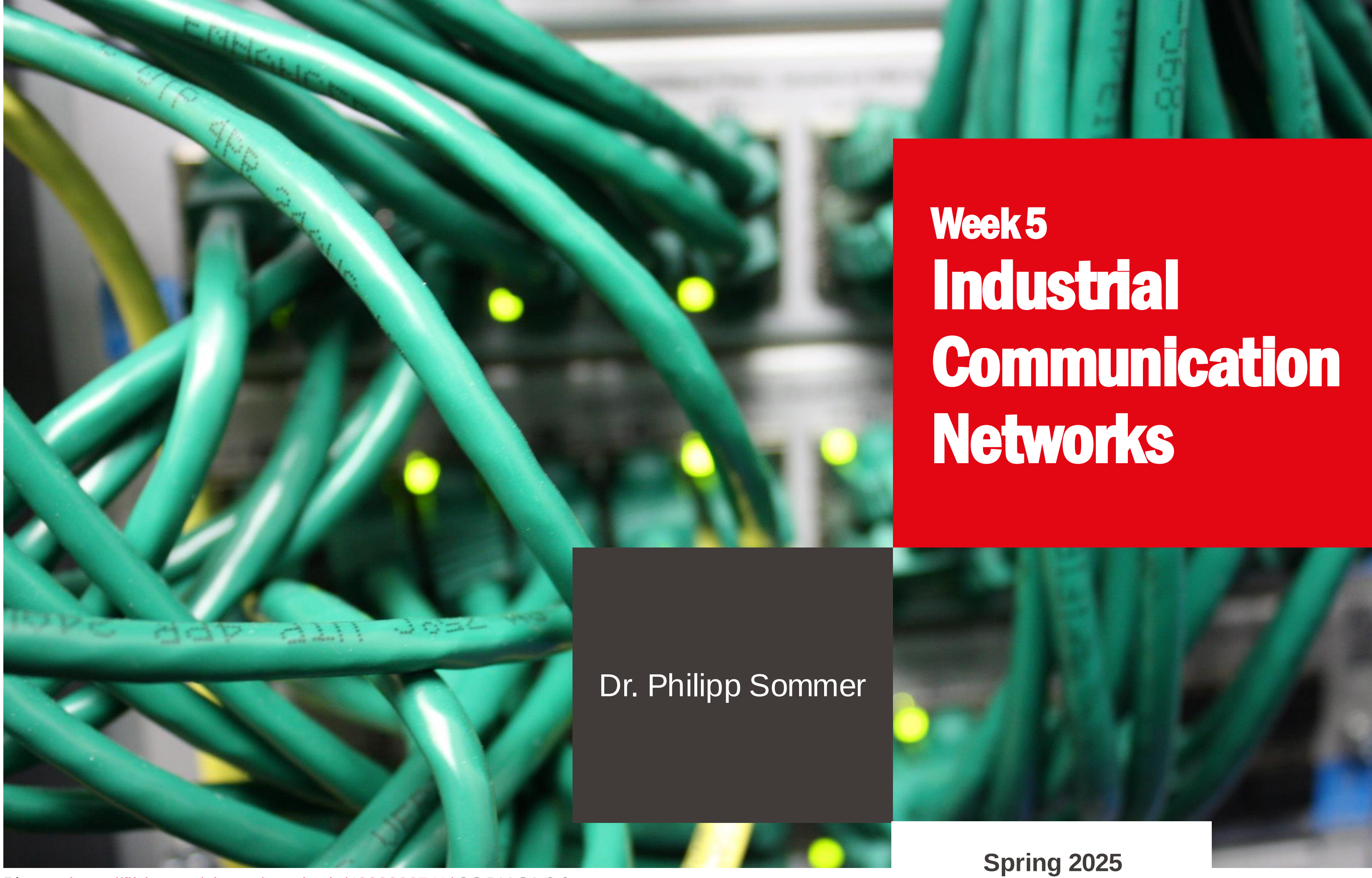
EPFL



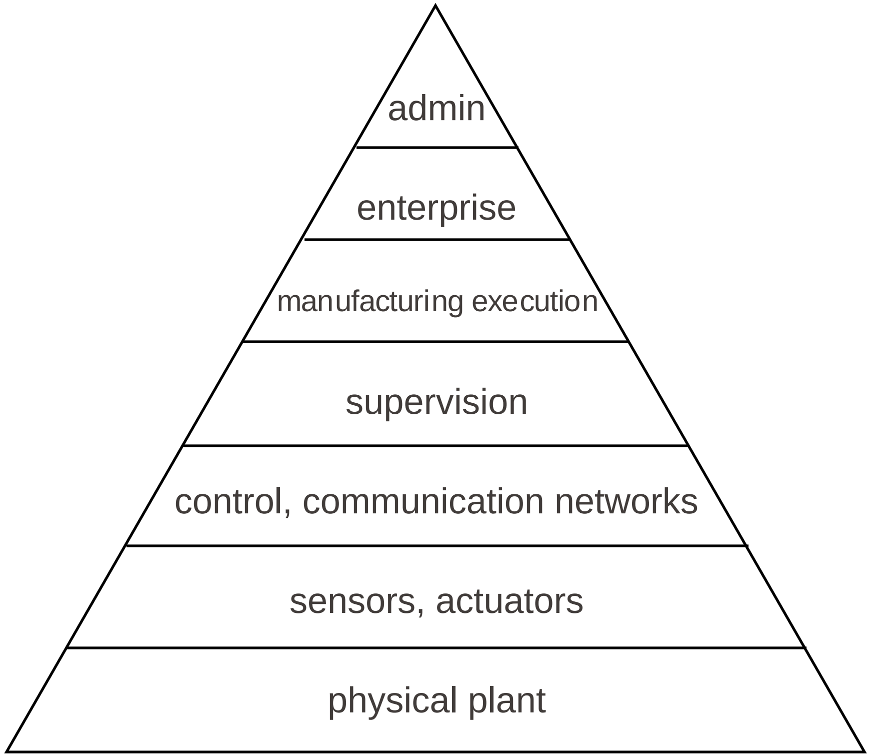
Week 5
Industrial Communication Networks

Dr. Philipp Sommer

Spring 2025

Industrial Communication Networks

- OT vs IT
- Field bus principles
- Field bus operation
- Standard field busses



OT vs IT

Operational Technology (OT):

- Factory floor
- Operation of physical processes and machines
- Examples: PLCs, SCADA, DCS
- Highly specialized equipment and software/protocols
- Stand-alone factory network

Information Technology (IT):

- Office environment
- Digital information (data)
- Examples: PCs, laptops, servers
- Highly standardized software and hardware components
- Connected to the cloud

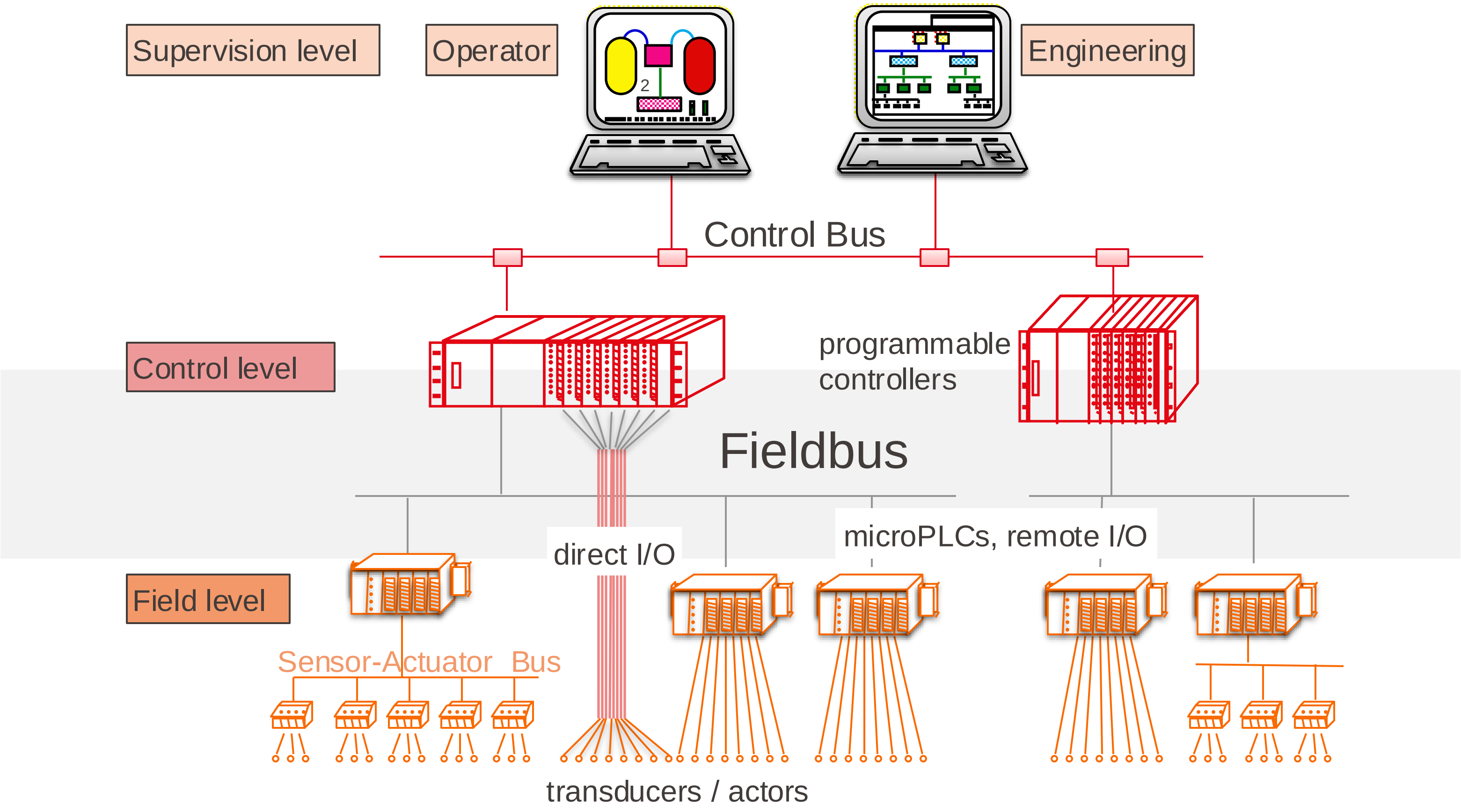
IT-OT Convergence: IT and OT systems will grow closer together.

Ethernet (IEEE 802.3)

- Family of wired computer networking technologies standardized by the IEEE from 1983 onwards
- Widely used for Local-Area Networking (LAN) in the IT domain
- Various physical layer variants (10/100/1000 Mbit/s, …)
- Gigabit speed over twisted-pair cables (CAT5 or better), 100 meters
- Can supply power to devices: Power-over-Ethernet (PoE)

https://www.netgear.com/business/wired/switches/plus/gs108e/

Networks in Automation Hierarchy

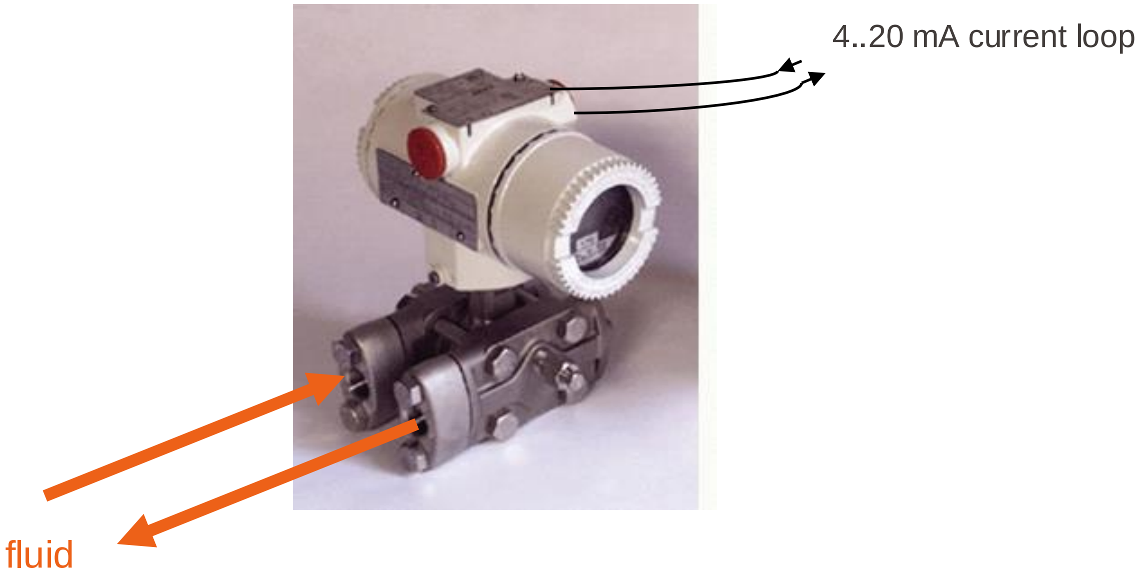


Ethernet and fieldbus roles

- Traditionally, Ethernet is used for the communication among the PLCs and for communication of the PLCs with the supervisory level and with the engineering tools.
- Fieldbus is in charge of the connection with the decentralized I/O and for time-critical communication among the PLCs.

Connecting field devices

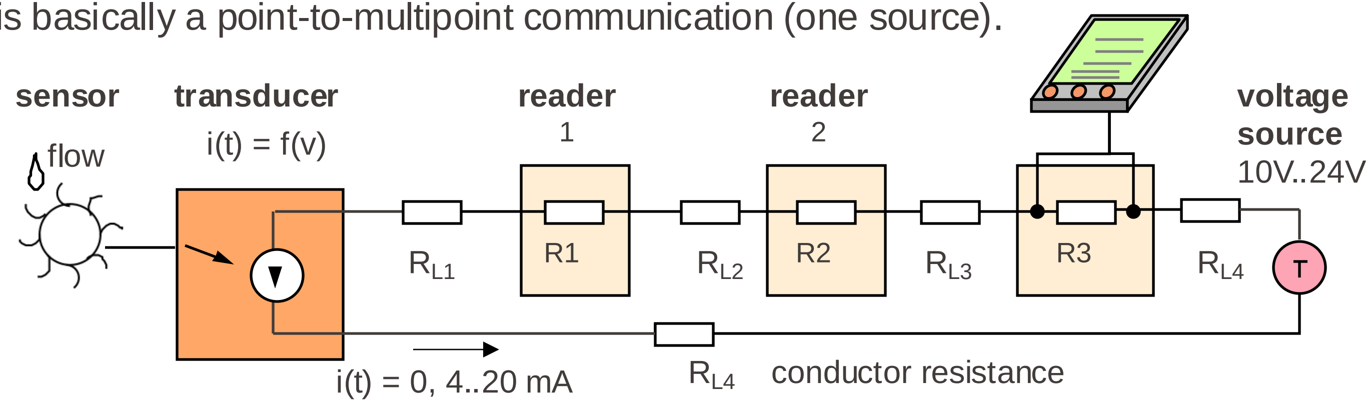
Field device: example differential pressure transducer



The device transmits its value by means of a current loop.

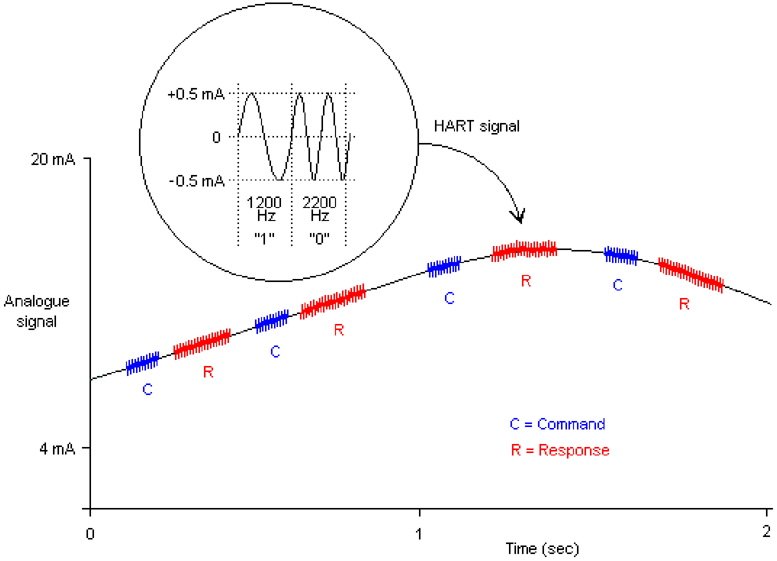
4-20 mA loop - the conventional, analog standard

- The 4-20 mA is the most common analog transmission standard in industry.
- The transducer limits the current to a value between 4 mA and 20 mA, proportional to the measured value, while 0 mA signals an error (wire break).
- The voltage drop along the cable and the number of readers induces no error.
- Simple devices are powered directly by the residual current (4 mA), allowing to transmit signal and power through a single pair of wires.
- 4-20mA is basically a point-to-multipoint communication (one source).



HART – Principle (1986)

- HART (Highway Addressable Remote Transducer) was developed to retrofit 4-to-20mA current loop transducers with digital data communication
  - HART modulates the 4-20mA current with a low-level frequency-shift-keyed (FSK) sine-wave signal, without affecting the average analogue signal.
  - HART uses low frequencies (1200Hz and 2200 Hz) to deal with poor cabling, slow - but sufficient for its purpose.
  - Transmission of device characteristics is normally not real-time critical



HART - Protocol

- Practically all 4..20 mA devices come equipped with HART today.
- HART communicates point-to-point, under the control of a server, e.g., a hand-held device.

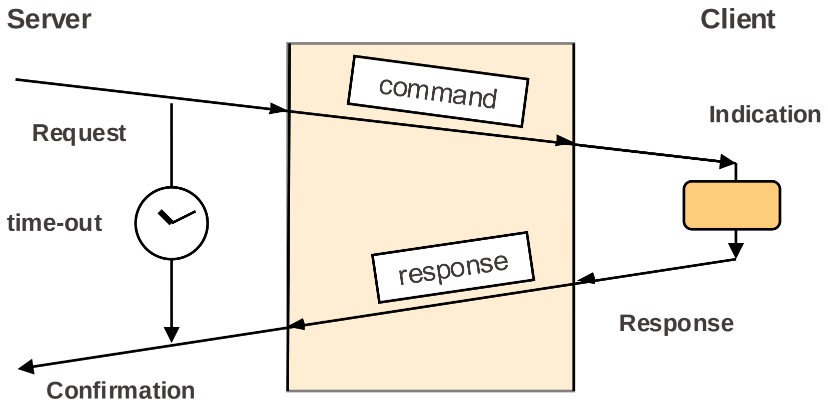


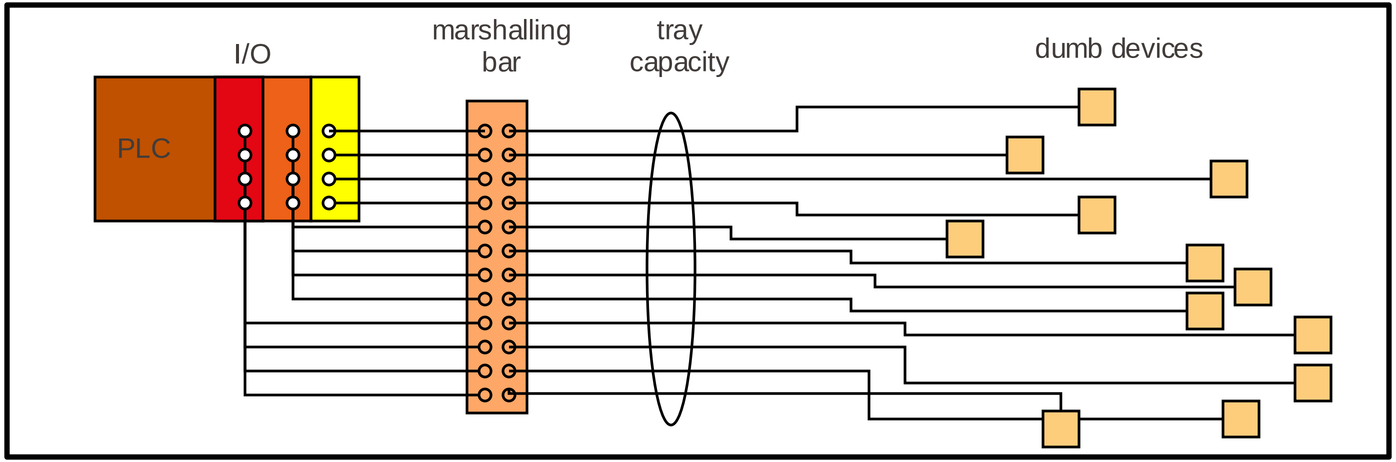
ABB TTH200 Temperature sensor

HART - Commands

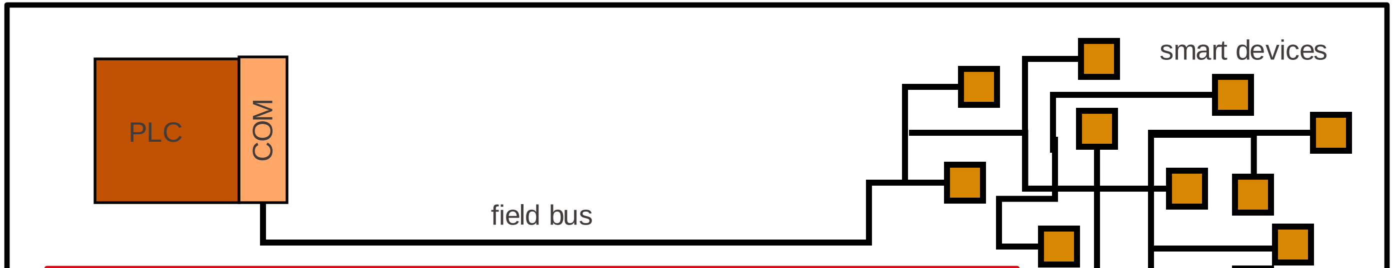
- Universal commands (mandatory):
  - Identification
  - primary measured variable and unit (floating point format)
  - loop current value (%) = same info as current loop
  - read current and up to four predefined process variables
  - sensor serial number
  - instrument manufacturer, model, tag, serial number, descriptor, range limits, …
- Total 44 standard commands, plus user-defined commands
- Transducer-specific (vendor-defined):
  - calibration data, trimming, …

Fieldbus

The original fieldbus idea: save wiring



Without fieldbus

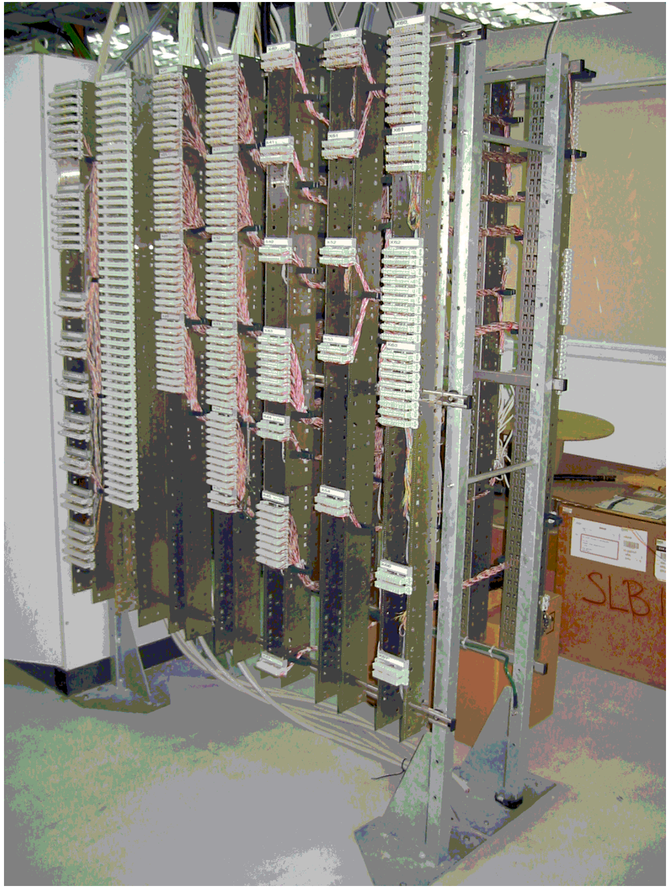


With fieldbus

But: the number of end-points remains the same!
energy must be supplied to smart devices

Marshalling Bar

- The marshalling bar is the interface between the PLC and the instrumentation (sensor/actuators).
- The fieldbus replaces the marshalling bar or rather moves it piecewise to the process
- intelligent concentrator / wiring



What is a fieldbus?

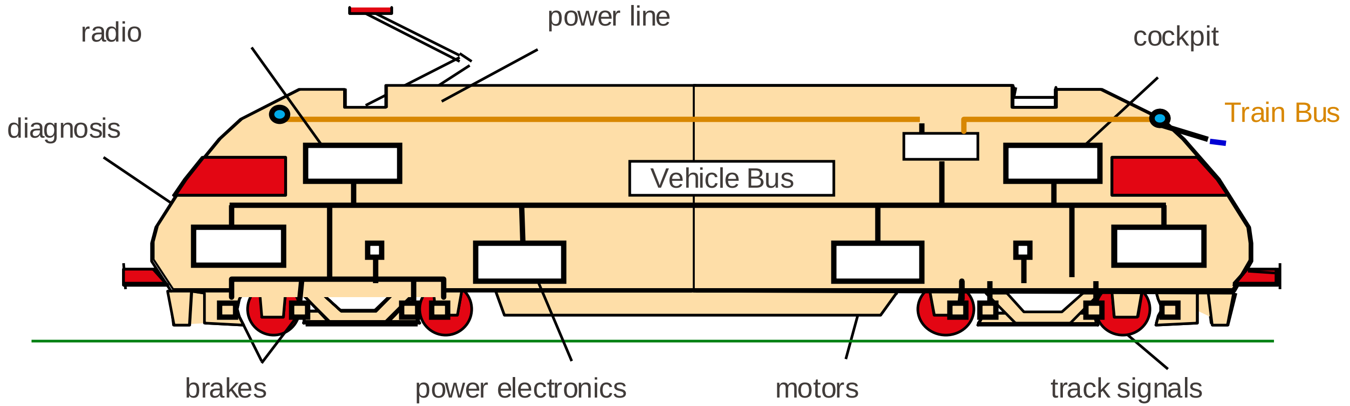
A data network, interconnecting an automation system, characterized by:

- many small data items (process variables) with bounded delay (1ms..1s)
- transmission of non-real-time traffic for commissioning and diagnostics
- harsh environment (temperature, vibrations, EM-disturbances, water, salt,…)
- robust and easy installation by skilled people
- high integrity (no undetected errors) and high availability (redundant layout)
- clock synchronization (milliseconds to microseconds)
- low attachment costs (€ 5.- .. €50 / node)
- moderate data rates (50 kbit/s - 5 Mbit/s), large distance range (10m - 20 km)

Expectations: Why use a fieldbus?

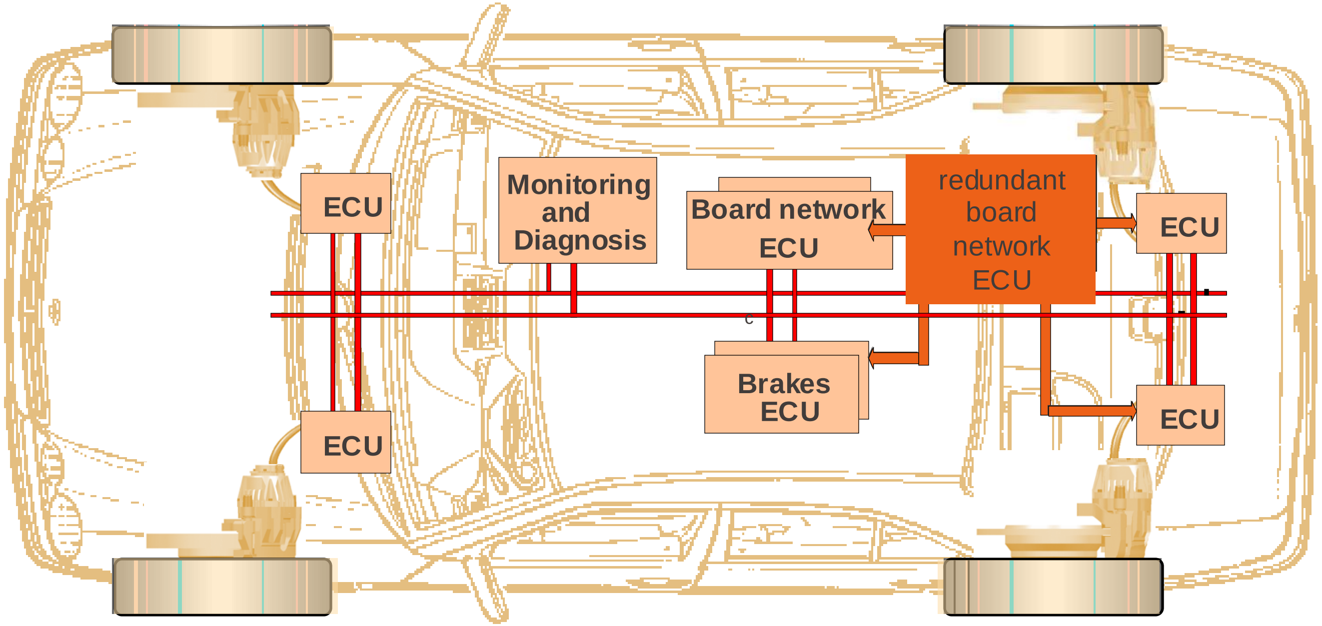
- reduce cabling
- increased modularity of plant (each object comes with a CPU and communication interface)
- easy fault location and maintenance
- simplify commissioning
- simplify extension and retrofit
- off-the-shelf standard products to build “Lego”-control systems

Fieldbus application example: locomotives and drives



data rate	1.5 Mbit/second
delay	1 ms (16 ms for skip/slip control)
medium	twisted wire pair, optical fibers (EM disturbances)
number of stations	up to 255 programmable stations, 4096 simple I/O
integrity	very high (signaling tasks)
cost	engineering costs dominate

Fieldbus application example: car



DAIMLERBENZ
AKTIENGESELLSCHAFT

- Redundant Engine Control Units
- Fault-tolerant 2-voltage on-board power supply
- Diagnostic System

Fieldbus operation

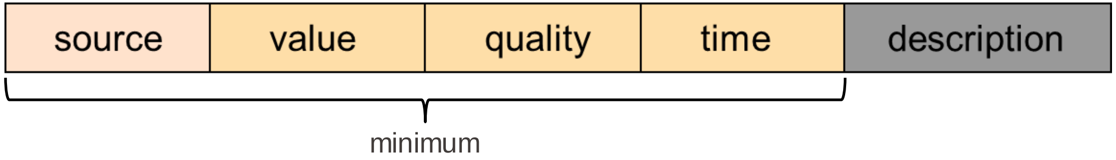
Objective of the fieldbus

Distribute **process variables** to all interested parties:

- source identification: requires a naming scheme
- accurate process value and units
- quality indication: {good, bad, substituted}
- time indication: how long ago was the value produced
- (optional description)

source	value	quality	time	description

Data format

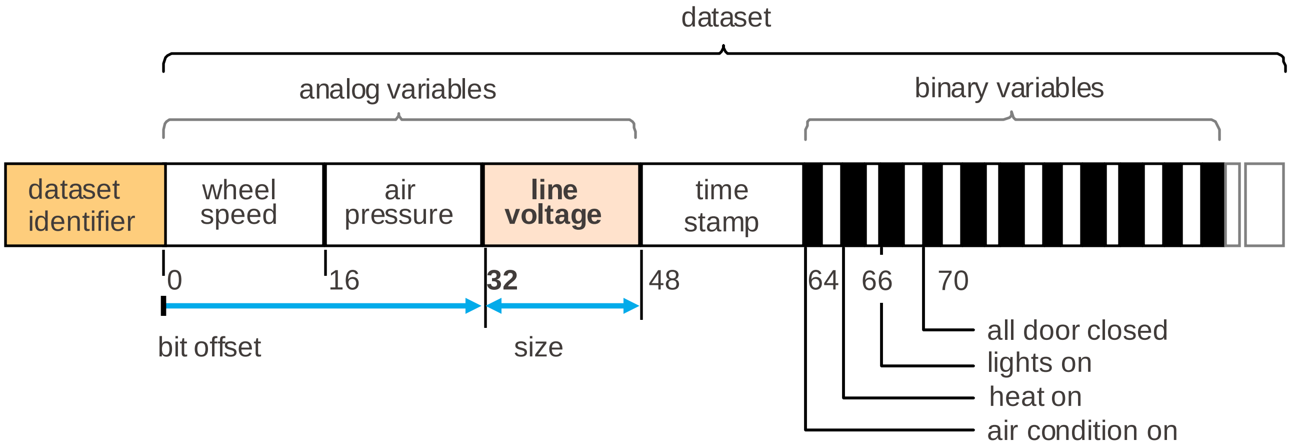


- In principle, the bus could transmit the process variable in clear text (even using XML, JSON, ..)
- However, this is quite expensive and only considered when the communication network offers some 100 Mbit/s and a powerful processor is available to parse the messages.
- More compact ways such as ASN.1 have been used in the past

ASN.1: (TLV)

- Fieldbusses are slower (50kbit/s ..12 Mbits/s) and thus more compact encodings are used.

Datasets



- Fieldbus devices have a low data rate and transmit always the same variables.
- It is economical to group variables of a device in the same frame as a dataset.
- A variable is identified within a dataset by its offset and its size.
- Variables may be of different types, types can be mixed.
- To allow later extension, room is left in the datasets for additional variables.

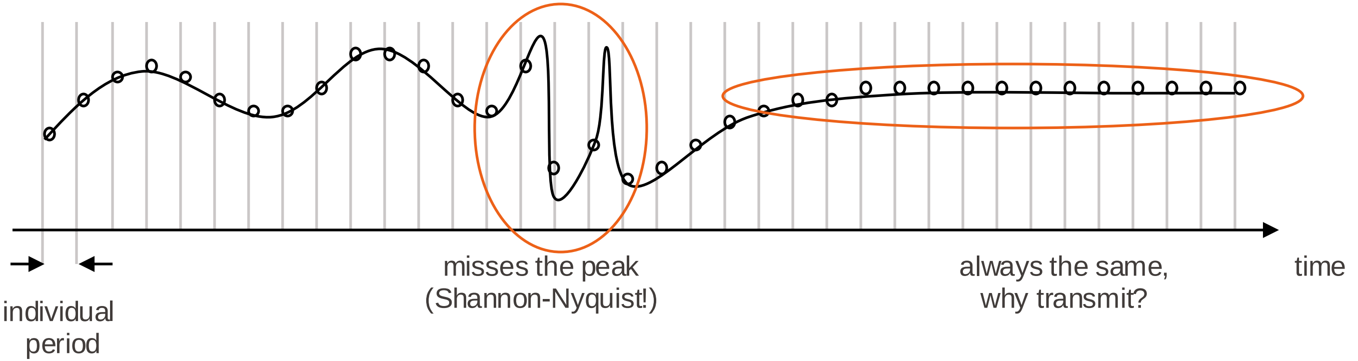
Transmission principle: When to transmit

- The previous operation modes made no assumption on <u>when</u> data are transmitted.

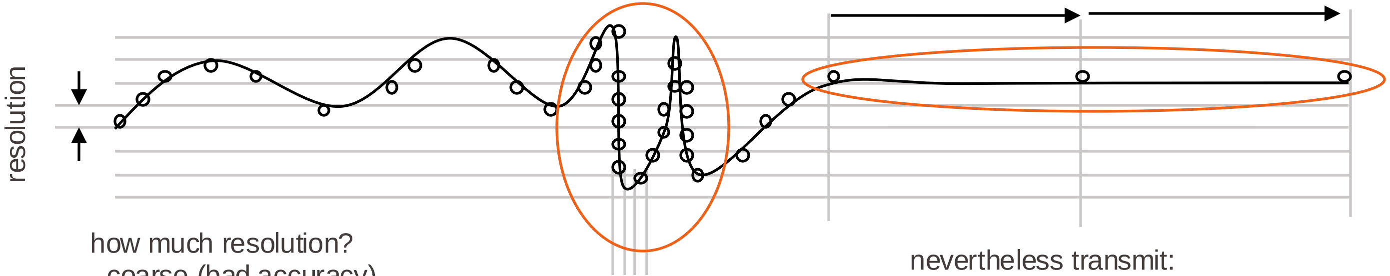
- The actual network can transmit data:
  - cyclically (time-driven) or
  - on demand (event-driven),
  - or a combination of both.

Cyclic versus Event-Driven transmission

cyclic: send value strictly every xx milliseconds



event-driven: send when value change by more than x% of range



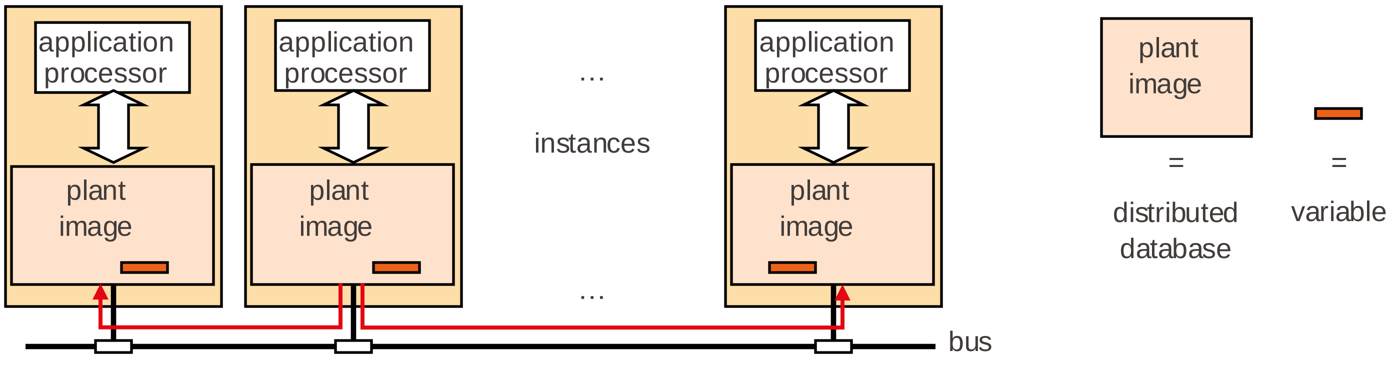
how much resolution?
- coarse (bad accuracy)
- fine (high frequency)

limit update frequency,
limit resolution

nevertheless transmit:
- every xx as “I’m alive” sign
- when data is internally updated
- upon quality change (failure)

Cyclic transmission

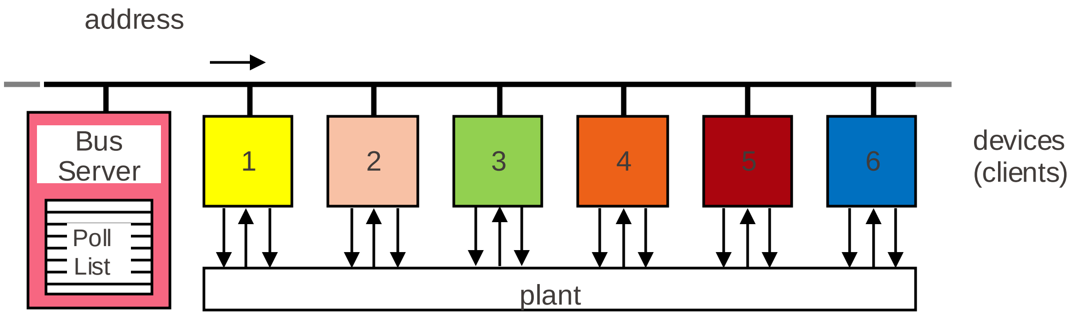
Cyclic Broadcasts



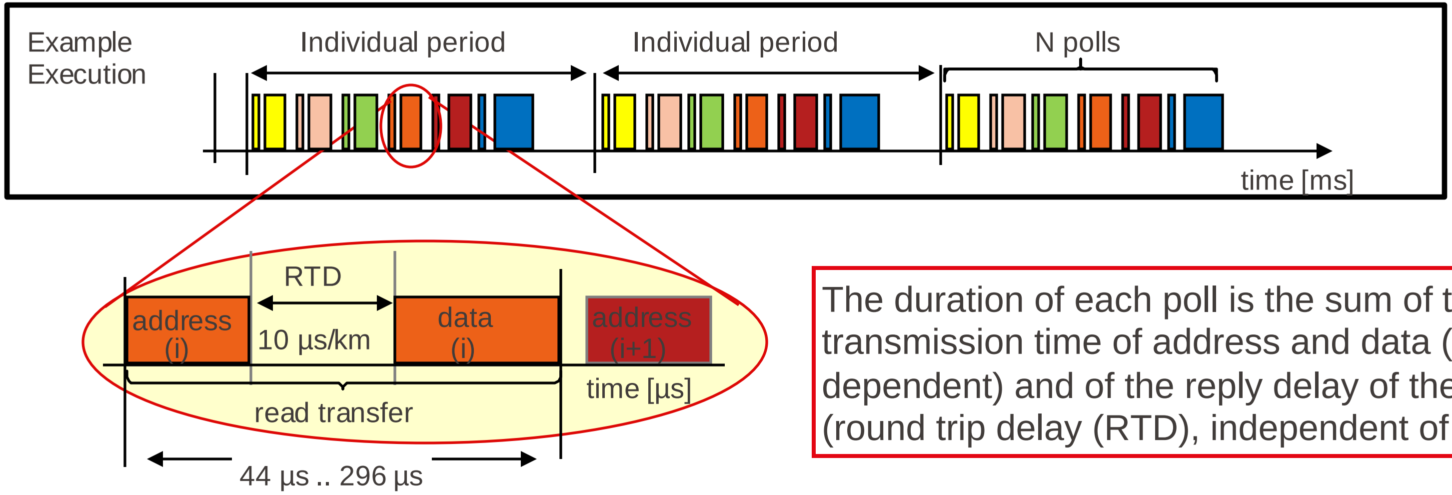
- Most variables are read in multiple devices.
- Broadcasting messages identified by their source (or contents) increases efficiency.
- Only one device is source of a certain process variable (otherwise collision).
- Bus refreshes plant image in the background.
- Replicated traffic memories can be considered as "caches" of the plant state (similar to caches in a multiprocessor system), representing part of the plant image.
- Each station snoops the bus and reads the variables it is interested in.

Each device is source or sink for some process variables

Cyclic Data Transmission with Source Address Broadcast



Principle: server polls addresses in fixed sequence (poll list)



The duration of each poll is the sum of the transmission time of address and data (bit-rate dependent) and of the reply delay of the signals (round trip delay (RTD), independent of bit-rate).

Cyclic operation characteristics

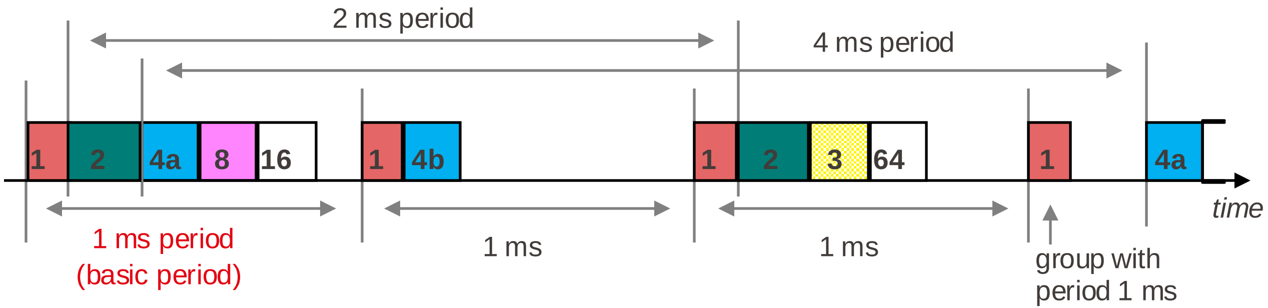
1. Data are transmitted at fixed intervals, whether they changed or not.
2. The delivery delay (refresh rate) is deterministic and constant.
3. The bus is under control of a central server (or distributed time-triggered algorithm).
4. No explicit error recovery needed since fresh value will be transmitted in next cycle. Use a freshness counter to detect stale data.

- Consequence: cycle time limited by product of number of data transmitted and the duration of each poll (e.g. 100 µs / variable x 100 variables → 10 ms)
- To keep the poll time low, only small data items may be transmitted (< 256 bits)

The bus capacity and usage pattern must be configured beforehand.
Determinism gets lost if the cycles are modified at run-time.

Optimizing Cyclic Operation

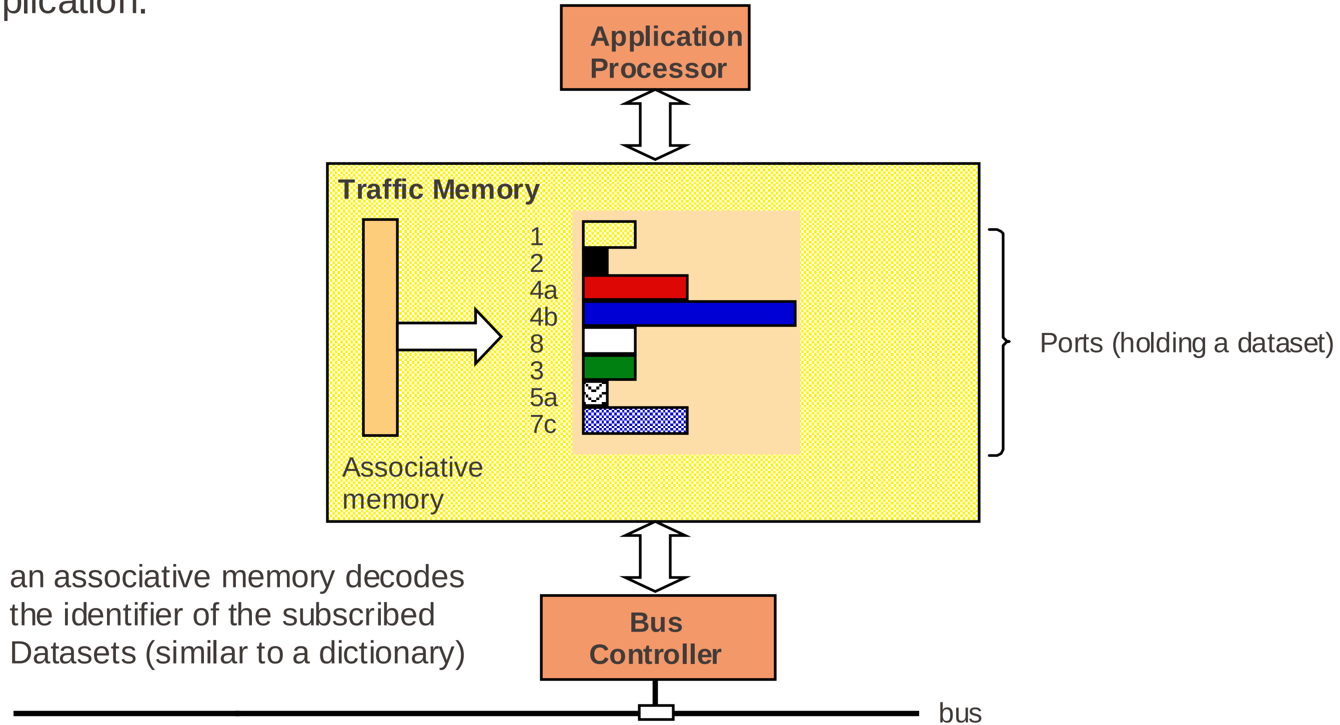
- **Problem:** fixed portion of the bus capacity used
  - load = #bytes transmitted per second
  - utilization = load/capacity
    → poll period increases with number of polled items
    → response time slows down
- **Solution:** introduce sub-cycles for less urgent periodic variables
  length: power of 2 multiple of the base period.



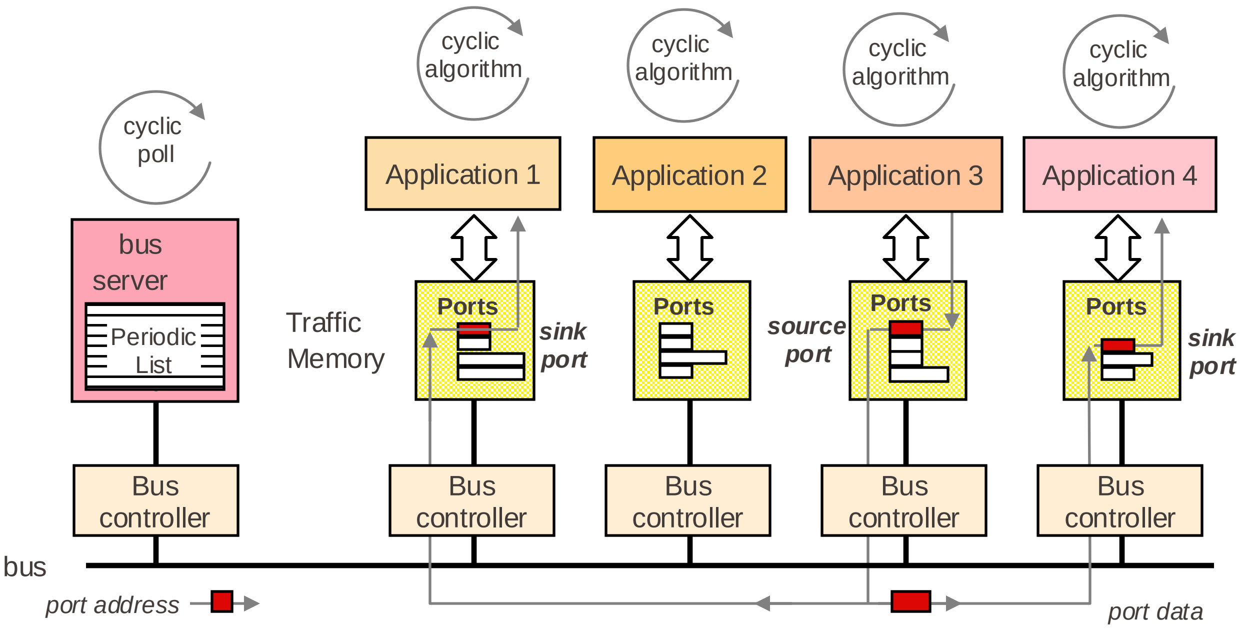
Poll cycles should not be modified at run-time (non-determinism)

Traffic Memory: Implementation

Communication bus and application processor are decoupled by shared memory, the *Traffic Memory* (content addressable memory). Process variables are directly accessible by the application.



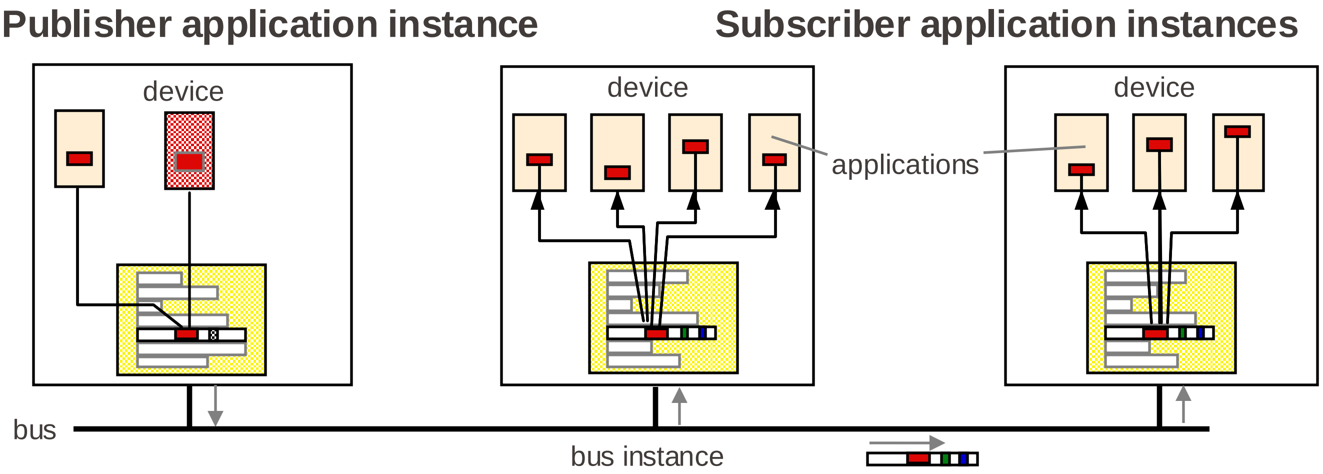
Cyclic Transmission with Decoupled Application



The bus traffic and the application cycles are **asynchronous** to each other.
The bus server scans the identifiers at its own pace.

Deterministic behavior, at expense of reduced bandwidth and geographical extension.

Example: delay requirement

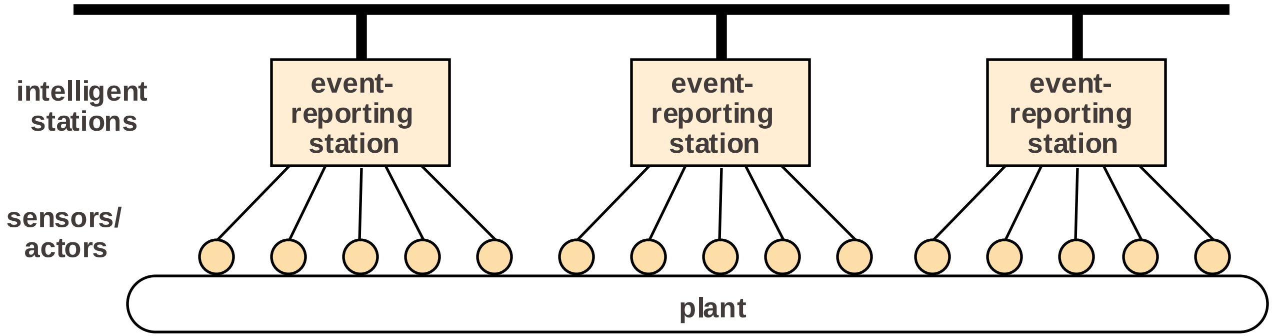


- Worst-case delay for transmitting all time critical variables is the sum of:
  - Source application cycle time 8 ms
  - Individual period of the variable on bus 16 ms
  - Sink application cycle time 8 ms

= 32 ms

Event-driven transmission

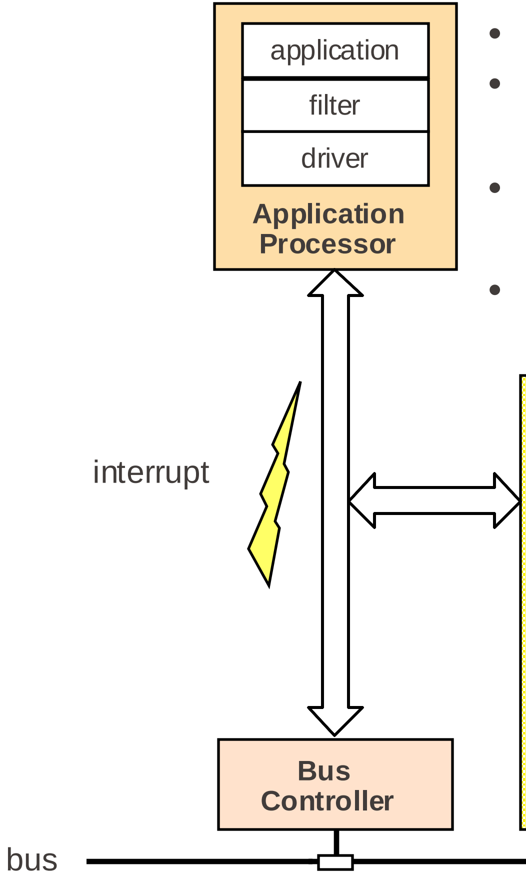
Event-driven Operation

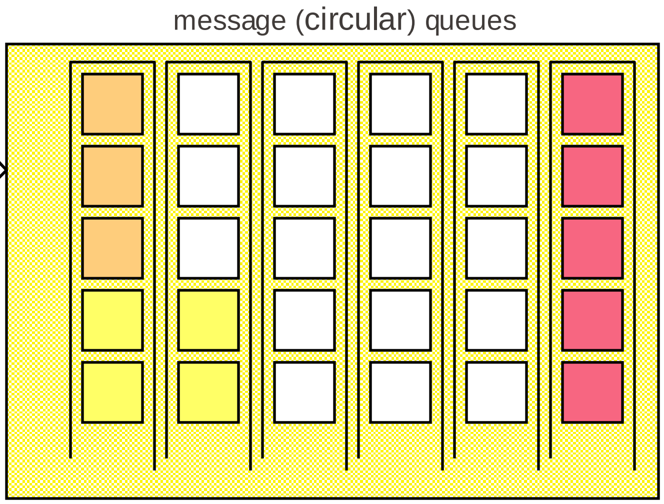


- Events cause transmission only when state changes.
- Bus load very low on average, but peaks under exceptional situations since transmissions are correlated by process.
- Detection of an event is an intelligent process:
  - Not every change of a variable is an event, even for binary variables.
  - Often, a combination of changes builds an event.
  - Only the application can decide what is an event, since only the application programmer knows the meaning of the variables.

Bus interface for event-driven operation

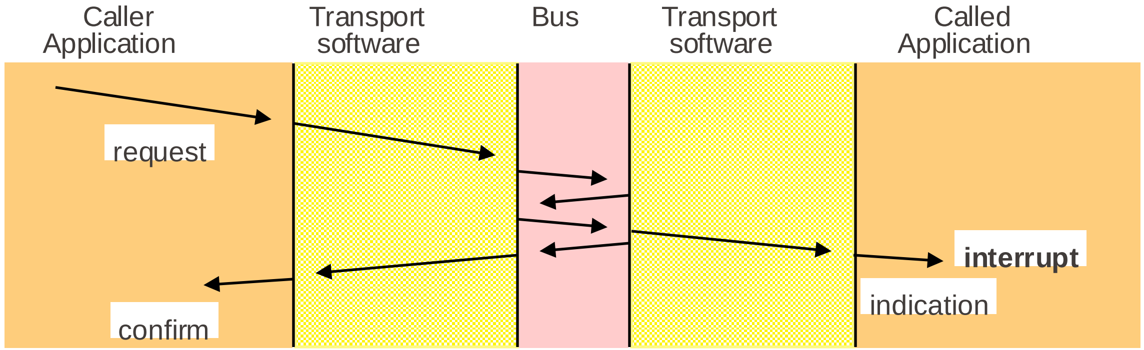
- Each transmission on bus causes an interrupt.
- Bus controller checks address and stores data in message queues.
- Driver is responsible for removing messages of queue memory and prevent overflow.
- Filter decides if message can be processed.





Response of Event-driven operation

- Since events can occur anytime on any device, stations communicate by spontaneous transmission, leading to possible collisions.
- Interruption of server at any instant can disrupt a time-critical task.
- Buffering of events can cause unbounded delays.
- The time required to transmit the event depends on the medium access (arbitration) procedure of the bus.



Events Pros and Cons

In an event-driven control system, there is only a transmission or an operation when an event occurs.

Advantages:

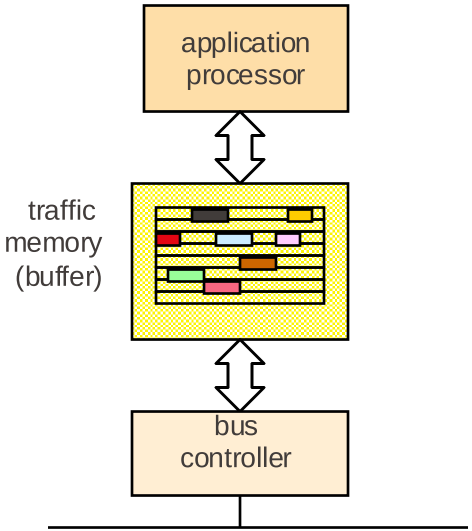
- Can treat a large number of events, but not all at the same time
- Supports a large number of stations
- System idle under steady - state conditions
- Better use of resources
- Suitable for standard (interrupt-driven) operating systems (Unix, Windows)

Drawbacks:

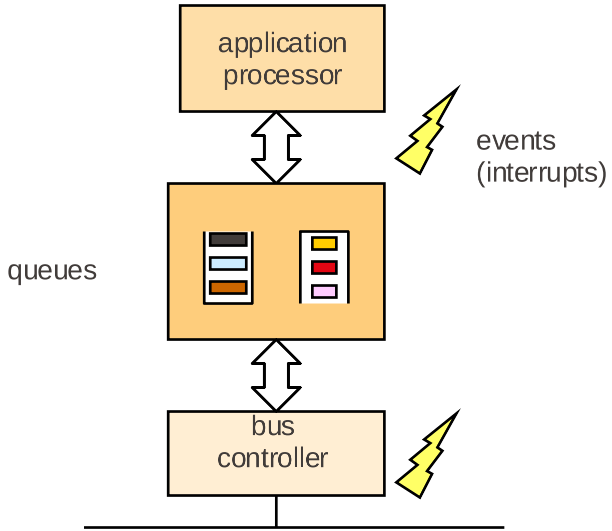
- Needs shared access to resources (arbitration)
- No upper limit to access time if some component is not deterministic
- Response time difficult to estimate, requires analysis
- Limited by congestion effects: process correlated events
- A background cyclic operation is needed to check liveness

Summary: Cyclic vs Event-Driven Operation

decoupled (asynchronous):



coupled (with interrupts):



sending: application writes data into memory

receiving: application reads data from memory

the bus controller decides when to transmit
bus and application are not synchronized

sending: application inserts data into queue and triggers transmission, bus controller fetches data from queue

receiving: bus controller inserts data into queue and interrupts application to fetch them, application retrieves data

How to combine cyclic and event-based transmissions?

Cyclic Transmission

represent the ***state of the plant***

short and urgent data items:

- motor current
- axle speed
- operator's commands
- emergency stops,...

Since variables are refreshed periodically, no retransmission protocol is needed to recover from transmission errors.

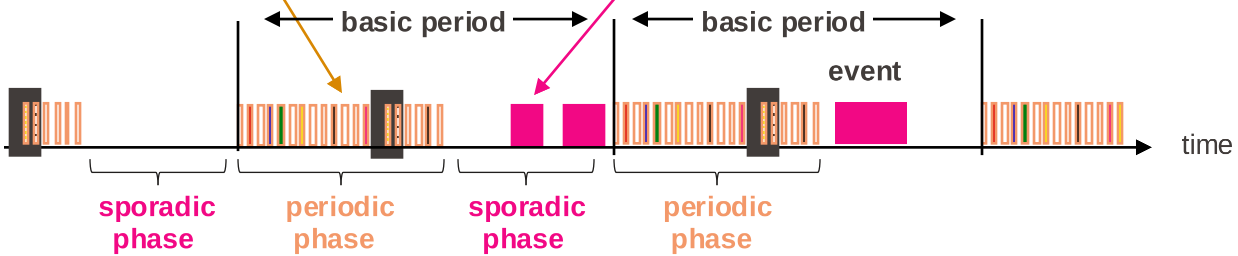
Event-based Transmission

represent ***state changes of the plant***

infrequent, sometimes long messages reporting events, for:

- Users: set points, diagnostics, status
- System: initialisation, down-loading, ...

Since messages represent state changes, a protocol must recover lost data in case of transmission errors.



Cyclic or Event-driven Operation For Real-time?

Cyclic operation:

- Data are transmitted at fixed intervals, whether they changed or not.
- Deterministic: delivery time is bound
- Worst case is normal case
- All resources are pre-allocated

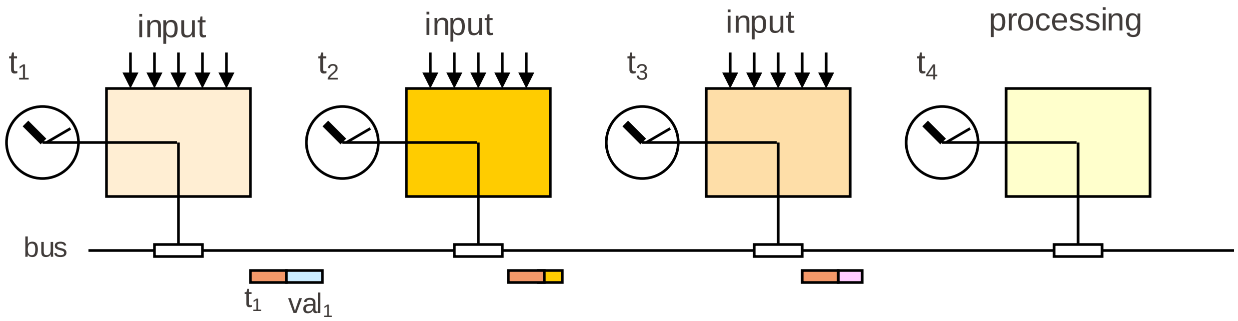
Event-driven operation:

- Data are only transmitted when they change or upon explicit demand.
- Non-deterministic: delivery time vary widely
- Typical case works most of the time
- Best use of resources

Time Synchronization

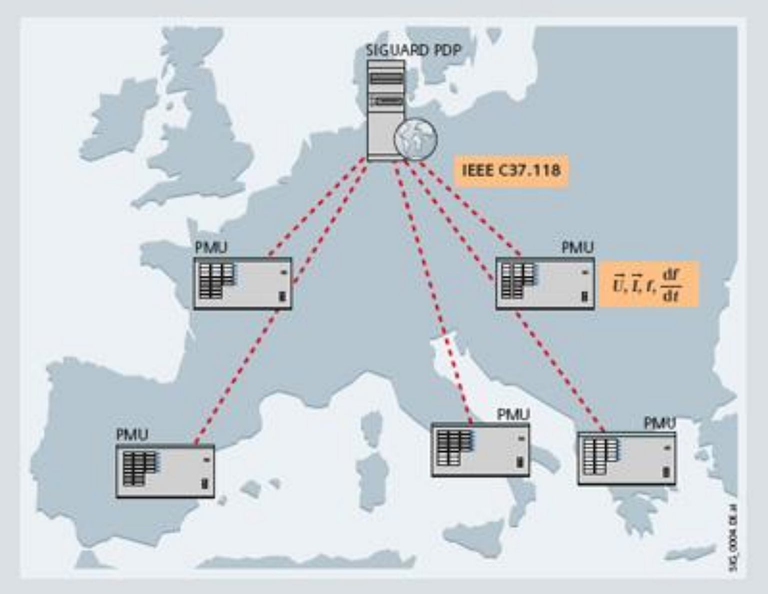
Time-stamping and synchronisation

- In many applications, e.g. disturbance logging and sequence-of-events, the exact sampling time of a variable must be transmitted together with its value.
  - Devices equipped with clock recording creation time of value (not transmission time).
- To reconstruct events coming from several devices, clocks must be synchronized, considering transmission delays and failures.



Example: Phasor information

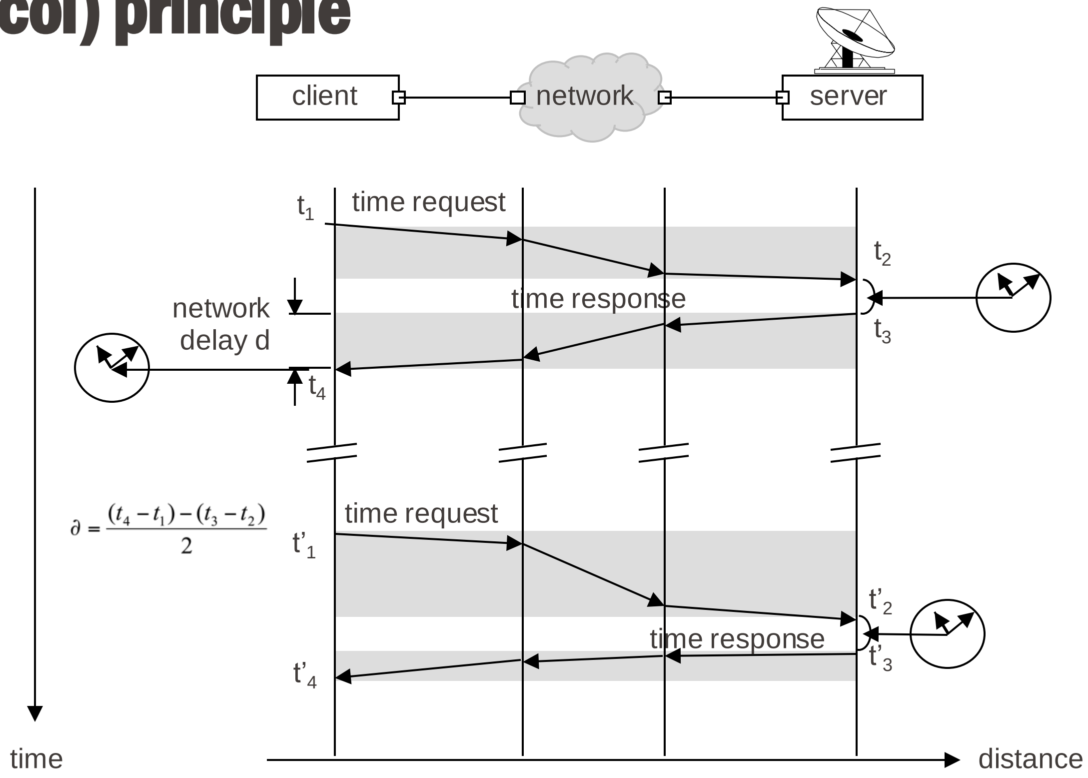
- Phasor transmission over the European grid: a phase error of 0,01 radian is allowed, corresponding to +/- 26 µs in a 60 Hz grid or 31 µs in a 50 Hz grid.



Time distribution

- In client-server busses, server distributes time as bus frame.
- Clients can compensate for path delays, time is relative to server.
- In demanding systems, time is distributed over separate lines as **relative time**, e.g. PPS = one pulse per second, or **absolute time**, with accuracy of 1 µs.
- In data networks, a reference clock (e.g. GPS or atomic clock) distributes time.
- A protocol evaluates **path delays** to compensate them:
  - NTP (Network Time Protocol): about 1 ms is usually achieved.
  - PTP (Precision Time Protocol, IEEE 1588): all network devices collaborate to estimate the delays, an accuracy below 1 µs can be achieved without need for separate cables (but hardware support for time stamping required).

NTP (Network Time Protocol) principle

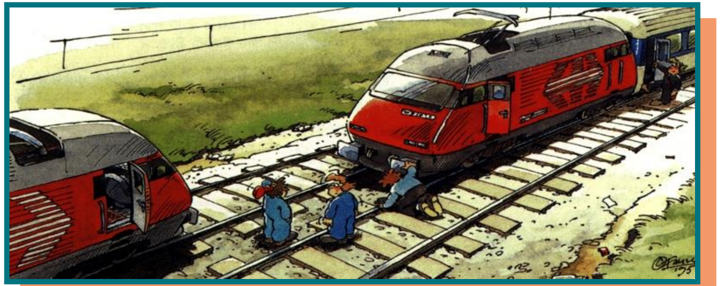


Measures delay end-to-end over the network (one calculation)
Problem: asymmetry in the network delays, long network delays

Assessment

1. What is the difference between a centralized and a decentralized industrial bus?
2. What is the principle of source-addressed broadcast?
3. What is the difference between a time-stamp and a freshness counter?
4. Why is an associative memory used for source-addressed broadcast?
5. What are the advantages / disadvantages of event-driven communication?
6. What are the advantages / disadvantages of cyclic communication?
7. How is time transmitted? Why does it matter?

Field Bus Standards

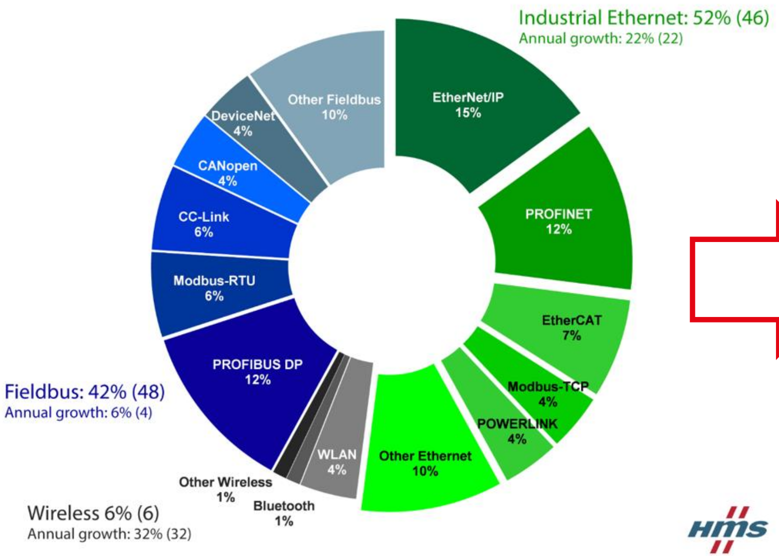


Fieldbus Selection Criteria

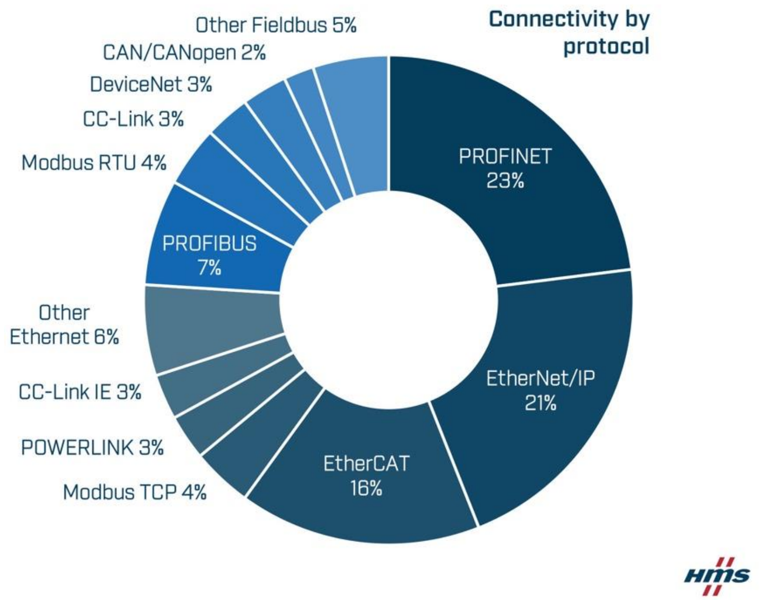
- Installed base, devices availability: processors, input/output
- Interoperability with devices from other vendors
- Topology and wiring technology (layout)
- Power distribution capabilities
- Connection costs per (input-output) point
- Response time
- Deterministic behavior
- Device and network configuration tools
- Bus monitor (baseline and application level) tools

Worldwide most popular field busses

2018



2024



Market shares held by the leading fieldbus and industrial Ethernet systems
Source: HMS Industrial Networks

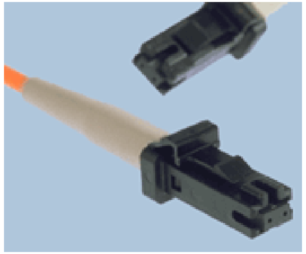
Profibus DP

- Profibus (Process Field Bus) is a field bus standard developed in the 1990s
- Two variants are in use today:
  - PROFIBUS DP (Decentralised Peripherals)
  - PROFIBUS PA (Process Automation)
- Twisted pair cables, bit rates from 9.6 kbit/s to 12 Mbit/s
- Cable length up to 1200m between repeaters

Source: https://en.wikipedia.org/wiki/Profibus

The Industrial Ethernet „Standards“

- IEC SC65C „standardized“ 22 different, incompatible "Industrial Ethernets“, driven by „market demand“.

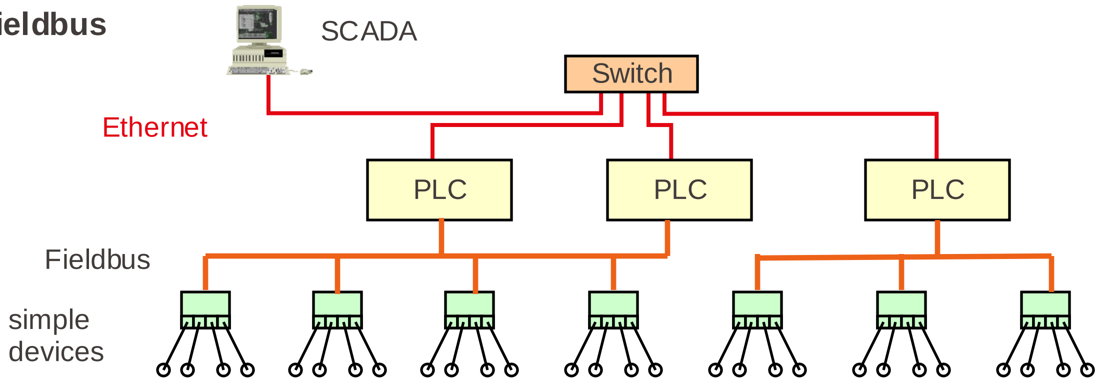


EtherNet/IP	(Rockwell. OVDA)
Profibus, Profinet	(Siemens, PNO)
P-NET	(Denmark)
INTERBUS	(Phoenix)
Vnet/IP	(Yokogawa, Japan)
TCnet	(Toshiba, Japan)
EtherCAT	(Beckhoff, Baumüller)
Powerlink	(BR, AMK)
EPA	(China)
Modbus-RTPS	(Schneider, IDA)
SERCOS	(Bosch-Rexroth / Indramat)
…	

Ethernet Paradigms

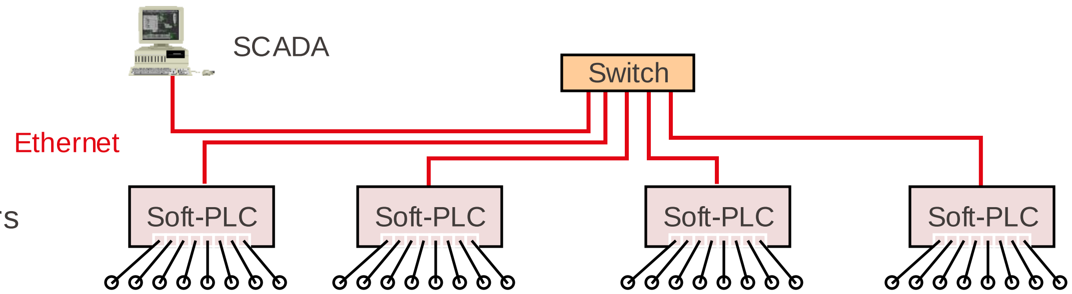
Classical Ethernet + Fieldbus

cheap field devices
decentralized I/O
cyclic operation



Ethernet as Fieldbus

costlier field devices
Soft-PLC as concentrators
Event-driven operation



Ethernet & Time-Sensitive Networking (TSN)

- Set of standards developed by the IEEE 802 TSN task group
- Goal: Allow **time-sensitive** transmissions of data using **deterministic** Ethernet networks
- TSN standards suite provides:
  - Clock synchronization (PTP)
  - Deterministic communication (OSI Layer 2)
  - Traffic scheduling
  - Path control and reservation
  - Redundancy
- Classical Industrial Ethernet protocols (e.g. PROFINET, EtherNet/IP) will be built upon TSN-enabled hardware in the future.

Ethernet-APL (Advanced Physical Layer)

ethernet-apl™
advanced physical layer

- Ethernet 10BASE-T1L (10 MBit/s, full-duplex) over two-wire cables (reuse cables for 4-20mA bus)
- Loop-powered (devices supplied with power over the same cables)
- Long cable lengths (up to 1000 meters)
- Intrinsic safety
- Industry standard support by major manufacturers (Siemens, ABB, Emerson, Rockwell Automation, etc.)

Future of field busses

- Non-time critical busses are being displaced by LANs (Ethernet) and cheap peripheral busses (USB, …)
- The cabling objective of field busses (more than 32 devices over 400 m) is out of reach for cheap peripheral busses such as USB.
- Field busses tend to live very long (10-20 years), contrarily to office products.
- There is no real incentive from the control system manufacturers to reduce the fieldbus diversity, since the fieldbus binds customers.
- TSN-based hardware will be widely available leading to lower costs for industrial networking equipment.
- Wireless plays a niche role, but will enable new applications (e.g. mobile robots connected through 5G)