Control System Networks and Protocols

Capacity Building for Control System Security Collaborative Project

Greg Randall

Program Chair Computer Information Systems

Snead State Community College

Outline

- Overview of Basic Networking and Protocols
- OSI Model
- TCP/IP Model
- Industrial Control Systems
- SCADA
- SCADA Communications

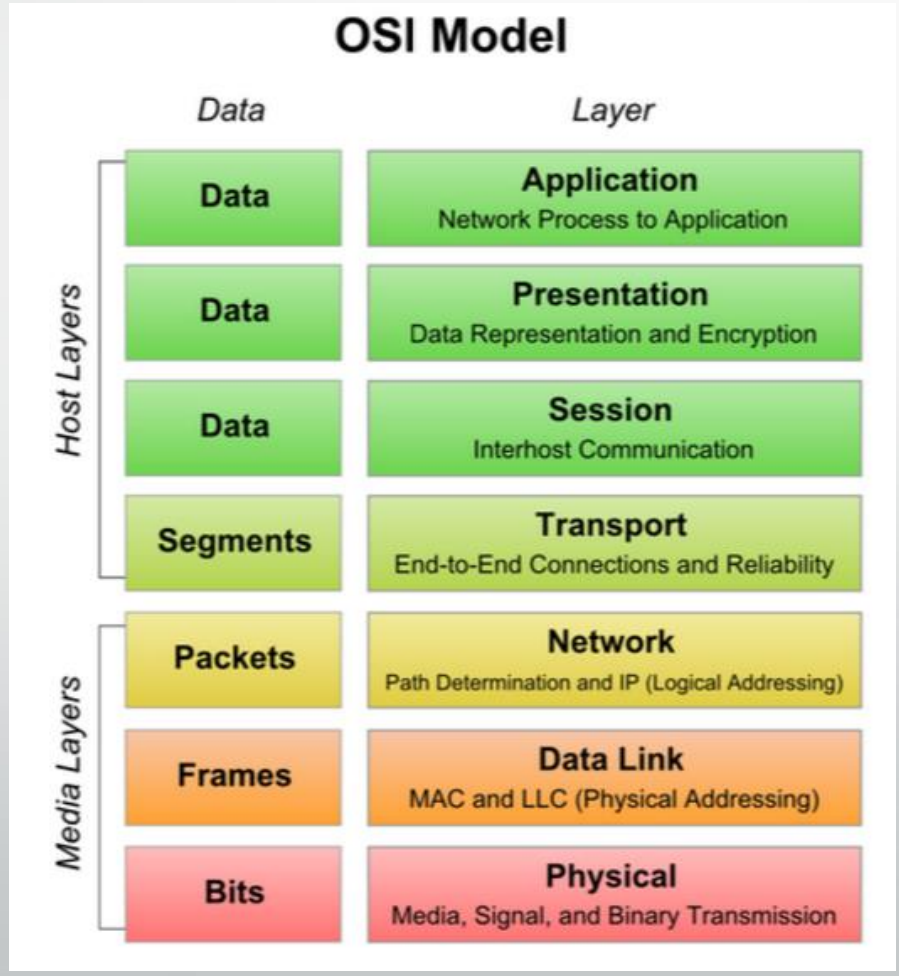
Basic Networking Overview- Protocols

- In the context of data communication, a network protocol is a formal set of rules, conventions and data structure that governs how computers and other network devices exchange information over a network.
- In other words, protocol is a standard procedure and format that two data communication devices must understand, accept and use to be able to talk to each other.

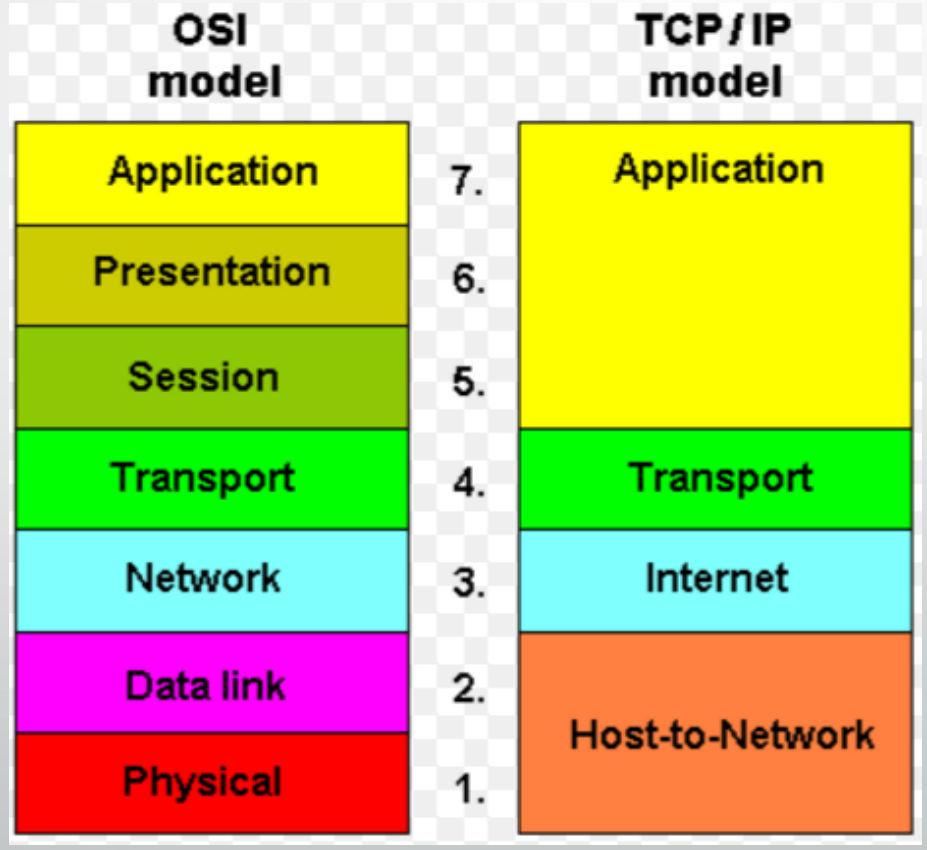
What does a protocol cover?

- A protocol is a set of rules that governs the communications between computers on a network.
- These rules include guidelines that regulate :
  - Access method
  - Allowed physical topologies
  - Types of cabling
  - Speed of data transfer
  - Data flow
  - Error control

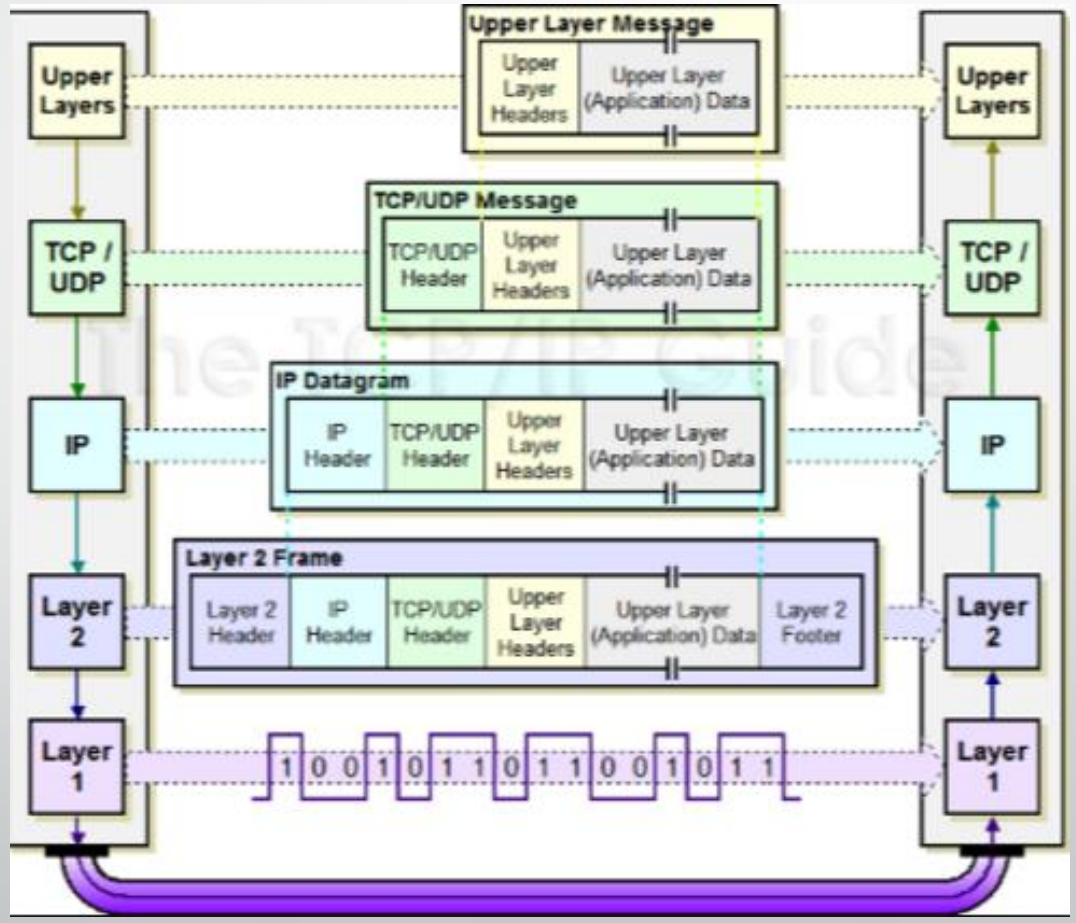
Open System Interconnect



TCP/IP Model


OSI model
TCP / IP model
Application
Presentation
Session
Transport
Network
Data link
Physical
7.
6.
5.
4.
3.
2.
1.
Application
Transport
Internet
Host-to-Network

Control Systems Model



IP Addressing

- IP Address- A unique 32 bit address that identifies each computer using the Internet Protocol to communicate over a network.
- For human reading, we group the address into 8 bits separated by a decimal point, and converted to decimal. I.e. 209.65.109.12

IP Addressing Cont.

- **Public Address**- An IP address that is routed publically on the Internet
- **Private Address**- An address that is used for internal communication
- **Network Address Translation- NAT** is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.
- A **NAT box** located where the LAN meets the Internet makes all necessary IP address translations.

IP Addresses Classes

Class	1st Octet Decimal Range
A	1 – 126*
B	128 – 191
C	192 – 223
D	224 – 239
E	240 – 254

Default Subnet Mask
255.0.0.0
255.255.0.0
255.255.255.0

Private IP Addresses

Class	Private Networks	Subnet Mask	Address Range
A	10.0.0.0	255.0.0.0	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.0.0	255.240.0.0	172.16.0.0 - 172.31.255.255
C	192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

Layer 2- Data Link Frame

Payloads such as control system data

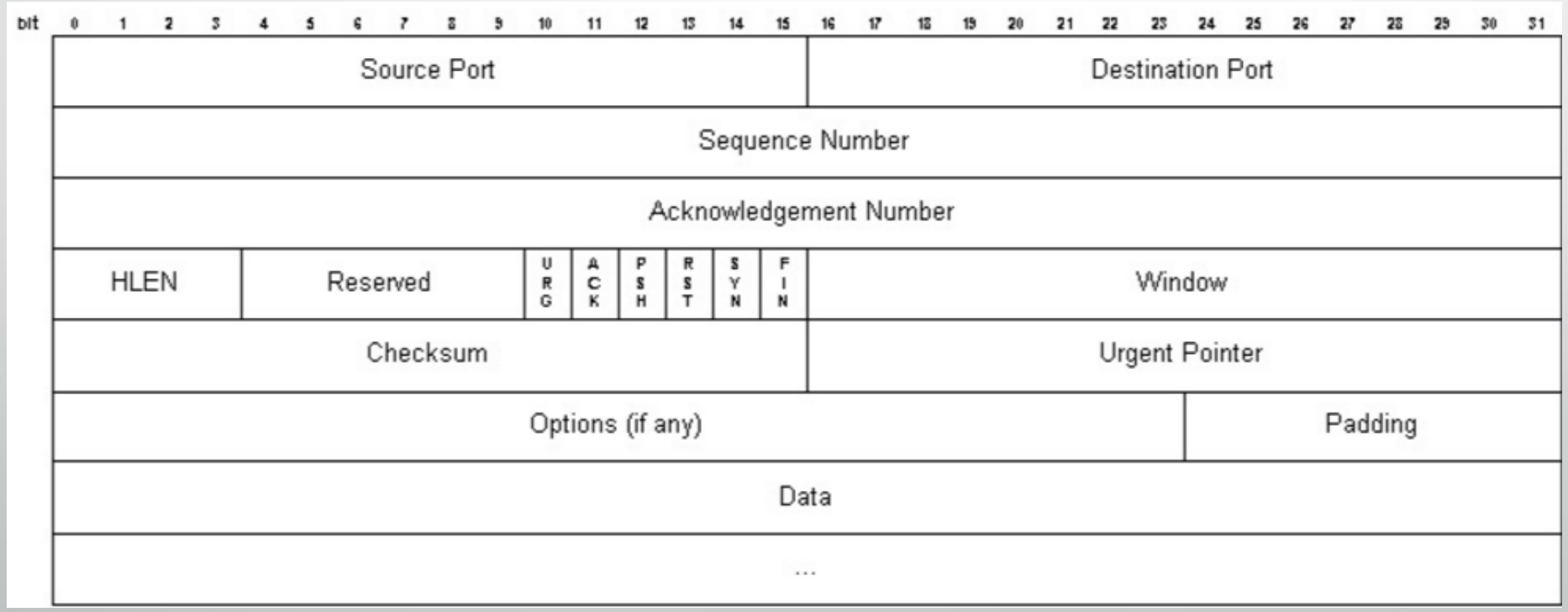
Ethernet Frame

62 bits	Preamble used for bit synchronization
2 bits	Start of Frame Delimiter
48 bits	Destination Ethernet Address
48 bits	Source Ethernet Address
16 bits	Length or Type
46 -1500 bytes	Data
32 bits	Frame Check Sequence

TCP/IP

- TCP and IP were developed by a Department of Defense (DOD) research project to connect a number different networks designed by different vendors into a network of networks
- **IP** - is responsible for moving packet of data from node to node. IP forwards each packet based the destination address (the IP address).
  - IP operates on gateway machines that move data from department to organization to region and then around the world.
- **TCP** - is responsible for verifying the correct delivery of data from client to server. Data can be lost in the intermediate network.
  - TCP adds support to detect errors or lost data and to trigger retransmission until the data is correctly and completely received.

TCP Frame Format



Protocol Ports

- A **port** is an endpoint of communication in an operating system.
- A port is always associated with an IP address of a host and the protocol type of the communication, and thus completes the destination or origination address of a communications session.
- A port is identified for each address and protocol by a 16-bit number, commonly known as the **port number**. The range is from 0-65535
- Specific port numbers are often used to identify specific services.
- Type of ports
  - **Ports 0-1023**- well-known port numbers. I.e. HTTP= port 80, FTP= port 20 and21
  - **Ports 1024-49151** - registered ports: use for vendor applications
  - **Ports >49151** - dynamic / private ports

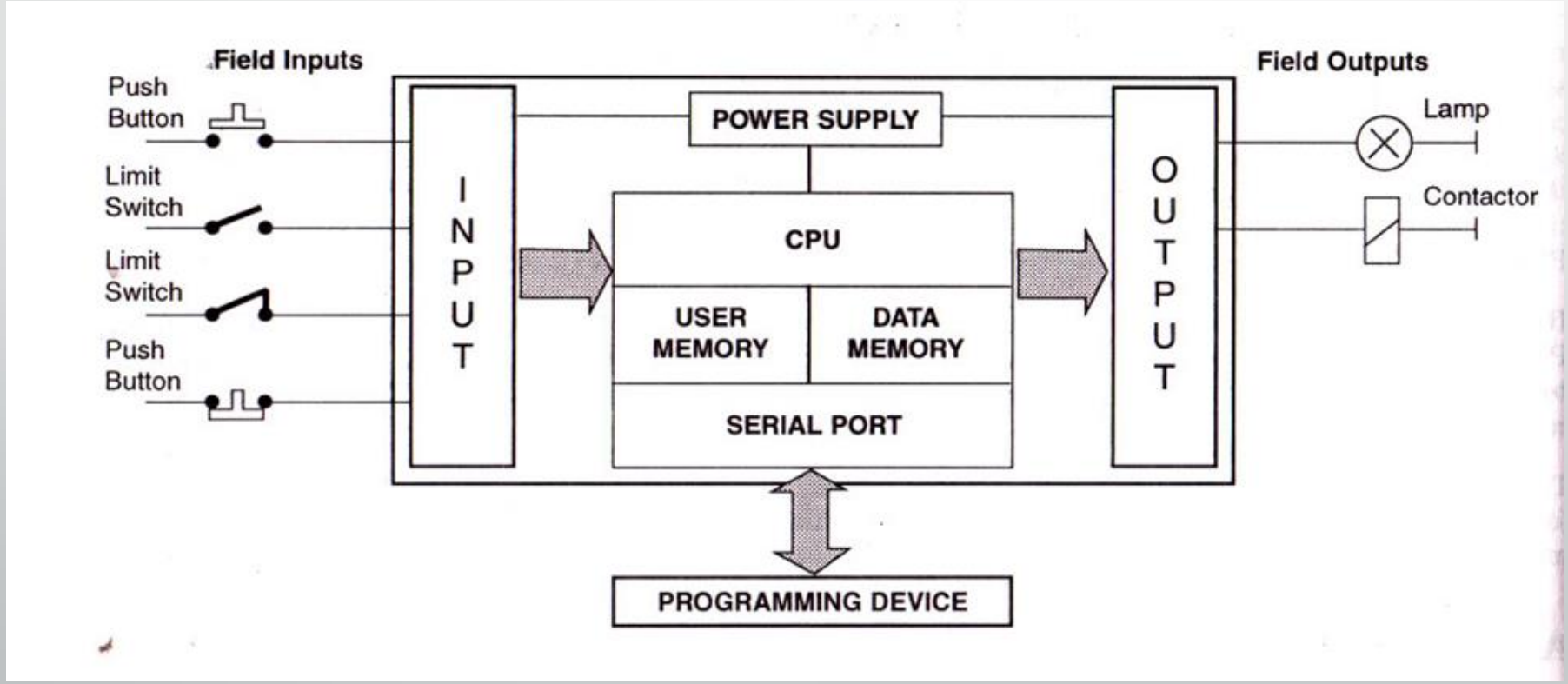
Industrial Control System (ICS)

- **Industrial control system (ICS)** is a general term that encompasses several types of control systems used in industrial production, including:
  - Supervisory Control and Data Acquisition (SCADA) systems
  - Distributed Control Systems (DCS)
  - Programmable Logic Controllers (PLC); often found in the industrial sectors and critical infrastructures

ICS

- **ICSs** are typically used in industries such as electrical, water, oil, gas and data.
- Automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices.
- Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

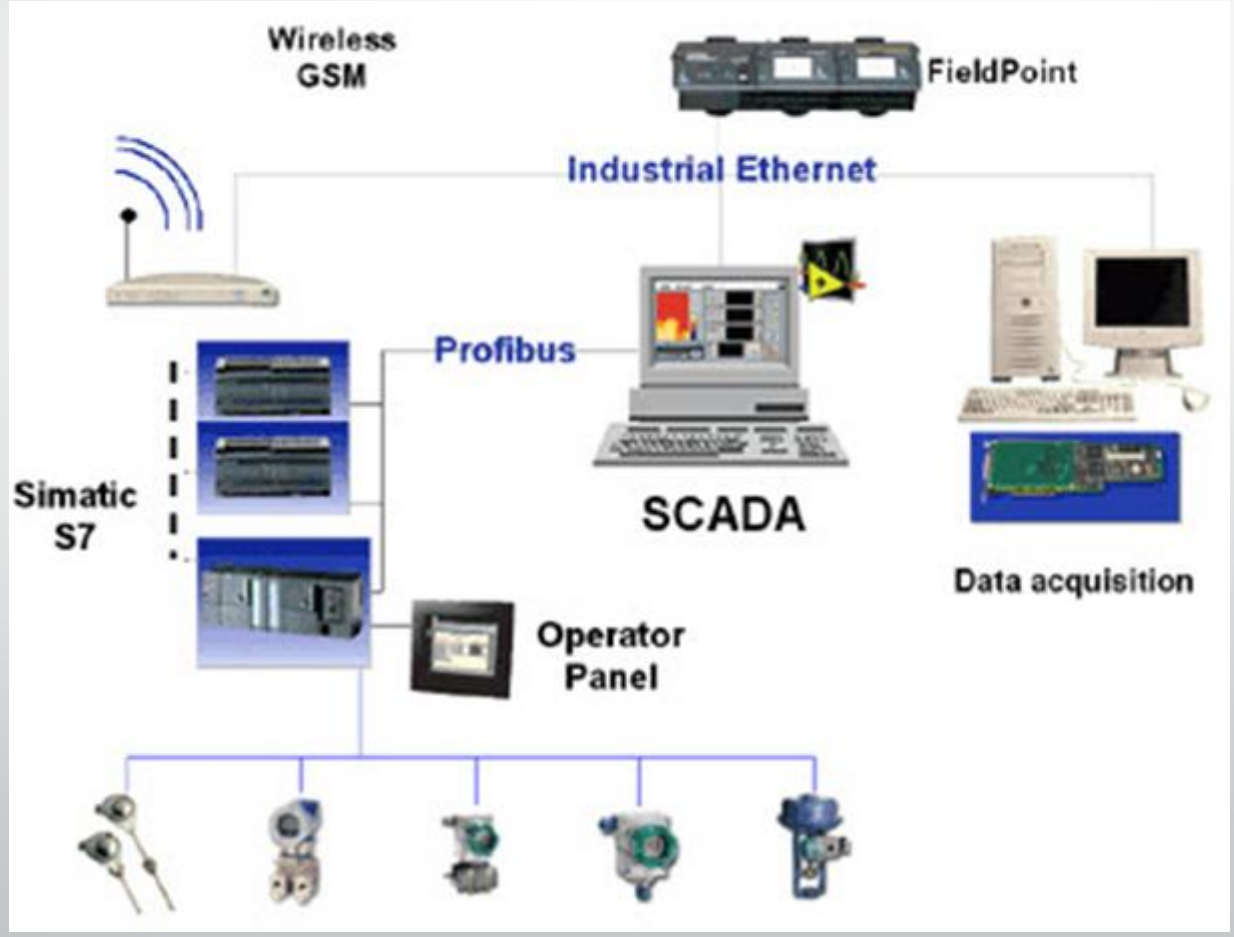
Basic PLC Device



Supervisory Control and Data Acquisition (SCADA)

- **SCADA** generally refers to an industrial computer system that monitors and controls a process.
- In the case of the transmission and distribution elements of electrical utilities, **SCADA** will monitor substations, transformers and other electrical assets.

General SCADA Diagram



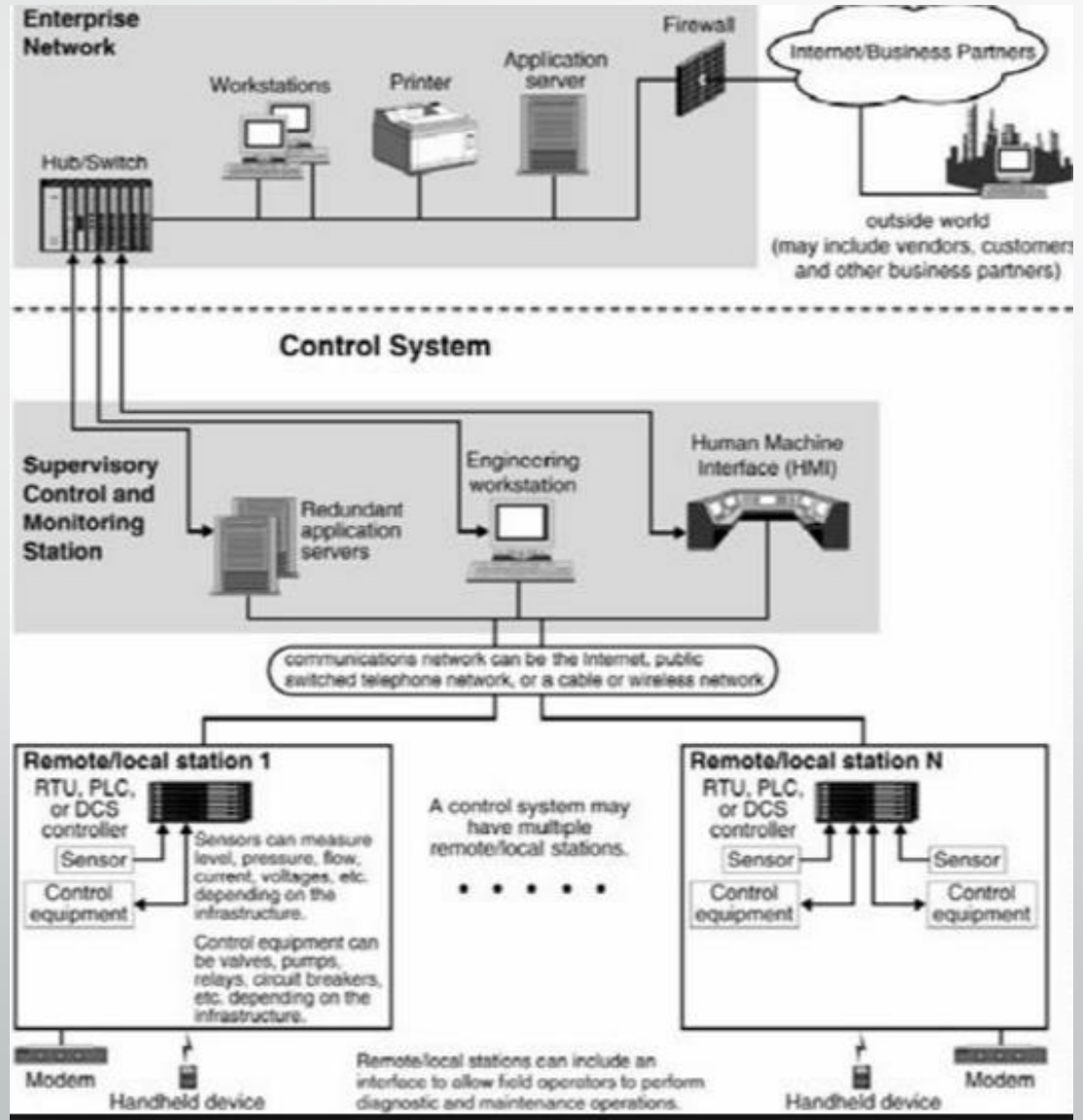
Remote Terminal Unit (RTU)

- A **Remote Terminal Unit** is an electronic device that is controlled by a microprocessor.
- The device interfaces with physical objects to a Distributed Control System (DCS) or Supervisory Control and Data Acquisition (SCADA) system by transmitting telemetry data to the system.

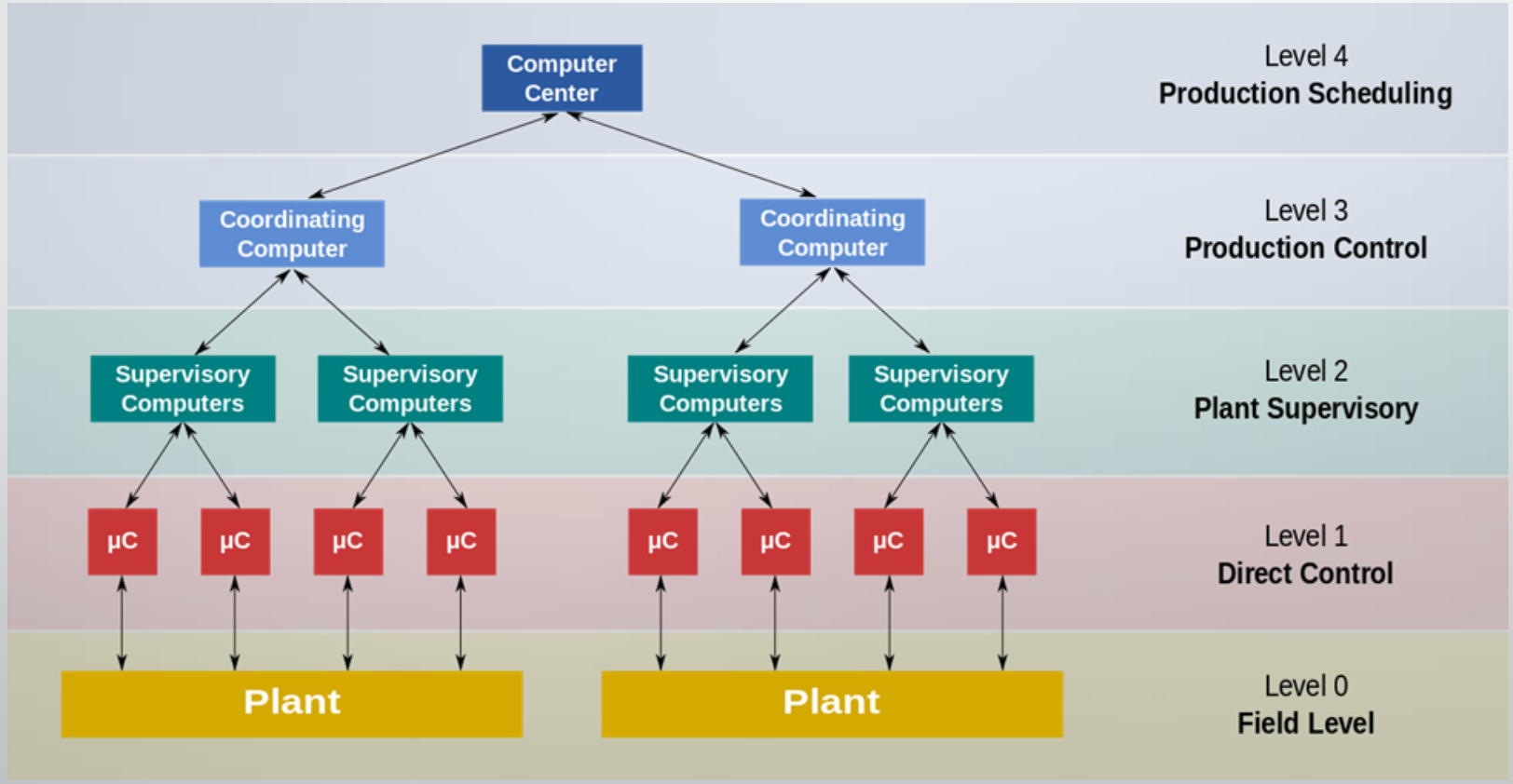
Distributed Control System (DCS)

- A **distributed control system** (**DCS**) is a **control system** for a process or plant, wherein control elements are distributed throughout the system.

DCS


Enterprise Network
Workstations
Printer
Application server
Firewall
Hub/Switch
Internet/Business Partners
outside world
(may include vendors, customers and other business partners)
Control System
Supervisory Control and Monitoring Station
Redundant application servers
Engineering workstation
Human Machine Interface (HMI)
communications network can be the Internet, public switched telephone network, or a cable or wireless network
Remote/local station 1
RTU, PLC, or DCS controller
Sensor
Control equipment
Sensors can measure level, pressure, flow, current, voltages, etc. depending on the infrastructure.
Control equipment can be valves, pumps, relays, circuit breakers, etc. depending on the infrastructure.
A control system may have multiple remote/local stations.
Remote/local station N
RTU, PLC, or DCS controller
Sensor
Control equipment
Modem
Handheld device
Remote/local stations can include an interface to allow field operators to perform diagnostic and maintenance operations.
Handheld device
Modem

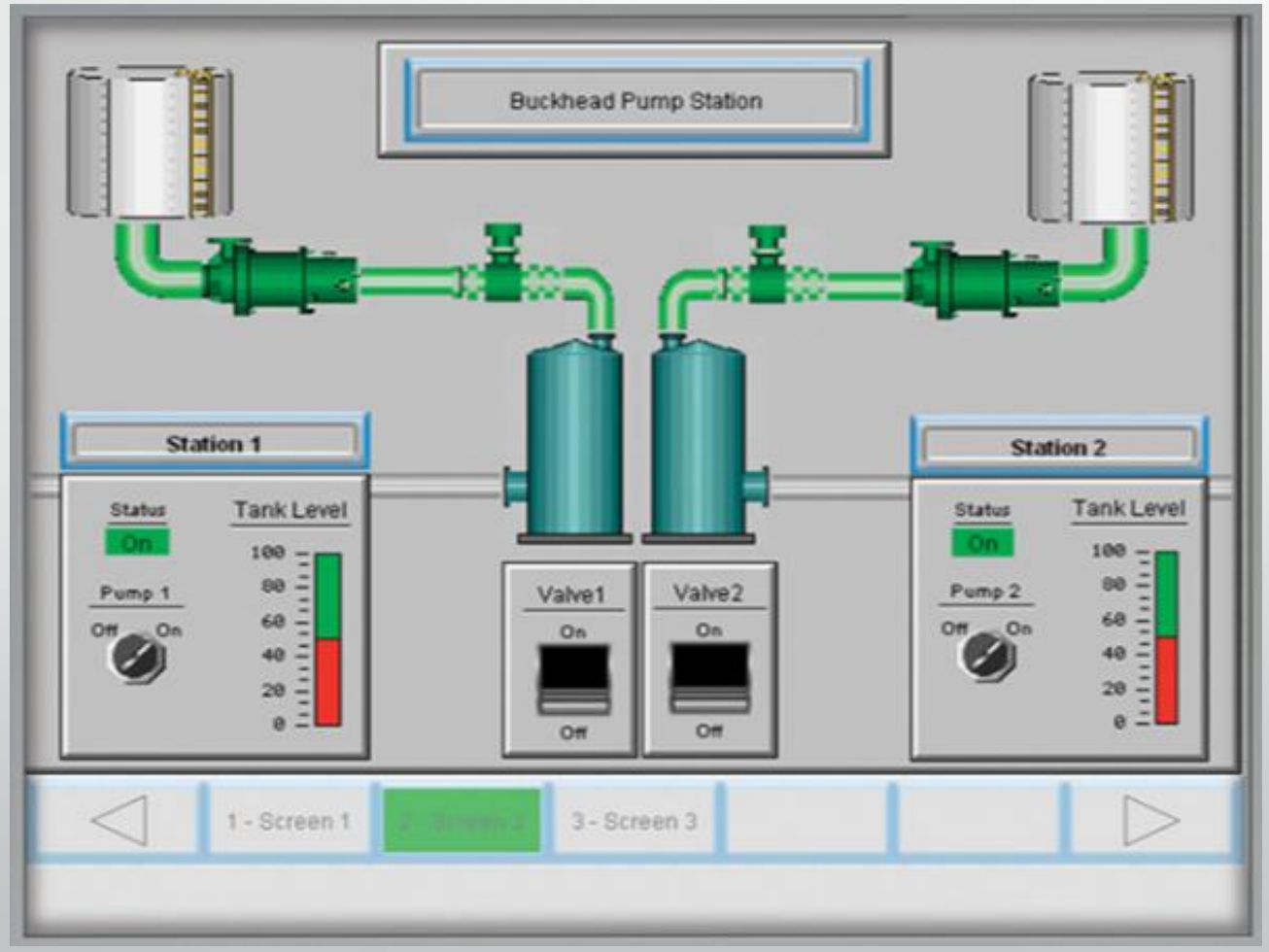
DCS Continued



Human Machine Interface

- An **HMI** is a software application that presents information to an operator or user about the state of a process, and to accept and implement the operators control instructions.
- Typically information is displayed in a graphic format (Graphical User **Interface** or GUI).

HMI


Buckhead Pump Station
Station 1
Status
On
Pump 1
Off
On
Tank Level
100
80
60
40
20
0
Valve1
On
Off
Valve2
On
Off
Station 2
Status
On
Pump 2
Off
On
Tank Level
100
80
60
40
20
0
1 - Screen 1
3 - Screen 3

Communication Protocols

- Communication Protocols are the rules used to send and receive data from the SCADA, DCS, and HMI
- This communication is facilitated through the use of:
  - Computer Systems
  - RTUs
  - TCP/IP Stack
  - Interaction with other protocol layers

Industry Communication Protocols

Distributed Network Protocol (DNP3)

- **DNP3** (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems.
- Its main use is in utilities such as electric and water companies. Usage in other industries is not common.
- It was developed for communications between various types of data acquisition and control equipment.
- It plays a crucial role in SCADA systems
- Used where RTUs, and Intelligent Electronic Devices (IEDs) reside.
- It is primarily used for communications between a master station and RTUs or IEDs.
- DNP3 maintains connection with telephone wire, fiber, Ethernet cable, and radio.

DNP3 Cont..

- DNP3 typically uses the TCP/IP protocol stack for communication

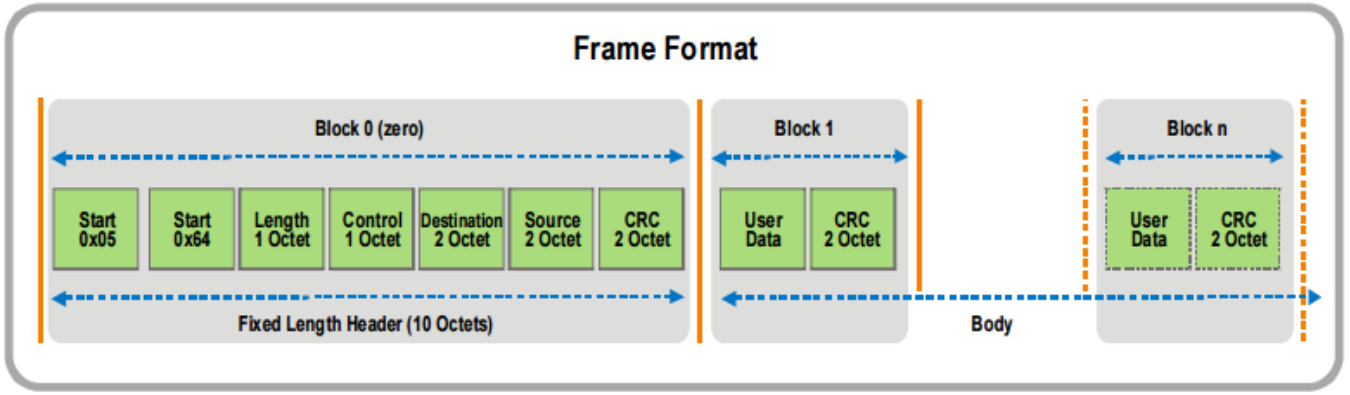


Figure 3 FT3 frame format

START	2 starting octets of the header (0x0564).
LENGTH	1 octet count of USER DATA in the header and body. This count includes the CONTROL, DESTINATION and SOURCE fields in the header however the CRC and other fields are not included in the count. The minimum value for LENGTH is 5, indicating only the header is present and the maximum value is 255.
CONTROL	Frame control octet.
DESTINATION	2 octet destination address. The first octet is the LSB and the second octet is the MSB.
SOURCE	2 octet source address. The first octet is the LSB and the second octet is the MSB.
CRC	2 octet Cyclic Redundancy Check.
USER DATA	Each block following the header has 16 octets of User defined data except the last block of a frame which contains 1 to 16 octets of User defined data as needed.

Open Platform Communications (OPC) Unified Architecture

- **OPC UA** is a series of standards and specifications for secure and reliable industrial telecommunication.
- An industrial automation industry task force developed the original standard in 1996 under the name **OLE for Process Control** (Object Linking and Embedding for Process Control).
- **OPC** specifies the communication of real-time plant data between control devices from different manufacturers. Hence, Unified Architecture
- Specifically used in windows-based platforms and HMI but now is used in Java and Linux
- Best used in a Web-based control system.

Profibus

- **PROFIBUS** (Process Field Bus) is a standard for fieldbus communication in automation technology first used by Siemens.
- Profibus uses a standard twisted-pair wiring system (RS485) or fiber optic cable.

Profibus Cont..

- **FMS**- Fieldbus Message Specification for PLC communication.
- **DP**- Decentralized Periphery, this new protocol is much simpler and faster.
- **FDL**-Field bus Data Link
- **MBP**- Manchester-Coded Power Bus- permits transmission of both data and power

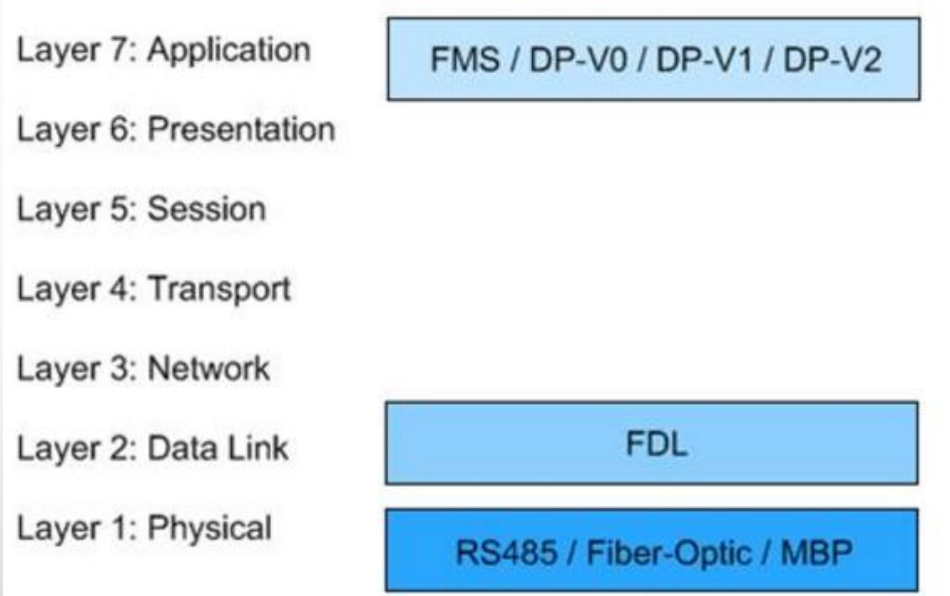
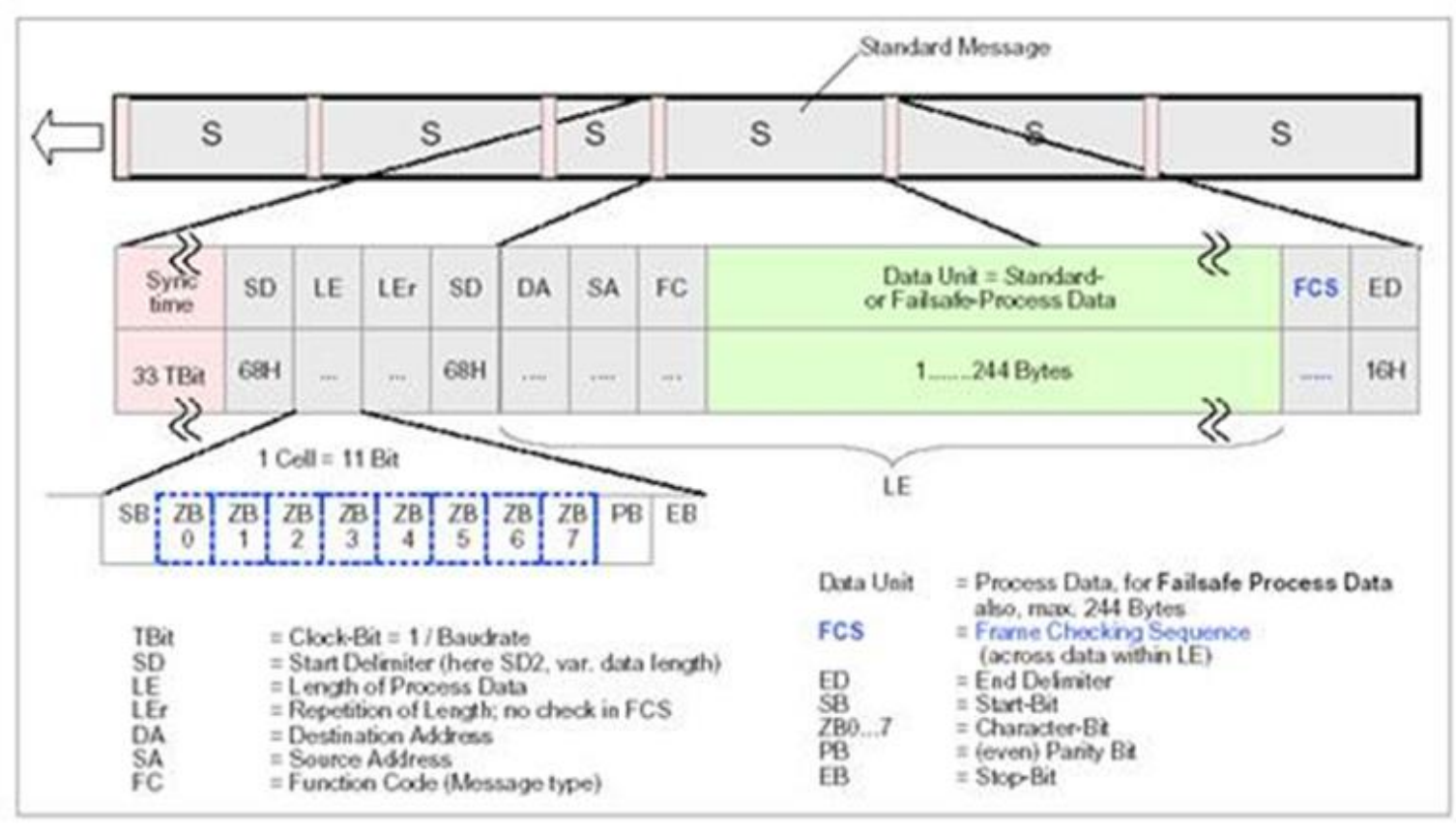


Figure 1 – PROFIBUS OSI Model

Profibus Frame Structure



EtherNet/Industrial Protocol

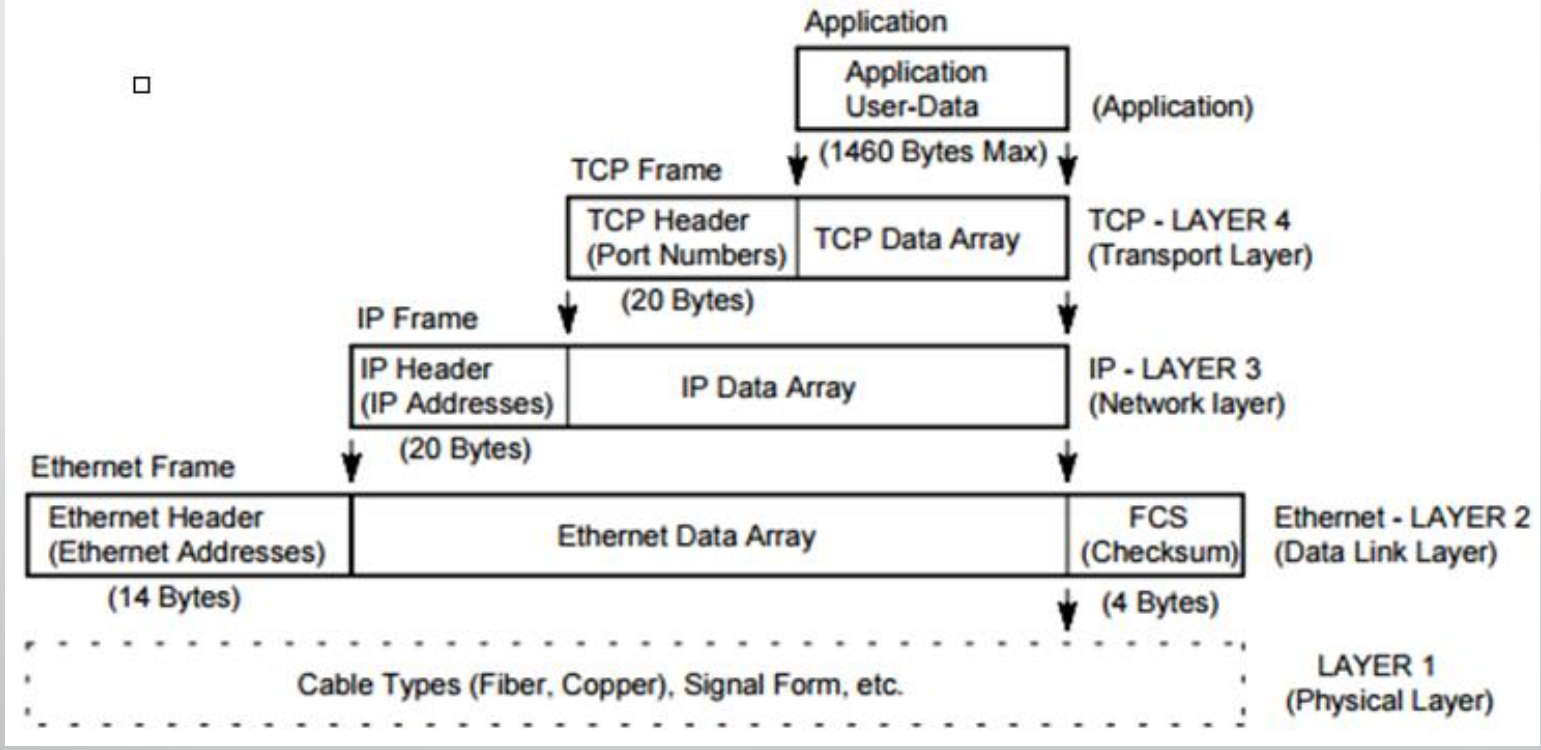
- Combines standard **Ethernet** with **Common Industrial Protocol** (CIP)
- The **Common Industrial Protocol** (CIP) is an industrial protocol for industrial automation applications
- Widely used in a range of industries
- CIP is capable of operations that provide three required services:
  - Control of Industrial Devices
  - Configuration of Devices
  - Collection of Real-Time Data

EtherNet/IP Communication Stack

- CIP provides for utilization of the top three layers of the OSI Model
- Standard Ethernet practices on the network of choice utilize the last three layers of the OSI Model

ETHERNET/IP COMMUNICATION STACK				
#	MODEL	IMPORTANT PROTOCOLS		Reference
7	Application	CIP™ (Control & Information Protocol)		EN 50170 IEC 61158
6	Presentation			
5	Session			
4	Transport	UDP	TCP	
3	Network	IP, ARP, RARP		
2	Data Link	Ethernet, CSMA/CD, MAC		IEEE 802.3 Ethernet
1	Physical	Ethernet Physical Layer		

EtherNet/IP Frame Structure

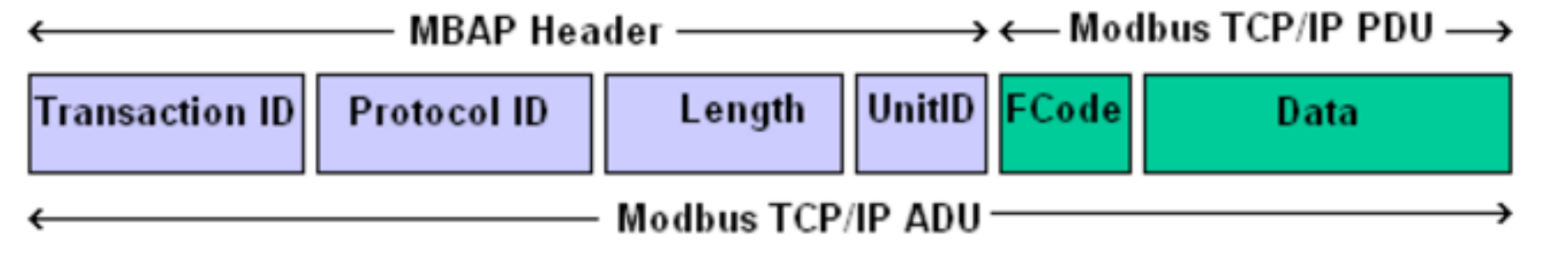


Modbus

- Original protocol used to communicate between Modicon devices.
- Modbus is a popular communication protocol in various industrial control settings.
- **Mo**dular **Di**gital **Con**troller was the name given to the first commercial Programmable Logic Controller built in 1969
- Two basic versions of Modbus include:
  - Modbus RTU- Open serial communication (RS-232 or RS-485)
  - Modbus/TCP- Ethernet attachment to control devices
- In Modbus/TCP, RTU messages are transmitted in a TCP/IP packet and sent over a network instead of serial lines.

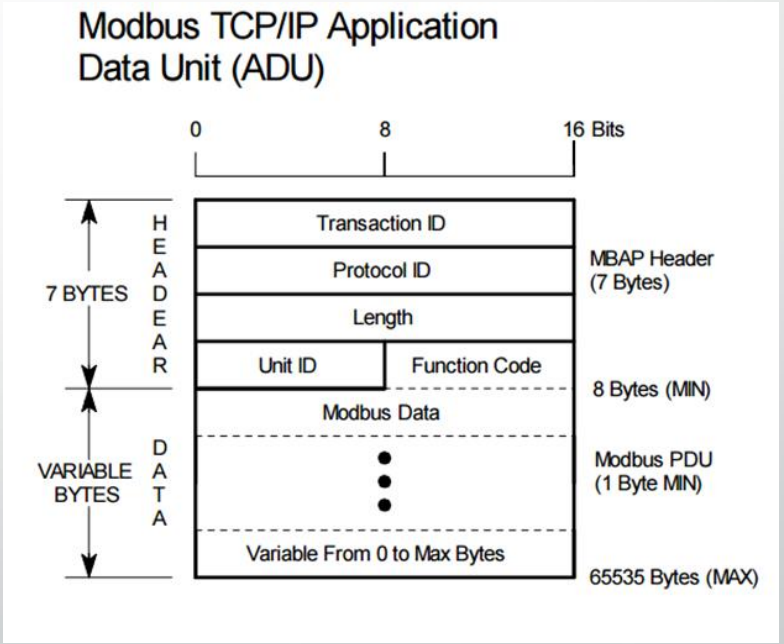
Modbus Frame Format

MBAP- Modbus Application Header

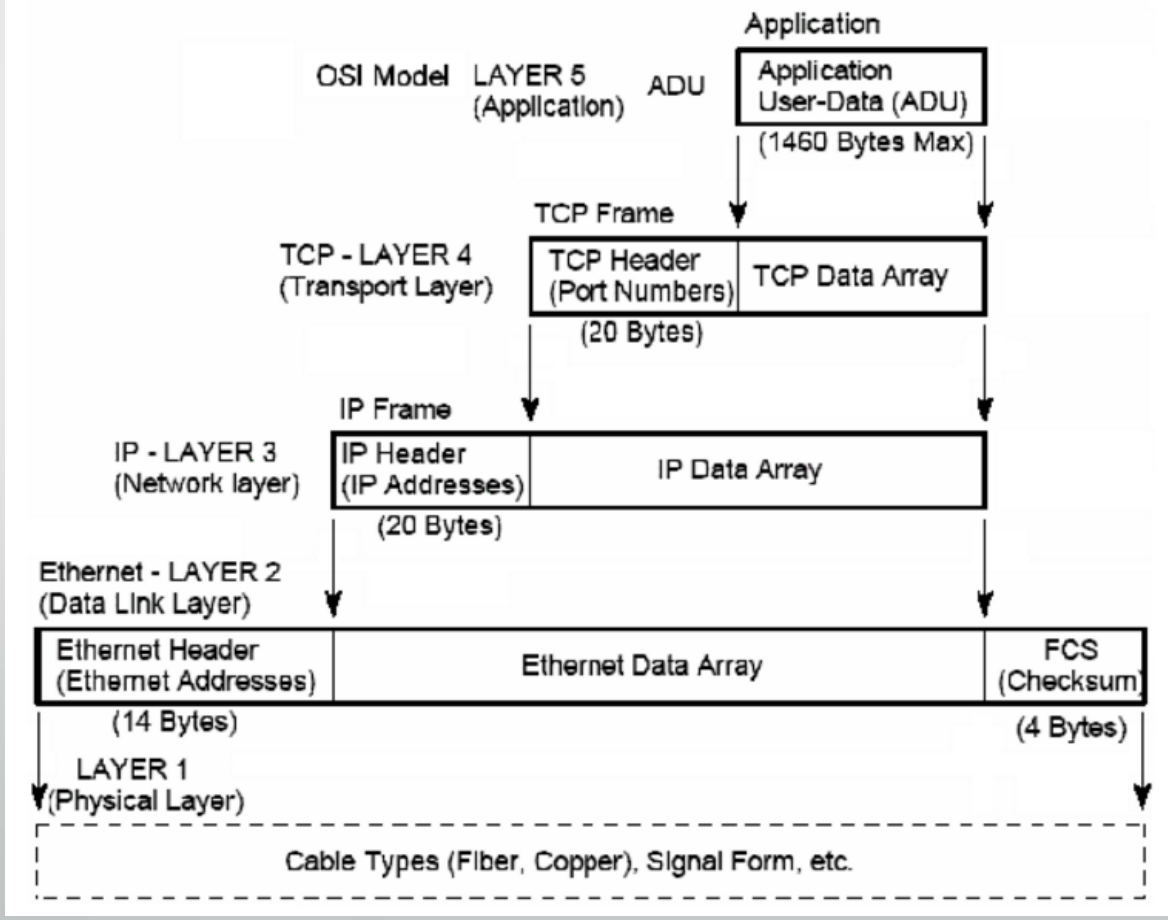


Modbus Packet Fields

Fields	Length	Description -	Client	Server
Transaction Identifier	2 Bytes	Identification of a MODBUS Request / Response transaction.	Initialized by the client	Recopied by the server from the received request
Protocol Identifier	2 Bytes	0 = MODBUS protocol	Initialized by the client	Recopied by the server from the received request
Length	2 Bytes	Number of following bytes	Initialized by the client (request)	Initialized by the server (Response)
Unit Identifier	1 Byte	Identification of a remote slave connected on a serial line or on other buses.	Initialized by the client	Recopied by the server from the received request



Modbus/TCP- Data Packet




JSU
JACKSONVILLE STATE UNIVERSITY

Gadsden State Community College
1898

NSF

Questions??