SIU Southern Illinois University
CARBONDALE

Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 10: Industrial Network Protocols

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

EMAIL: AYDEGER@CS.SIU.EDU

Outline

Etnernet/IP

Profibus

EtherCat

Recall: Inter Control Center Protocol (ICCP)

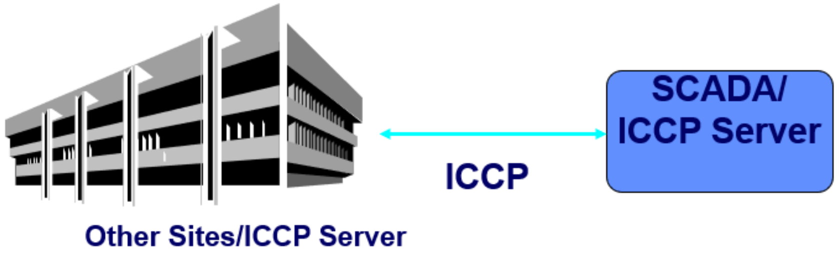
Also known as TASE.2 or IEC 60870-6

Designed for communication between control centers within the energy industry

- Bidirectional Wide Area Network (WAN) communication between a utility control center and other control centers; power plants, substations, and even other utilities

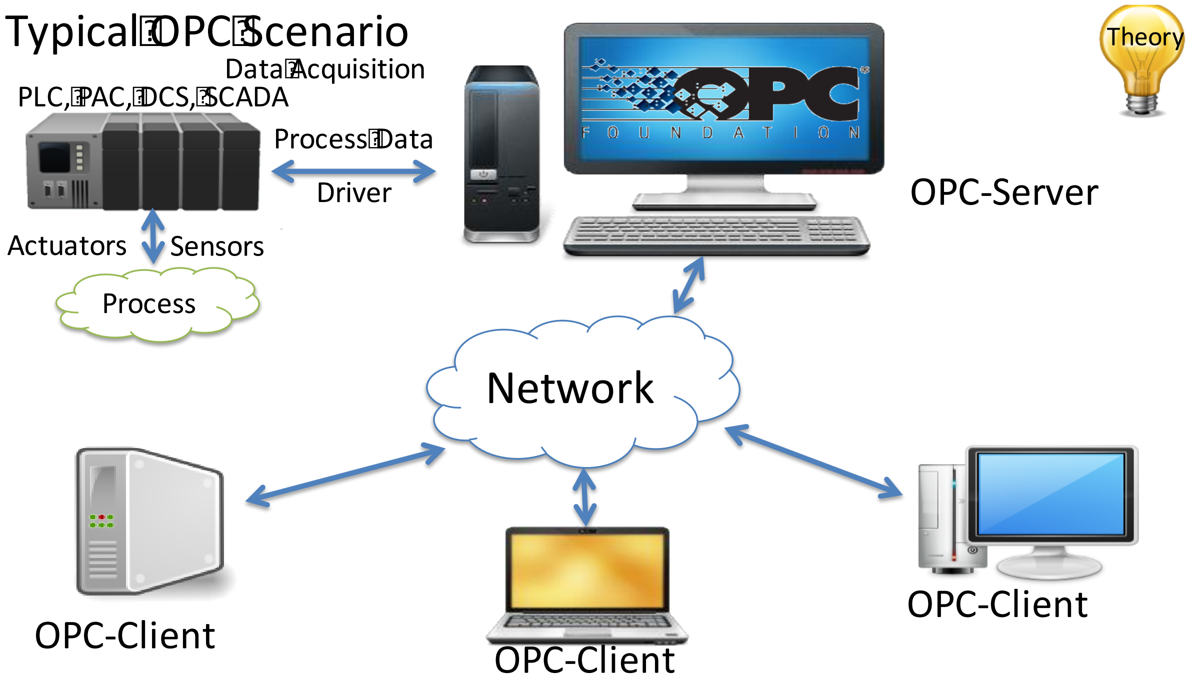
Why is it required?

- To provide standardization for different entities managing regional utilities
- Vendor interoperability over any network



Recall: OPC Characteristics

Primary function is to interconnect other distributed control systems with Windows hosts



Typical OPC Scenario

Data Acquisition

PLC, PAC, DCS, SCADA

Process Data

Driver

Actuators

Sensors

Process

OPC-Server

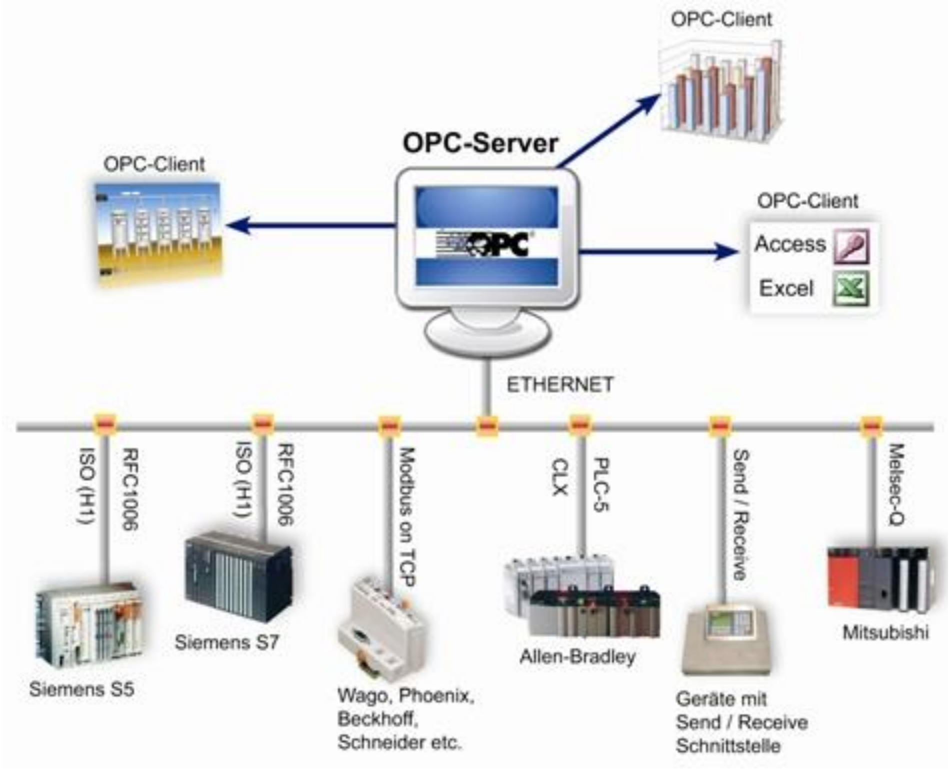
Theory

Network

OPC-Client

OPC-Client

OPC-Client



EtherNet/IP

Uses standard Ethernet frames (ethertype 0x80E1) in conjunction with the Common Industrial Protocol (CIP)

- EtherNet/IP is a member of a family of networks that implements CIP at its upper layers

Typically client/server

- “implicit” mode is supported to handle real-time requirements

Implicit mode uses connectionless transport—specifically the User Datagram Protocol (UDP) and multicast transmissions

- To minimize latency and jitter

Common Industrial Protocol (CIP)

Object models to define the various qualities of a device

- Required Objects: define attributes such as device identifiers, routing identifiers
  - Other attributes of a device such as the manufacturer, serial number, date of manufacture, etc.
- Application Objects: define input and output profiles for devices
- Vendor-specific Objects: enable vendors to add proprietary objects to a device

Objects (other than vendor-specific objects) are standardized by device type and function,

- To facilitate interoperability

CIP

Required Objects provide a common and complete set of identifying values

Application Objects contain a common and complete suite of services for control, configuration, and data collection

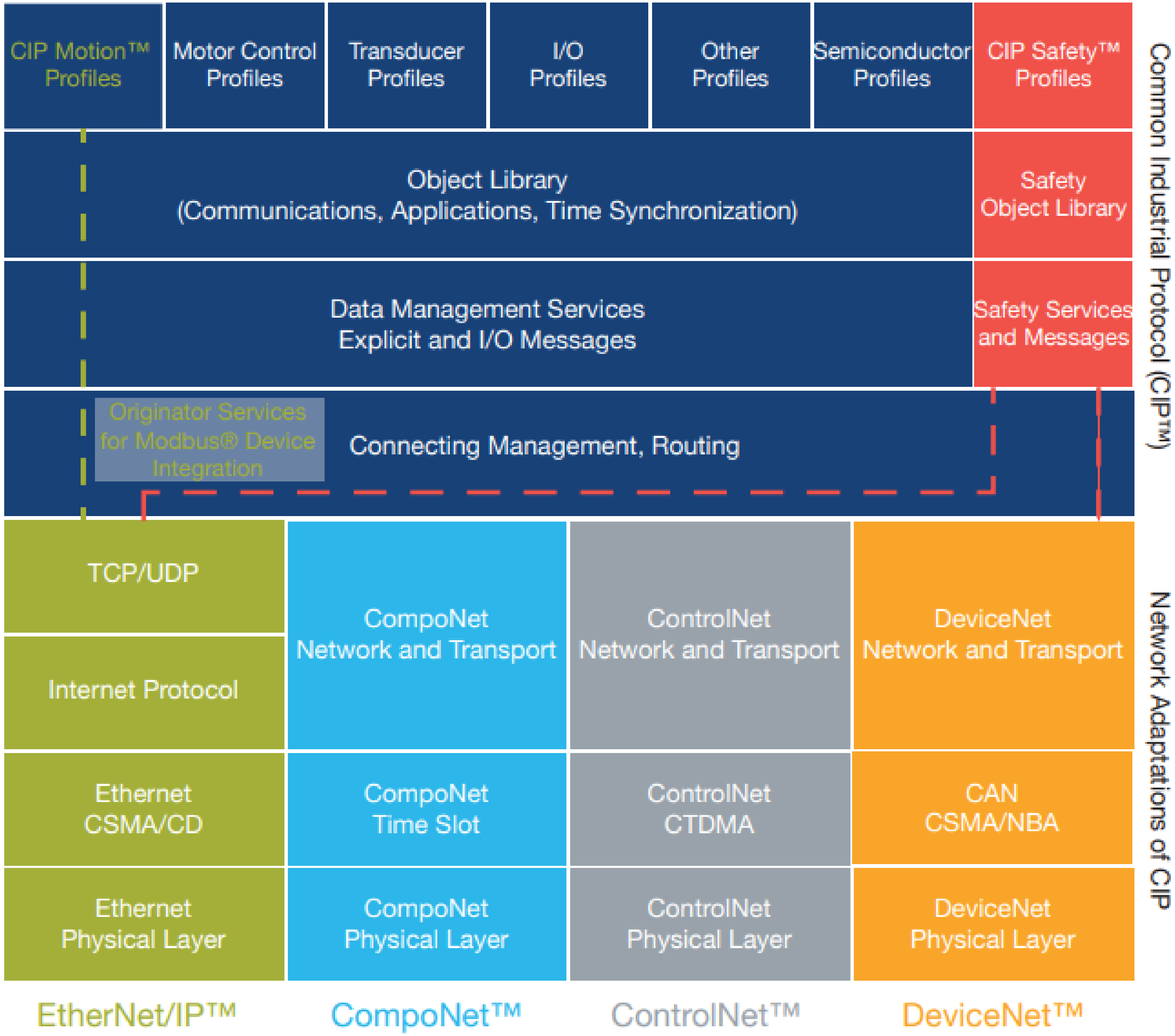
<u>Media-independent</u> protocol that is supported by hundreds of vendors around the world

- CIP provides users with a unified communication architecture throughout the manufacturing enterprise
- Media independence comes the ability to choose the CIP Network best suited for each application
  - One of these possible choices is EtherNet/IP, which adapts CIP to Ethernet technology

CIP Protocol Stack

For EtherNet/IP:

- Data Link Layer: Ethernet
- Network Layer: IP
- Transport Layer: TCP or UDP



CIP Motion™ Profiles
Motor Control Profiles
Transducer Profiles
I/O Profiles
Other Profiles
Semiconductor Profiles
CIP Safety™ Profiles

Object Library
(Communications, Applications, Time Synchronization)

Safety Object Library

Data Management Services
Explicit and I/O Messages

Safety Services and Messages

Originator Services for Modbus® Device Integration

Connecting Management, Routing

TCP/UDP
Internet Protocol
Ethernet CSMA/CD
Ethernet Physical Layer
EtherNet/IP™

CompoNet Network and Transport
CompoNet Time Slot
CompoNet Physical Layer
CompoNet™

ControlNet Network and Transport
ControlNet CTDMA
ControlNet Physical Layer
ControlNet™

DeviceNet Network and Transport
CAN CSMA/NBA
DeviceNet Physical Layer
DeviceNet™

Common Industrial Protocol (CIP™)

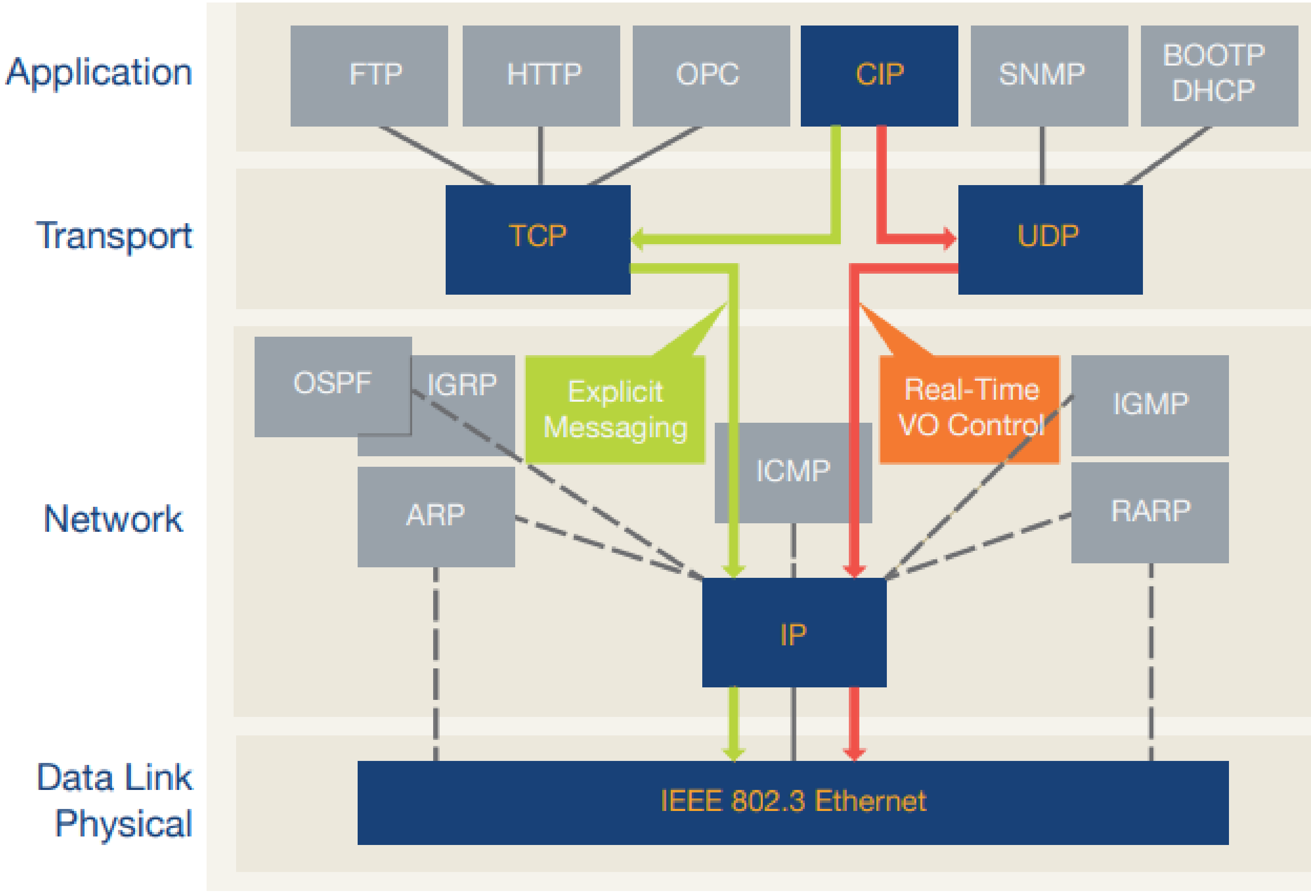
Network Adaptations of CIP

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



Ethernet/IP Advantages

Complete producer-consumer services

- Simultaneously and seamlessly control, configure and collect data

Compatible with standard Internet protocols

EtherNet/IP network infrastructure can accommodate a virtually unlimited number of point-to-point nodes

- Can also support linear and ring topologies providing users
  - Accommodate user current requirements while enabling cost-effective expansion in the future

Security Concerns of EtherNet/IP

Real-time Ethernet protocol, and as such it is susceptible to any of the vulnerabilities of Ethernet

The CIP does not define any explicit or implicit mechanisms for security

- Never designed as a secure communications transport

CIP Security

Authentication of the endpoints:

- Ensuring that the target and originator are both trusted entities
- End point authentication is accomplished using digital certificates or pre-shared keys

Message integrity and authentication:

- Ensuring that the message was sent by the trusted endpoint and was not modified in transit
- Message integrity is accomplished via TLS and authentication via Hash Message Authentication Codes (HMAC)

Message confidentiality:

- Optional capability to encrypt the communications,
  - Provided by the encryption algorithm that is negotiated via the TLS (transport layer security) handshake

EtherNet/IP Resources

https://www.odva.org/wp-content/uploads/2020/05/PUB00138R6-Tech-Series-EtherNetIP.pdf

https://www.rumsey.com/cip-security-how-does-it-work

https://ir.rockwellautomation.com/press-releases/press-releases-details/2018/Rockwell-Automation-Introduces-First-Industrial-Control-Devices-to-Support-CIP-Security/default.aspx

Profibus (Process fieldbus)

Initially designed to allow communication from PLC to host computer

A digital network responsible for providing the communication between the field sensors and the control system or the controllers

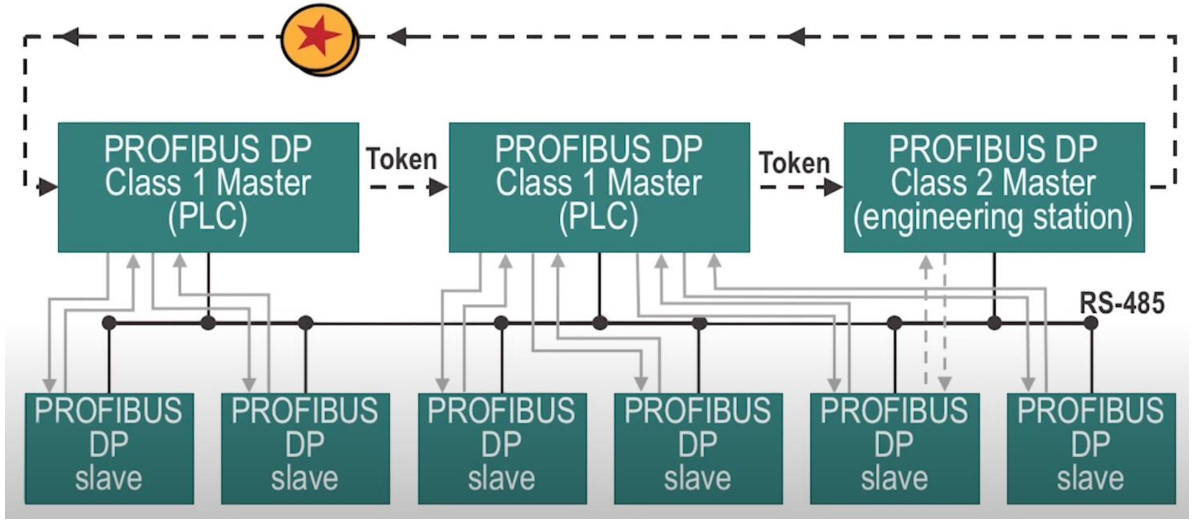
- First in factory automation industries,
  - Then process industries, manufacturing, etc.

Via a single bus cable, PROFIBUS links controller or control systems with decentralized field devices (sensors and actuators) on the field level

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



Profibus Variants

Profibus-DP (Decentralized Periphery)

- DP-V0, DP-V1, and DP-V2
- In V2, slaves can initiate communications to the master or to other slaves under certain conditions.
    - Typically, a master Profibus node is a PLC or RTU, and a slave is sensor, motor, or some other control system device

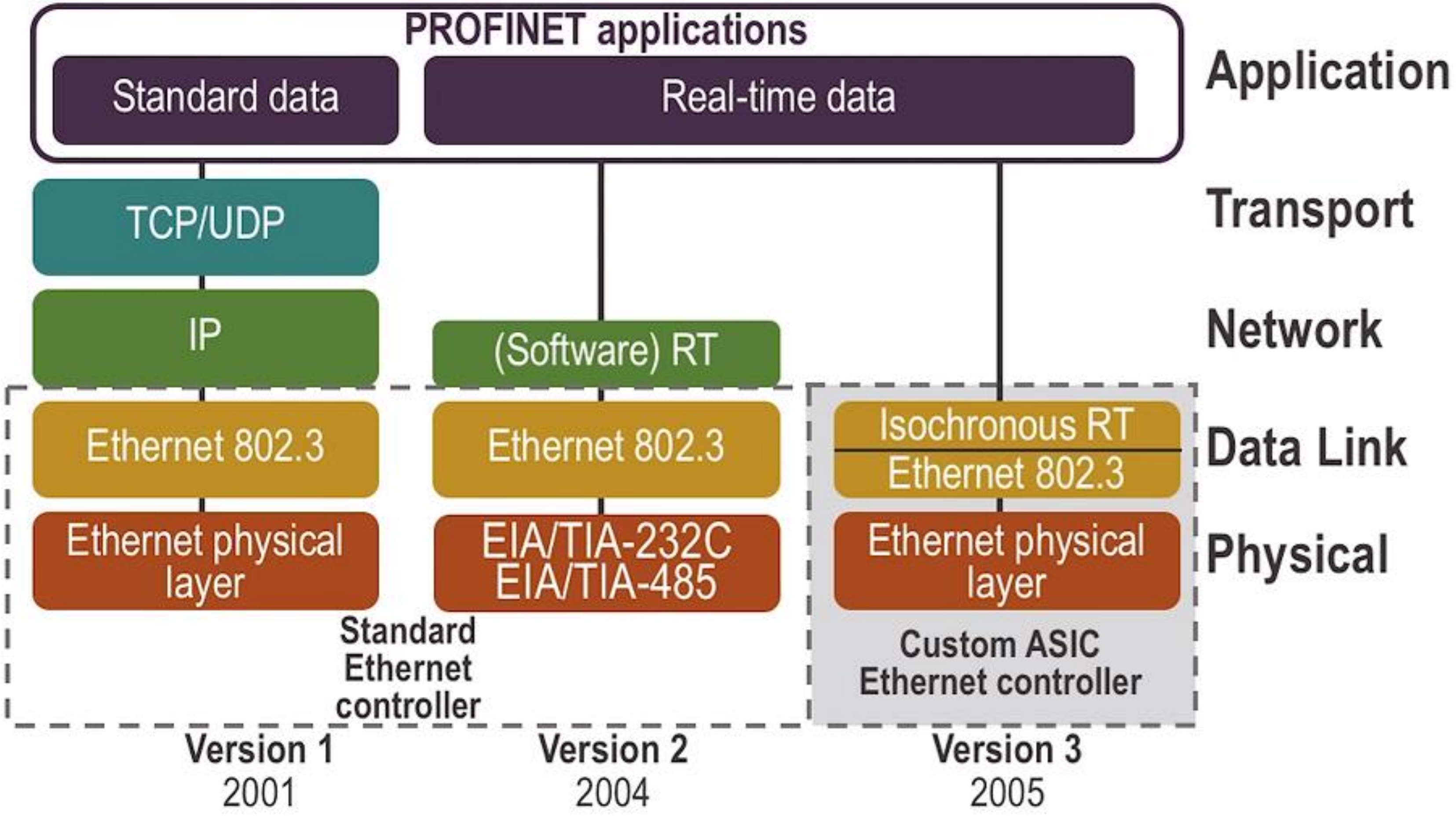
Profibus-PA (Process Automation)

Profibus-FMS (Fieldbus Messaging System): Outdated

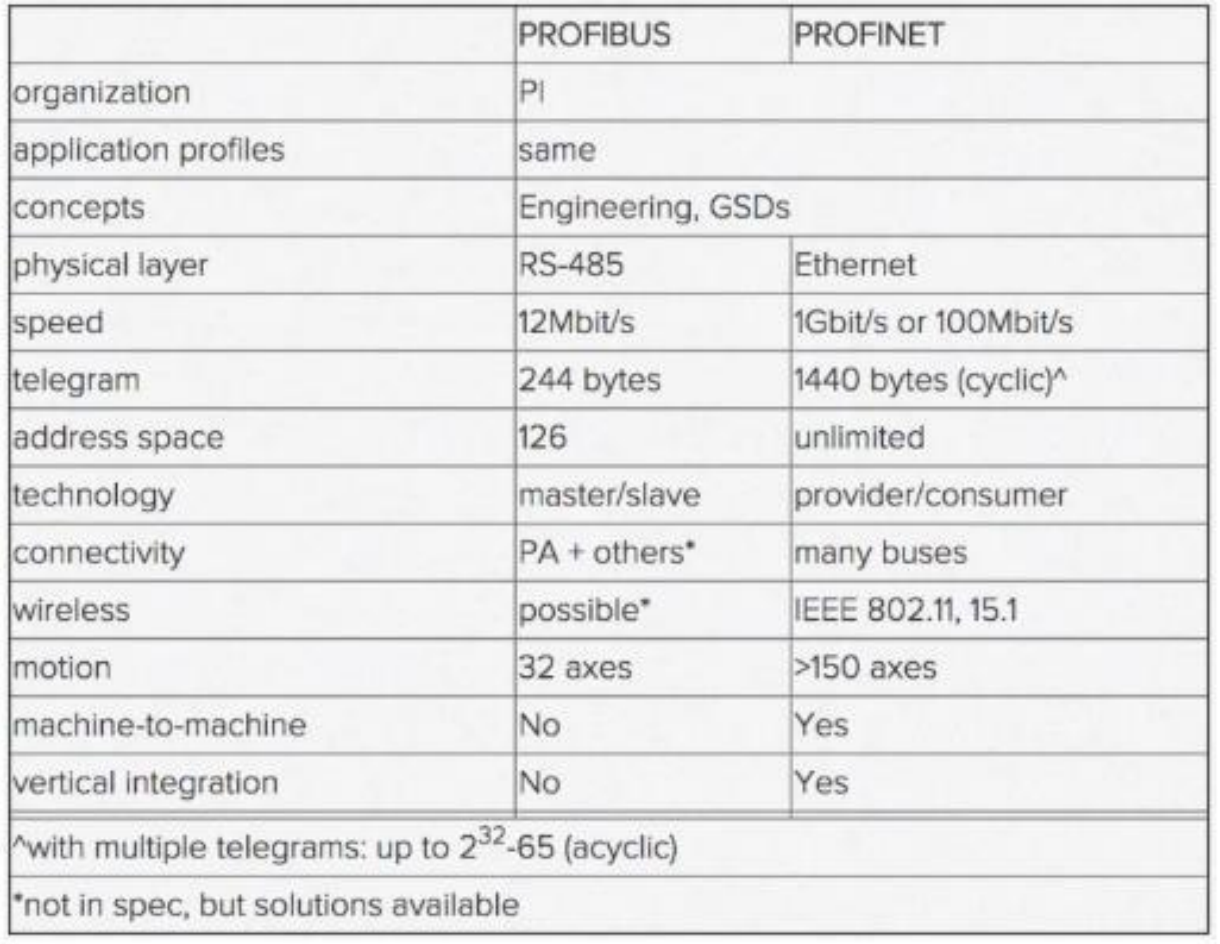
Three profiles for Profibus communication: asynchronous, synchronous, and via Ethernet

- Profibus over Ethernet is also called Profinet

Profinet


PROFINET applications
Standard data
Real-time data
Application
TCP/UDP
Transport
IP
(Software) RT
Network
Ethernet 802.3
Ethernet 802.3
Isochronous RT
Ethernet 802.3
Data Link
Ethernet physical layer
EIA/TIA-232C
EIA/TIA-485
Ethernet physical layer
Physical
Standard Ethernet controller
Custom ASIC Ethernet controller
Version 1
2001
Version 2
2004
Version 3
2005

Profibus vs. Profinet



	PROFIBUS	PROFINET
organization	PI	
application profiles	same	
concepts	Engineering, GSDs	
physical layer	RS-485	Ethernet
speed	12Mbit/s	1Gbit/s or 100Mbit/s
telegram	244 bytes	1440 bytes (cyclic)^
address space	126	unlimited
technology	master/slave	provider/consumer
connectivity	PA + others*	many buses
wireless	possible*	IEEE 802.11, 15.1
motion	32 axes	>150 axes
machine-to-machine	No	Yes
vertical integration	No	Yes

^with multiple telegrams: up to 2^{32}-65 (acyclic)

*not in spec, but solutions available

Case studies of Profibus

https://www.profibus.com/index.php?id=5013

EtherCAT

Real-time Ethernet fieldbus protocol

To maximize the efficiency of distributed process data communications over Ethernet frames

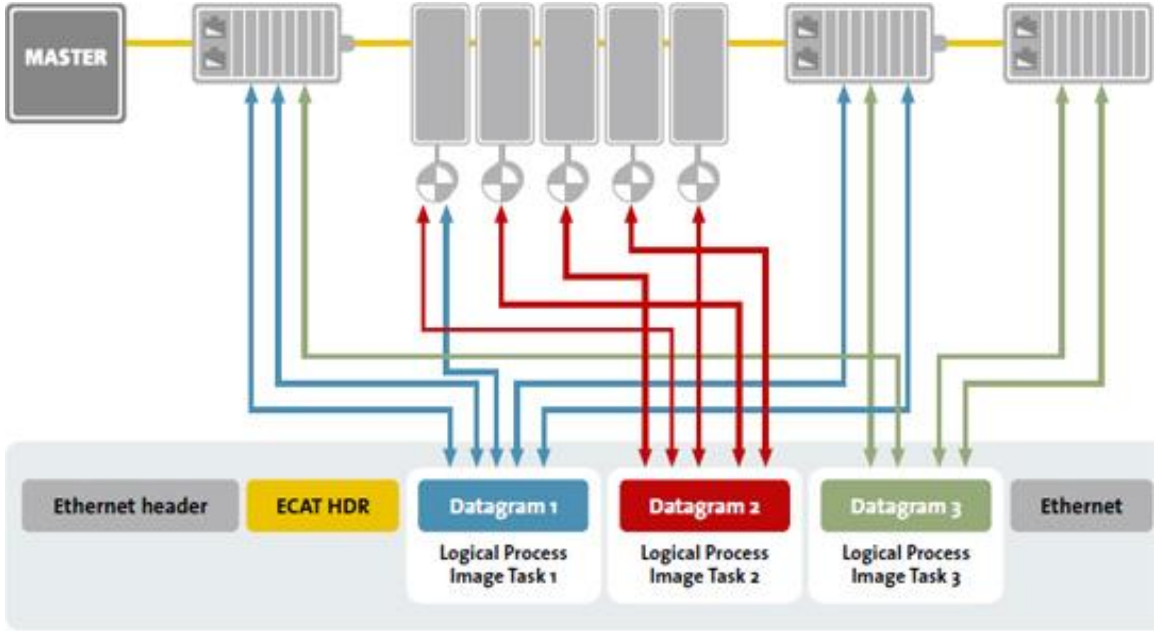
- EtherCAT communicates large amounts of distributed process data with just one Ethernet frame, so that typically only <u>one or two Ethernet frames</u> are required for a complete cycle
- Slaves pass the frame(s) to other slaves in sequence, appending its appropriate response, until the last slave returns the completed response frame back

IEC-Standards (IEC 61158 and IEC 61784)

EtherCAT Characteristics

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

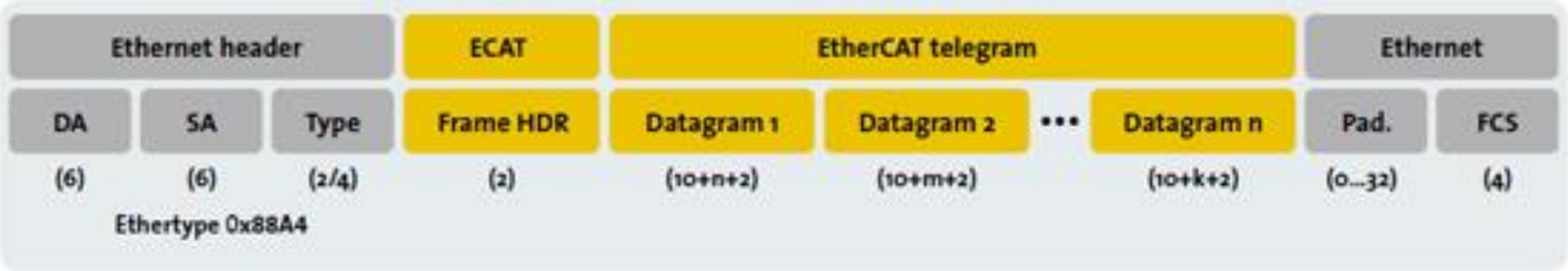
- Each EtherCAT slave device reads the data addressed to it “on the fly”, and inserts its data in the frame as the frame is moving downstream
- The frame is delayed only by hardware propagation delay times
- The last node in a segment (or drop line) detects an open port and sends the message back to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


MASTER
Ethernet header
ECAT HDR
Datagram 1
Logical Process Image Task 1
Datagram 2
Logical Process Image Task 2
Datagram 3
Logical Process Image Task 3
Ethernet

EtherCAT Characteristics

The EtherCAT master is the only node within a segment allowed to actively send an EtherCAT frame;

- All other nodes merely forward frames downstream.
- This concept prevents unpredictable delays and guarantees real-time capabilities.



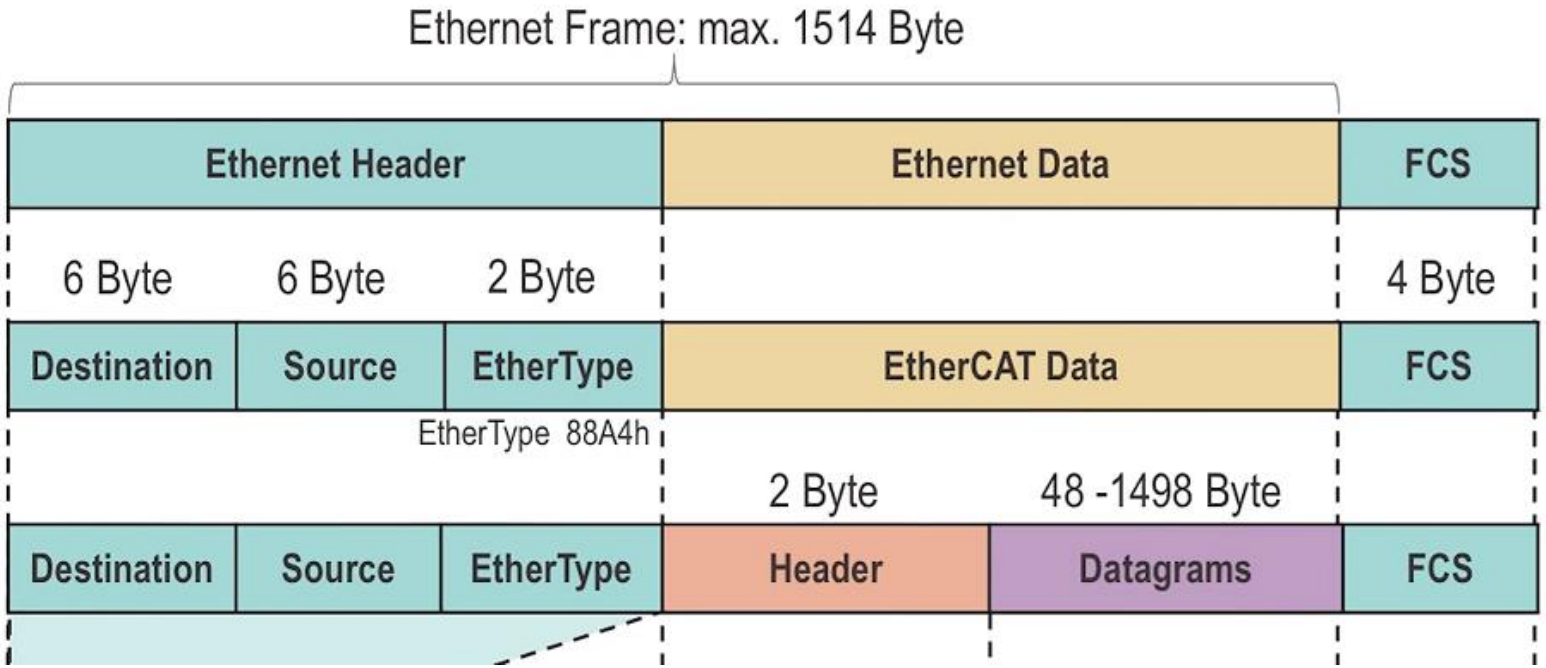
Ethernet header			ECAT	EtherCAT telegram				Ethernet	
DA	SA	Type	Frame HDR	Datagram 1	Datagram 2	•••	Datagram n	Pad.	FCS
(6)	(6)	(2/4)	(2)	(10+n+2)	(10+m+2)		(10+k+2)	(0...32)	(4)
	Ethertype 0x88A4								

EtherCAT Characteristics

The master uses a standard Ethernet Media Access Controller (MAC) without an additional communication processor.

- Allows a master to be implemented on any hardware platform with available Ethernet port,
  - Regardless of which real-time operating system or application software is used.
- EtherCAT Slave devices use an EtherCAT Slave Controller to process frames on the fly and entirely in hardware, making network performance predictable and independent of the individual slave device implementation

EtherCat in Ethernet Frame



Ethernet Frame: max. 1514 Byte

Ethernet Header

Ethernet Data

FCS

6 Byte

6 Byte

2 Byte

4 Byte

Destination

Source

EtherType

EtherCAT Data

FCS

EtherType 88A4h

2 Byte

48 -1498 Byte

Destination

Source

EtherType

Header

Datagrams

FCS

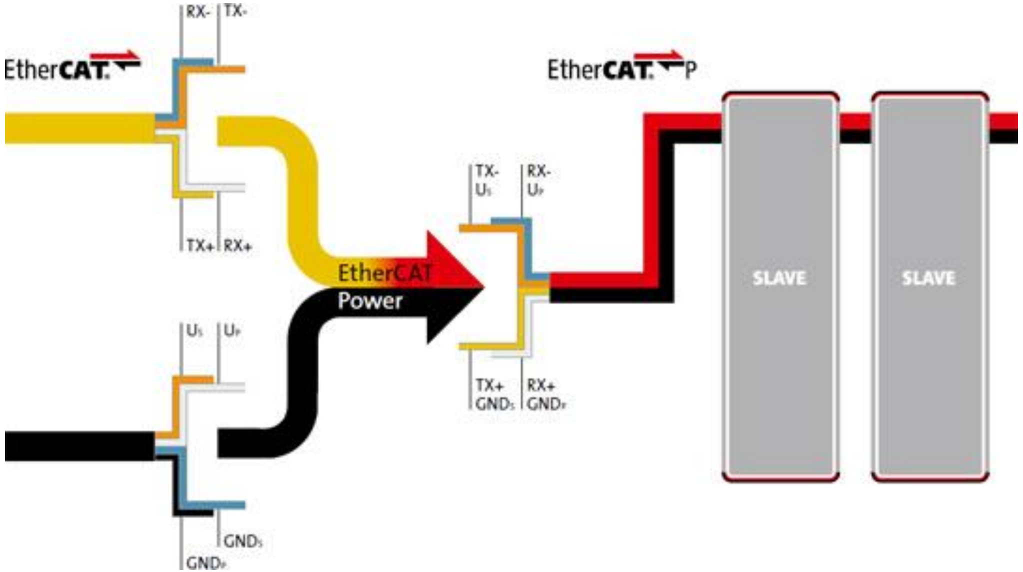
EtherCAT P

EtherCAT P (P = power) is an addition to EtherCAT protocol standard

It enables not only the transmission of communication data, but also the peripheral voltage via a single, standard four-wire Ethernet cable.

EtherCAT P: data and power via one cable

Have you heard Powerline Ethernet?



Ethercat Resources

Most of the resources require membership

https://www.ethercat.org/en/technology.html