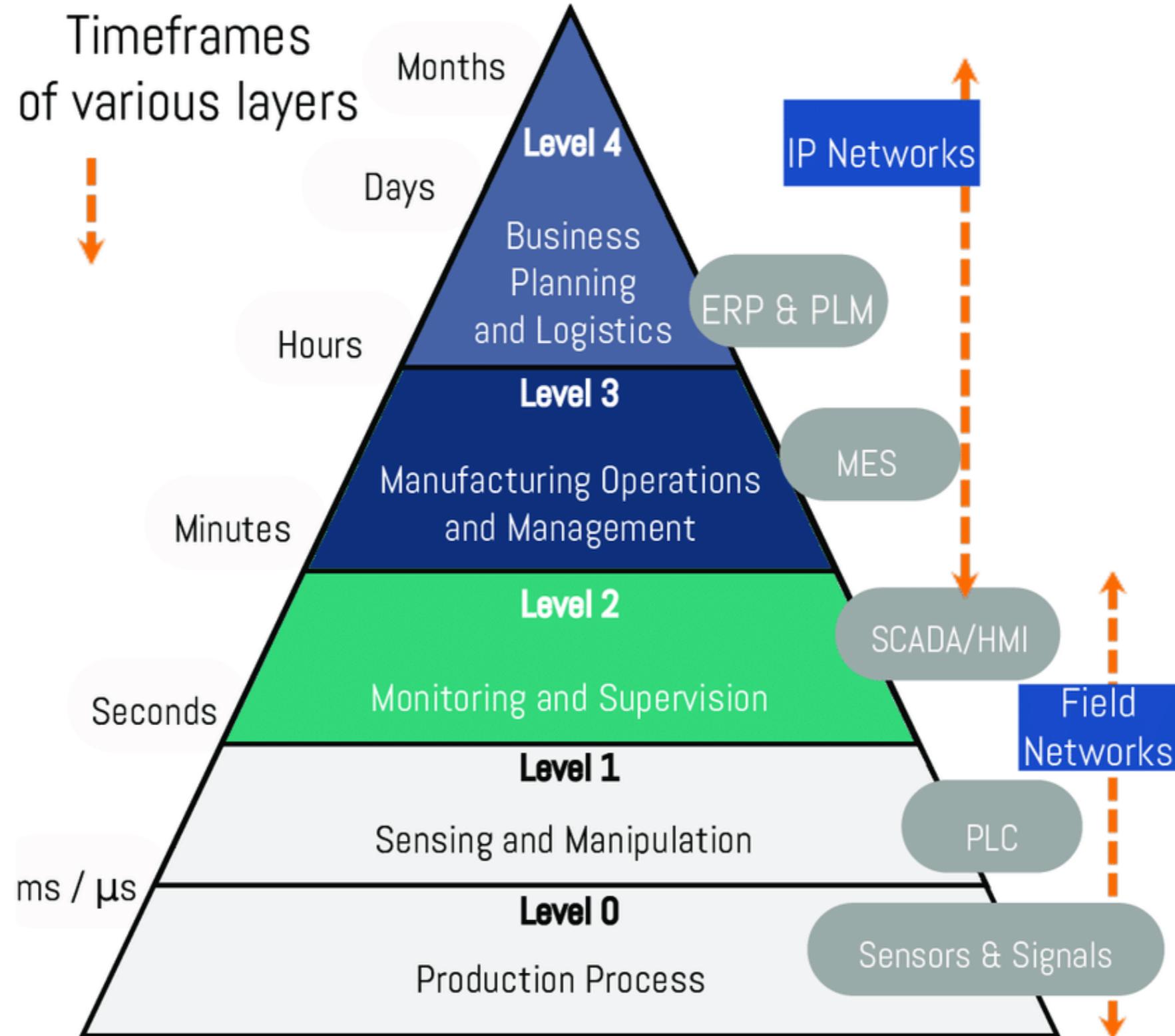
3

# Outline

- Industrial communication – Who is talking?
- Fieldbus, what and where?
- Modbus as an example
- Features/Properties of Fieldbuses
- CanOpen
- Ethernet as a basis
- PowerLink (CanOpen over Ethernet)
- Profinet
- Timeline

## Fieldbus defined

- Fieldbus - an industrial network system for real-time distributed control
- Fieldbus – open/proprietary, digital, multi-drop communications network for intelligent field devices



## Pre – fieldbus 1/2

How would the PLC communicate with sensors or actuators?

- Digital In / Digital out

- +24V / 0V

- Analog

- Voltage based

- 0 .. 10V; ...

- Current based

- 4 ... 20mA; ...

## Pre – fieldbus 2/2

### Challenges:

- Many cables
  - Limited distances (especially for voltage base analog)
  - Resolution (Analog)
  - Not easily scaleable
  - Diagnostics missing. Can errors be detected? (E.g., broken cable for 0...10V analog)

## First Iteration

Custom digital communication protocols, e.g., RS232

- Using established physical layer (e.g. cable, connector, voltage levels)
- User (Vendor) defined meaning of messages being sent around
  - **How to interpret the data the sensor is sending?**

# Outline

- Industrial communication – Who is talking?
- Fieldbus, what and where?
- **Modbus as an example**
- Features/Properties of Fieldbuses
- CanOpen
- Ethernet as a basis
- PowerLink (CanOpen over Ethernet)
- Profinet
- Timeline

# Modbus

- 1979 by Schneider Electric
- Royalty-free
- Different implementations:
  - Modbus RTU (serial based)
  - Modbus TCP/IP (ethernet based)
- Master / Slave
- **Register types:**



Primary tables	Object type	Type of	Comments
Discretes Input	Single bit	Read-Only	This type of data can be provided by an I/O system.
Coils	Single bit	Read-Write	This type of data can be alterable by an application program.
Input Registers	16-bit word	Read-Only	This type of data can be provided by an I/O system
Holding Registers	16-bit word	Read-Write	This type of data can be alterable by an application program.

# Modbus - Addressing

**coils - read/write**

**00001 - 09999**

**discrete inputs - read only**

**10001 - 19999**

**input registers - read only**

**30001 - 39999**

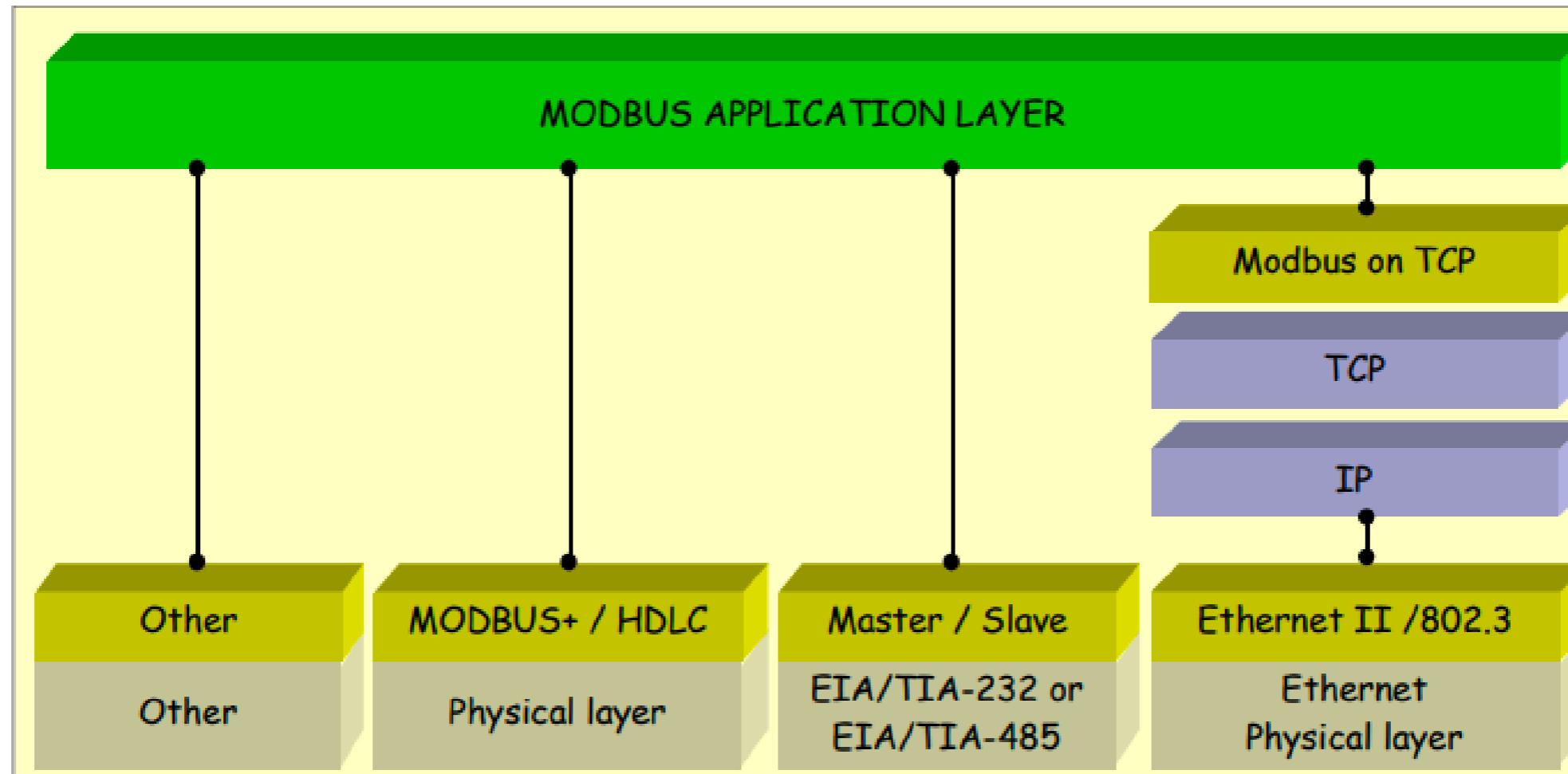
**holding registers - read/write**

**40001 - 49999**

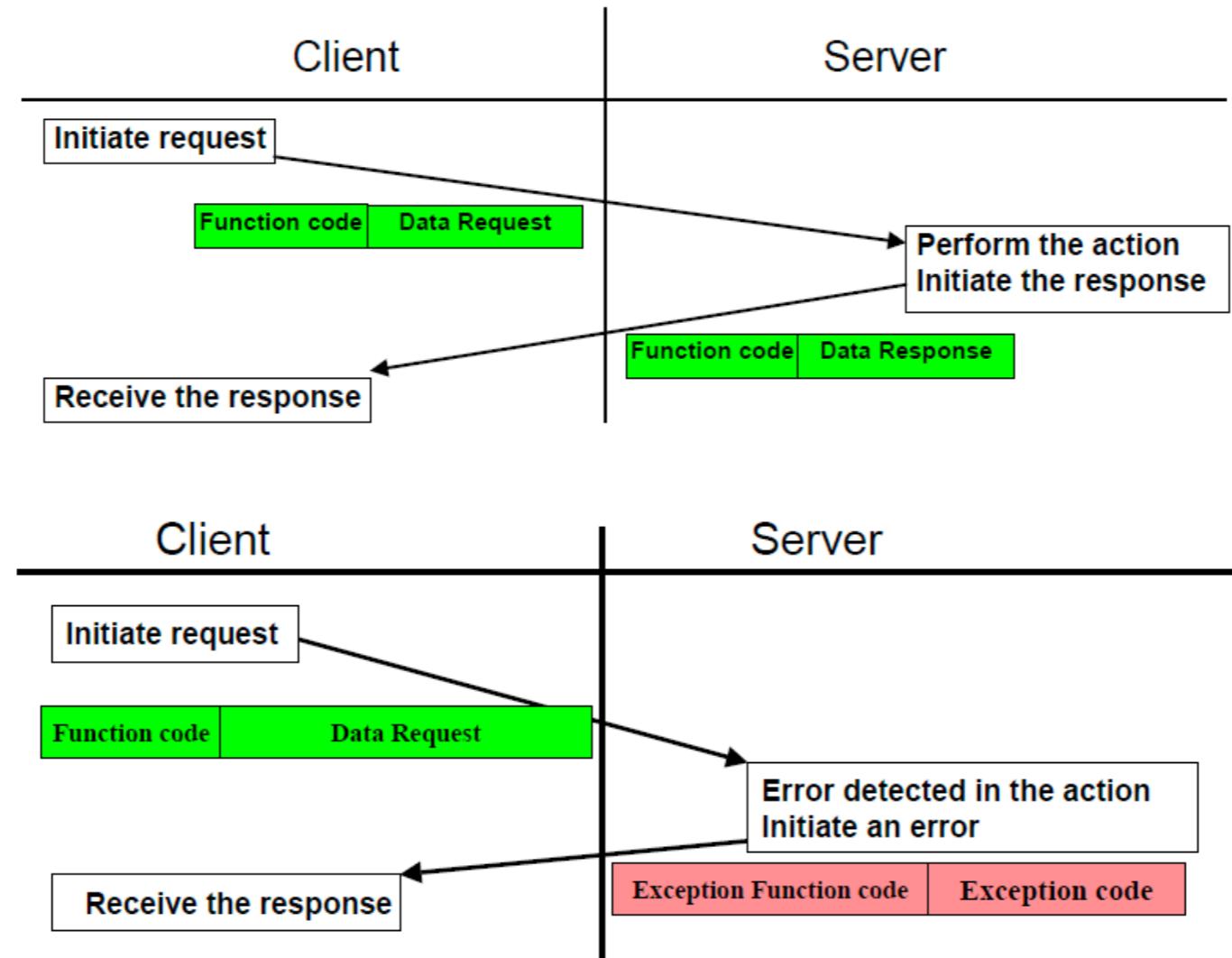
# Modbus – Function code

				Function Codes			
				code	Sub code	(hex)	Section
Data Access	Bit access	Physical Discrete Inputs	Read Discrete Inputs	02		02	6.2
		Internal Bits Or Physical coils	Read Coils	01		01	6.1
			Write Single Coil	05		05	6.5
			Write Multiple Coils	15		0F	6.11
	16 bits access	Physical Input Registers	Read Input Register	04		04	6.4
			Read Holding Registers	03		03	6.3
			Write Single Register	06		06	6.6
			Write Multiple Registers	16		10	6.12
			Read/Write Multiple Registers	23		17	6.17
			Mask Write Register	22		16	6.16
			Read FIFO queue	24		18	6.18
		Internal Registers Or Physical Output Registers	Read File record	20		14	6.14
			Write File record	21		15	6.15
Diagnostics		Read Exception status	07		07	6.7	
		Diagnostic	08	00-18,20	08	6.8	
		Get Com event counter	11		OB	6.9	
		Get Com Event Log	12		0C	6.10	
		Report Server ID	17		11	6.13	
		Read device Identification	43	14	2B	6.21	
		Encapsulated Interface Transport	43	13,14	2B	6.19	
		CANopen General Reference	43	13	2B	6.20	

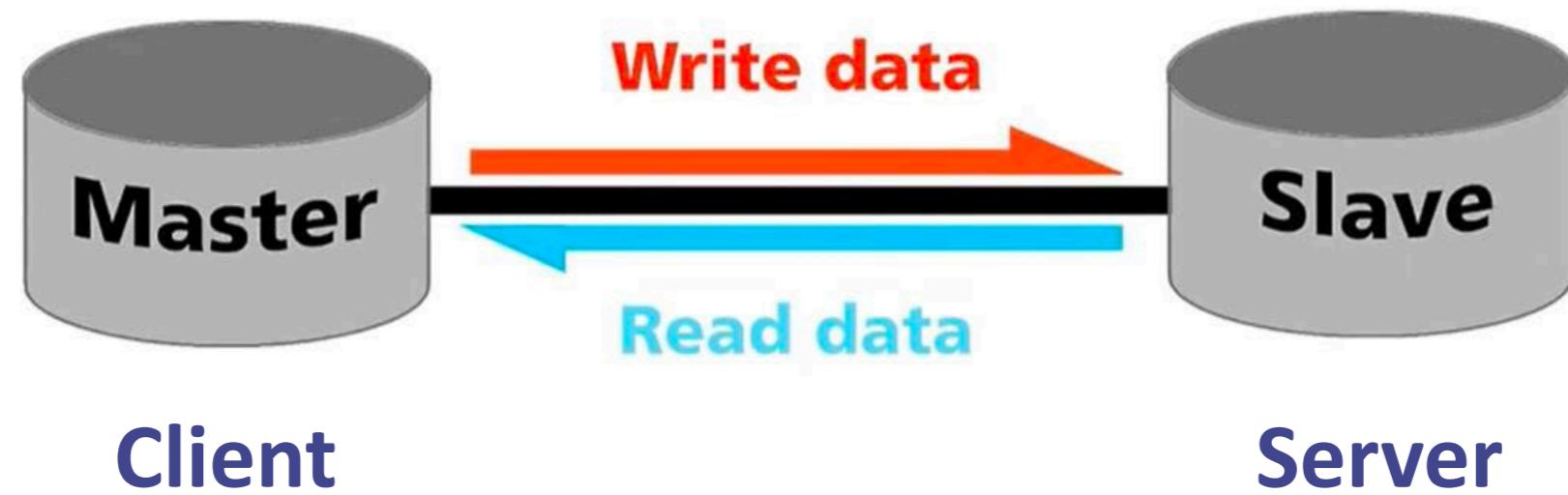
# Modbus – Communication Stack



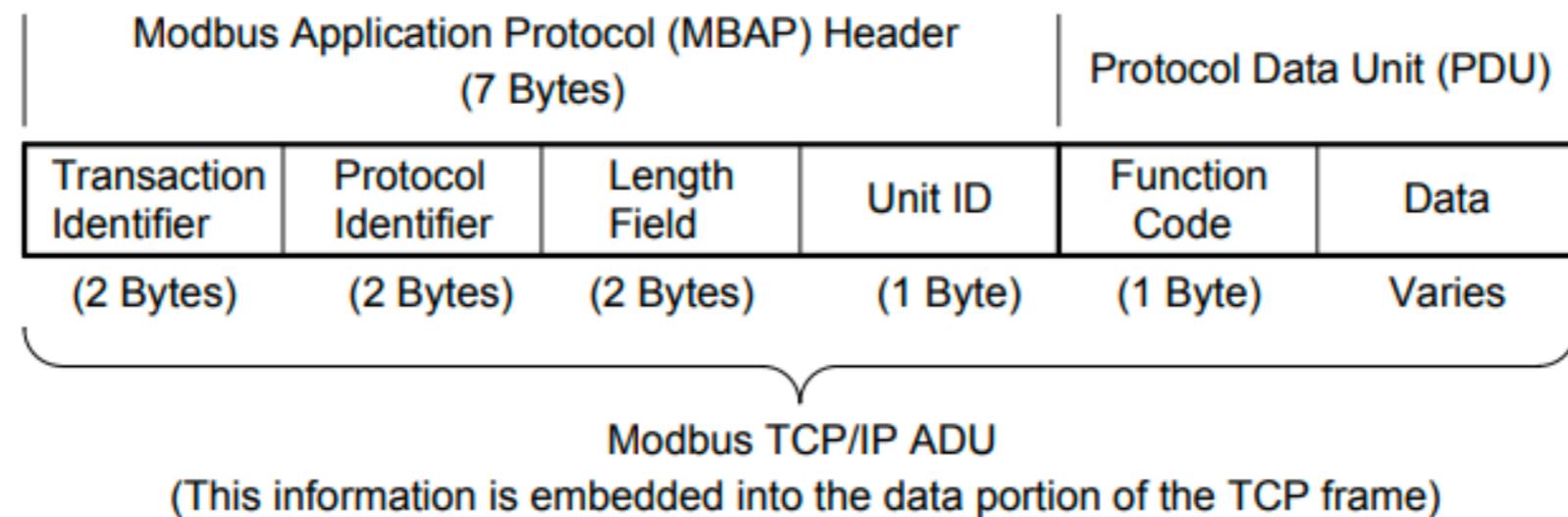
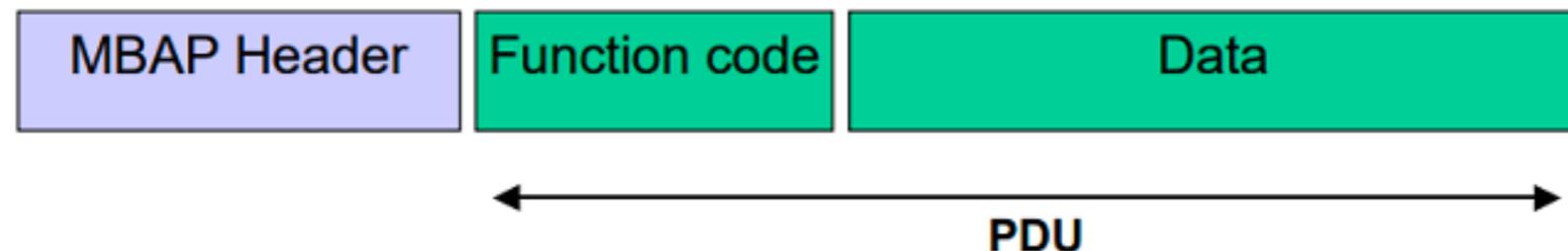
# Modbus TCP/IP –Communication structure



# Modbus TCP/IP



## Modbus TCP/IP - Frame



# Outline

- Industrial communication – Who is talking?
- Fieldbus, what and where?
- Modbus as an example
- **Features/Properties of Fieldbuses**
- CanOpen
- Ethernet as a basis
- PowerLink (CanOpen over Ethernet)
- Profinet
- Timeline

## Fieldbuses – again

- 10s if not 100s of different Fieldbuses out there
- (Some/Many) Fieldbus profiles are standardized by the International Electrotechnical Commission (IEC) as IEC 61784/61158

# Fieldbus - examples

## IEC 61784-1

- CPF 1 FOUNDATION Fieldbus
- CPF 2 ControlNet
- CPF 3 PROFIBUS
- CPF 4 P-NET
- CPF 5 WorldFIP
- CPF 6 INTERBUS
- CPF 7 SwiftNet

## IEC 61784-2 (Real time)

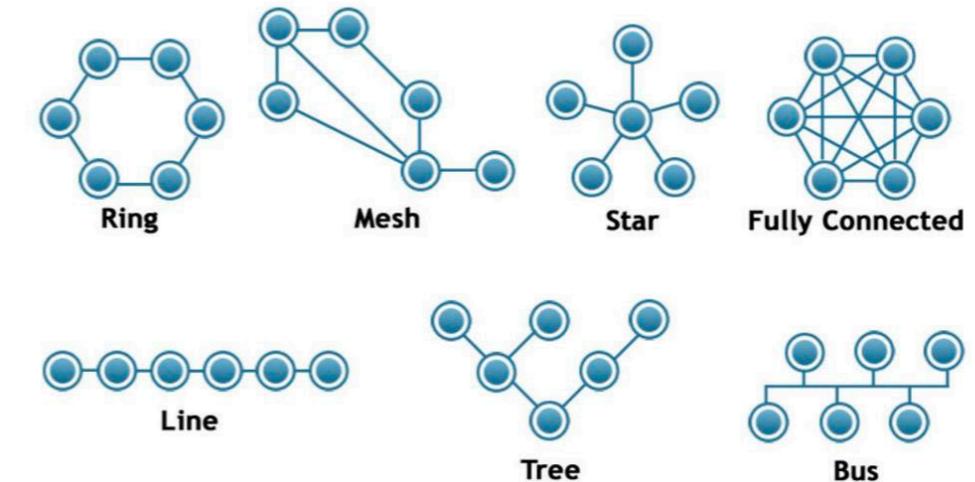
- CPF 2 CIP
- CPF 3 PROFIBUS & PROFINET
- CPF 4 P-NET[28]
- CPF 6 INTERBUS
- CPF 10 Vnet/IP[29]
- CPF 11 TCnet[30]
- CPF 12 EtherCAT
- CPF 13 ETHERNET Powerlink
- CPF 14 Ethernet for Plant Automation (EPA)
- CPF 15 MODBUS
- CPF 16 SERCOS
- CPF 17 RAPIEnet
- CPF 18 SafetyNET p
- CPF 19 FL-net
- CPF 20 ADS-net
- CPF 21 AUBUS

## IEC 61784-3 (safety)

- CPF 1 FOUNDATION Fieldbus[35]
- CPF 2 CIP with CIP safety
- CPF 3 PROFIBUS & PROFINET with PROFIsafe
- CPF 6 INTERBUS
- CPF 8 CC-Link
- CPF 12 EtherCAT with Safety over EtherCAT
- CPF 13 Ethernet POWERLINK with openSAFETY
- CPF 14 EPA

# Criteria for Fieldbuses - Physical

- Topology
- Redundancy
- (Bus) power
- Wired/wireless (not typical for Level 0)
- Electromagnetic immunity



## Criteria for Fieldbuses - Performance

- Transmission Speed
- Distance
- Number of participants
- Simplex, Half duplex, Full duplex
- Cycle time

## Criteria for Fieldbuses - Logical

- Addressing
- Communication mode
  - Multiple master
  - Single master
- Communication mode
  - Master/Slave
  - Client server
  - Peer to peer

## Criteria for Fieldbuses - Features

- Realtime capable
- Safety capable
- Security features
- Control capable

# Outline

- Industrial communication – Who is talking?
- Fieldbus, what and where?
- Modbus as an example
- Features/Properties of Fieldbuses
- **CanOpen**
- Ethernet as a basis
- PowerLink (CanOpen over Ethernet)
- Profinet
- Timeline

# Controller Area Network

- CAN is a network specification used originally in cars
  - Multi-Master Bus
  - Priority-based message handling
  - CAN does only specify **physical** and **data link** layers -> We only have a communication channel but have no common understanding what data we are communicating
    - CanOpen extended CAN to include that!

# CanOpen

## Topologies:

- Two-wire bus: differential signalling, high EMI immunity (especially with twisted-pairs)
- Single-wire bus: Low cost, more susceptible to EMI.
- Fiber optic bus: Total immunity to EMI, much longer transmission lines possible, used to interconnect distant “local” networks.

# CanOpen

- Object Dictionary
- Protocols:
  - SDO protocol (Service Data Object)
  - PDO protocol (Process Data Object)
  - NMT protocol (Network Management)
  - Error control protocols



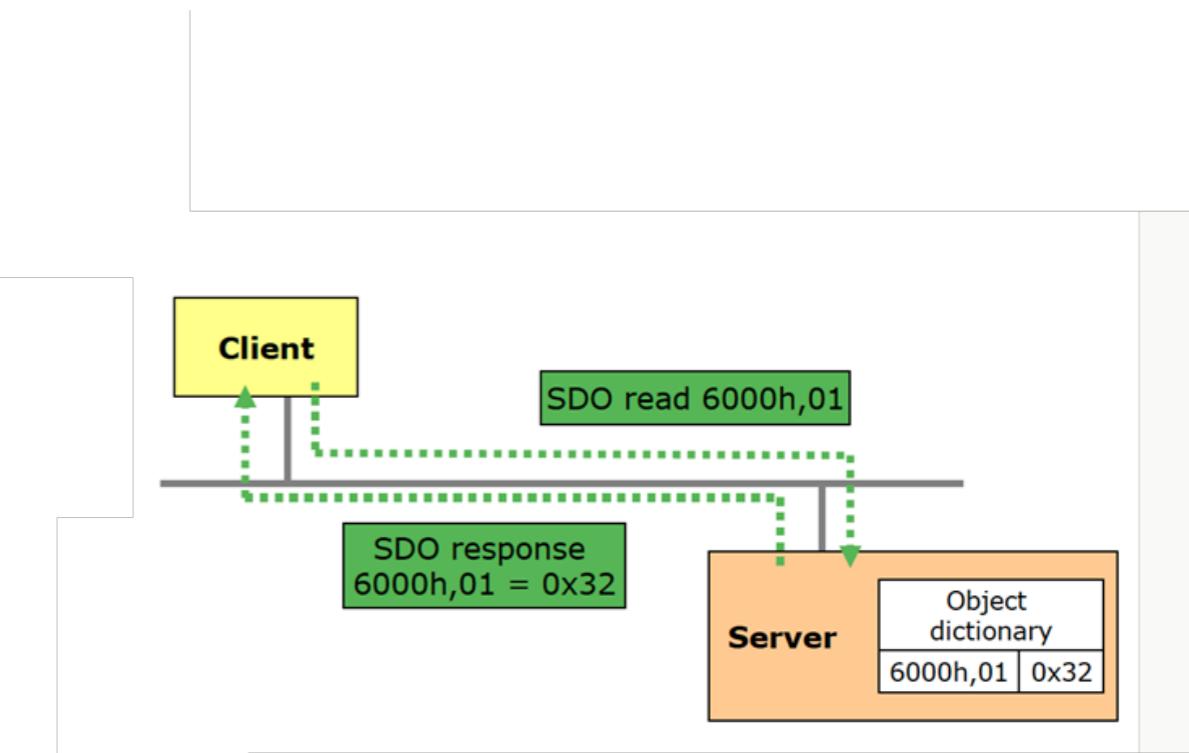
# CANOpen SDO

## Service Data Objects (SDO)

1. Direct access to Object Dictionary of nodes
2. Local and remote read and write
3. Based on client/server model

## SDO are used for

1. Non-cyclic read/write data access
2. POWERLINK configuration
3. Data and file download, diagnosis



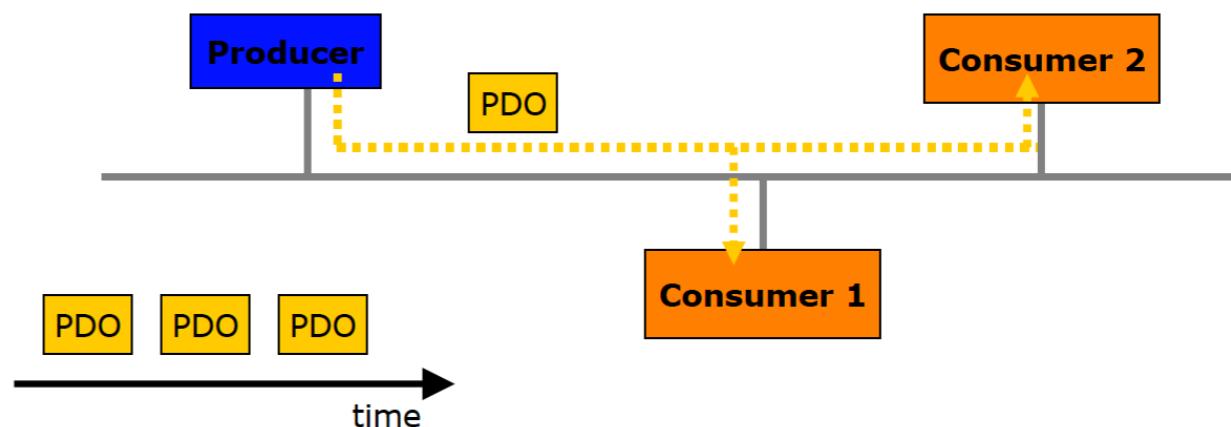
# CANOpen PDO

## Process Data Objects

- Efficient real-time process data exchange
- No protocol overhead, only data are exchanged
- Size up to 1490 bytes

## Producer-consumer principle

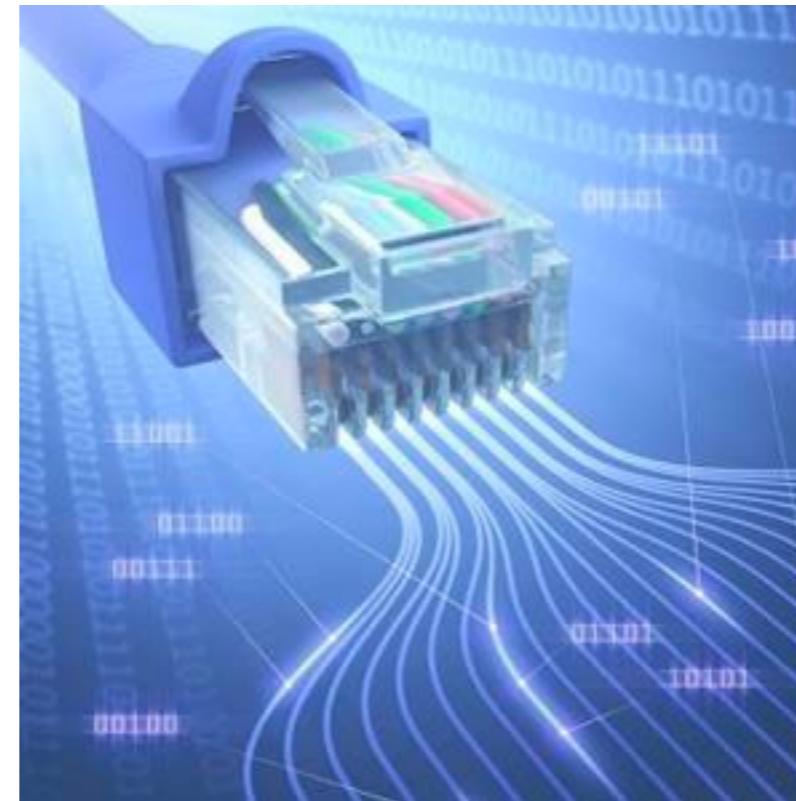
- Continuous cyclic transmission
- One producer, several consumers



# Outline

- Industrial communication – Who is talking?
- Fieldbus, what and where?
- Computer networking – recap
- Modbus as an example
- Features/Properties of Fieldbuses
- CanOpen
- **Ethernet as a basis**
- PowerLink (CanOpen over Ethernet)
- Profinet
- Timeline

# Why Ethernet?



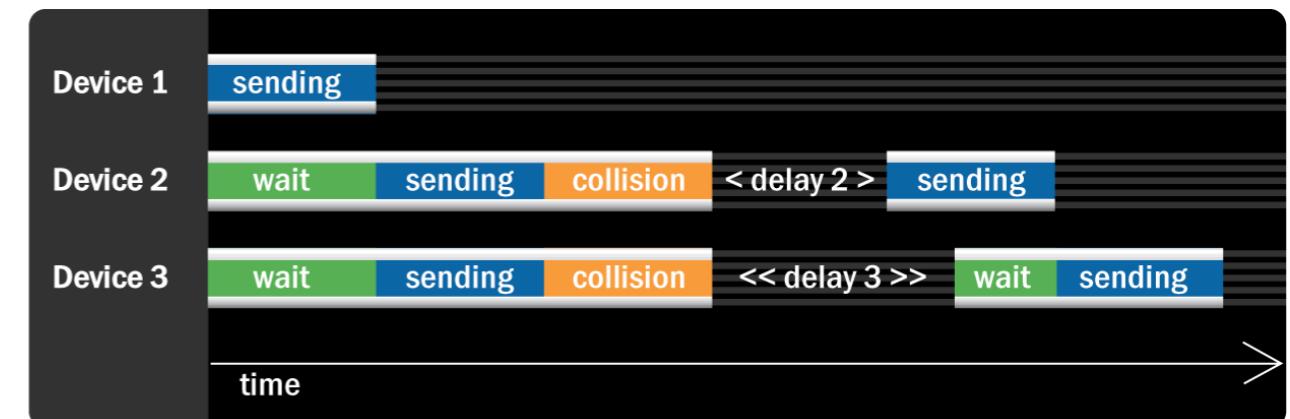
# Standard Ethernet – Not Real-Time

Ethernet Medium access: CSMA/CD

- Carrier-Sense Multiple Access with Collision Detection (bus)
- Collisions generate retransmission after random delay
- Induces unpredictable delays

Standard Ethernet is not deterministic

- Designed for office application



# Industrial Ethernet

- Lot's of Fieldbuses today use Ethernet as a basis, e.g.,:
  - Ethernet Powerlink,
  - Profinet
  - EtherCAT
  - Ethernet/IP, (CIP over Ethernet)
  - ModbusTCP (Modbus over Ethernet)

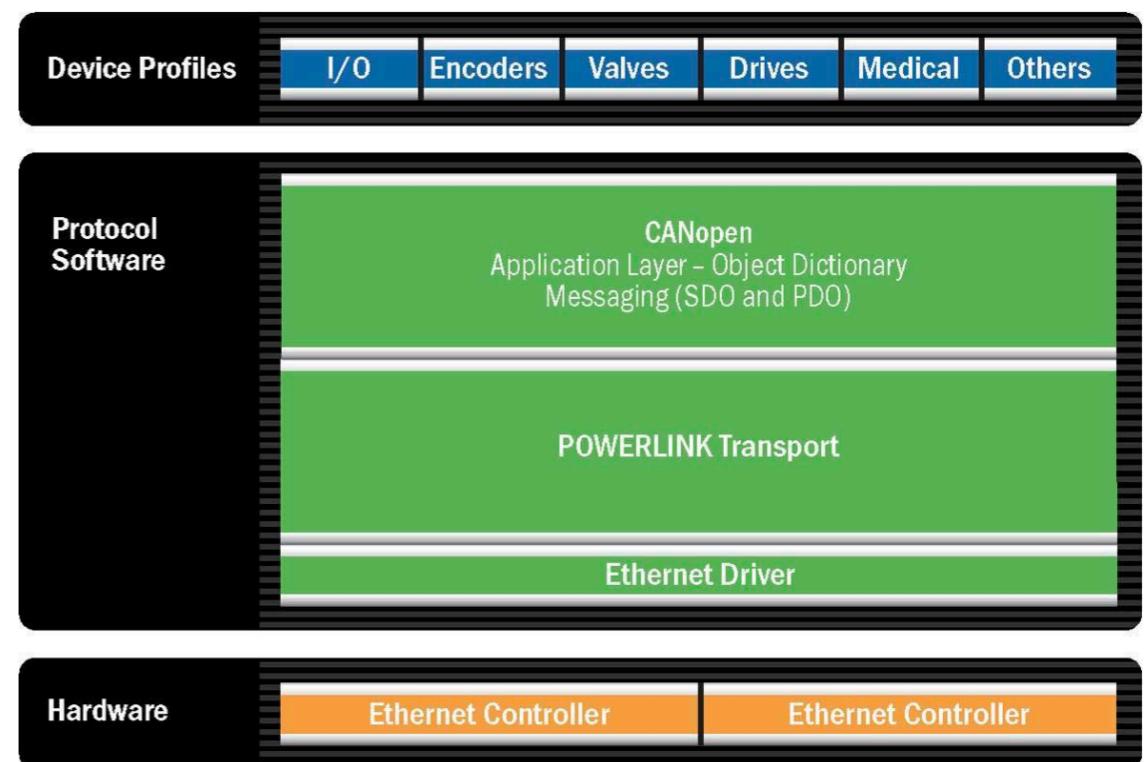
# Outline

- Industrial communication – Who is talking?
- Fieldbus, what and where?
- Computer networking – recap
- Modbus as an example
- Features/Properties of Fieldbuses
- CanOpen
- Ethernet as a basis
- PowerLink (CanOpen over Ethernet)
- Profinet
- Timeline

# POWERLINK

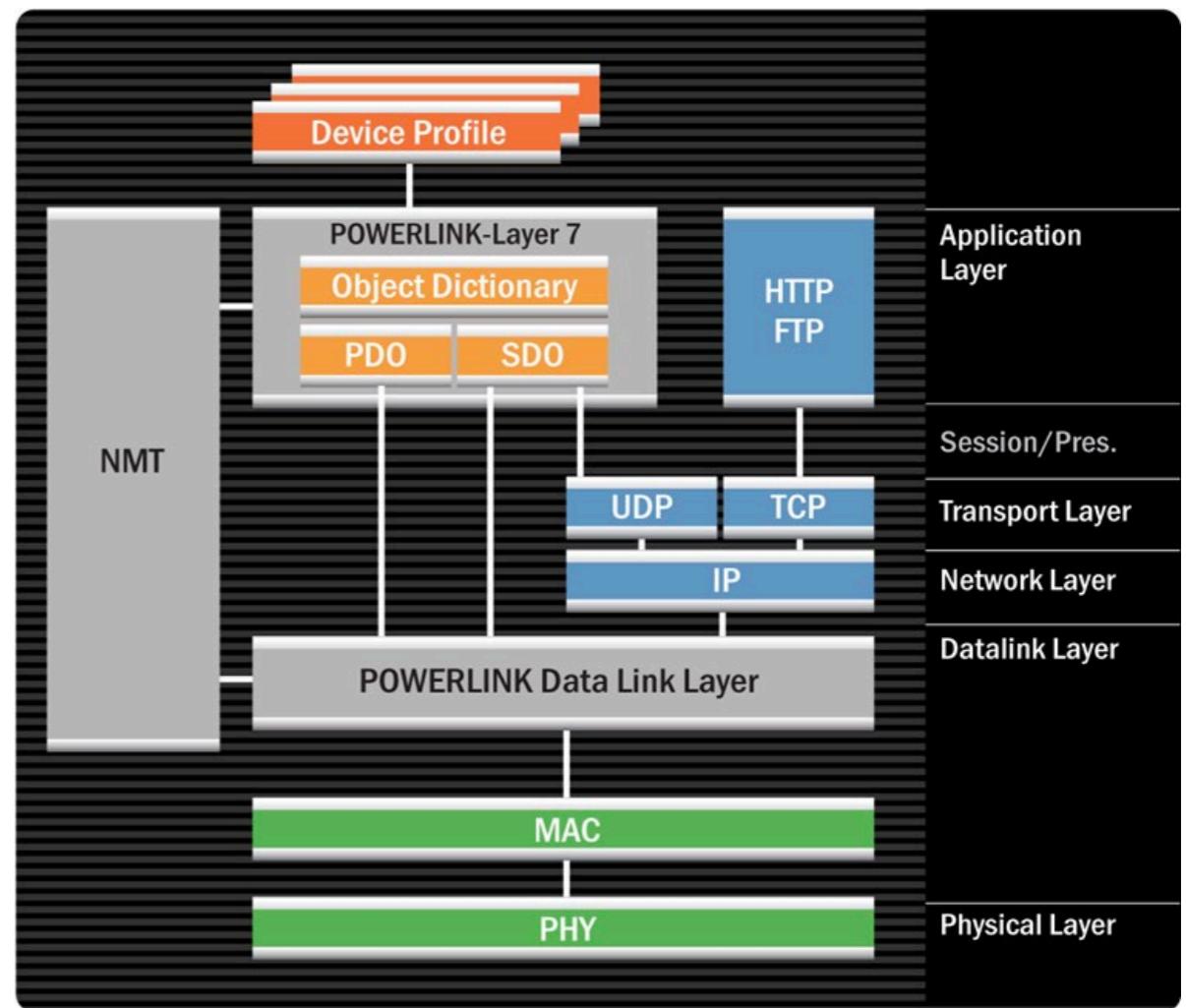
POWERLINK “is” CANopen over Ethernet

- Same device profiles
- CANopen application layer
- Same mechanisms (PDO, SDO, Object Dictionary...)



# POWERLINK

- Object dictionary – POWERLINK application layer:



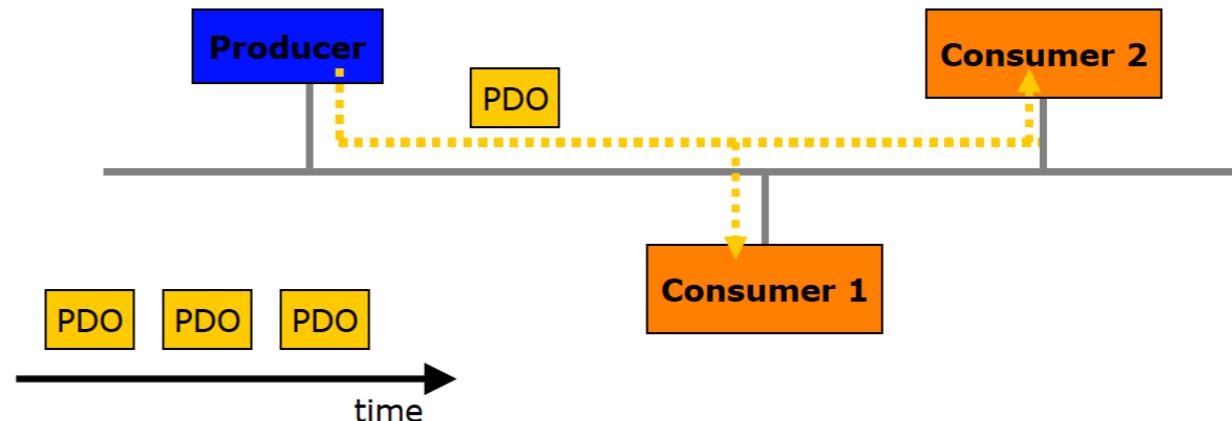
# POWERLINK PDO

## Process Data Objects

- Efficient real-time process data exchange
- No protocol overhead, only data are exchanged
- Size up to 1490 bytes

## Producer-consumer principle

- Continuous cyclic transmission
- One producer, several consumers

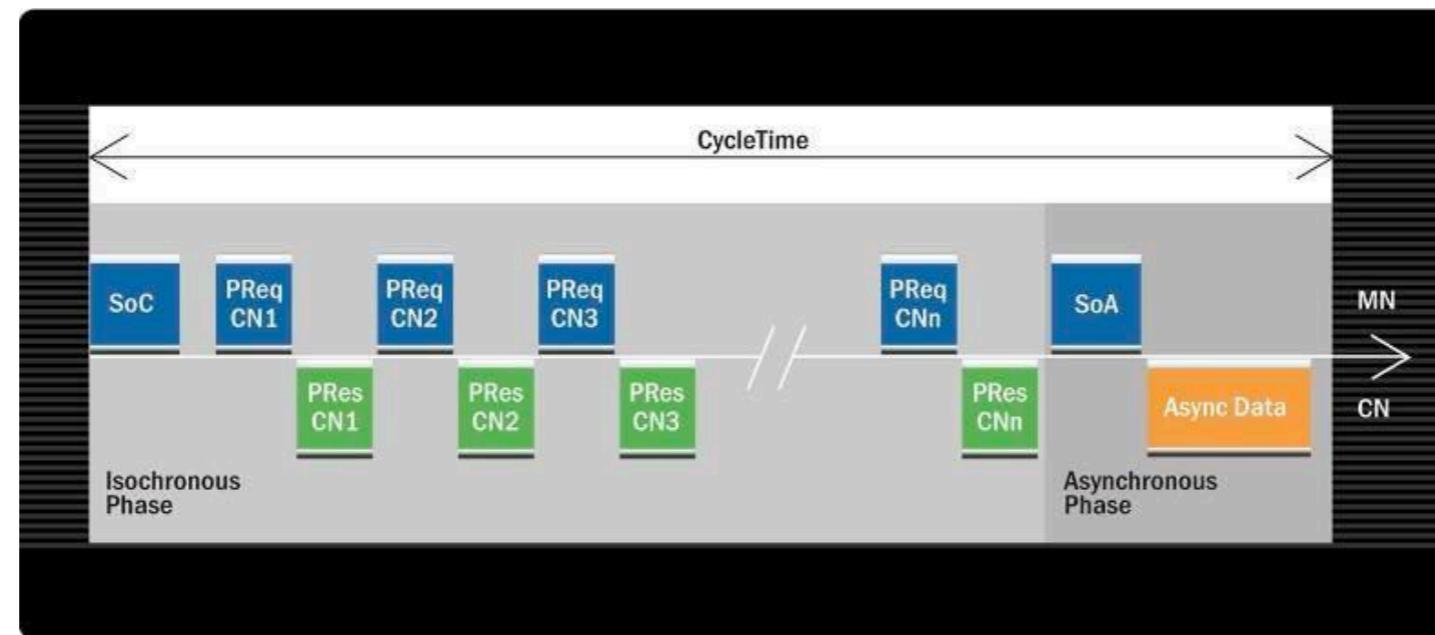


# Cycle time

Managing node (master) vs. Controlled nodes (slaves)

The shortest possible cycle time depends on:

- Number of nodes
- Size of PDO frames
- Response times of individual nodes
- Transmission delay (i.e. topology)

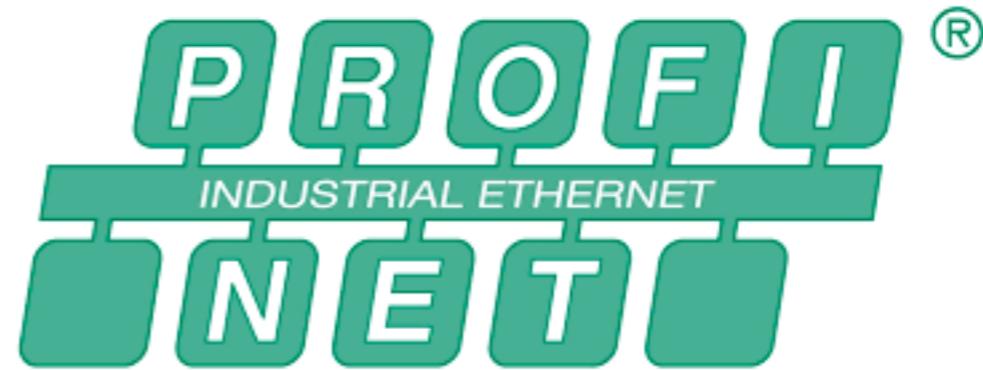


# Outline

- Industrial communication – Who is talking?
- Fieldbus, what and where?
- Modbus as an example
- Features/Properties of Fieldbuses
- CanOpen
- Ethernet as a basis
- PowerLink (CanOpen over Ethernet)
- **Profinet**
- Timeline

# Profinet

PROcess FieldNet



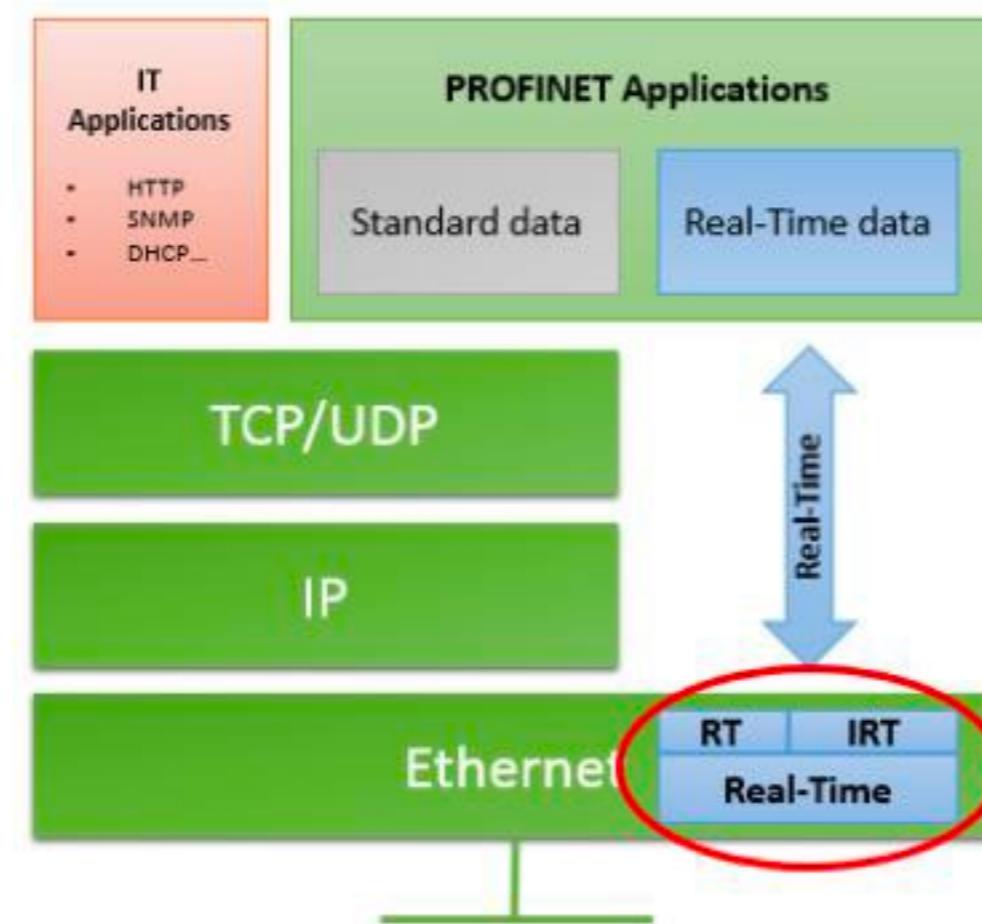
- The umbrella group PROFIBUS & PROFINET International (PI)
- Industrial Ethernet solution for automation

# Profinet – Communication Channels

- **Standard TCP/IP**
  - Parameterization
  - Configuration
  - Acyclic read/write operations
- **ProfiNetRT(Real Time)**
  - Standard cyclic data transfer and alarms
- **ProfiNetIRT(Isochronous Real Time)**
  - High-speed channel used for Motion Control applications

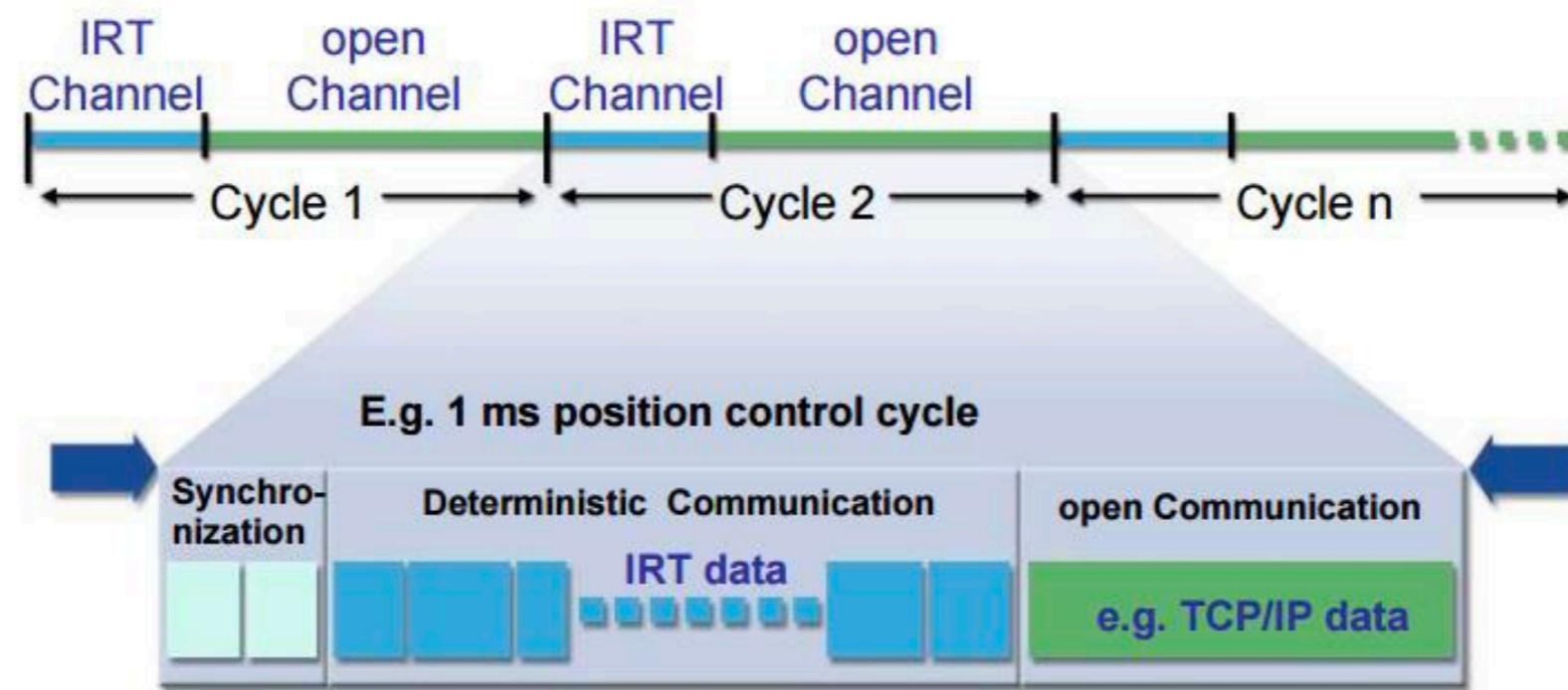
All services can be used on the same network!

# Profinet RT/IRT



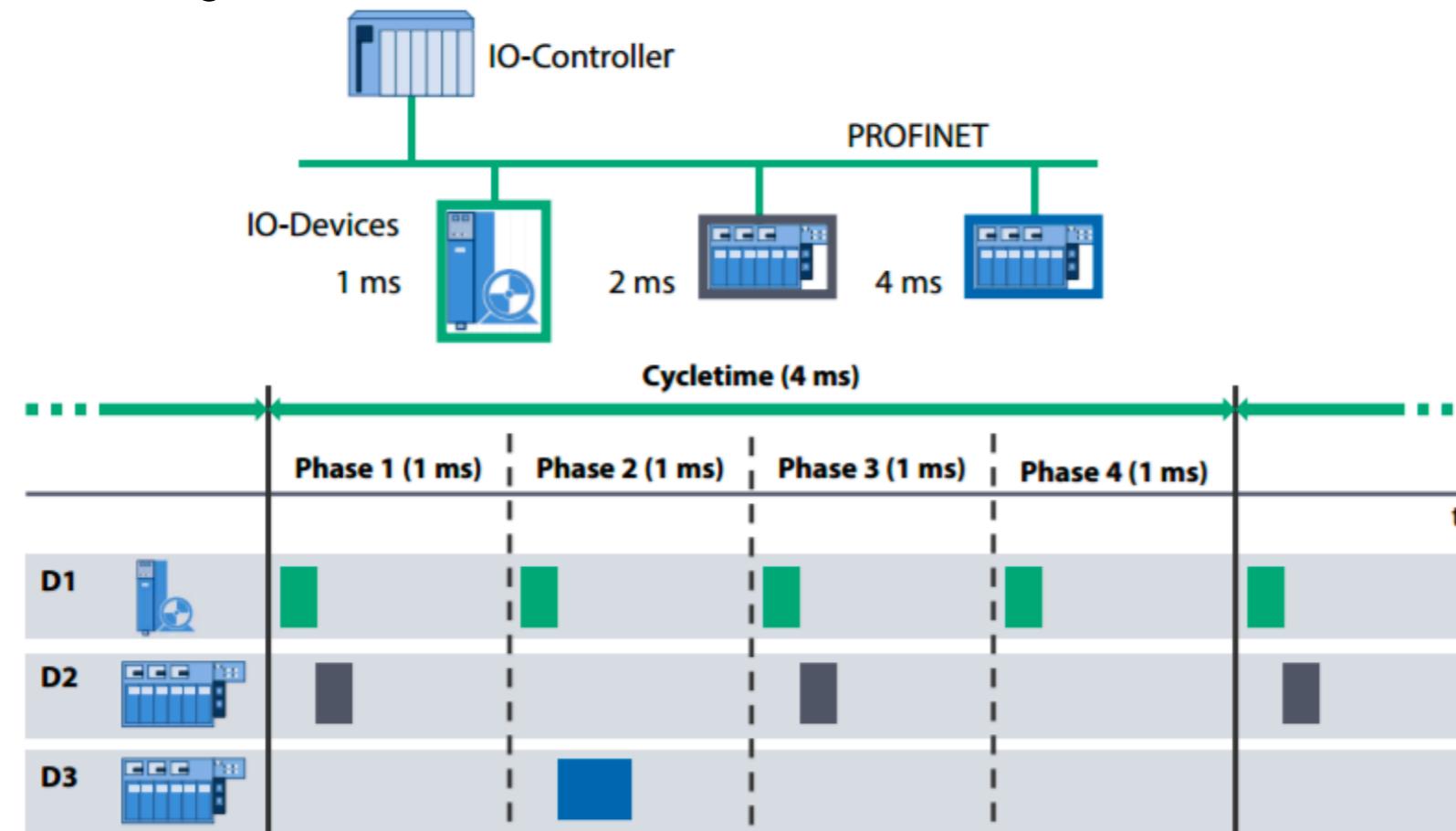
# Profinet - Isochronous Real Time

- Cyclic data frames are transferred as synchronized frames on a reserved bandwidth (time slots)
- Common clock through Precision Time Protocol (PTP)



# Profinet - Cyclic Data Exchange

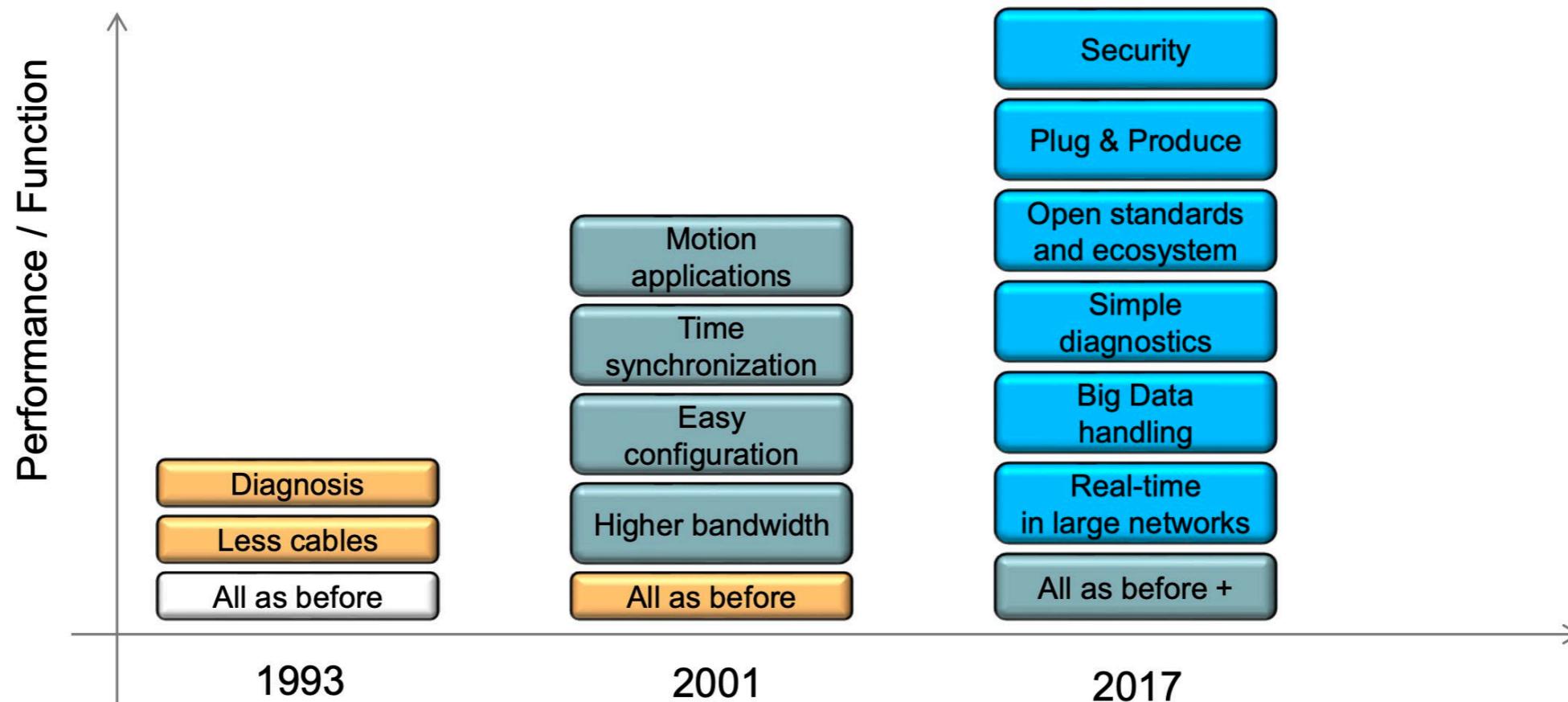
- Cycle time can be specified individually
- Smallest time partitioning



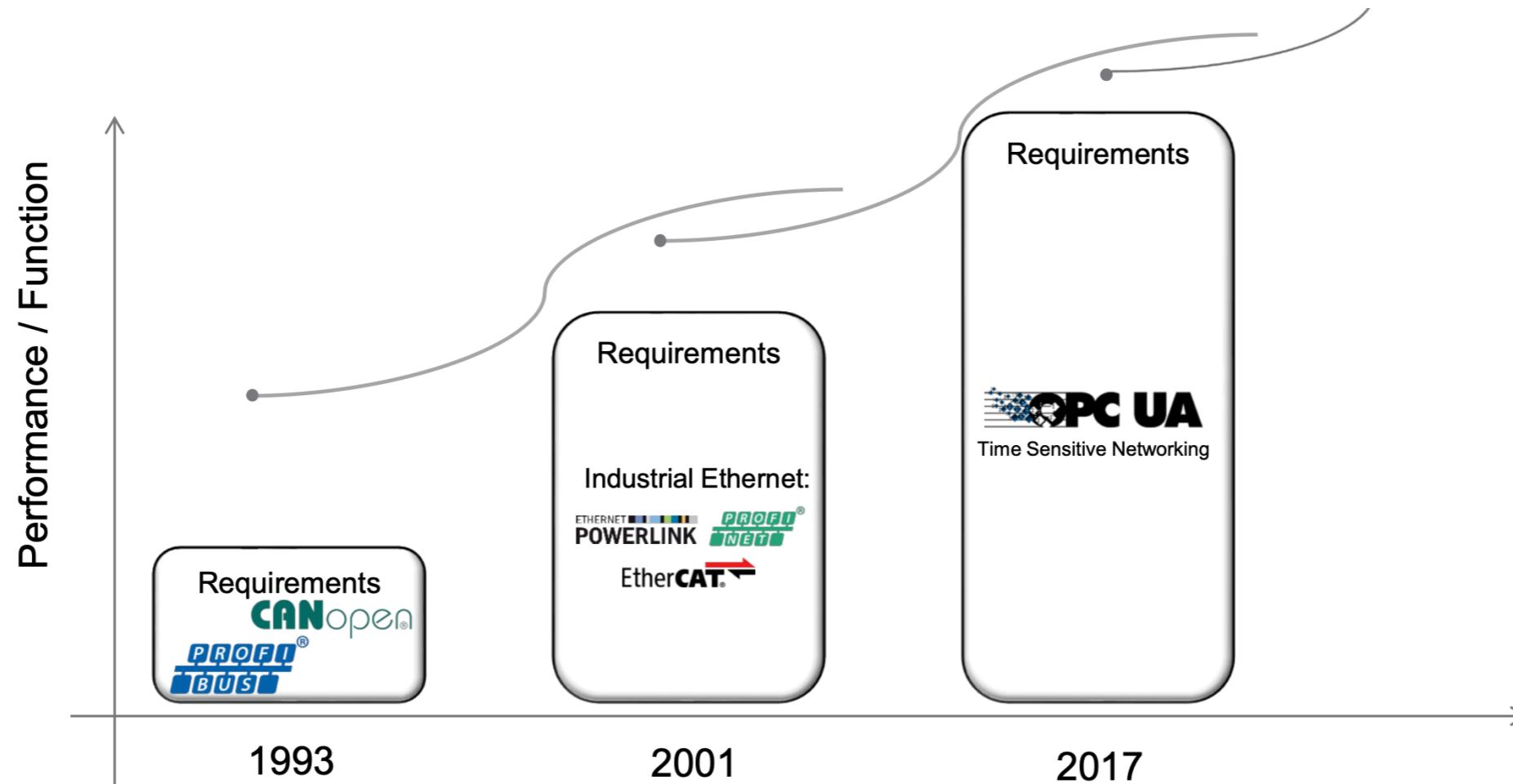
# Outline

- Industrial communication – Who is talking?
- Fieldbus, what and where?
- Modbus as an example
- Features/Properties of Fieldbuses
- CanOpen
- Ethernet as a basis
- PowerLink (CanOpen over Ethernet)
- Profinet
- **Timeline**

# Timeline



# Timeline



OPCUA: <https://www.youtube.com/watch?v=-tDGzwsBokY>

# Recap

- Industrial communication – Who is talking?
- Fieldbus, what and where?
- Computer networking – recap
- Modbus as an example
- Features/Properties of Fieldbuses
- CanOpen
- Ethernet as a basis
- PowerLink (CanOpen over Ethernet)
- Profinet
- Timeline