SIU Southern Illinois University
CARBONDALE

Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 16: Review

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

EMAIL: AYDEGER@CS.SIU.EDU

Outline

Introduction to CPS

Computer Networks

Cybersecurity

Industrial Networks

ICS Components

Industrial Network Protocols

Introduction to CPS

Cyber Physical System

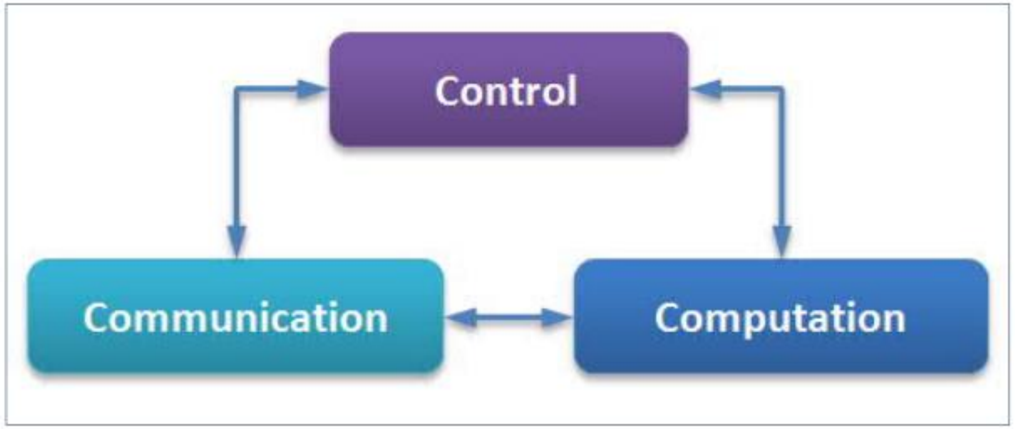
Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the **seamless integration** of computation and physical components.

CPS technologies are transforming the way people interact with engineered systems,

- just as the Internet has transformed the way people interact with information.

Cyber-physical systems integrate;

- sensing, computation, control and networking into physical objects and infrastructure,
- connecting them to the Internet and to each other



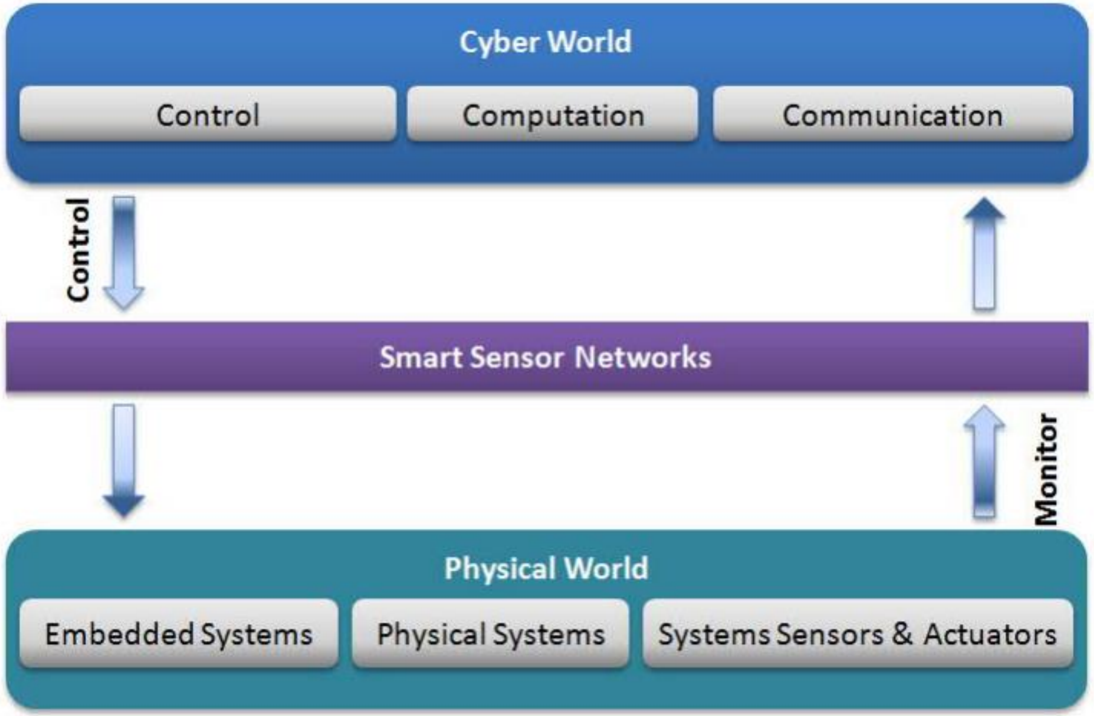
Minimal requirements a for a cyber physical system

Cyber Physical System

NIST: CPS comprises interacting digital, analog, physical, and human components engineered for function through integrated physics and logic.

- These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas.
- Cyber-physical systems will bring advances in personalized health care, emergency response, traffic flow management, etc.

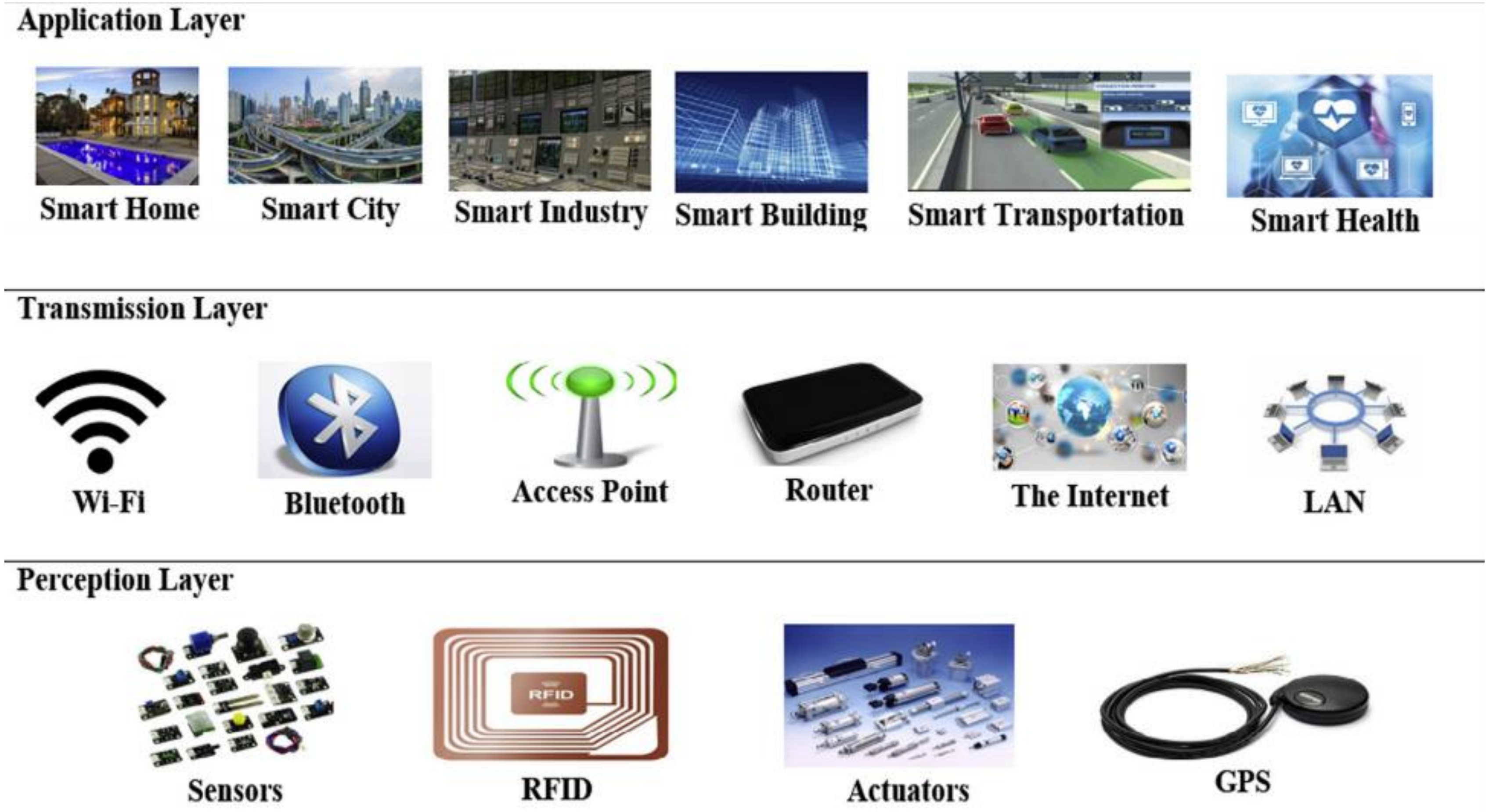
Enabling a smart and connected world



Main building blocks of a cyber physical system

CPS Architecture

Typical three layers cyber-physical system



Characteristics of CPS

Cyber

- Cyber capability in each physical component
- Networking of the components

System of systems

- Unconventional computational and physical substrates (Bio? Nano?)

Interaction between control/computing/communication

- High degrees of automation, control loops must close at all scales

Ubiquity

- Causes security and privacy concerns

CPS Use Case Example: Health care

Monitoring and control devices in health

Mobile health became a new market with our smart phones and wearable

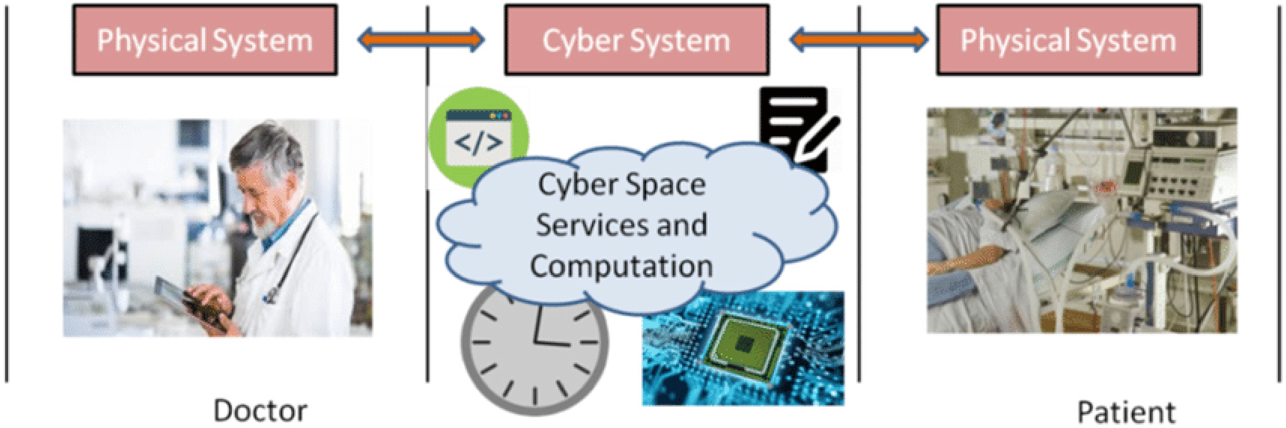
- Numerous Medical IoT devices

At the CPS side, there are also many new devices

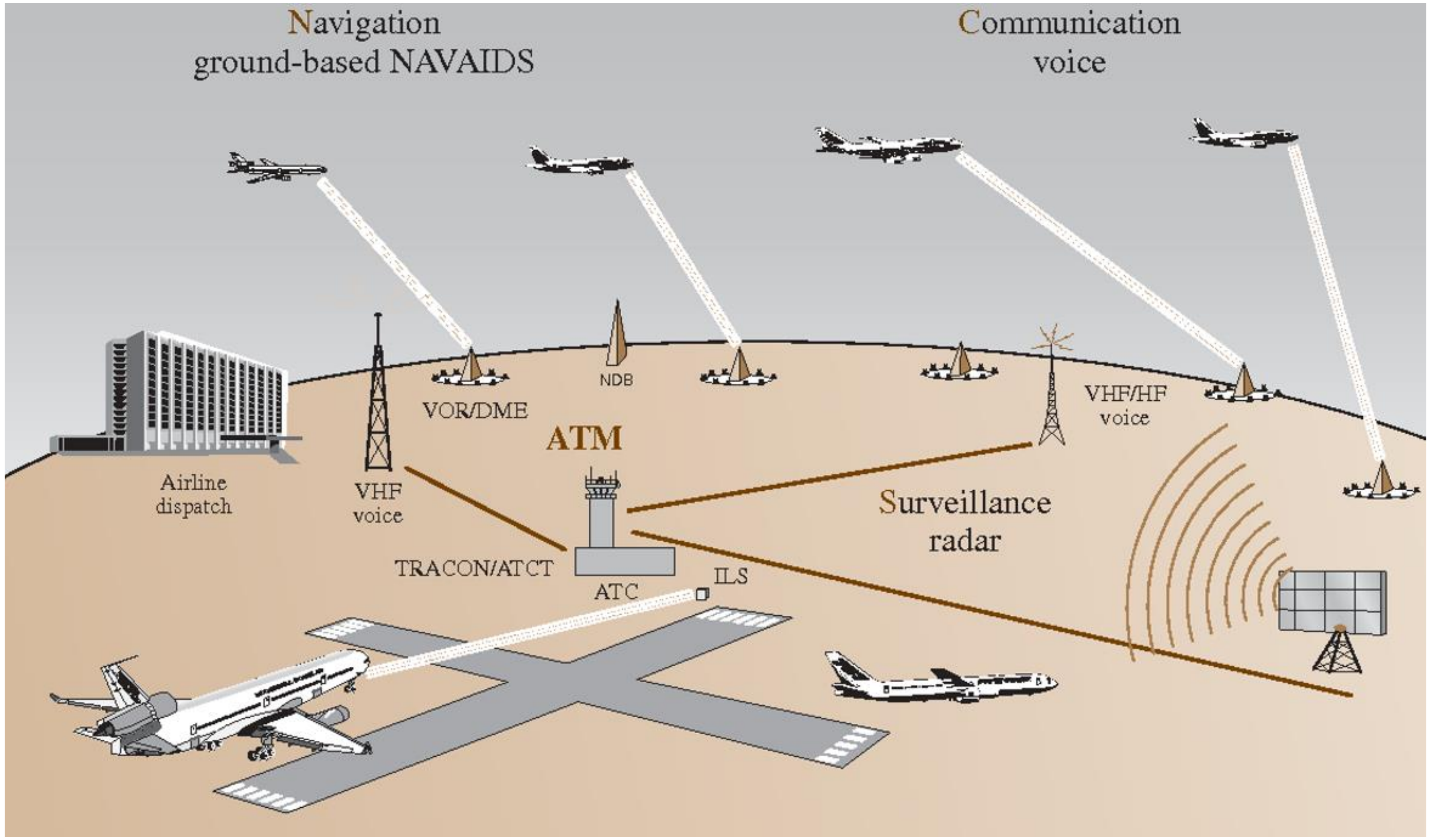
- Insulin pumps, pulse oximeters, sleep apnea devices, etc.

Telemedicine

- Remote surgery, robotic surgery
- System coordination



Another Transportation CPS Example



CPS Challenges

Integration of different components

- CPS include many components to work together smoothly
- Large scale heterogenous environment – hard to predict

Communication requirements

- Cyber domain needs new protocols that would fulfill time critical requirements

Software validation

- Specific software design for each CPS systems

Societal concerns

- Will people trust anyway?

CPS Security Challenges

Security

- Authentication, authorization, encryption, etc.

Resiliency

- If one part fails, will system collapse?
- Is failure due to (cyber) attack or physical conditions?

Privacy

- Who will see which kind of personal data?

CPS Distinguishing Characteristics: Security Aspect

Traditional (IT) security:

Access restriction and control can be applied without affecting the system services.

Confidentiality is ranked the first security objective for IT systems

Traditional security techniques individually focus on addressing security for system components

CPS security:

Could affect or delay the real-time response of the physical parts of CPS

Availability comes first for CPS, then integrity, confidentiality and authenticity.

The interactions among these components

Computer Networks

Computer Networks

Connects two or more computing devices

- Computers, phones, smart grid, IoT

Various ***<u>protocols</u>*** between different device set

- Protocol define the rules of how they interact

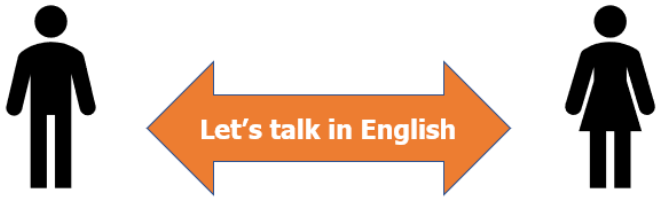
Example daily uses:

- Virtual classrooms, messaging, emails, social media, etc.

Protocols

"The official procedure or system of rules governing affairs of state or diplomatic occasions"

PROTOCOL = Set of rules to communicate.



A communication protocol:

- System of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity
- Defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods

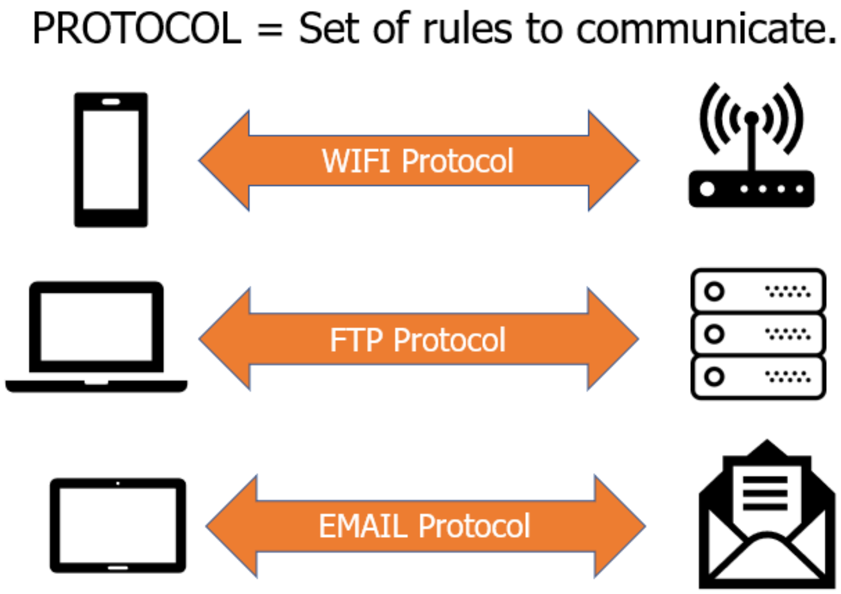
Communication/Network Protocols

Each protocol defines different set of:

- Format of messages
- Order
- Actions
- Security?

Protocol runs on multiple nodes, and implements certain functionality of a single layer

- Works through packet header


PROTOCOL = Set of rules to communicate.

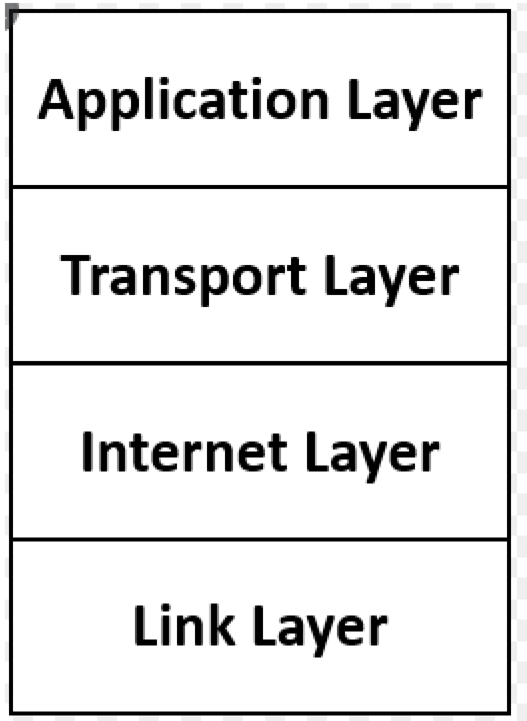
Network Protocol Stack

Application Layers: End-user applications

Transport Layer: Data transfer from end to end

Internet (Network) Layer: Routing of data from source to destination

Link (Physical) Layer: Physical media carrying the data



Application Layer

Transport Layer

Internet Layer

Link Layer

Data Communication through Network Layers

Application data; user input

Transport layer adds its header

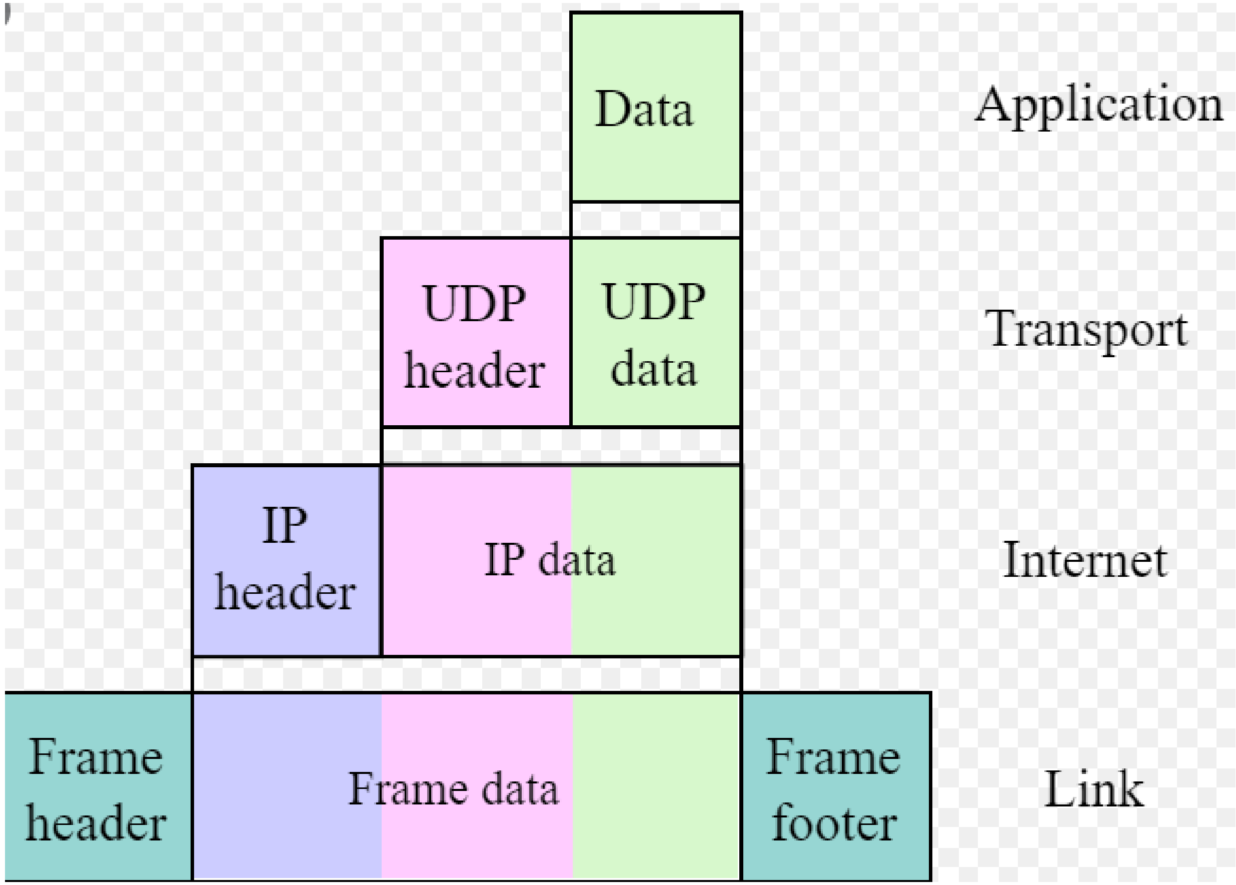
- TCP or UDP

Internet layer adds

- IP header (or ICMP)

Link Layer adds extra info

- Such as error correction, etc.

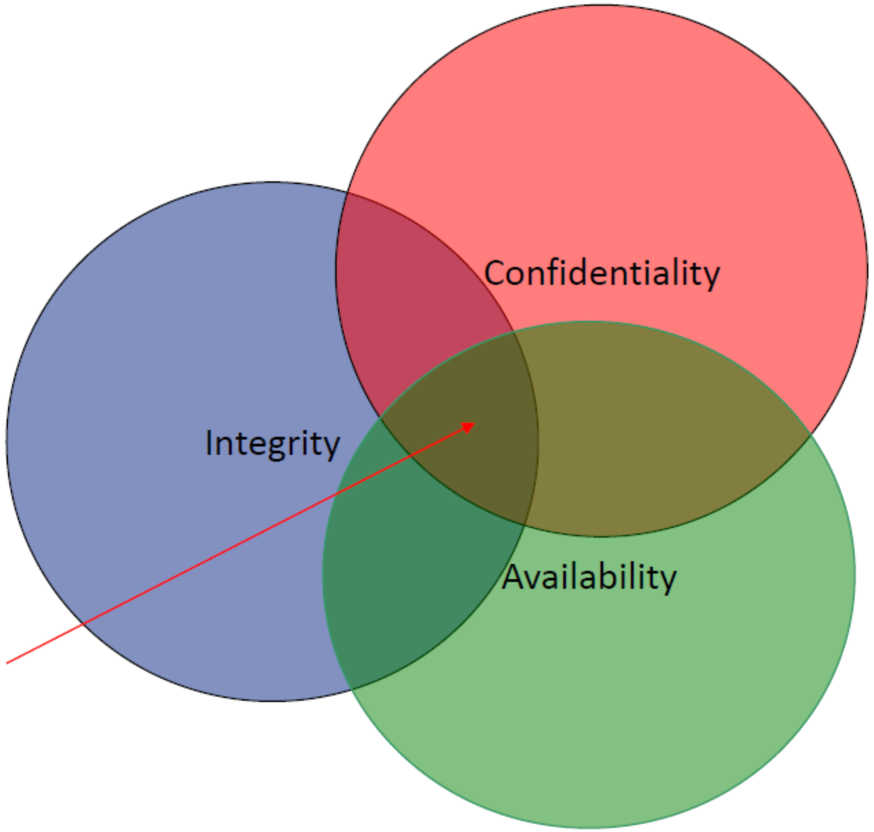


Cybersecurity

Cybersecurity goals

CIA Triad:

- Confidentiality
- Integrity
- Availability



Some Additional Required Concepts

Authenticity

- Being able to be verified and trusted
- Confidence in the validity of a message (originator)

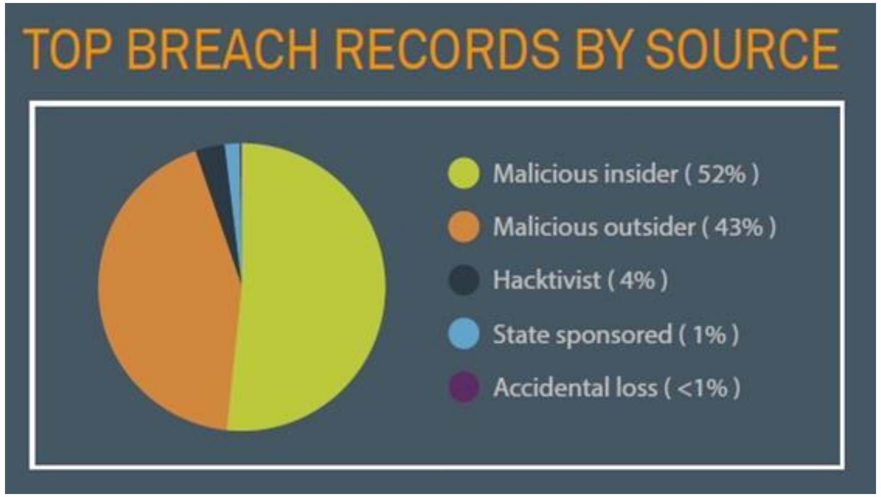
Accountability

- Actions of an entity can be traced to it
- Tracing a security breach to a responsible party

Type of Cyberattacks: Attacker’s Location

Insider vs. Outsider Attacks:

- An inside attack is an attack initiated by an entity inside the security perimeter (an "insider"),
  - An entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization
- An outside attack is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider")



Some Common Attack Types

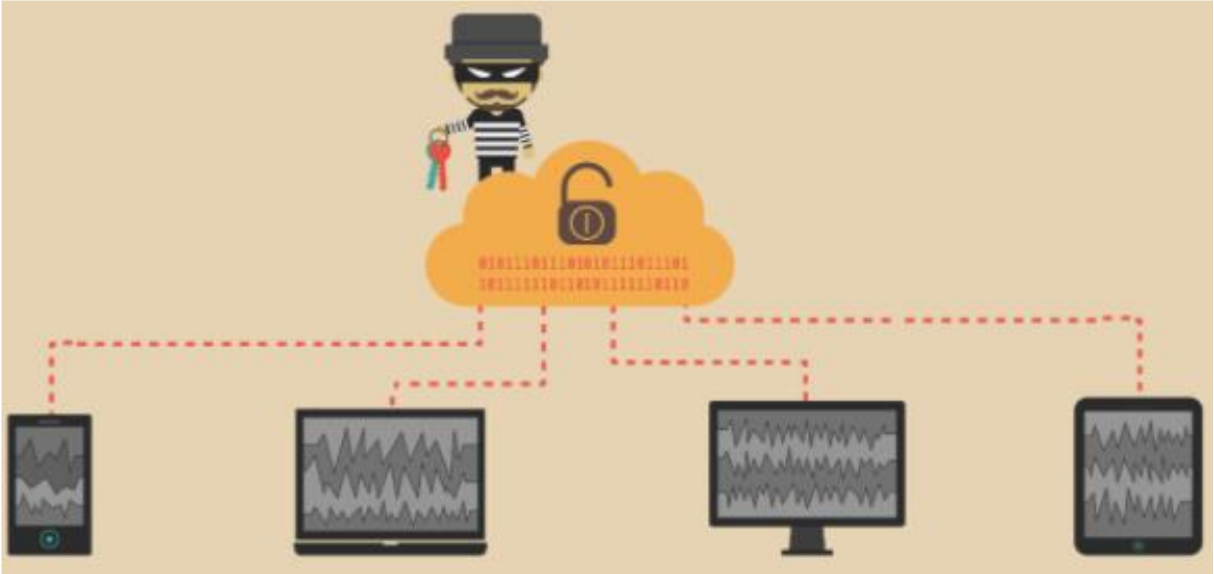
Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks

Man-in-the-middle (MitM) attack

Phishing and spear phishing attacks

SQL injection attack

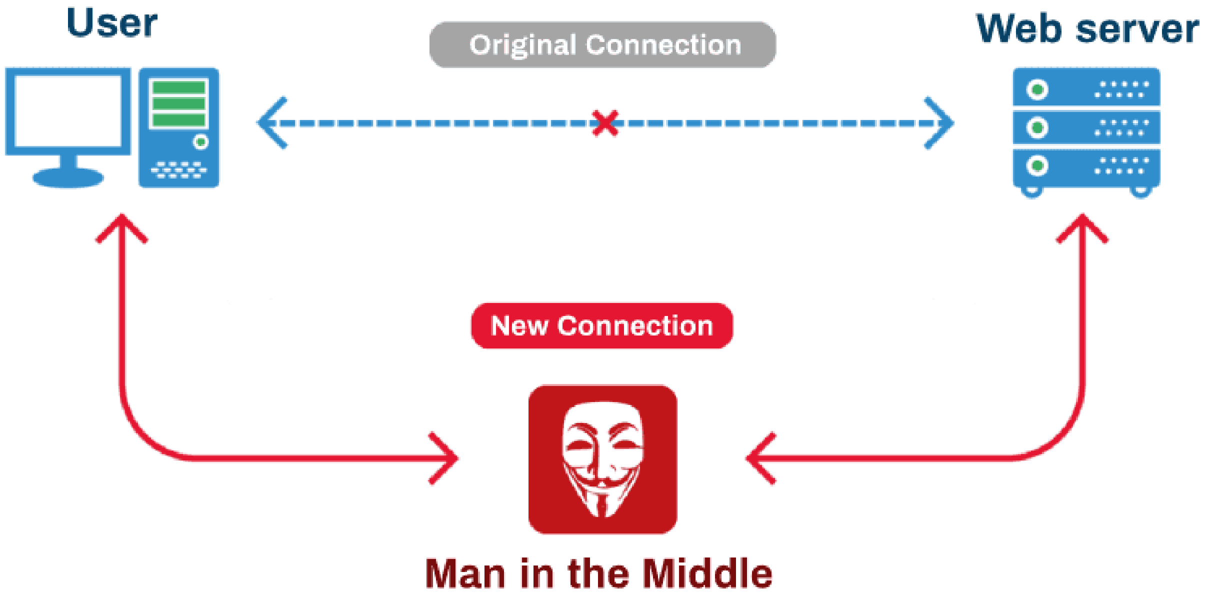
Malware attack



Man-in-the-middle (MitM) attack

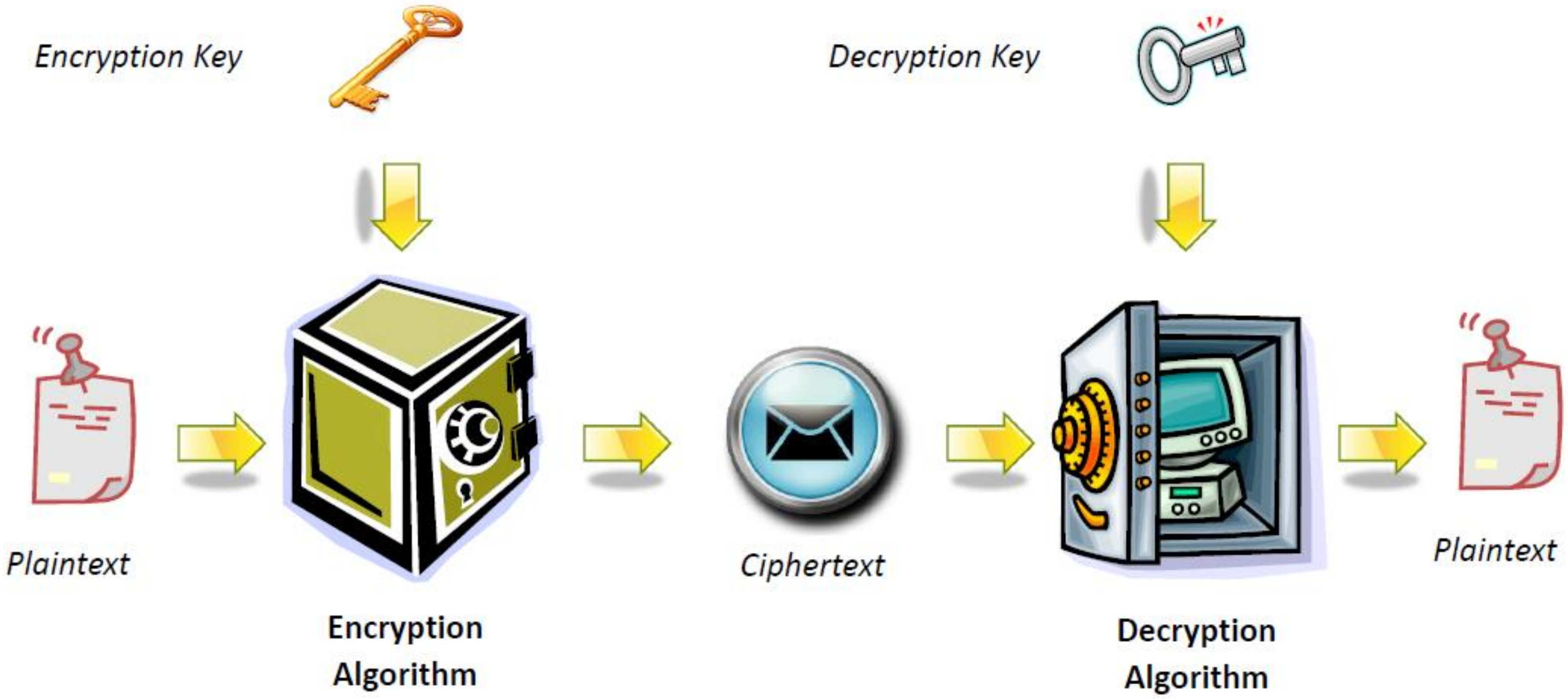
A MitM attack occurs when a hacker inserts itself between the communications of a client and a server. Some common MitM attacks:

- Session hijacking
- IP Spoofing
- Replay



Symmetric Encryption

Secret key known only to sender / receiver



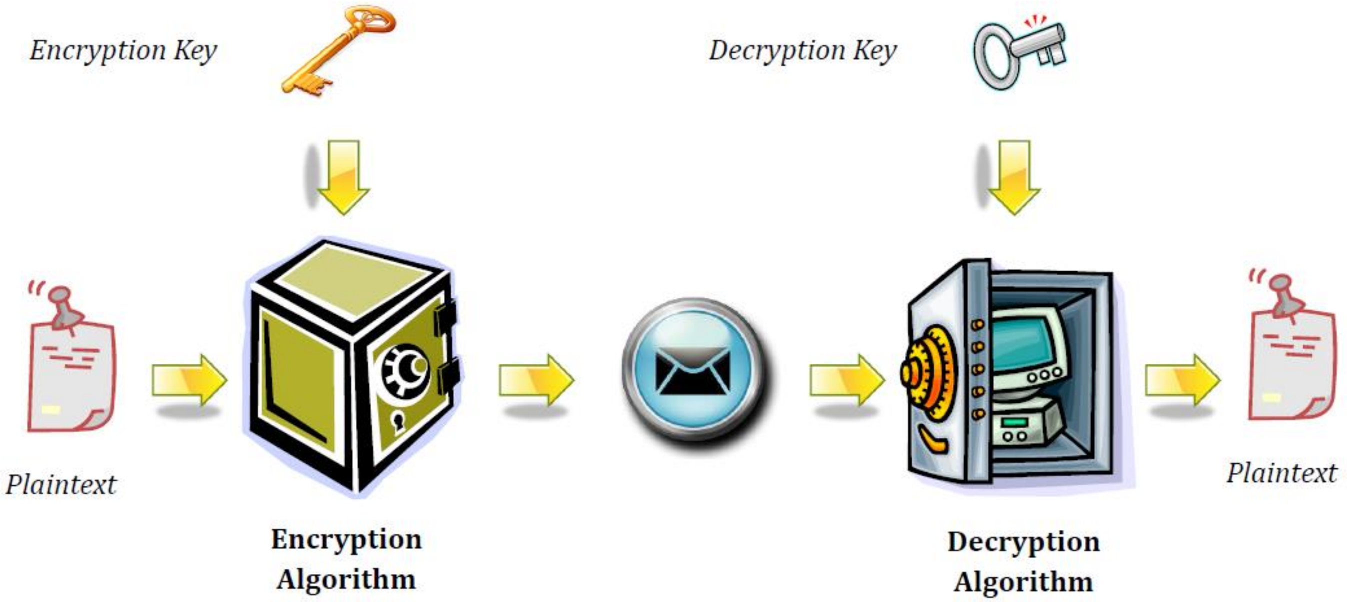
Asymmetric Encryption

Uses two keys – **a public and a private key**

Asymmetric: parties are <u>not equal</u>

User encrypts data using his or her own private key

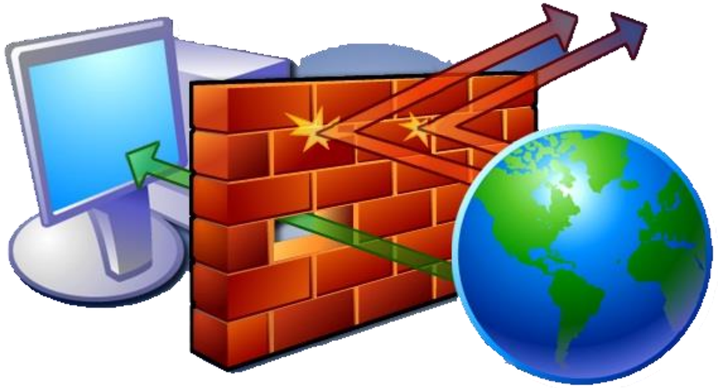
Anyone who knows the corresponding public key will be able to decrypt the message (or vice versa)



Cyberattack Prevention Tools: Firewall

Network security device that

- Monitors incoming and outgoing network traffic
- Permits or blocks data packets based on a set of security rules



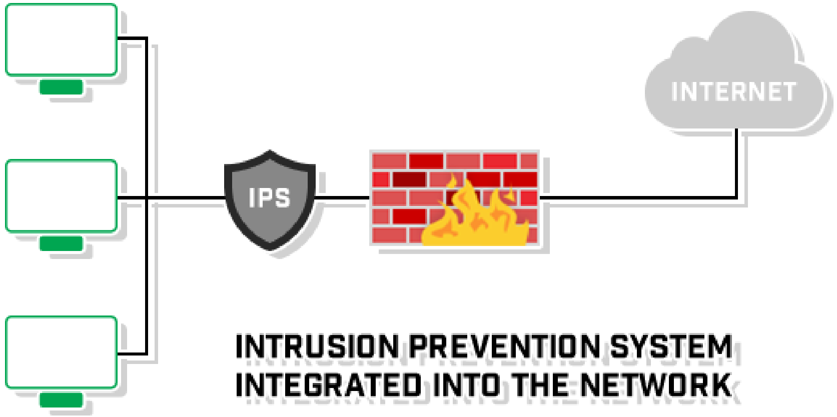
Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic

Cyberattack Prevention Tools: Intrusion Prevention System

IPS must work efficiently to avoid degrading network performance

- It must also work fast because exploits can happen in near real-time
- The IPS must also detect and respond accurately, so as to eliminate threats and false positives (legitimate packets misread as threats).

It often sits directly behind the firewall and provides a complementary layer of analysis that negatively selects for dangerous content



Industrial Networks

Industrial Control Systems (ICS)

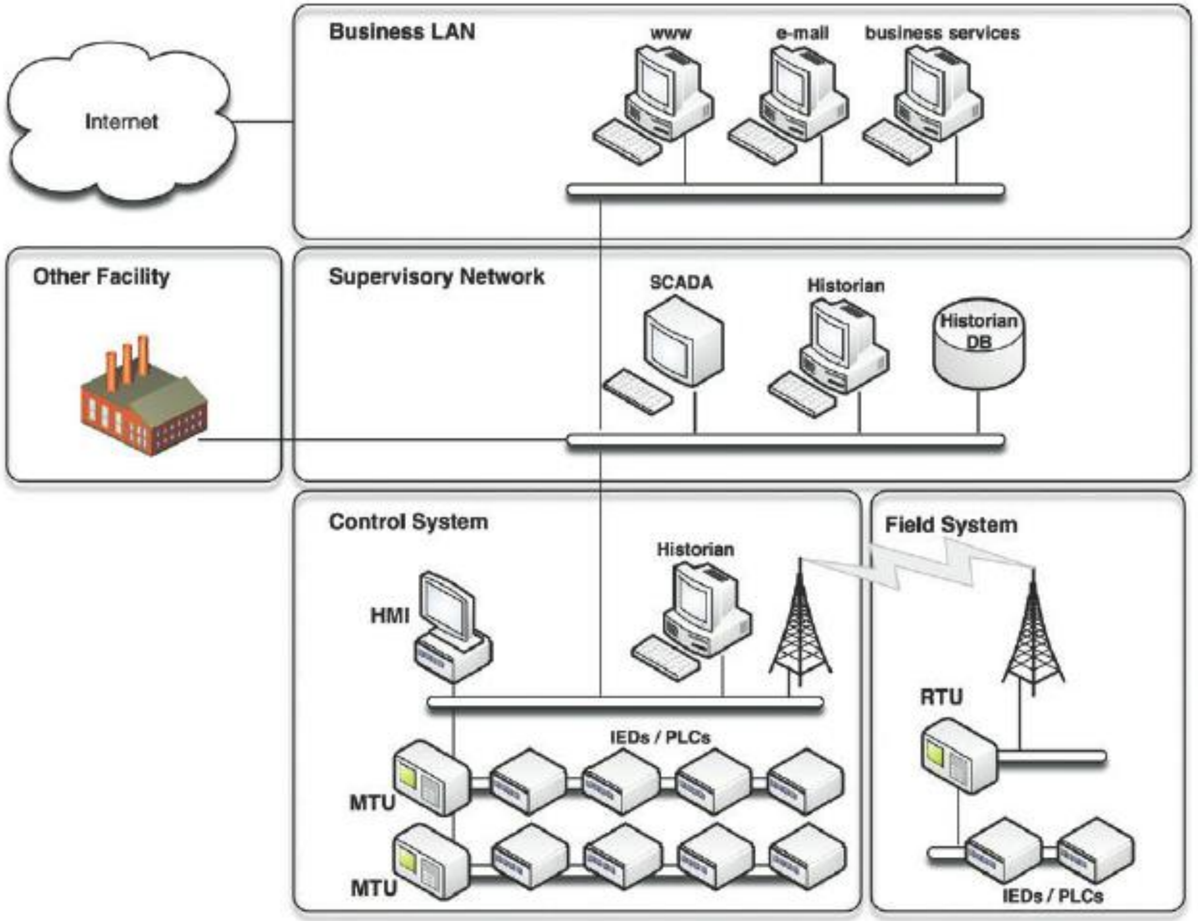
Refers to control systems used to enhance the control, monitoring, and production in different industries such as the nuclear plants, water and sewage systems, and irrigation systems

Sometimes ICS is called *Supervisory Control and Data Acquisition* (SCADA) or *Distributed Control Systems* (DCS) => For consistency, we will use the term ICS

Different controllers with different capabilities collaborate to achieve numerous expected goals

- A popular controller is the *Programmable Logic Controller* (PLC), which is a microprocessor designed to operate continuously in hostile environments

Sample Industrial Automated Control System Network



Smart Grid Systems

The smart grid is envisioned as the next generation of the power grid that has been used for decades for electricity generation, transmission, and distribution

The smart grid provides several benefits and advanced functionalities:

- At the national level, it provides enhanced emission control, global load balancing, smart generation, and energy savings
- At the local level, it allows home consumers better control over their energy use that would be beneficial economically and environmentally

Smart cars/Modern vehicles

More environment-friendly, fuel-efficient, safe, and have enhanced entertainment and convenience features

These advancements are made possible by the reliance on a range of 50 to 70 computers networked together, called Electronic Control Units (ECUs)

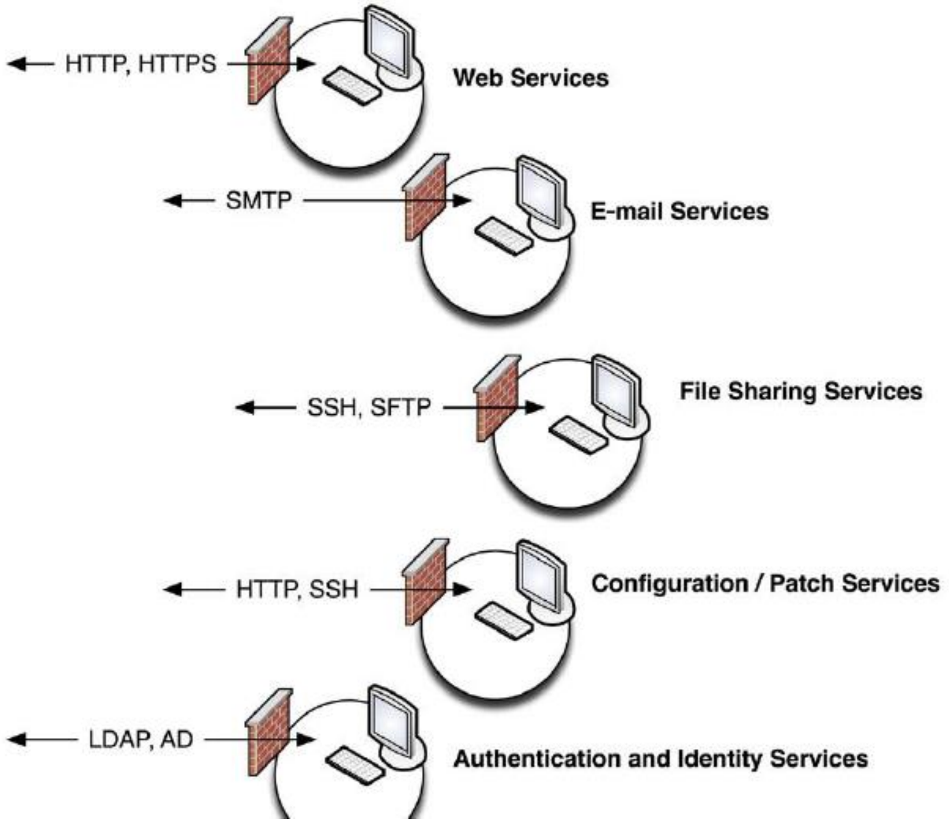
- ECUs are responsible for monitoring and controlling various functions such as engine emission control, brake control, entertainment (radio, multimedia players) and comfort features (cruise control)

Common Industrial Security Recommendations

Network Segmentation/Isolation of Systems

If each specific service is grouped functionally and separated from all other services,

- All web servers are grouped together in one group, all e-mail services in another group, etc.
  - The firewall can be configured to disallow anything other than the desired service, preventing an e-mail server from being exposed to a threat that exploits a weakness in HTTP



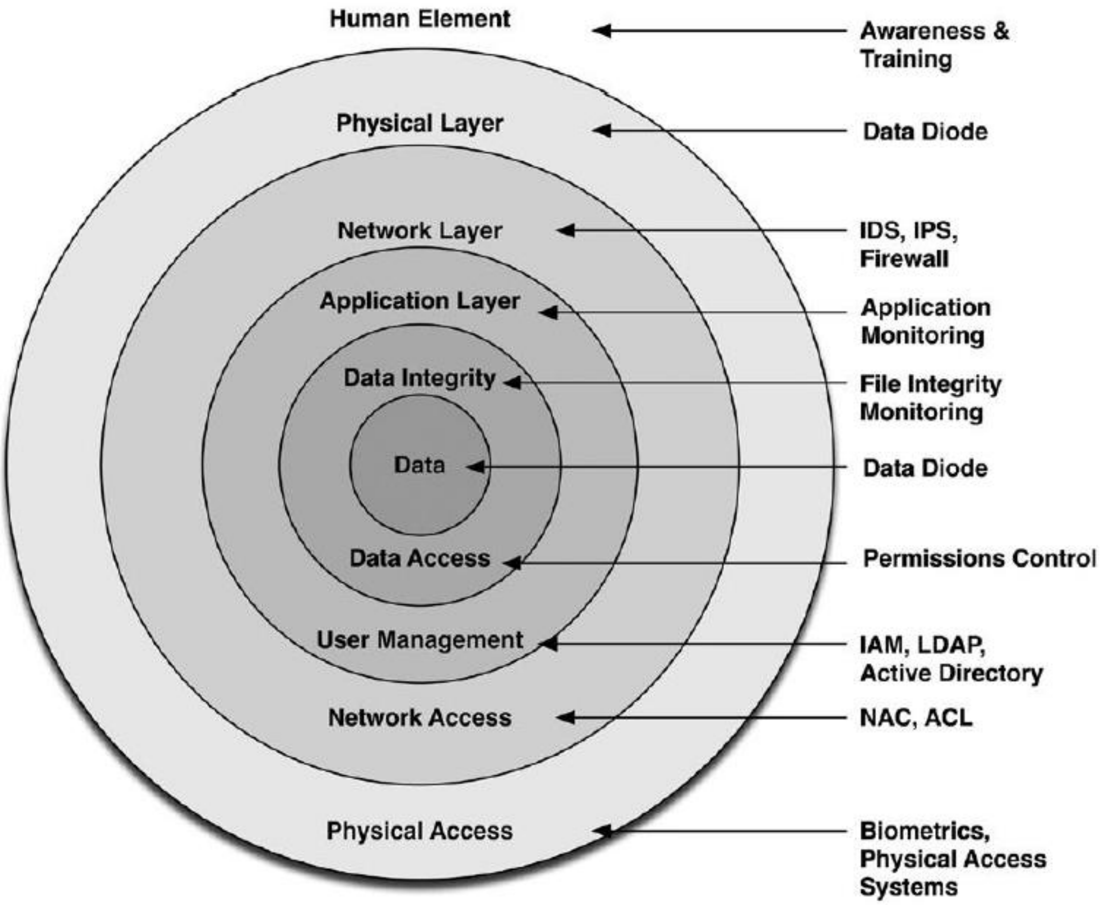
Separation into Functional Groups Reduces the Attack Surface to a Given System

Common Industrial Security Recommendations

Defense in Depth

Layered or tiered defensive strategy

- The layers of the networks
- Physical or Topological layers consisting of subnetworks and/or functional groups
- Policy layers, consisting of users, roles, and privileges
- Multiple layers of defense devices at any given demarcatio point (such as implementing a firewall and an IDS or IPS)



ICS Components

Intelligent Electronic Device (IED)

Any device commonly used within a control system—such as a sensor, actuator, motor, transformers, circuit breakers, and pumps

- Equipped with a small microprocessor that enables it to communicate digitally

Can be controlled by an upstream RTU or PLC

- Can be polled either by an RTU at a field site via serial, Ethernet or even a wireless link

Programmable Logic Controller (PLC)

Specialized computer used to automate functions within industrial networks

Materially hardened

- May be specialized for specific industrial uses with multiple specialized inputs and outputs
- Making them suitable for deployment on a production floor
  - 10-15 years of deployment, maybe even longer

Typically control real-time processes and are designed for simple efficiency

- Usually based on **ladder logic**
- Usually RTOS (Real-time Operating System)
  - Modern PLCs may use a UNIX-derived micro-kernel and present a built-in web interface

Remote Terminal Unit (RTU)

Resides in a substation or other remote location as Station and field RTUs

- Field RTUs are interfaces between field devices/sensors and the station RTU
- Station RTUs can also be found at remote sites and receive data from field RTUs as well as orders from supervisory controllers
- Two types of RTUs may be combined in a single physical RTU

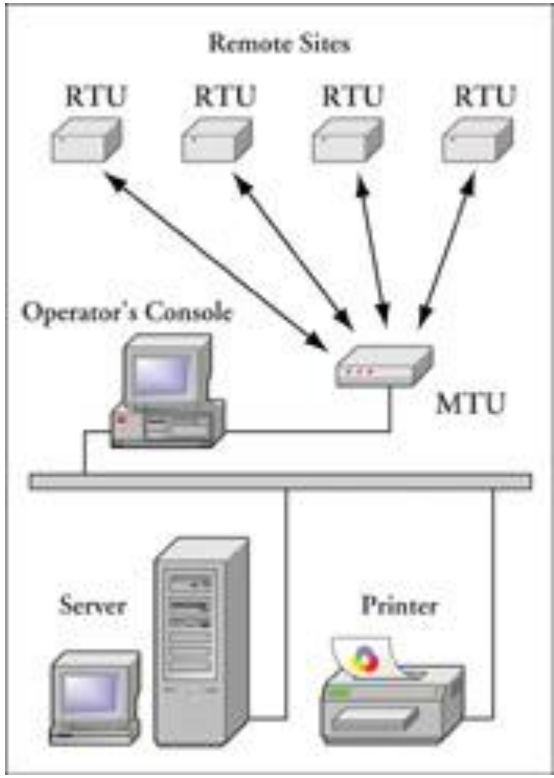
Master Terminal Unit

NIST: A controller that also acts as a server that hosts the control software that communicates with lower-level control devices, such as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), over an ICS network

- In a SCADA system, this is often called a SCADA server, MTU, or supervisory controller

Issues the commands to the Remote Terminal Unit (RTUs)

- Gathers the required data, stores the information, and process the information
- Display the information in the form of pictures, curves and tables to human interface
- Helps to take control decisions



Human Machine Interfaces (HMIs)

Used as an operator control panel to PLCs, RTUs

- In some cases directly to IEDs

Replace manually activated switches and other controls with graphical representations of the control process

- Software based
    - Replace physical wires with software parameters
    - Allowing them to be adapted and adjusted very easily

Data Historian

Specialized software which collects data from industrial devices and store them in a purpose-built database

Typically proprietary (each company has its own) or third-party companies

The same data which is displayed by HMI is stored in the Data Historian

- Each data point is timestamped and are called tags
    - Eg. Frequency of a motor

Data Historians are often replicated in industrial networks for resilience and efficiency

- Used by operations and business
- Should be isolated and secured

Supervisory Workstations

Collects information from assets

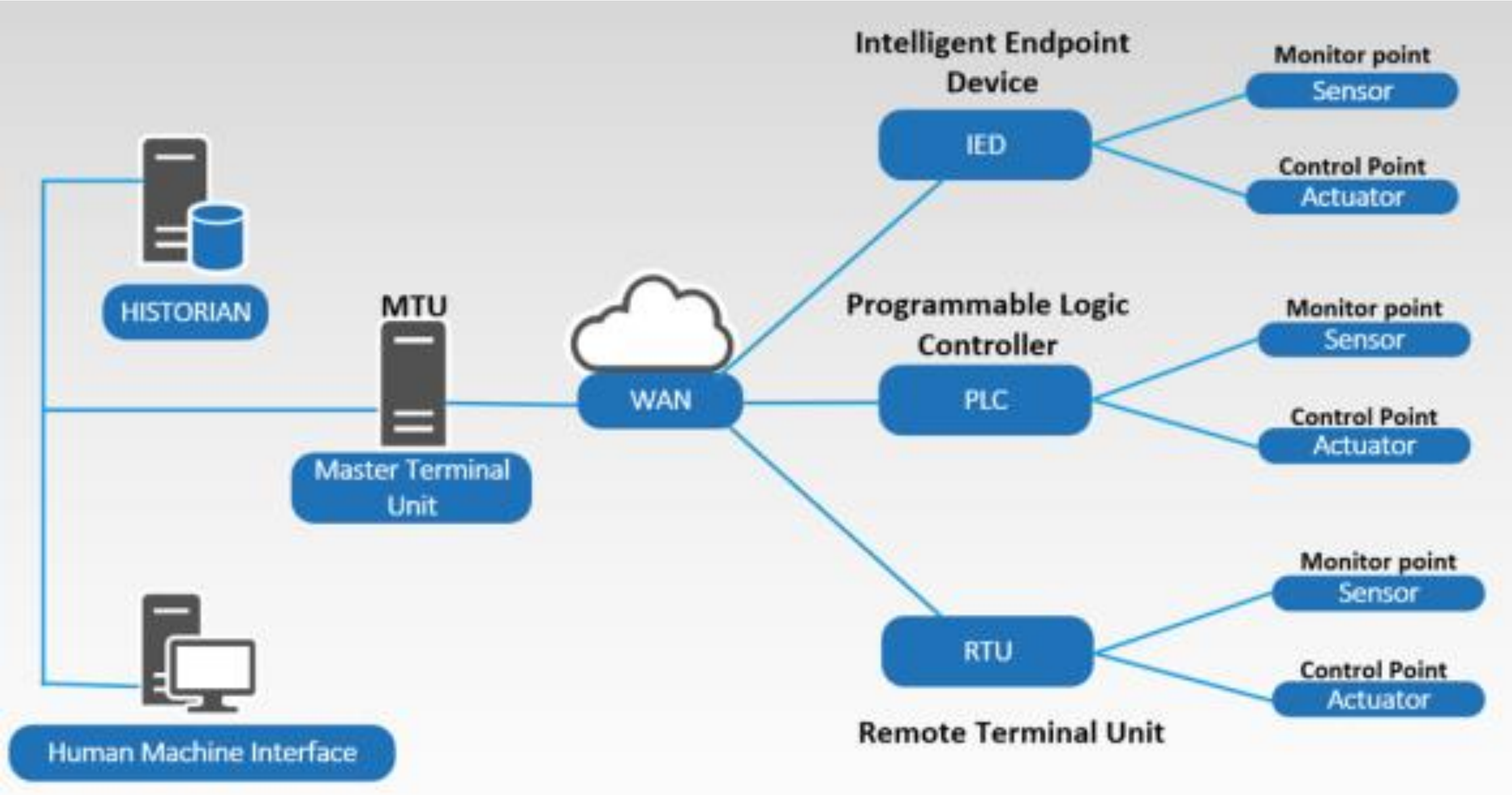
Presents them for supervisory purposes

Read-only system

- Different than HMI

Can be employing an HMI or Data Historian

Abstract Topology Example for ICS



Industrial vs. Business Network

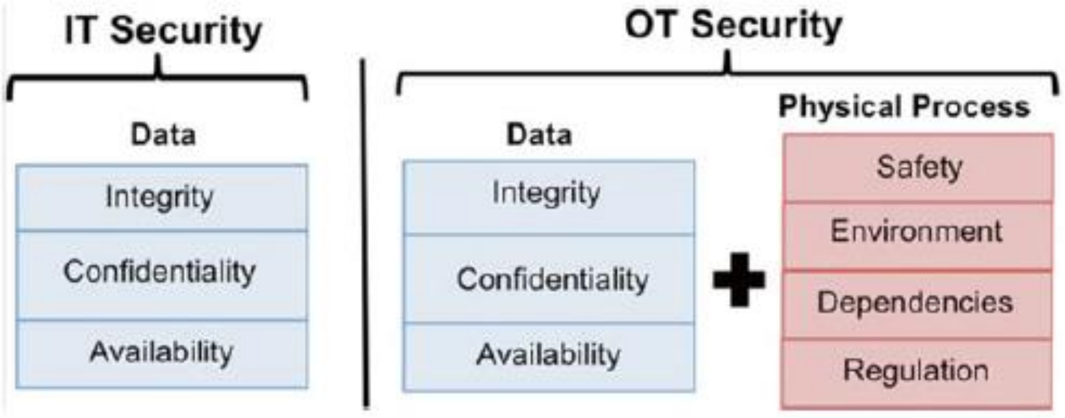
ICS vs SCADA vs Enterprise

Function	Industrial Control	SCADA	Enterprise
Real-time operation	Critical	High	Best Effort
Reliability Req.	Critical	High	Best Effort
Bandwidth Req.	Low	Low/Medium	High
Latency	Low, Consistent	Low, Consistent	NA, Retransmission is acceptable
Protocols Used	Realtime	Realtime	Non realtime

Operational Technology vs. Information Technology

IT: involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data

OT: hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise



OT Operational Objectives (Differences)

Maintaining profitable margins

Minimizing the safety or environmental impacts

Limiting damage or wear to physical assets

Managing broader society dependences on the ICS

OT’s Technical Differences

Unique communication protocols and architectures

Real-time performance demands

Dependence on resource constrained embedded devices

Domains specific device manufactures and integrators

Complex integration of digital, analog, and mechanical controls

Industrial Network Protocols

Modbus Characteristics

Application layer messaging protocol

Efficient communications between interconnected assets

Can be used by extremely <u>simple devices</u> such as <u>sensors</u> or motors

- Communicate with a more complex computers that read measurements and perform analysis and control

Requires very little processing overhead

- Suitable for PLCs and RTUs to communicate supervisory data to a SCADA system

Modbus Characteristics

Request/response protocol

Three Protocol Data Units (PDUs):

- Modbus Request
- Modbus Response
- Modbus Exception Response

Each devices is assigned unique address

- All of them may hear the message, only the addressed device responds

Modbus Operation

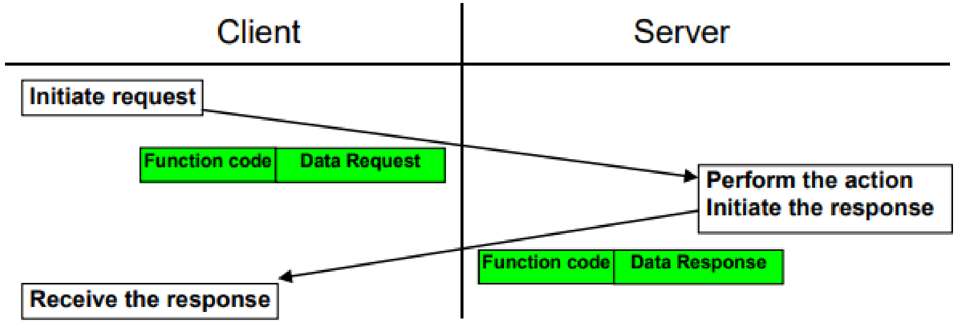
Starts with initial Function Code and a Data Request within a Request PDU

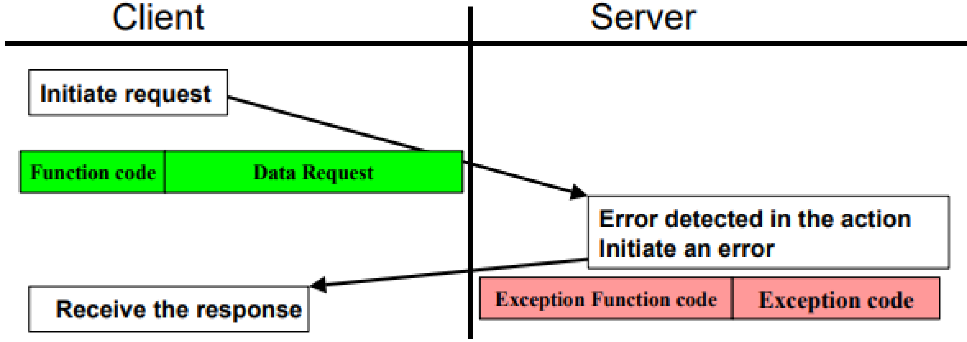
Response either:

- Function Code and Data Response, if no error
- Exception Function Code and Exception Code, if error

Examples of Function Codes and Data Requests:

- Read from an I/O interface
- Write a value to a register (i.e., change the value in register)

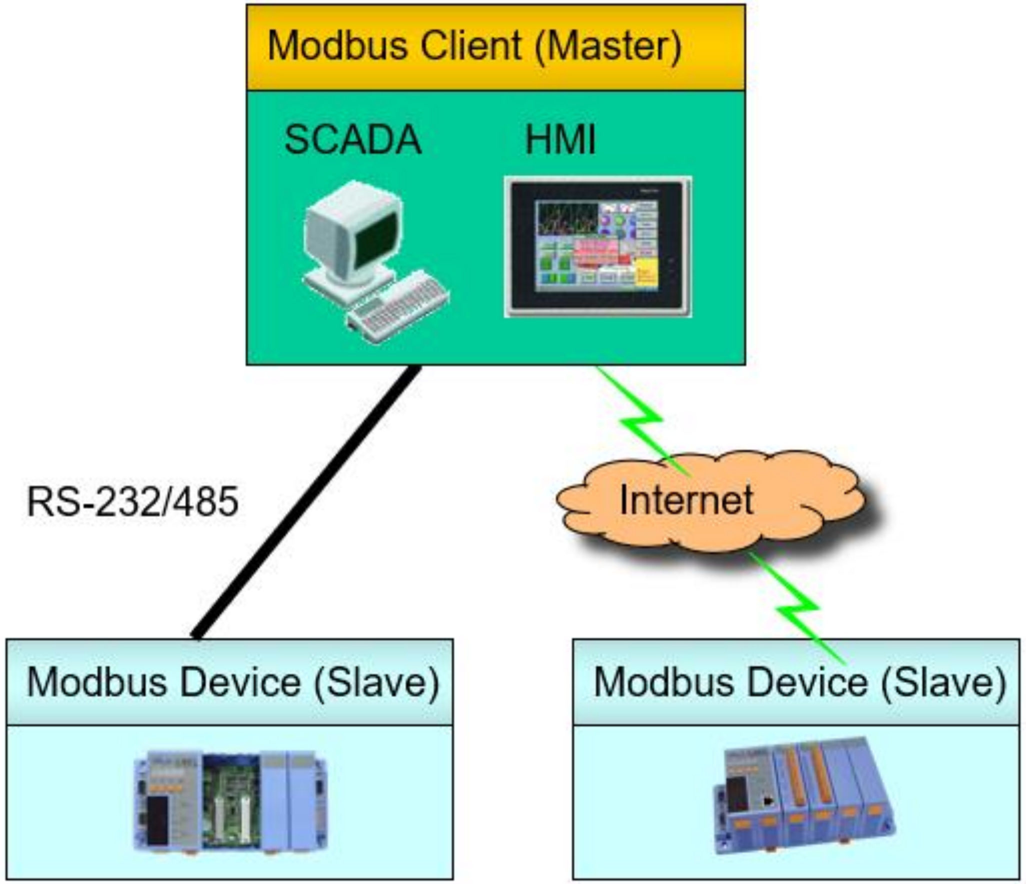




Modbus TCP

Uses Transmission Control Protocol/Internet Protocol (TCP/IP) to transport Modbus commands and messages over Ethernet

- Uses TCP/IP layers
- Port 502
- Client/server model



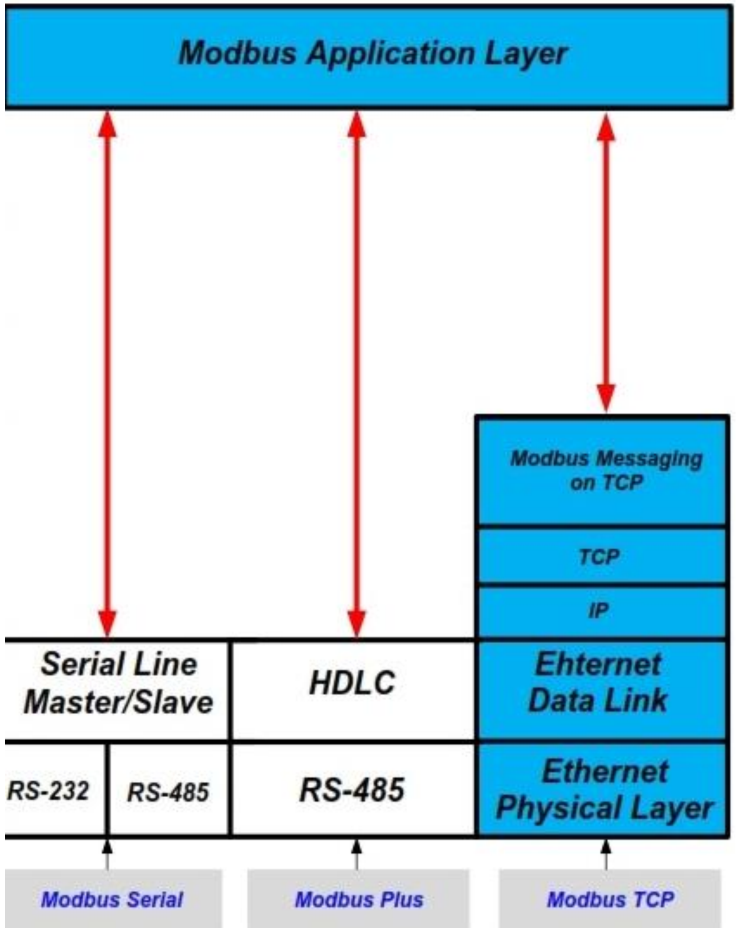
Modbus Protocol Stack

Modbus RTU/ASCII

Modbus TCP

Modbus Plus

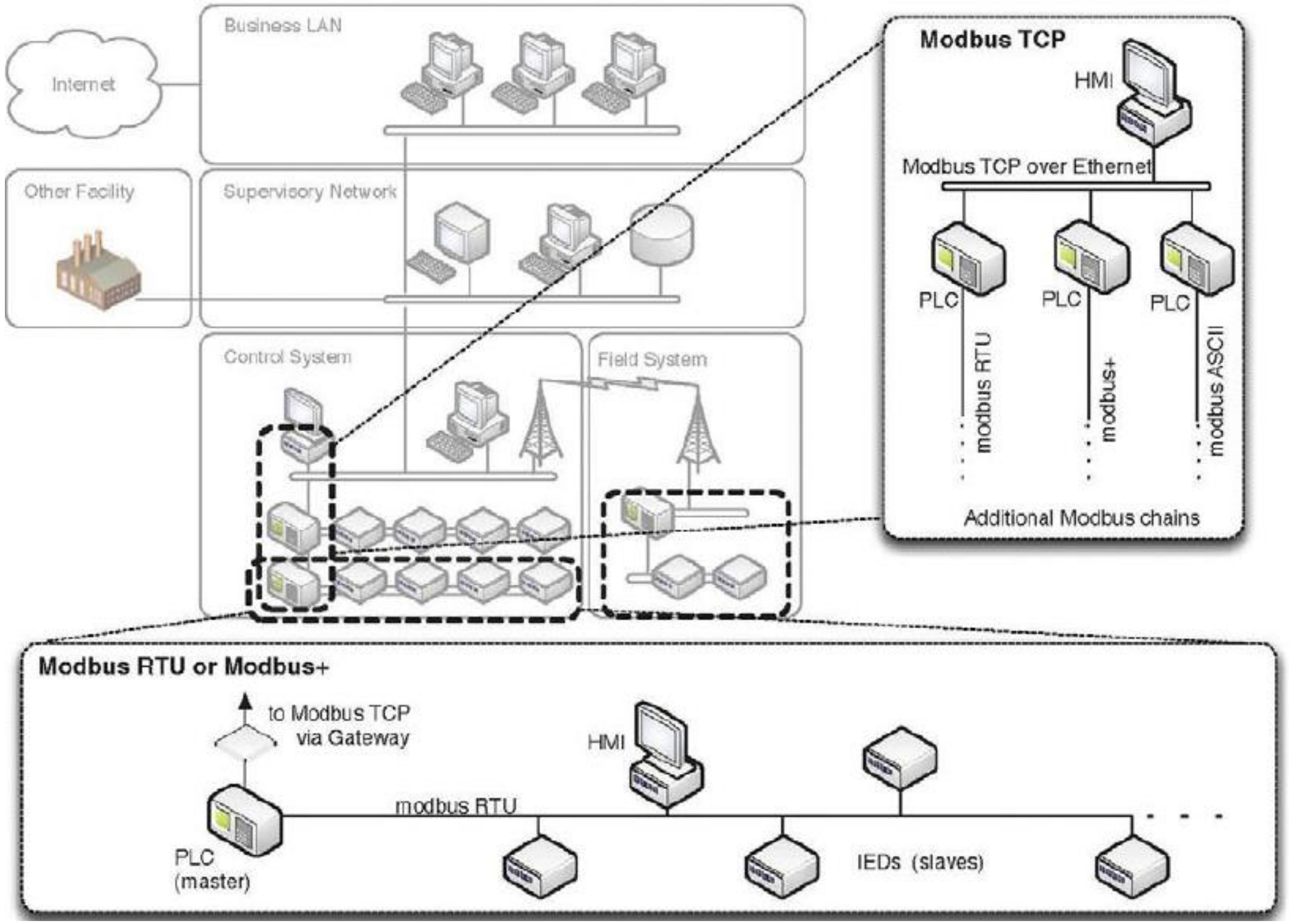
- Proprietary



Where Modbus is used

Typically deployed:

- Between PLCs and HMIs, or
- Between a Master PLC and slave devices such as PLCs, HMIs, IEDs



Distributed Network Protocol (DNP3)

Began as a serial protocol designed for use between master control stations and slave devices, as well as for RTUs and IEDs within a control station

Was extended to work over IP

- Encapsulated in TCP or UDP packets
- In order to make remote RTU communications more easily accessible over modern networks

Very reliable, while remaining efficient and well suited for real-time data transfer

- CRC (Cyclic redundancy check) checks

DNP3 Characteristics

Primary motivation: reliable communication that include high level of electromagnetic interference

Based on International Electrotechnical Commission (IEC) 60870-5 standard

Several standardized data formats and supports time-stamped (and time-synchronized) data,

- Making real-time transmissions more efficient and thus even more reliable

Optional retransmission in case of no confirmation received

DNP3 Characteristics

The payload is very flexible and can be used to

- Simply transfer informational readings, or
- Send control functions, or
  - Direct binary or analog data for direct interaction with devices such as Remote Terminal Units (RTUs), as well as other analog devices such as IEDs

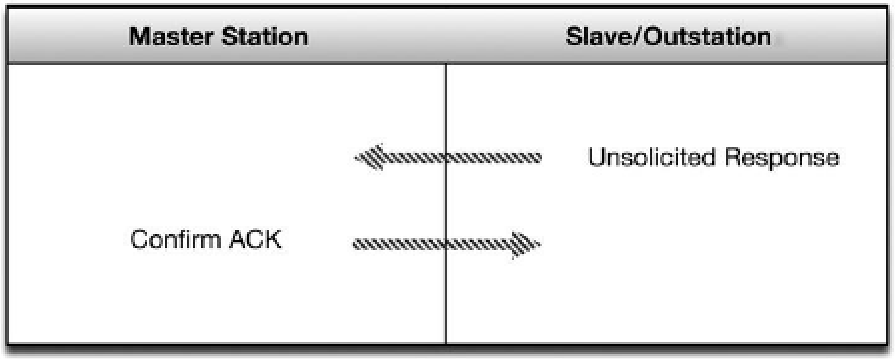
Supports two kinds of data

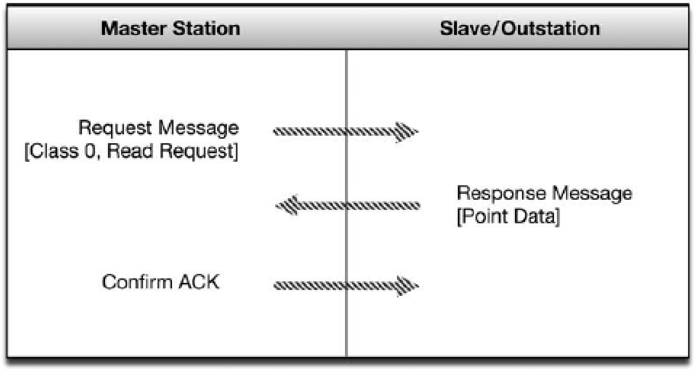
- Static or Class 0 such as point readings
- Event data such as alarm:
  - Priority class 1 (highest) - 3 (lowest) allows operate more efficiently

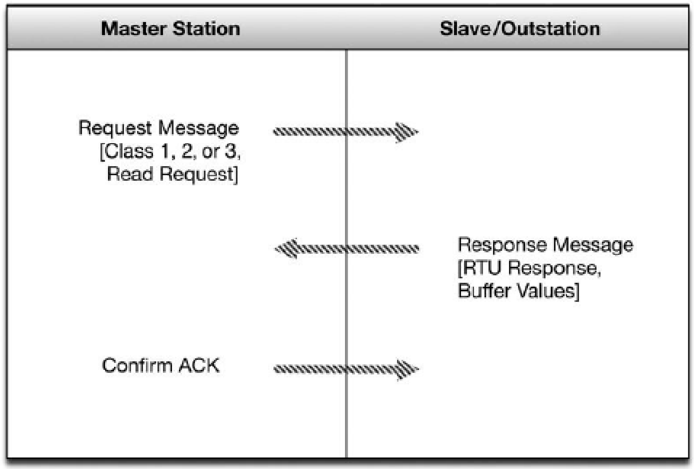
DNP3 Characteristics

Bidirectional (supporting communications from both Master to Slave and from Slave to Master) and supports exception-based reporting

- Possible for a DNP3 outstation to initiate an unsolicited response to notify the Master of an event outside of the normal polling interval
  - Such as an alarm condition




Master Station
Slave/Outstation
Request Message [Class 0, Read Request]
Response Message [Point Data]
Confirm ACK


Master Station
Slave/Outstation
Request Message [Class 1, 2, or 3, Read Request]
Response Message [RTU Response, Buffer Values]
Confirm ACK

DNP3 Layers

Runs on application layer

- However, proposes its lower layer protocols as well
  - Transport and Link Layer

Link Layer Responsibility:

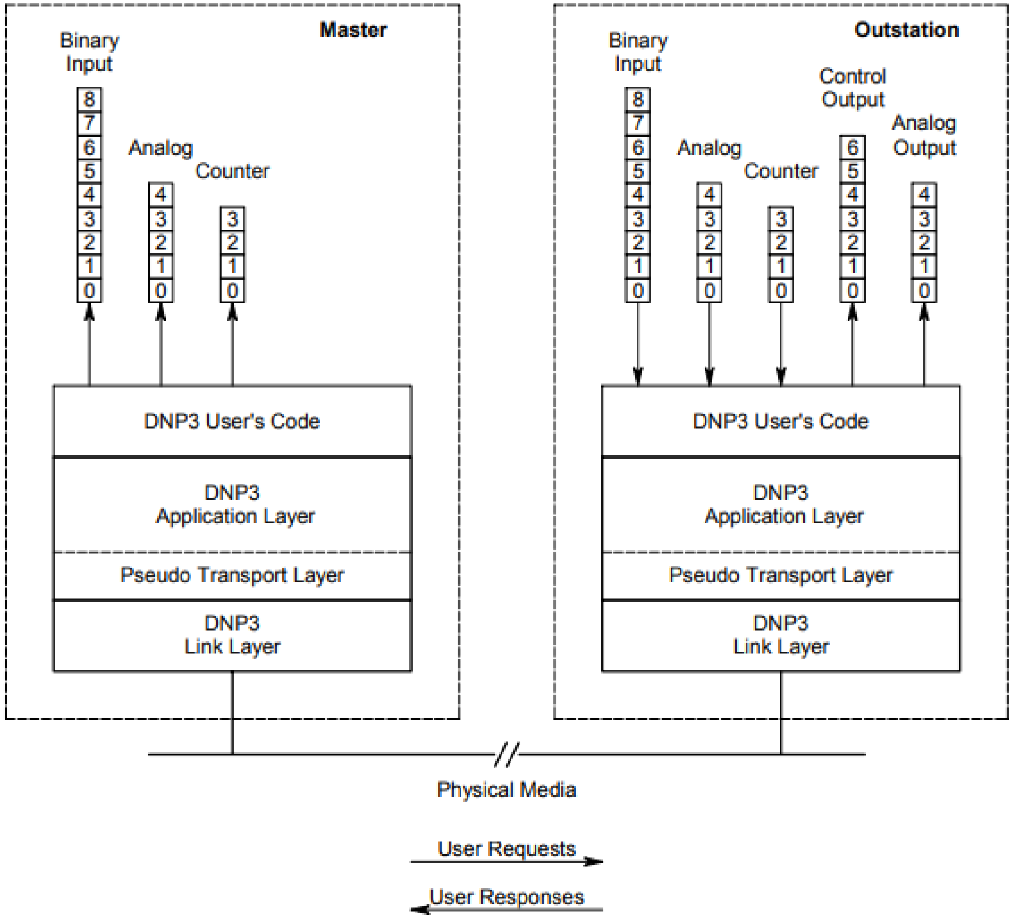
- Making the physical link reliable
  - Error detection
  - Multiple frame detection

DNP3 Frame

Header	Data Section

Header

Sync	Length	Link Control	Destination Address	Source Address	CRC



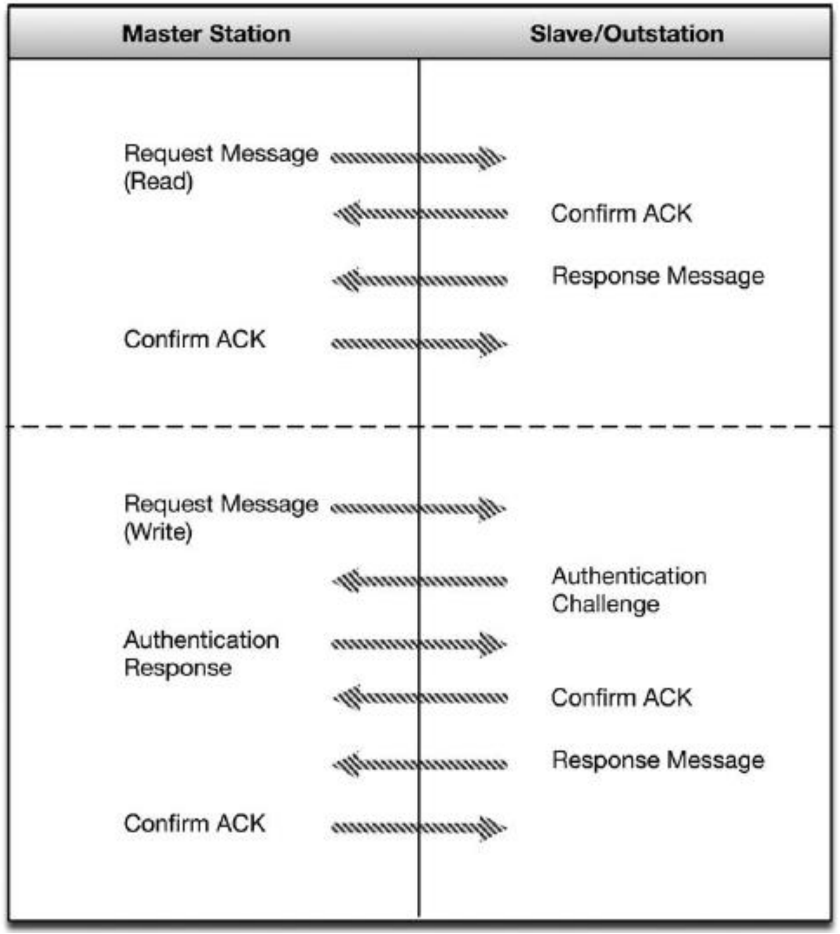
Secure DNP3

Adds authentication to the response/request process

- Challenge by the receiving device
  - Upon session initiation after a preset period of time
  - Or upon a critical request
- Unique session key hashed with message data

Verifies authority, integrity, and pairing

- Difficult to perform data manipulation, code injection, or spoof



Where DNP3 is used

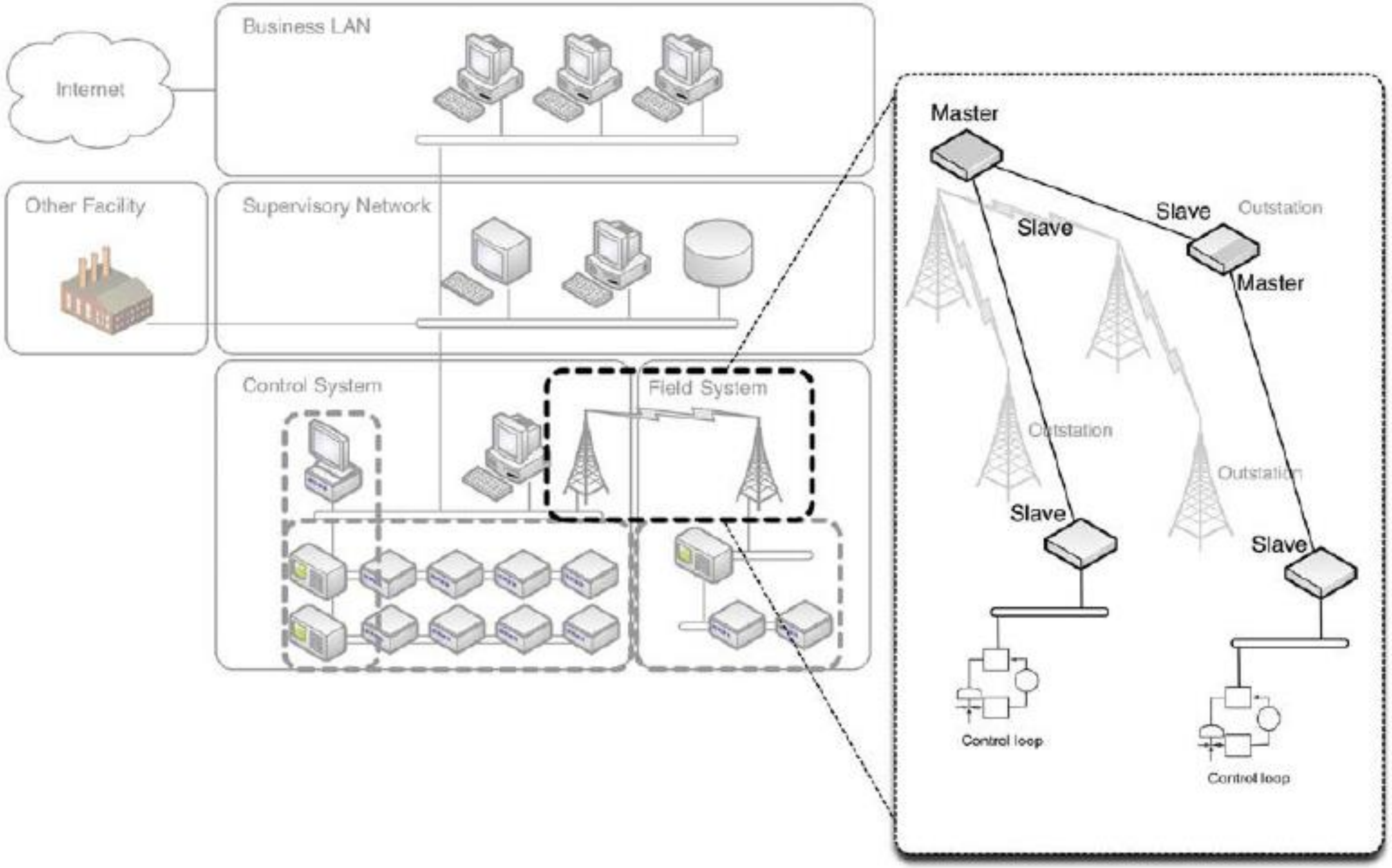
Between a master control station and an RTU in a remote station

- Over almost any medium including wireless, radio, and dial-up

Between RTUs and IEDs

- Competes with Modbus

Well suited for hierarchical and aggregated point-to-multipoint topologies



Inter Control Center Protocol (ICCP)

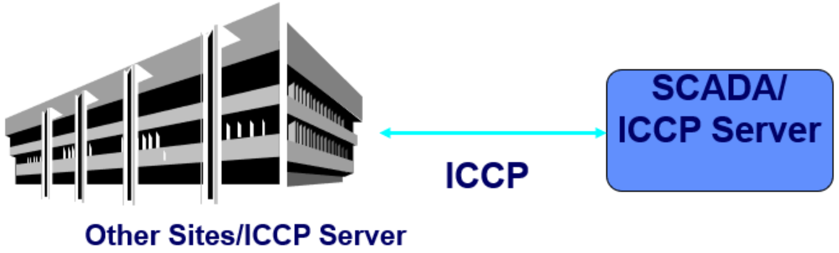
Also known as TASE.2 or IEC 60870-6

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



ICCP Characteristics

Client/server model

ICCP support is integrated either:

- Directly into a control system
- Provided via a gateway product
- Provided as software running on Unix that can then be installed to perform gateway functions

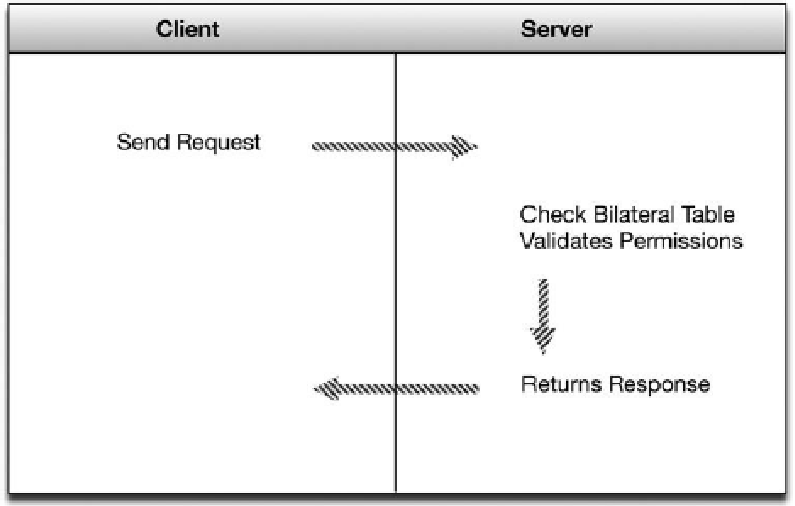
Primarily designed as a unidirectional client/server protocol

- Most modern implementations are bidirectional

ICCP Characteristics

Point-to-point protocol

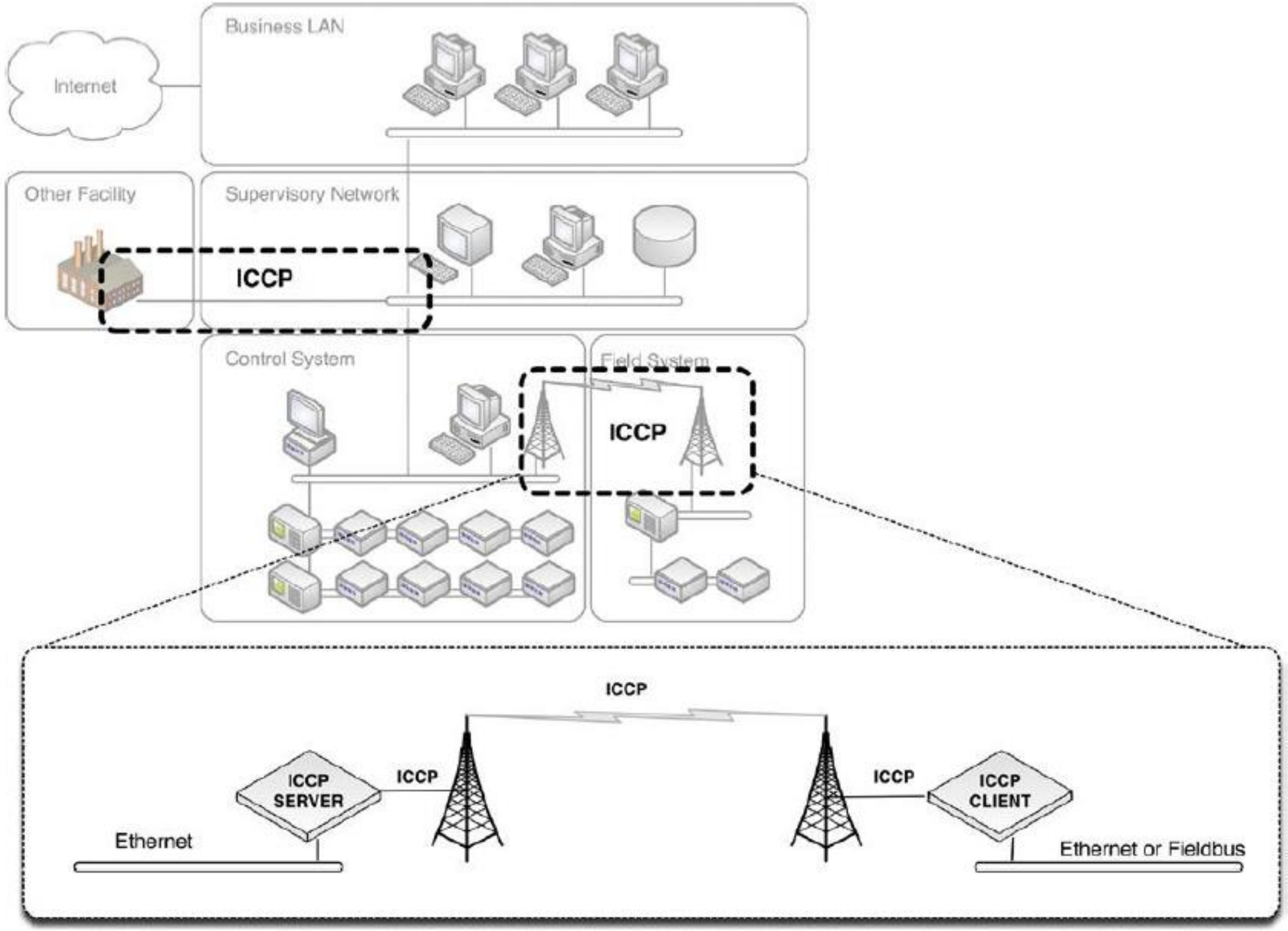
- "Bilateral table" defines an agreement between two control centers connected with an ICCP link
  - Access control list that identifies which data elements a client can access



Where ICCP is used

A few examples:

- Between two electric utilities
- Between two control systems within a single electric utility
- Between a main control center and a number of substations

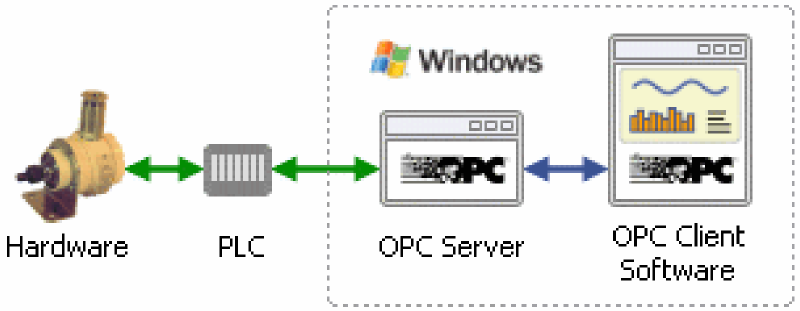


OLE FOR PROCESS CONTROL (OPC)

Not an INP

- Operational framework for the communication of Windows-based process control systems
- Uses Microsoft's Object Linking and Embedding (OLE) protocol

Suite of protocols that collectively enable process control systems to communicate using some of the underlying networking capabilities of Windows



OPC Characteristics

Server/client pairs

OPC Server is a software program that converts the hardware communication protocol used by a PLC into the OPC protocol

- Client needs to connect to the hardware,
  - Such as an HMI

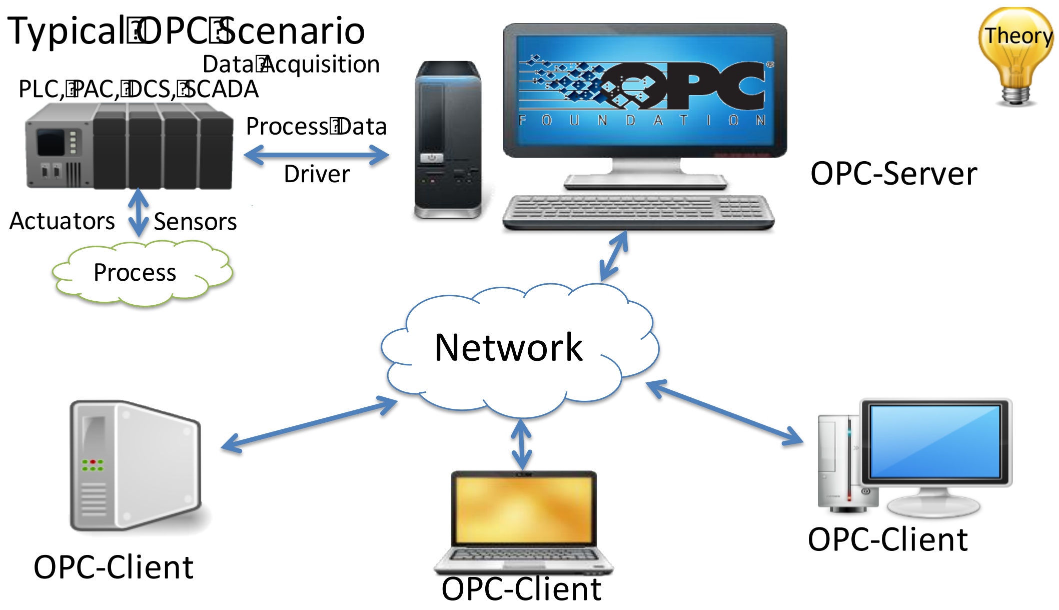
Open source

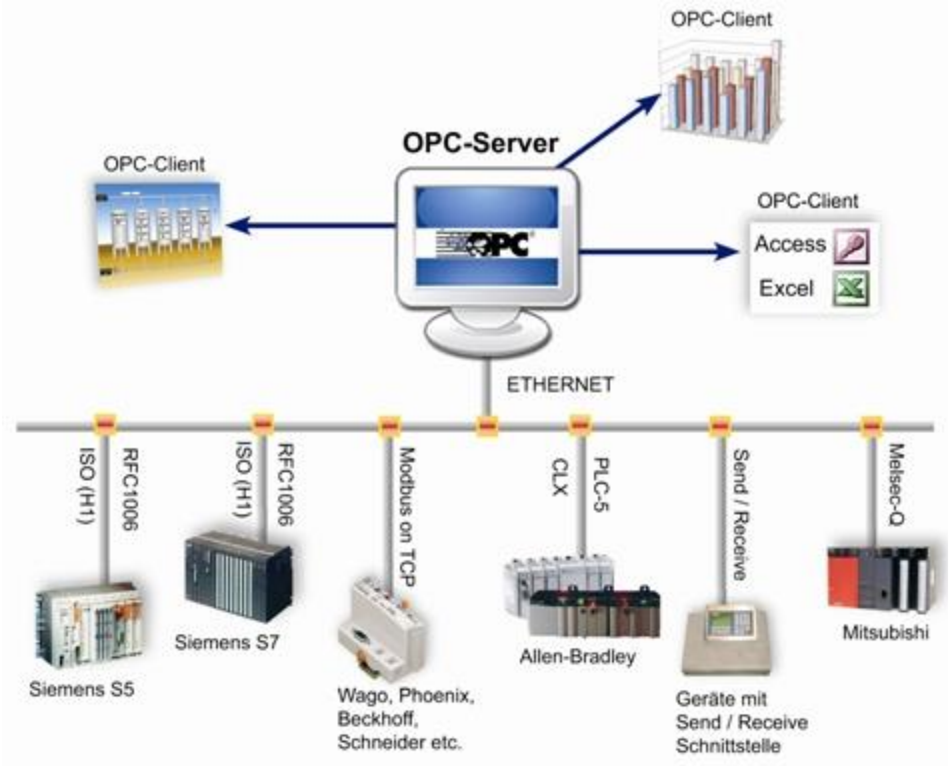
OPC stands for Open Platform Communications

OPC Characteristics

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

- Typically connected via an Ethernet TCP/IP network

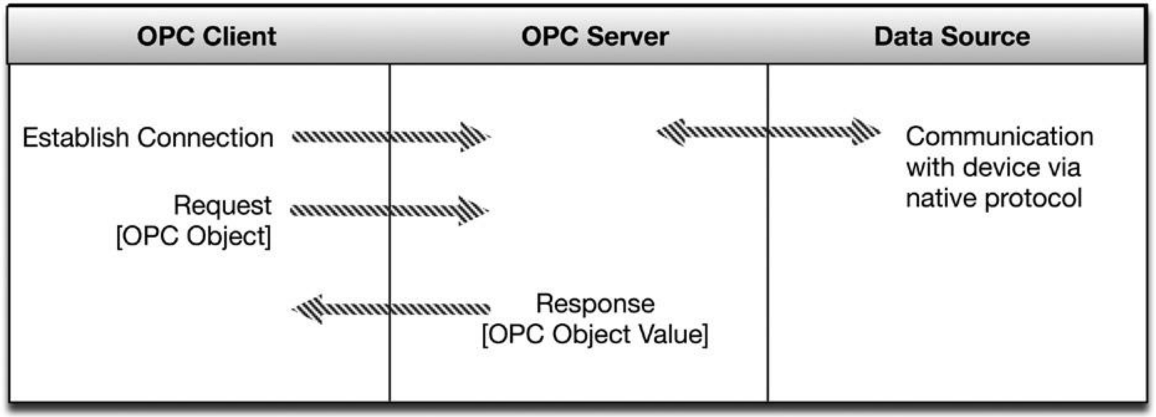




OPC Operation

Client application calls a local process,

- But instead of executing the process using local code, the process is executed on a remote server
  1. The process is performed remotely (on the server)
  2. Server Remote Procedure Call (RPC) functions then transmit the requested data back to the client computer
  3. Finally, the client process receives the data over the network, provides it to the requesting application, and closes the session

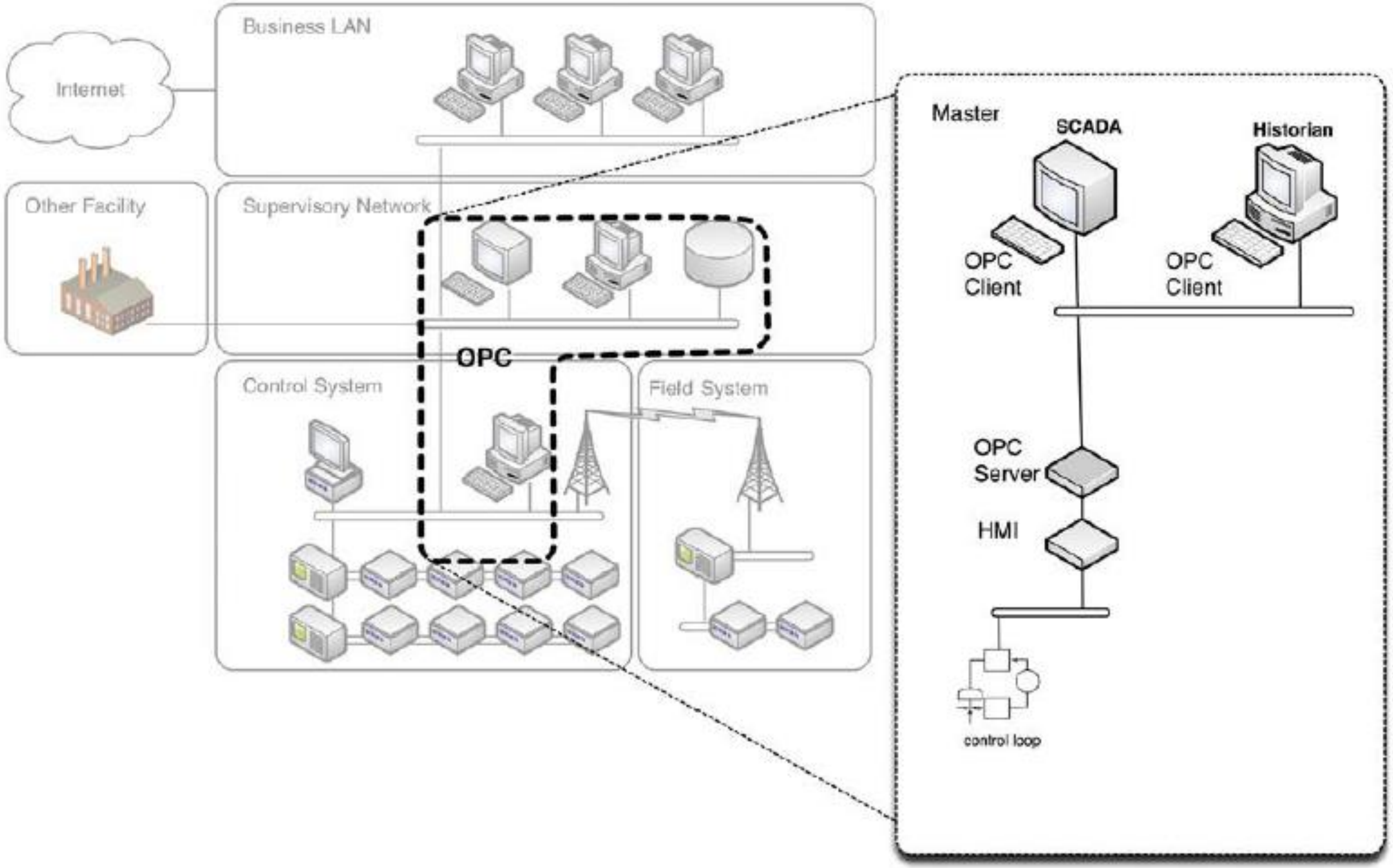


Where OPC is used

Data transfer to data historians, data collection within HMIs, and other supervisory controls

- Either between Windows-based devices,
- Or via OPC gateways

Also widely used within an industrial system's business network, including connections to corporate intranets, and even the Internet



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

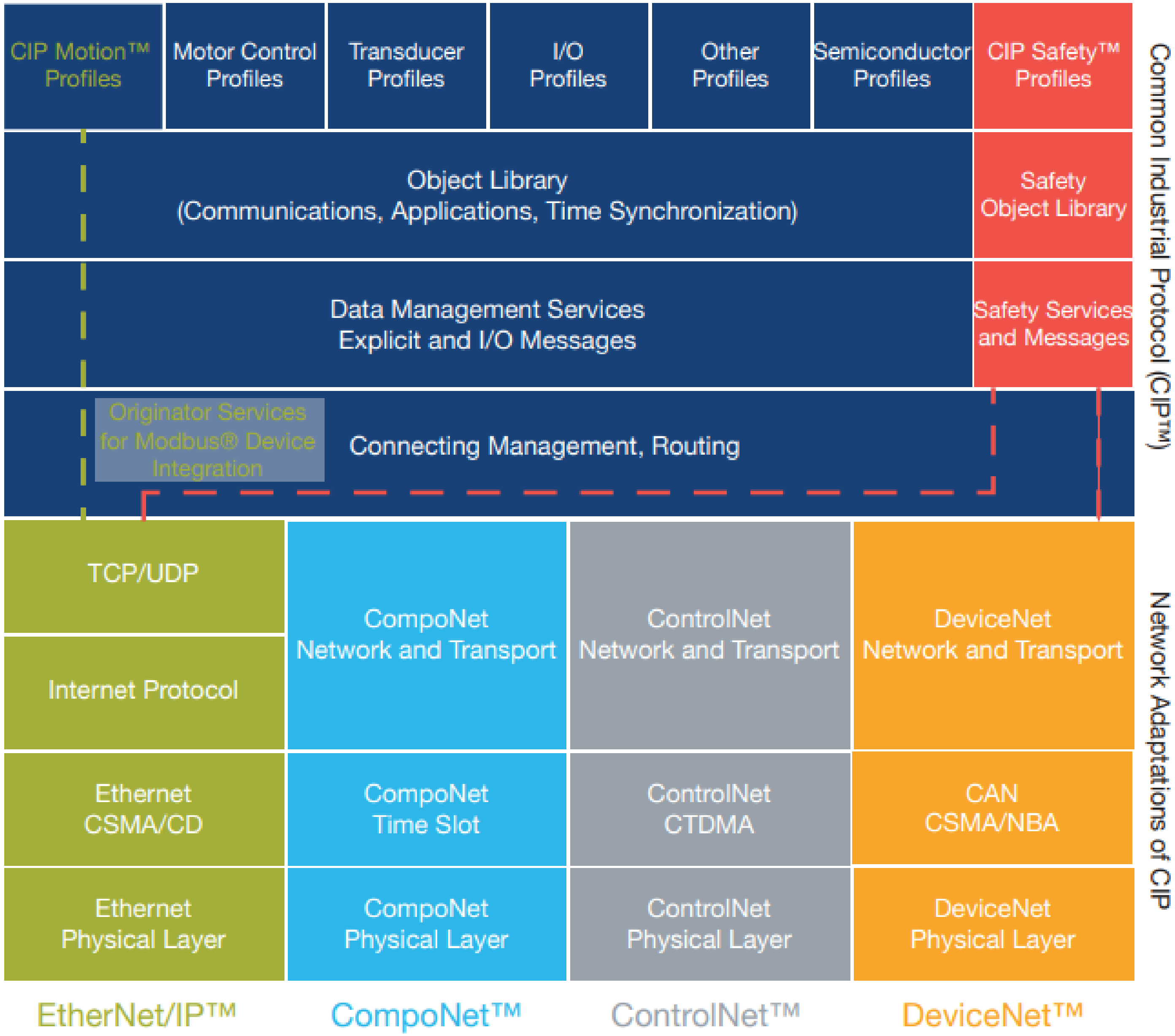
Implicit mode uses connectionless transport—specifically the User Datagram Protocol (UDP) and multicast transmissions

- To minimize latency and jitter

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

CompoNet Network and Transport
CompoNet Time Slot
CompoNet Physical Layer

ControlNet Network and Transport
ControlNet CTDMA
ControlNet Physical Layer

DeviceNet Network and Transport
CAN CSMA/NBA
DeviceNet Physical Layer

EtherNet/IP™
CompoNet™
ControlNet™
DeviceNet™

Common Industrial Protocol (CIP™)

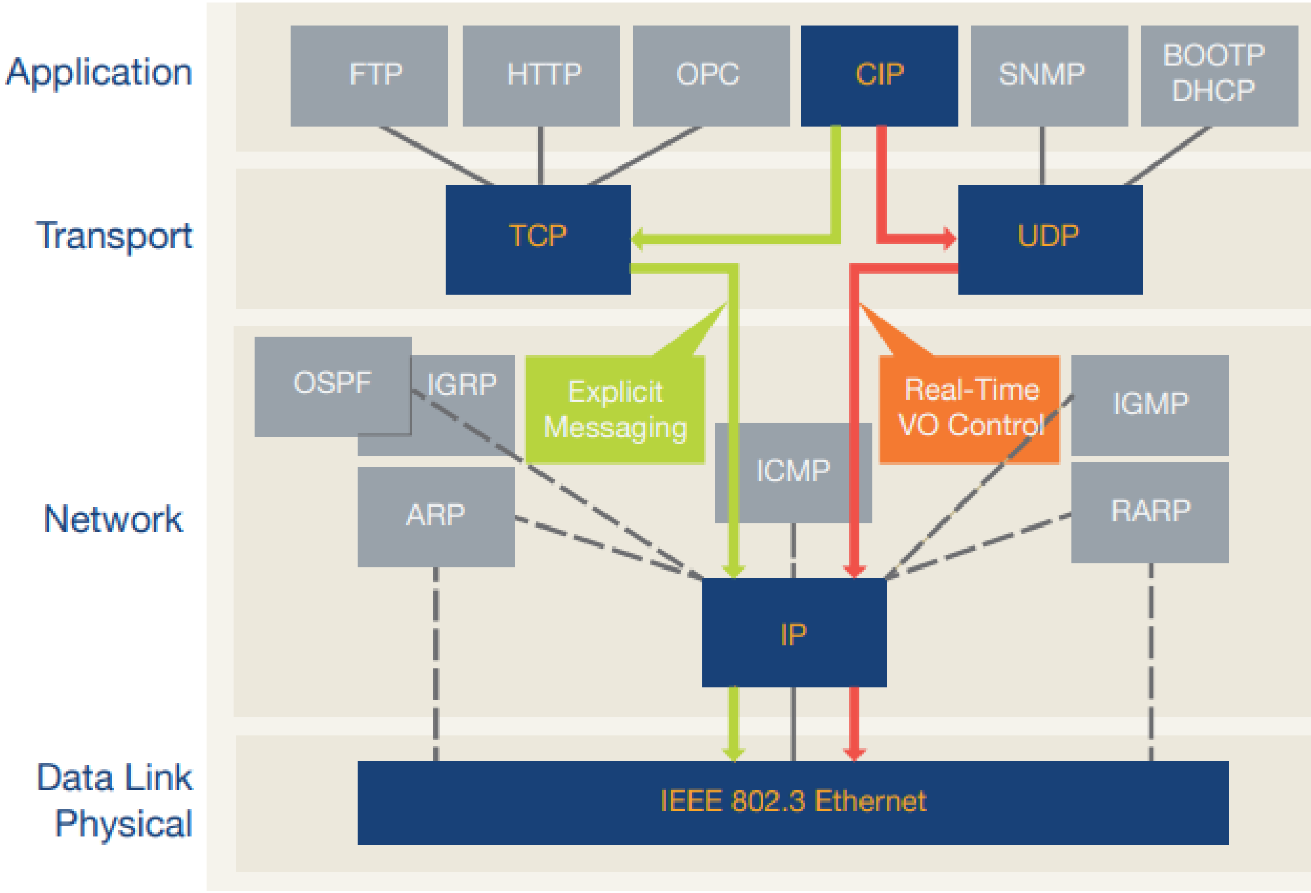
Network Adaptations of CIP

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



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

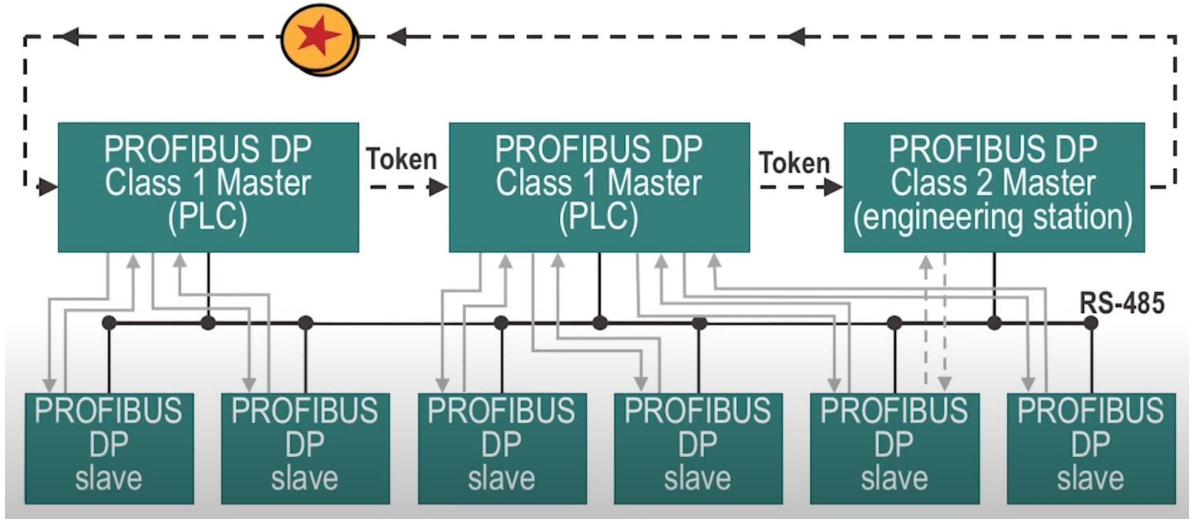
- First in factory automation industries,
  - Then process industries, manufacturing, etc.

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

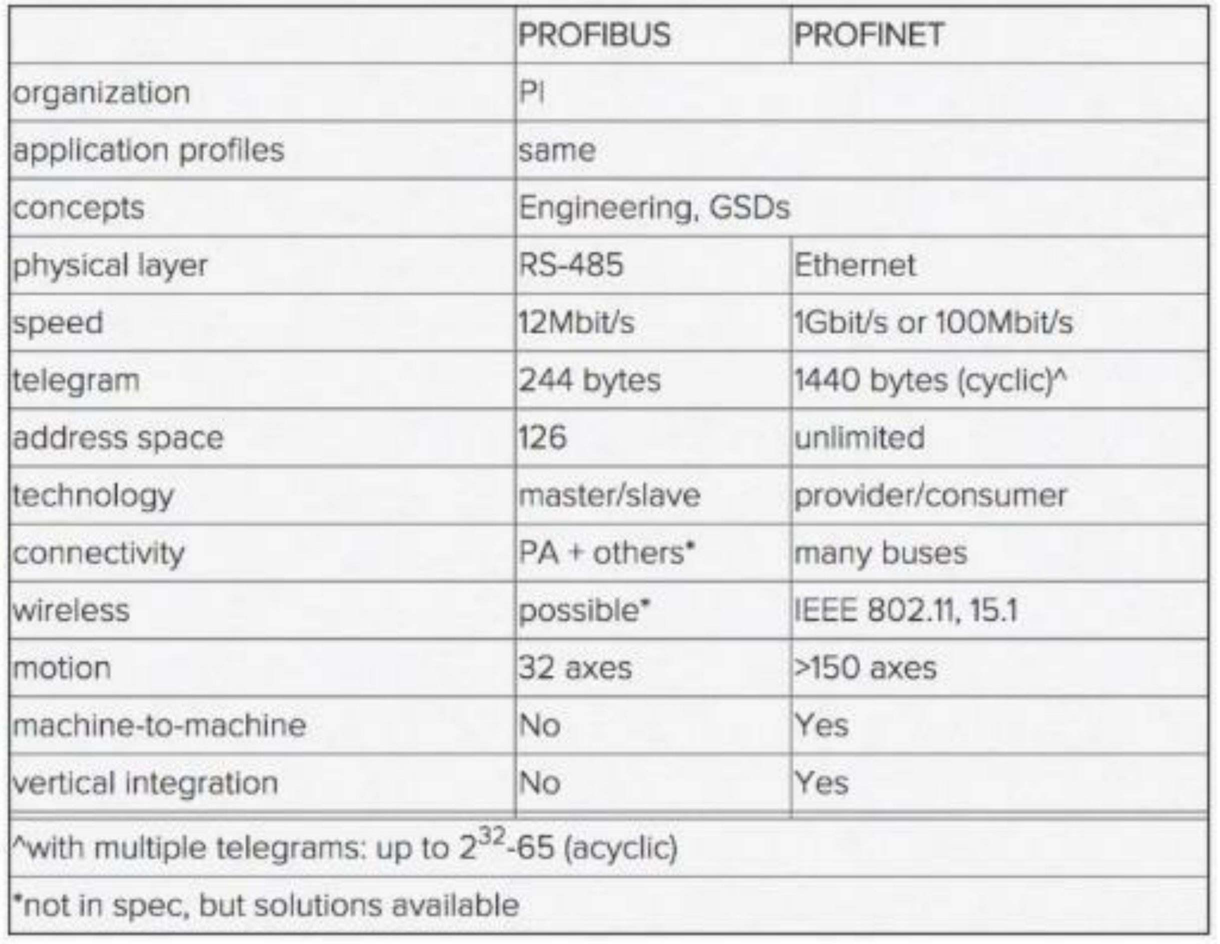
Profibus Characteristics

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 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		

EtherCAT

Real-time Ethernet fieldbus protocol

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

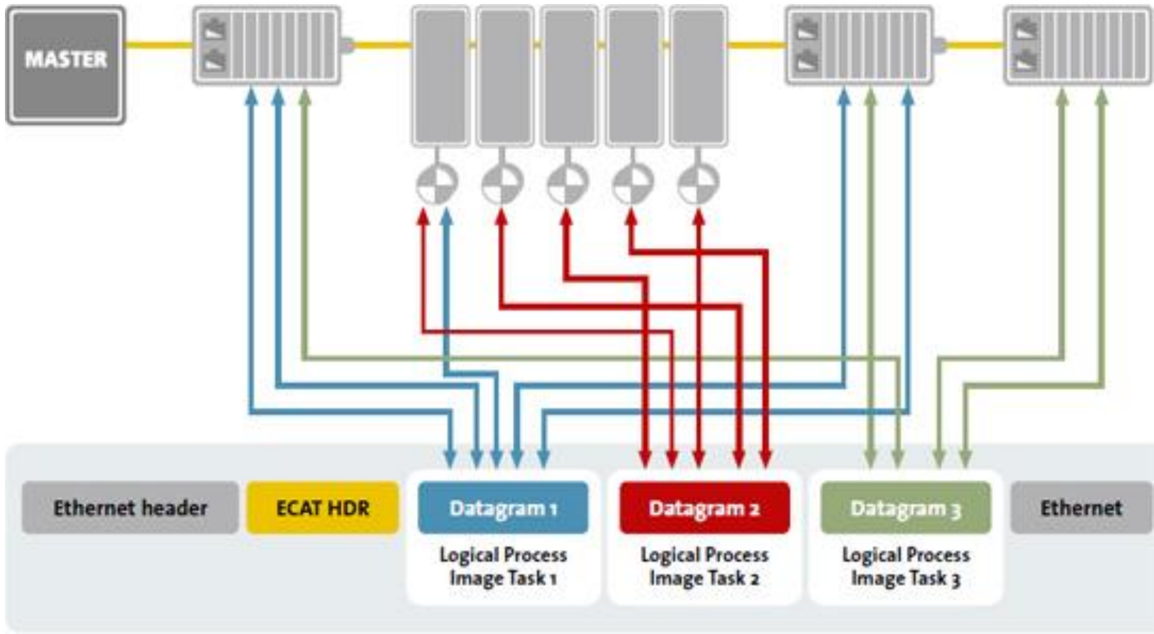
- EtherCAT communicates large amounts of distributed process data with just one Ethernet frame, so that typically only one or two Ethernet frames are required for a complete cycle
- Slaves pass the frame(s) to other slaves in sequence, appending its appropriate response, until the last slave returns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

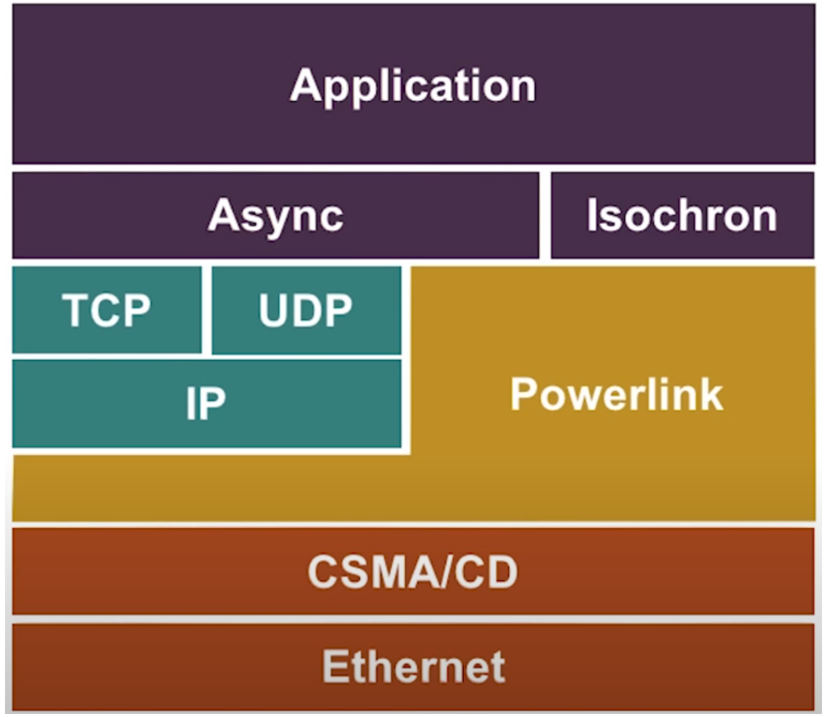
- Each EtherCAT slave device reads the data addressed to it “on the fly”, and inserts its data in the frame as the frame is moving downstream
- The frame is delayed only by hardware propagation delay times
- The last node in a segment (or drop line) detects an open port and sends the message back to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

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)

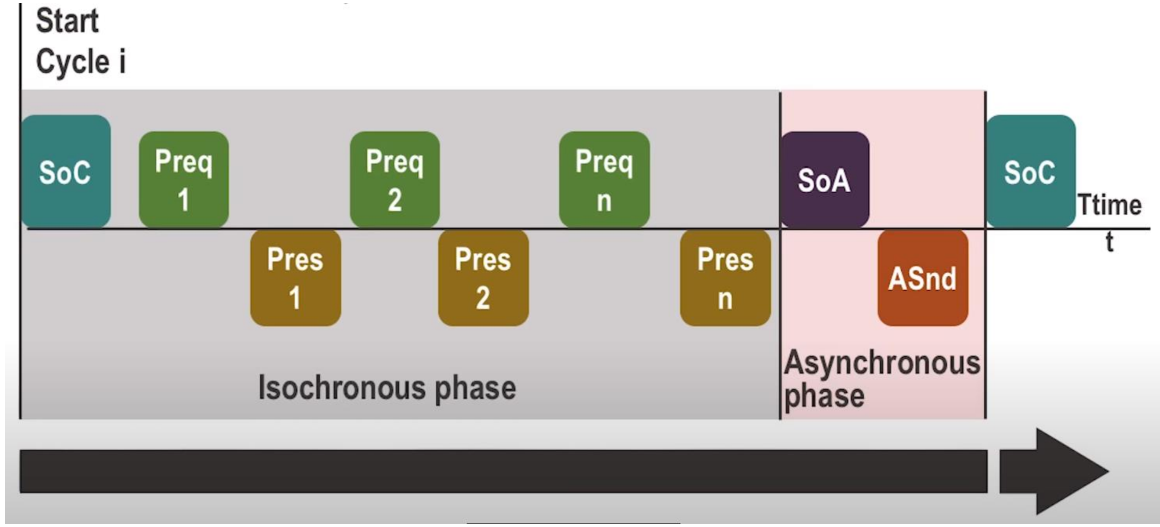
MN defines the clock pulse for synchronizing all devices and manages data communication cycle

- 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



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

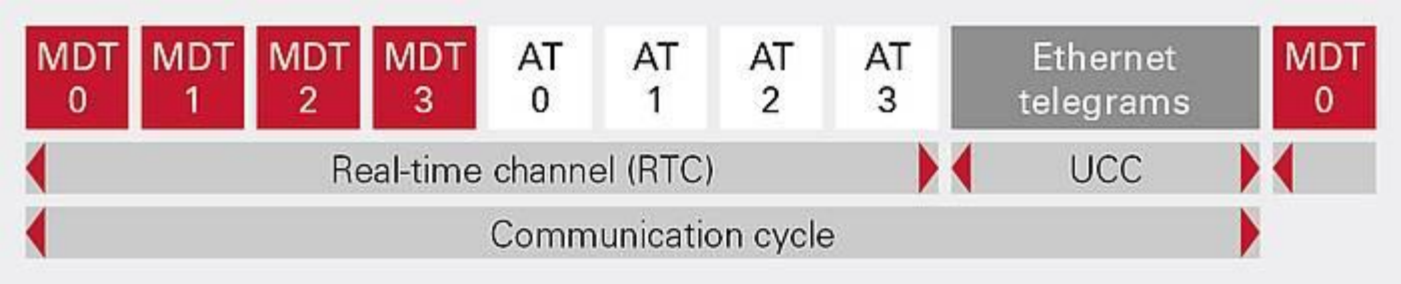
How Sercos III works?

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

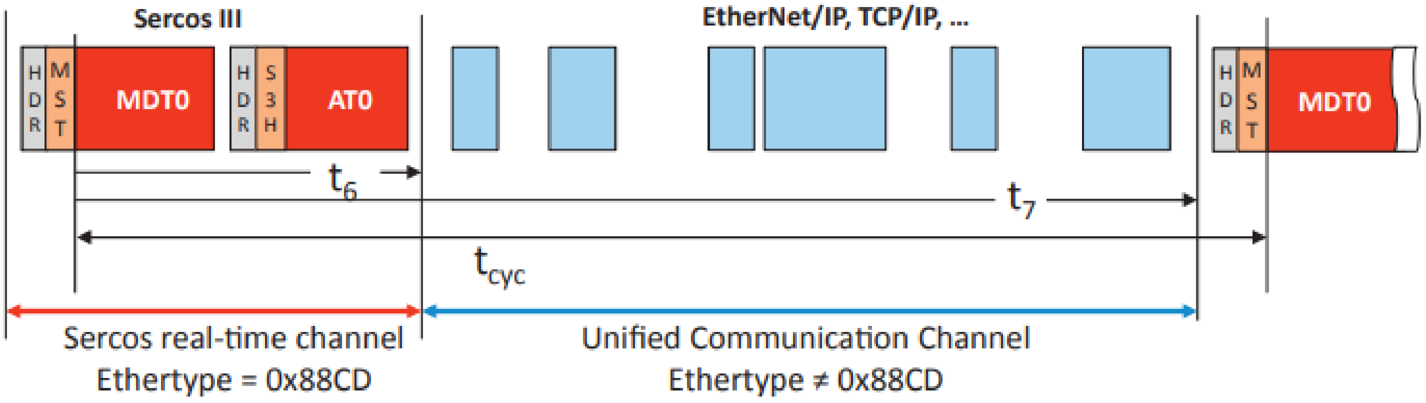
- Each node knows which portion of the MDT it should read based upon a predetermined byte allocation



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

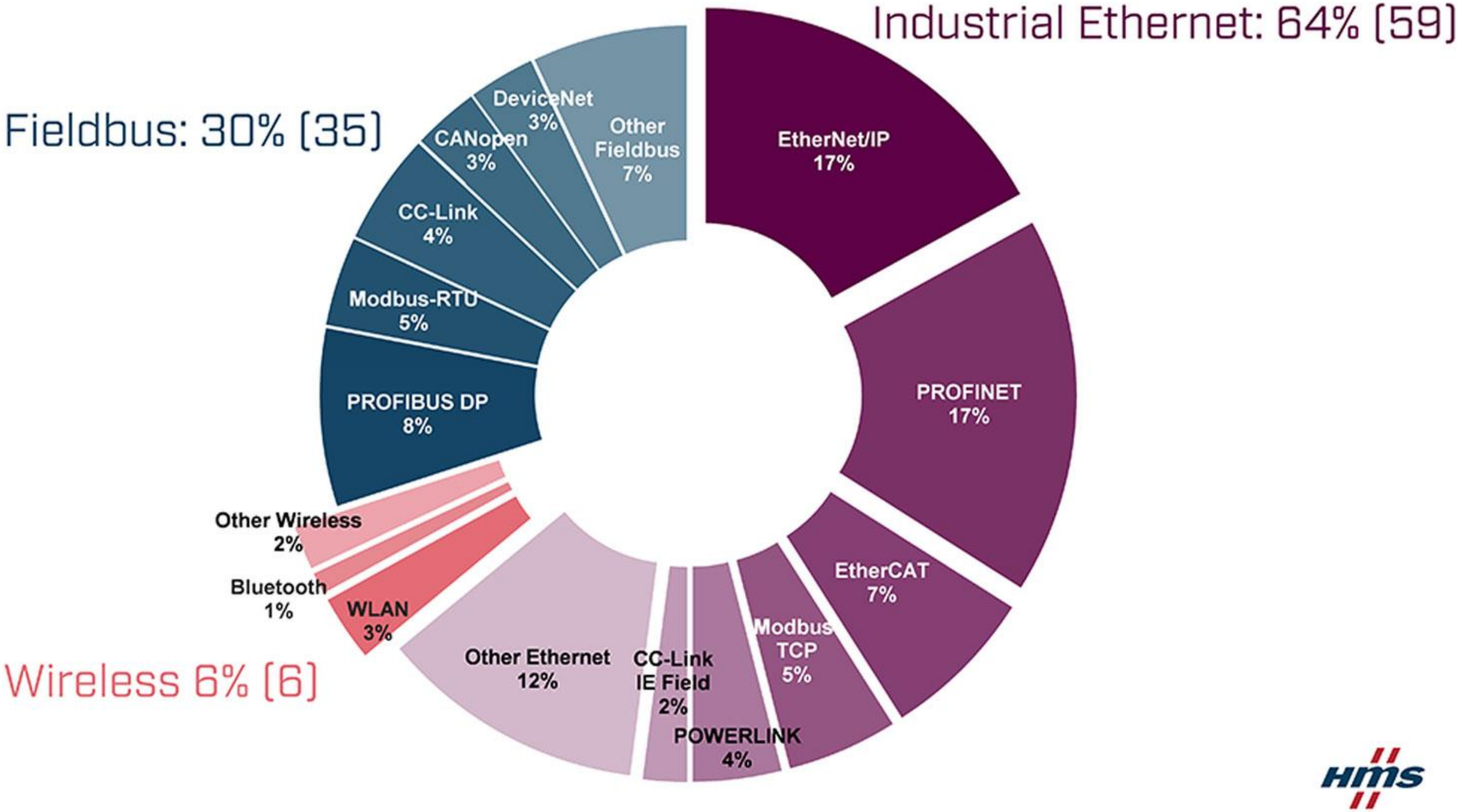


HDR: Header
S3H: Sercos III header

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

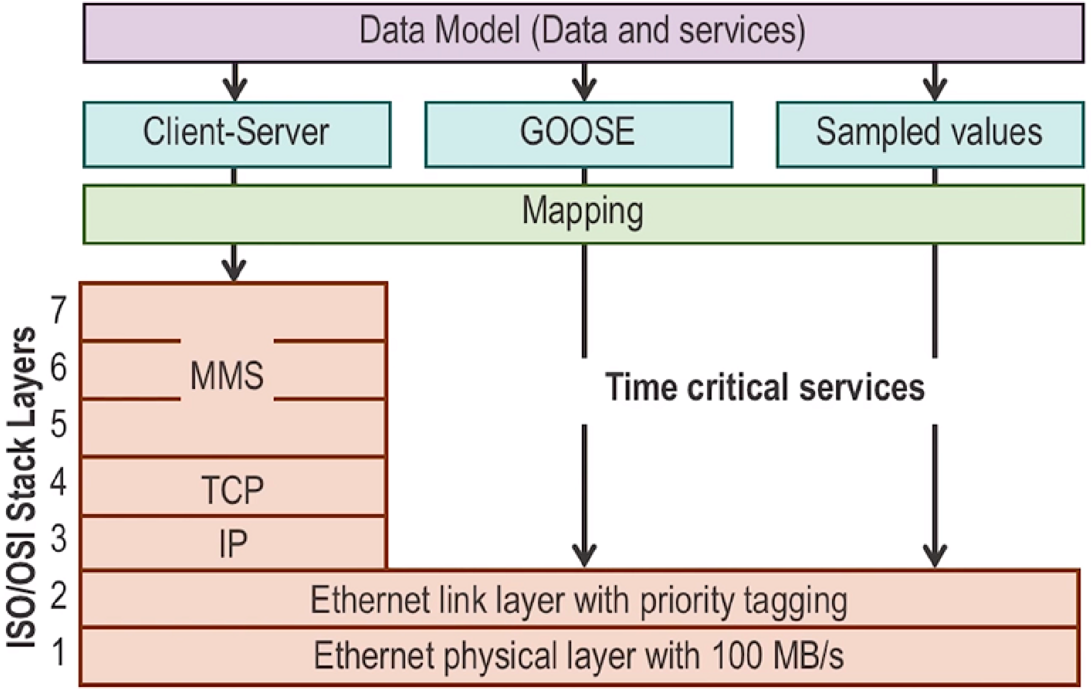
Recent Trend in INPs (2020)



Protocols supported by IEC 61850

Machine to machine (M2M) or device to device:

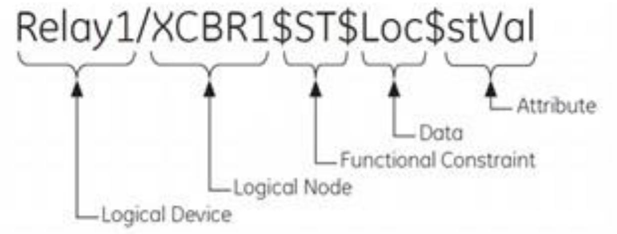
- Generic Substation Event (GSE)
- Peer to peer layer 2 protocol that multicasts events to multiple devices typically IEDs to IEDs
  - Generic Substation State Events (GSSE)
  - Generic Object Oriented Substation Events (GOOSE)
    - Status updates/sending command requests
    - Designed for layer 2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

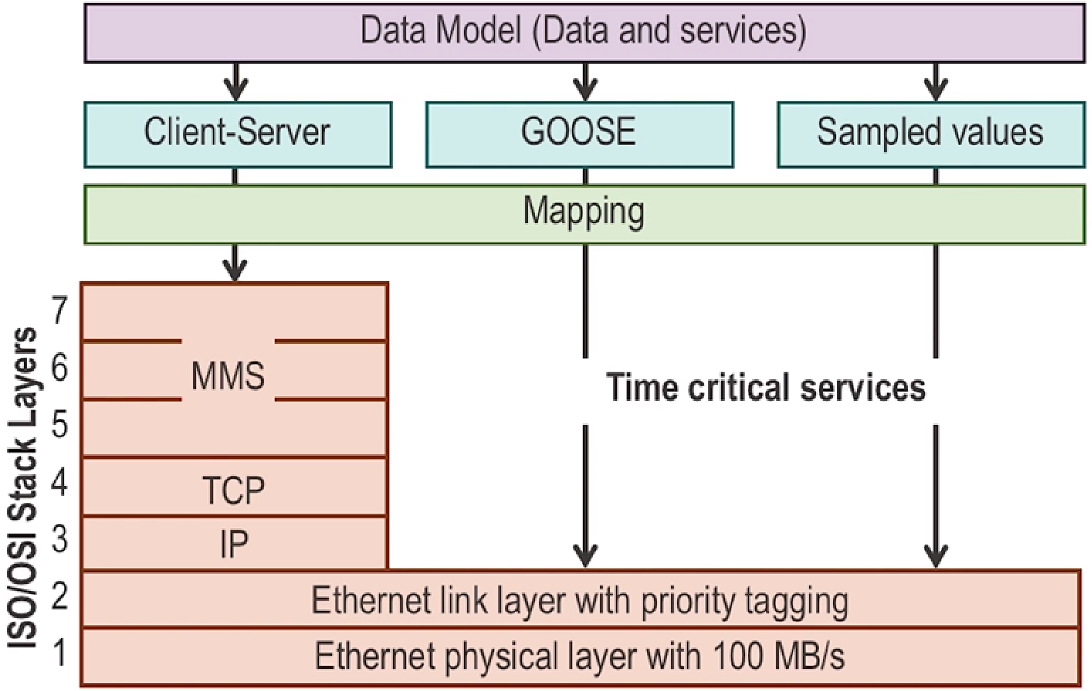

Data Model (Data and services)
Client-Server
GOOSE
Sampled values
Mapping
ISO/OSI Stack Layers
7
6
5
4
3
2
1
MMS
TCP
IP
Time critical services
Ethernet link layer with priority tagging
Ethernet physical layer with 100 MB/s

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




Data Model (Data and services)
Client-Server
GOOSE
Sampled values
Mapping
MMS
TCP
IP
Time critical services
Ethernet link layer with priority tagging
Ethernet physical layer with 100 MB/s
ISO/OSI Stack Layers
7
6
5
4
3
2
1