SIU Southern Illinois University
CARBONDALE

Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 11: Industrial Network Protocols

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

EMAIL: AYDEGER@CS.SIU.EDU

Outline

Other INPs

- Etnernet Powerlink
- SERCOS III

IEC 61850

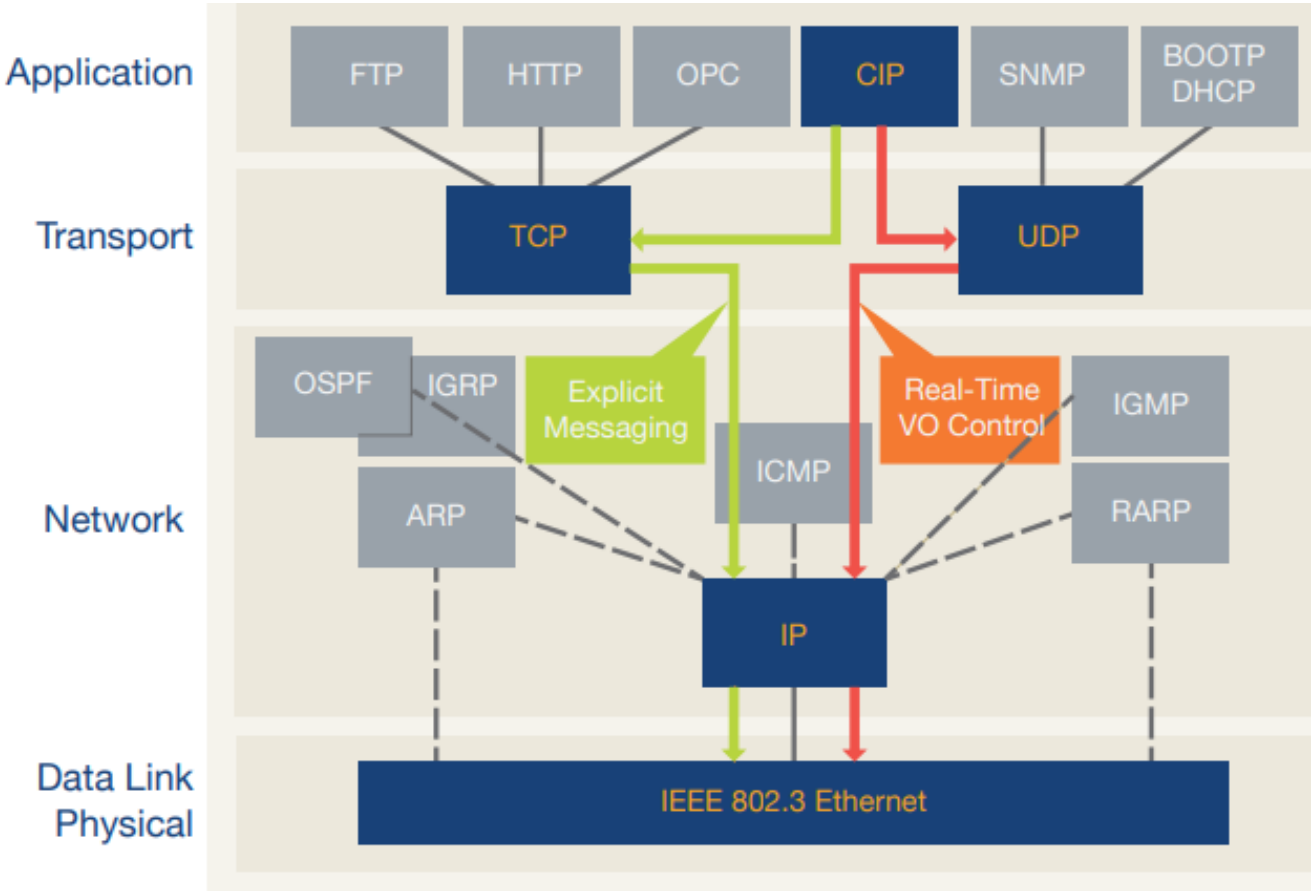
INP Simulators

Recall: Transport Layer of EtherNet/IP

For real-time data transfer, EtherNet/IP also employs UDP over IP to transport messages that contain time-critical control data

- Implicit (I/O data) connections

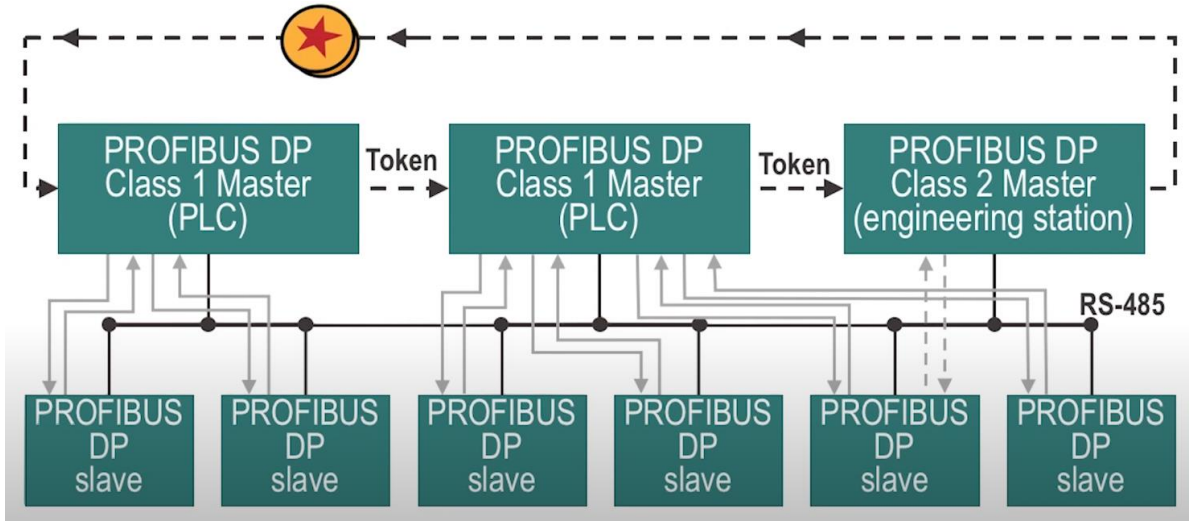
TCP/IP is used in EtherNet/IP to send CIP explicit messages, which are used to perform client-server type transactions between nodes



Recall: Profibus Characteristics

Master/Slave protocol that supports multiple master nodes through the use of token sharing

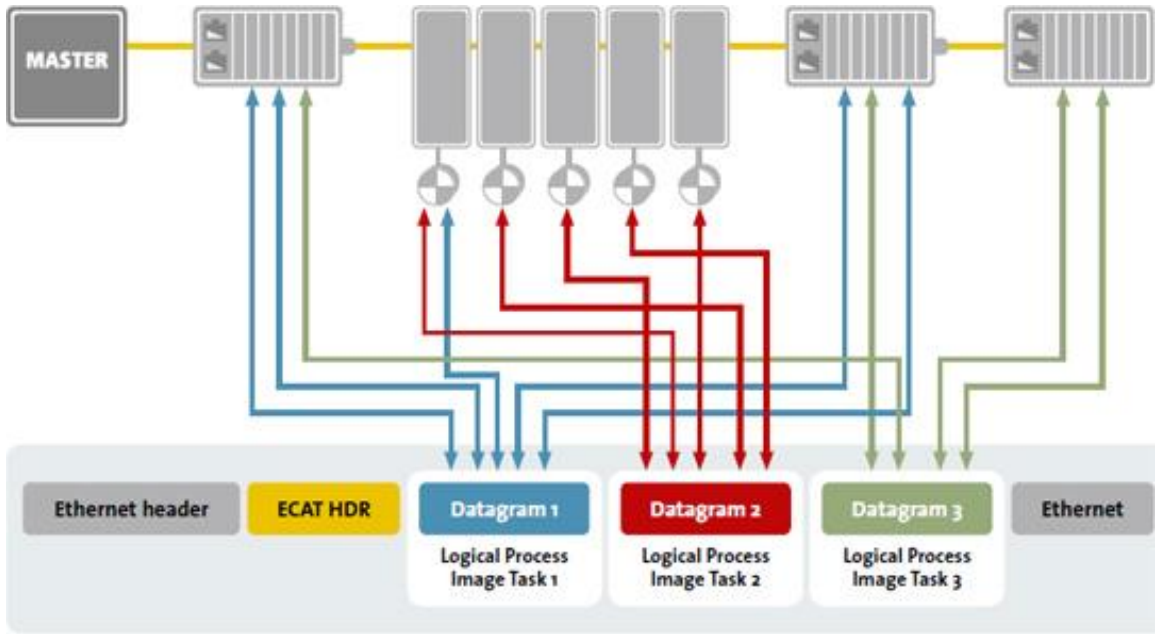
- When a master has control of the token, it can communicate with its slaves
  - Each slave is configured to respond to a single master



Recall: EtherCAT Characteristics

The EtherCAT master sends a telegram that passes through each node.

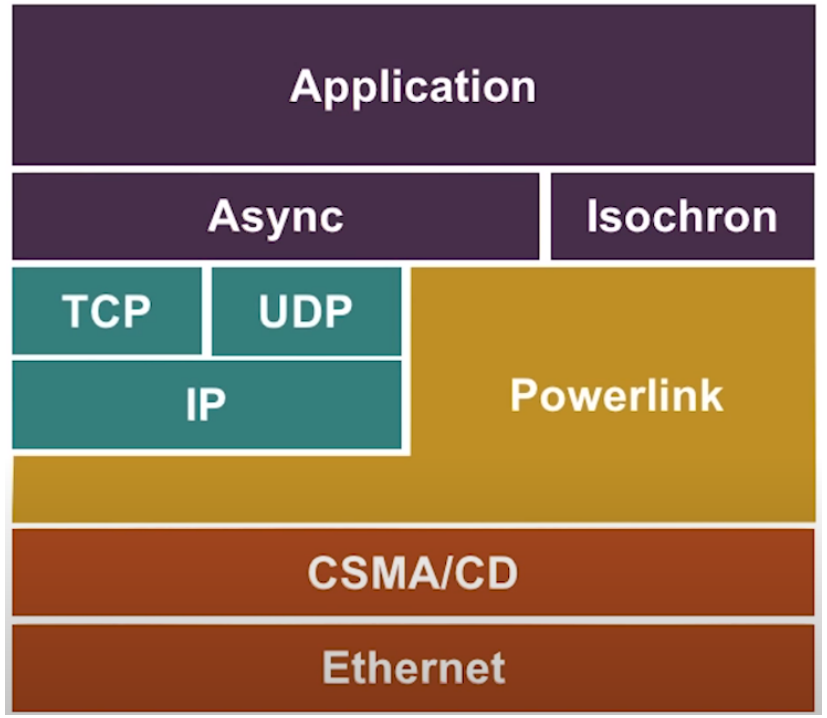
- Each EtherCAT slave device reads the data addressed to it "on the fly", and inserts its data in the frame as the frame is moving downstream
- The frame is delayed only by hardware propagation delay times
- The last node in a segment (or drop line) detects an open port and sends the message back to the master using Ethernet technology's full duplex feature



Ethernet Powerlink

Standard Ethernet in combination with an Internet protocol like TCP/IP is unsuitable for data transmission in hard real time

- Data traffic can be delayed in unforeseeable ways due to the Carrier Sense Multiple Access/Collision Detection (CSMA/CD) mechanism
- Various approaches in their efforts to eliminate such delays
  - Powerlink



How Powerlink Works

Completely software-based solution that is 100% compliant with the IEEE 802.3 Ethernet standard

In order to achieve its real-time capabilities, POWERLINK relies on a mixed polling and time-slot procedure that allows only one node at a time to transmit data

- Managing node (MN) and controlled nodes (CN)

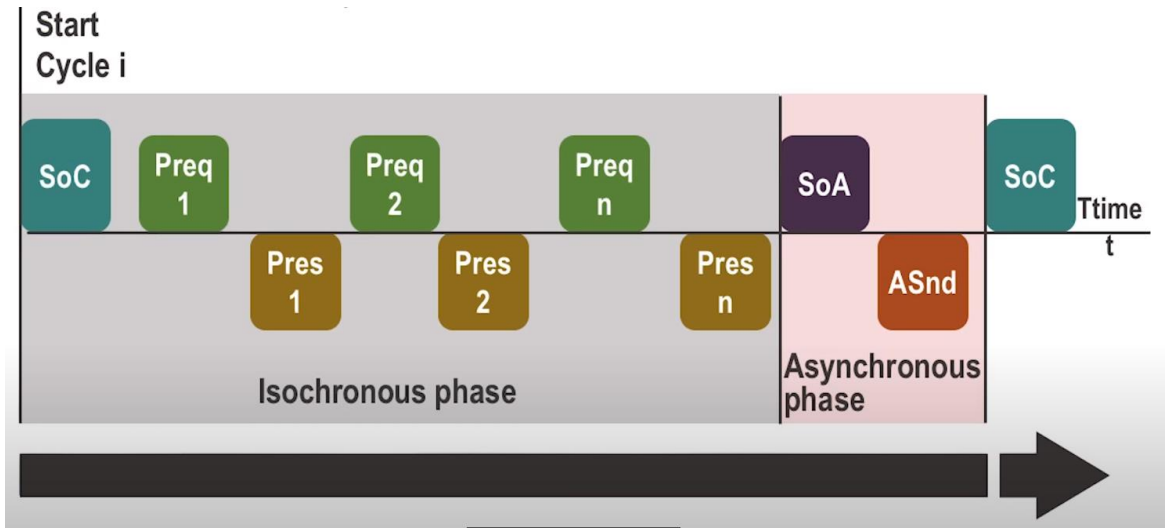
MN defines the clock pulse for synchronizing all devices and manages data communication cycle

- Over the course of one cycle, the MN successively polls each CN using PollRequest messages that also convey additional data from the MN to each polled CN
- Each CN then transmits its own data to all other nodes, this time via PollResponse messages

How Powerlink Works

POWERLINK cycle consists of three phases

- (1) MN sends a "Start of Cycle" (SoC) frame to all CNs to synchronize the devices
- (2) Payload data is then exchanged or isochronous, phase
  - Slave responses are broadcast, eliminating source address resolution
- (3) The third phase of a cycle is the asynchronous phase, which is where non-time-critical data such as TCP/IP data or parameter configuration data is transferred



Powerlink Features

Absolute openness

- Technology is free of any patents. Released under the BSD license in 2008
  - The open source version, openPOWERLINK, is available free of charge

Based on standard Ethernet

- Fully compliant with IEEE 802.3 is a safe choice for the future
  - Will benefit from the long-term evolution of Ethernet technology without requiring further investment

Unmatched features

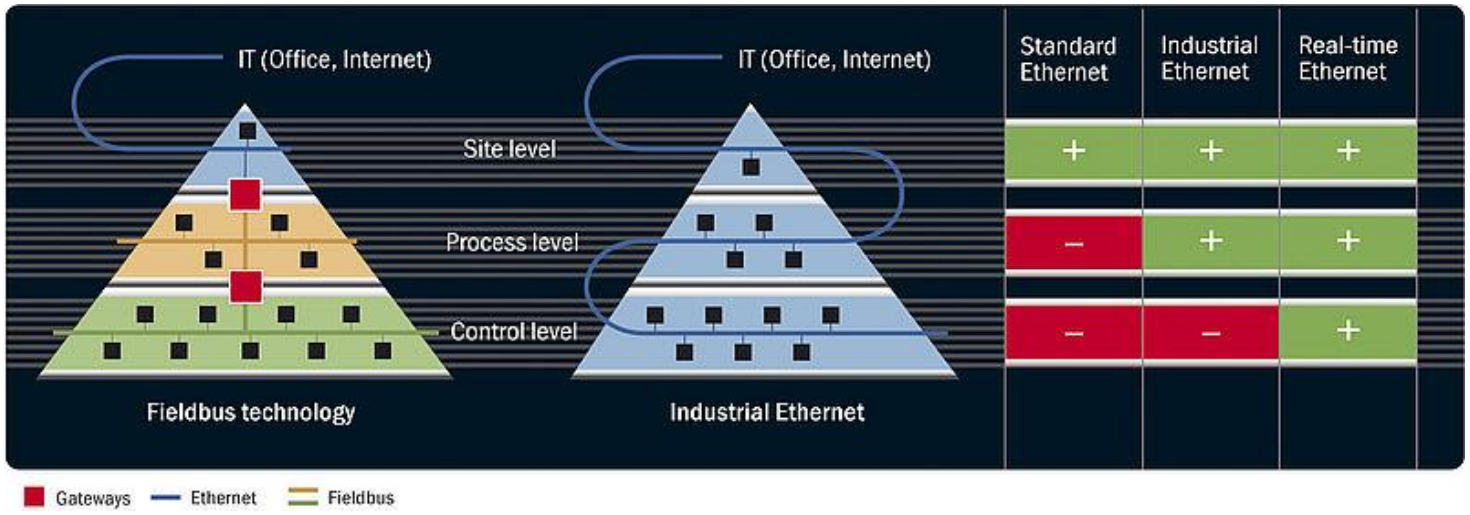
- Ethernet, CANopen, and hard real-time capabilities
- Redundancy, hot plugging, direct cross-traffic, multiplexing, poll response chaining, and more

Powerlink Features

Clear diagnostics

- POWERLINK mechanisms ensure clear diagnostics for installations

Maximum performance



Powerlink Security Concerns

Sensitive and highly susceptible to DoS attacks

Easily disrupted via the insertion of rogue Ethernet frames into the network

- Requiring the separation of Ethernet Powerlink from other Ethernet systems

Powerlink Resources

https://www.ethernet-powerlink.org/powerlink/technology

https://www.kalycito.com/quick-start-powerlink-on-raspberry-pi2/

SERCOS III

Real-time Ethernet communication protocol specifically designed for serial communications between PLCs and IEDs

- Fast Ethernet (100 Mb)

Open digital interface for high speed real-time communications between industrial controls, motion devices, I/O, other peripheral devices and standard Ethernet nodes

Direct cross communication between slaves is possible

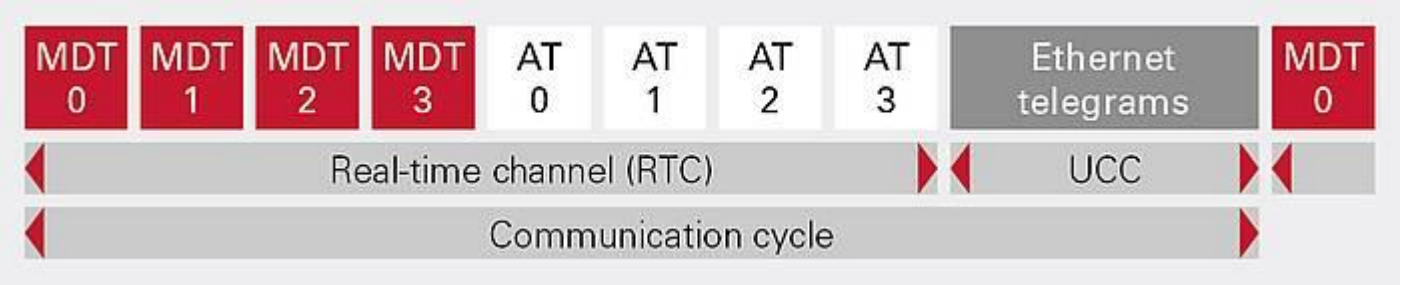
How Sercos III works?

Master/Slave protocol that operates cyclically,

- Using a mechanism in which a single Master Synchronization Telegram is used to communicate to slaves, and the slave nodes are given a predetermined time synchronized by the master node during which they can place their data on the bus

All messages for all nodes are packaged into a Master Data Telegram

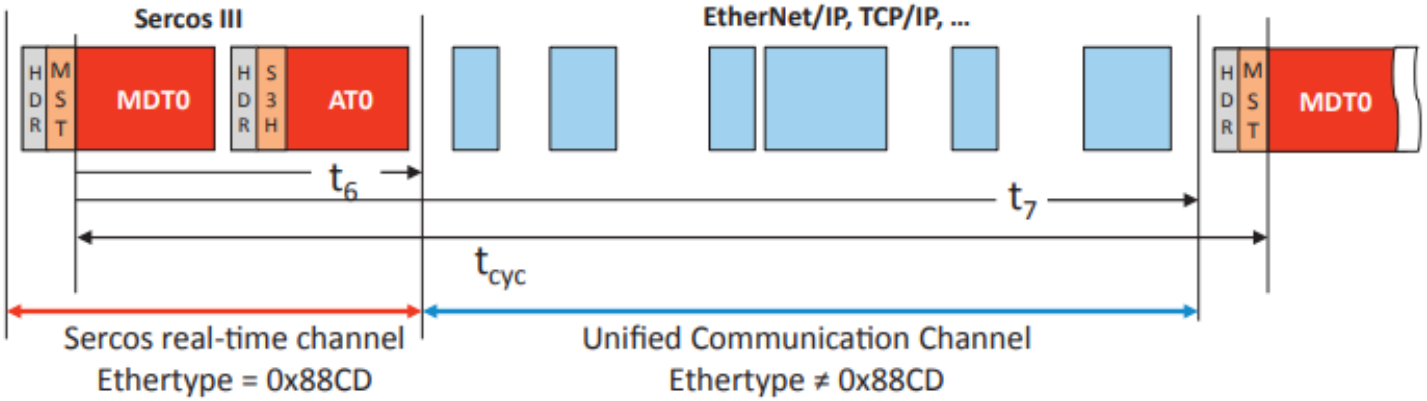
- Each node knows which portion of the MDT it should read based upon a predetermined byte allocation



Sercos III: IP Channel

Unallocated time within a cycle to be freed up for other network protocols such as IP

- This "IP Channel" allows the use of broader network applications from the same device—for example, a web-based management interface that would be accessible to business networks



HDR: Header
S3H: Sercos III header

MDT: Master Data Telegram (MDT):
AT: Reply telegram
MST: Master Sync Telegram

t_{cyc}: Cycle time (31.25 µs ... 65 ms)
t_6: Start of the UC channel
t_7: End of the UC channel

Sercos III: Realtime Channel

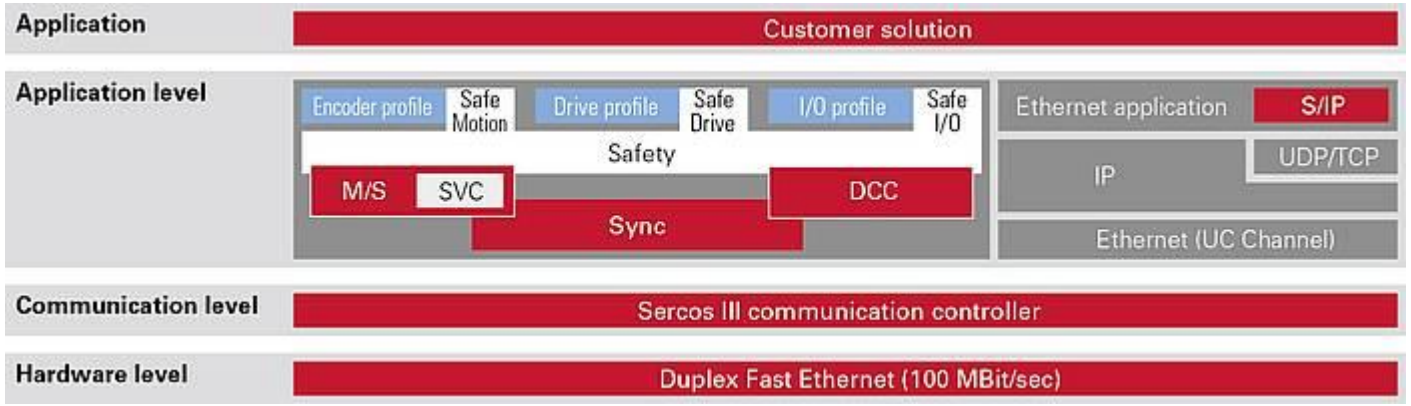
Sercos telegrams in the real-time channel are processed on the fly via individual network devices during the cycle

- The telegrams are therefore only delayed by a few nanoseconds because the whole protocol process is carried out in hardware
  - Network performance is independent of protocol stack, CPU performance or software implementation transmission times

M/S (Master/Slave)

DCC (Direct Cross Communication)

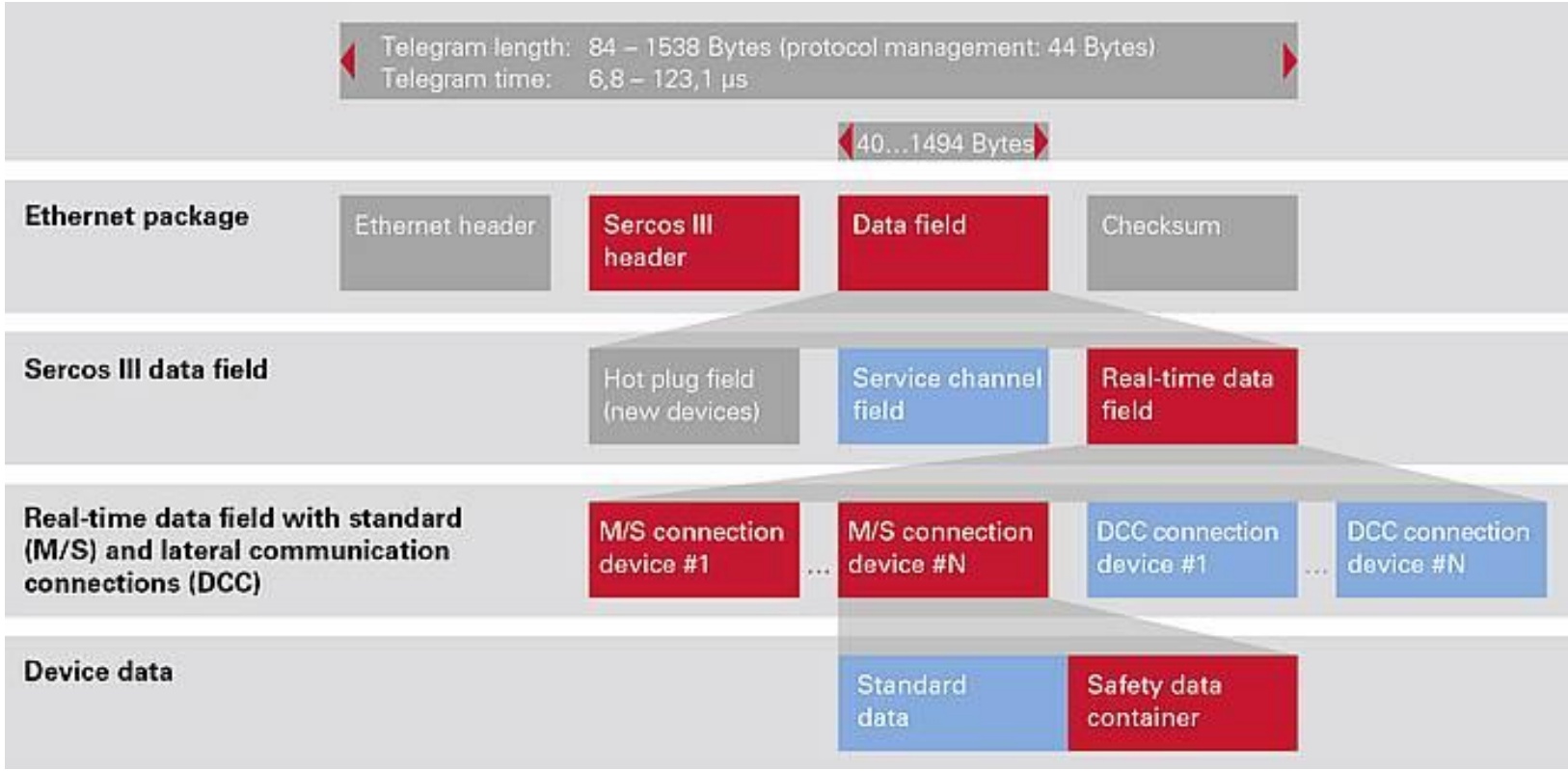
SVC (Service Channel)



Sercos III: Protocol (Data) Structure

Clear and robust data structure

- This increases operational reliability and simplifies application development
- The network status is always clear and entirely transparent
- Easy diagnoses with current Ethernet diagnosis tools



Sercos III: Protocol (Data) Structure

Hot plug field:

- Exchanges data with slaves that have been added to the network while the operation is running

Service channel field:

- Total number of communication channels that exchange acyclic data between master and slaves

Real-time data field:

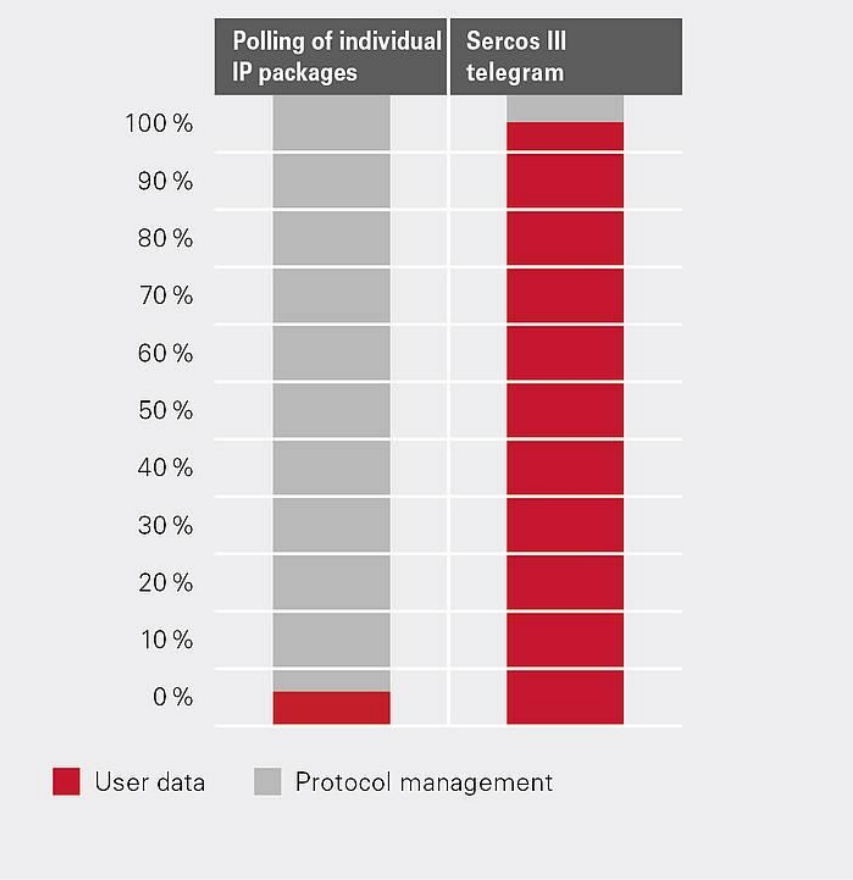
- Used to create acyclic, cyclic or clock-synchronous connections, and so also real-time communication between any devices in the Sercos network

Sercos Performance

If status data of 4 bytes per device for 20 devices were sent individually, that would take up 1,680 bytes = 20*84 bytes altogether (smallest packet size with Ethernet: 64 bytes)

- However, only 80 bytes would be used productively for the application - that's approximately. 5% of the bandwidth, even during low-peak cycle times

In Sercos telegrams, however, up to 1,494 bytes of all device user data is packed together with an additional 44 bytes of overhead. With packets that are a maximum size of 1,538 bytes, the bandwidth available for productive data increases to up to 97%



Sercos Resources

https://www.sercos.org/technology/what-is-sercos/

https://www.kunbus.com/sercos-3.html

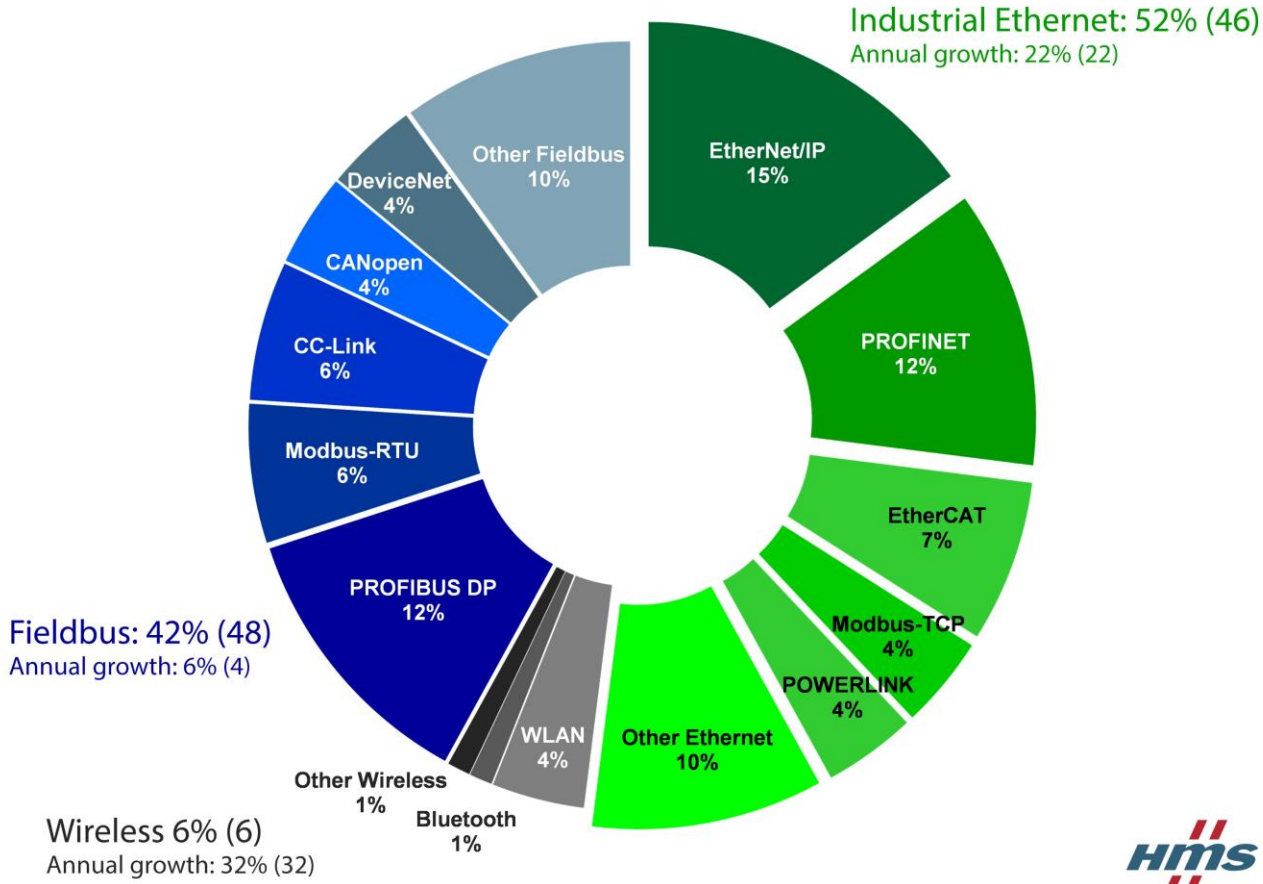
Recent Trend in INPs (2018)

Industrial Ethernet has overtaken traditional fieldbuses in terms of new installed nodes in factory automation.

- Industrial Ethernet now accounts for 52% of new installed nodes (46% last year), while fieldbuses are on 42% (48)

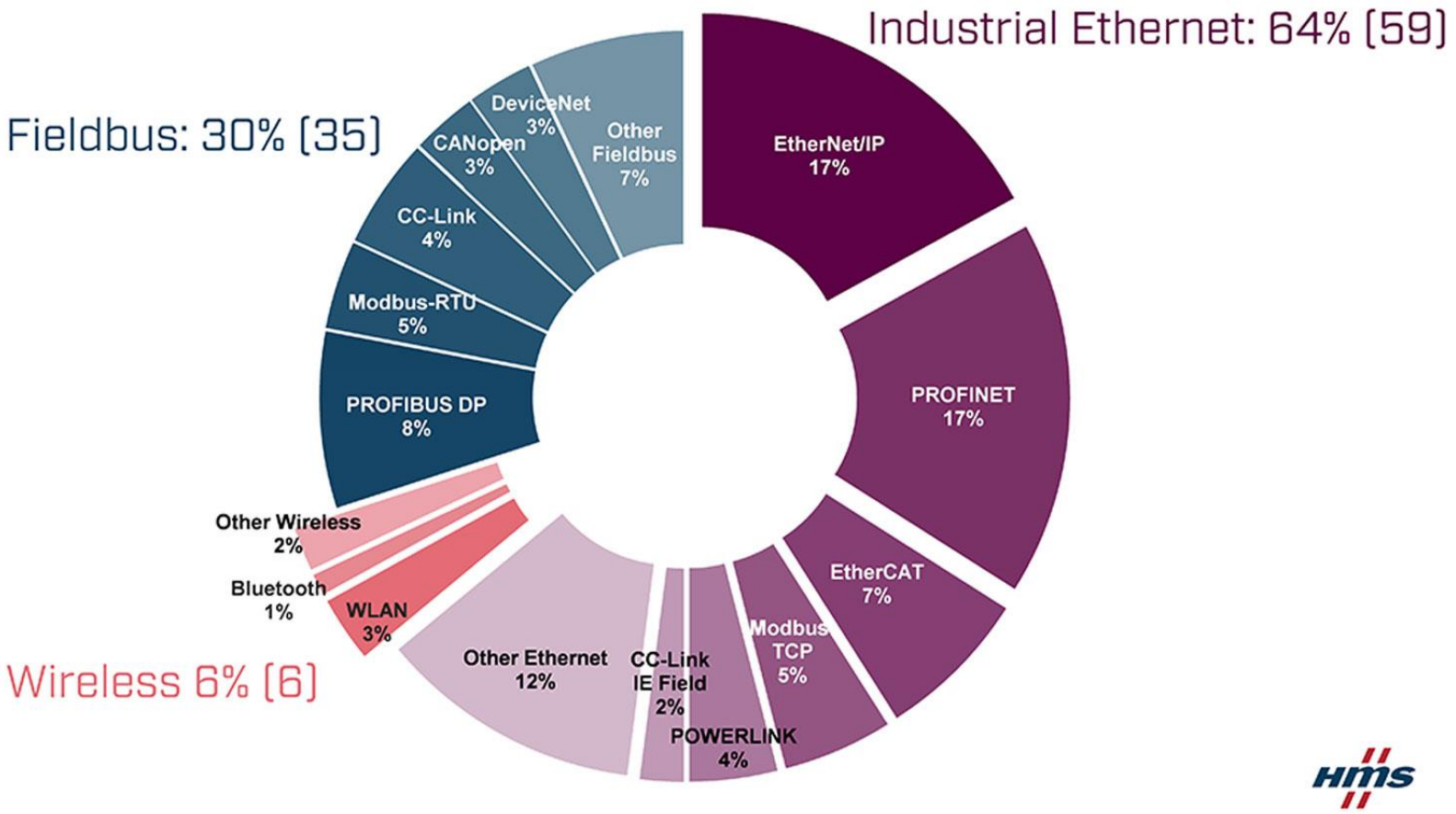
EtherNet/IP is now the most widely installed network at 15%, followed by PROFINET and PROFIBUS, both at 12%

Wireless technologies are also coming on strong with 6% market share



https://www.anybus.com/about-us/news/2018/02/16/industrial-ethernet-is-now-bigger-than-fieldbuses

Recent Trend in INPs (2020)



IEC 61850

Was originally conceived for substation automation

- Called "Communication networks and systems in substation"

Design concepts are incorporated in the areas of power industry

- Generation, transmission, and distribution

Extension of use cases:

- 61850-7-410: Hydroelectric power plants
- 61850-90-1: Communication between substations
- Now called "Communication network and system for power utility automation"

IEC 61850: Design Goals

Permit interoperability of equipment from different manufacturers

Single complete standard for:

- Configuring
- Monitoring
- Reporting
- Storing
- Communicating

IEC 61850 Characteristics

Has a data and communication model, and engineering

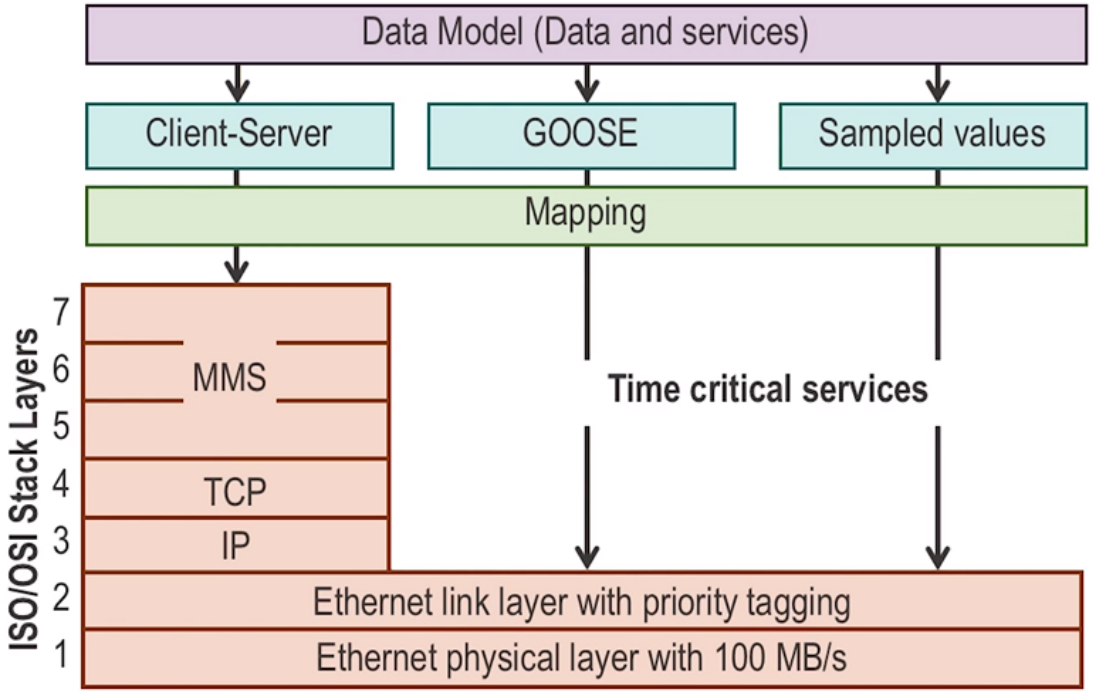
Designed to run on top of Ethernet LAN

- Mostly using fiber cables (even though copper wire can be used)

Protocols supported by IEC 61850

Machine to machine (M2M) or device to device:

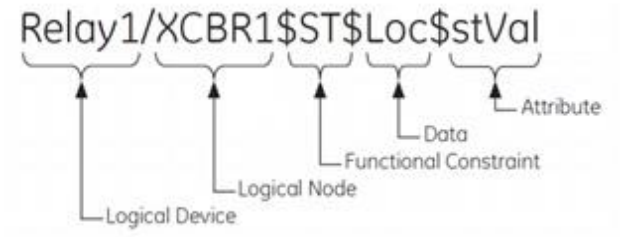
- Generic Substation Event (GSE)
- Peer to peer layer 2 protocol that multicasts events to multiple devices typically IEDs to IEDs
  - Generic Substation State Events (GSSE)
  - Generic Object Oriented Substation Events (GOOSE)
    - Status updates/sending command requests
    - Designed for layer 2 for time critical services
    - Set in Virtual LANs (VLAN)

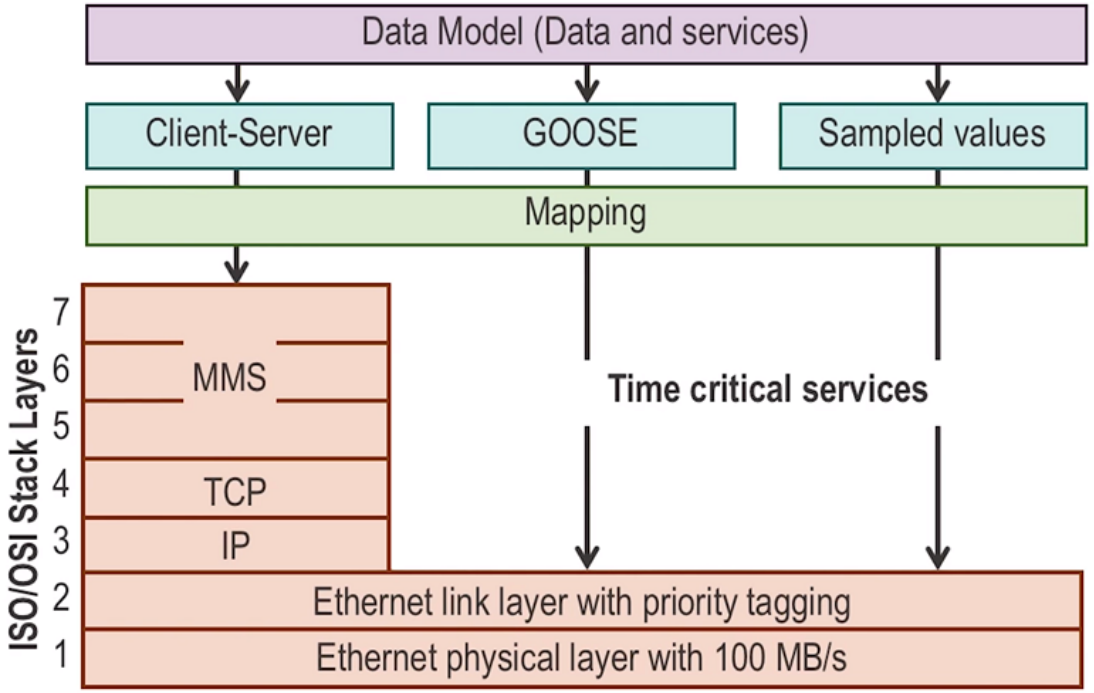


Protocols supported by IEC 61850

Client-server:

- MMS (Manufacturing Message Specification)
  - Monitoring substation status
- Between RTUs (SCADA) and IEDs
  - RTU request field data from IED
- Use XML-based substation configuration language (SCL) to define configuration parameters of IEDs





IEC 61850 Security

No security defined

IEC 62351:

- Requires TLS and message encryption for MMS messages
  - Suggests RSA for message Authentication
- For GOOSE, no security due to its time requirements of 4 ms
  - VLANs are used
    - Easy to spoof

IEC 61850 Resources

Overview of IEC 61850 and Benefits

https://ieeexplore.ieee.org/document/4075831

INP Simulators

For Modbus:

- Modbus simulator: https://sourceforge.net/projects/modrssim/
- Modsak - Modbus diagnostic program: https://wingpath.co.uk/modbus/modsak.php
- ModbusPal - Java MODBUS simulator: http://modbuspal.sourceforge.net/
- Triangle Microworks, Communication Protocol Test Harness (also DNP3): https://www.trianglemicroworks.com/products/testing-and-configuration-tools/test-harness-pages/overview

INP Simulators

For DNP3:

- Axon Group: https://www.axongroup.com.co/dnp3/?lang=en

For OPC:

- Matrikon OPC Tools: https://www.matrikonopc.com/products/opc-desktop-tools/index.aspx
- Kepware: https://www.kepware.com/en-us/products/kepserverex/drivers/torque-tool-ethernet/

For ICCP:

- Iron - IEC 60870-6 (TASE.2/ICCP) Test Tool: https://www.trianglemicroworks.com/products/testing-and-configuration-tools/iron-pages/overview