Critical Infrastructure Security

Lecture 5

Dr. Naveed Anwar Bhatti

Webpage: naveedanwarbhatti.github.io

Information Technology Attacks

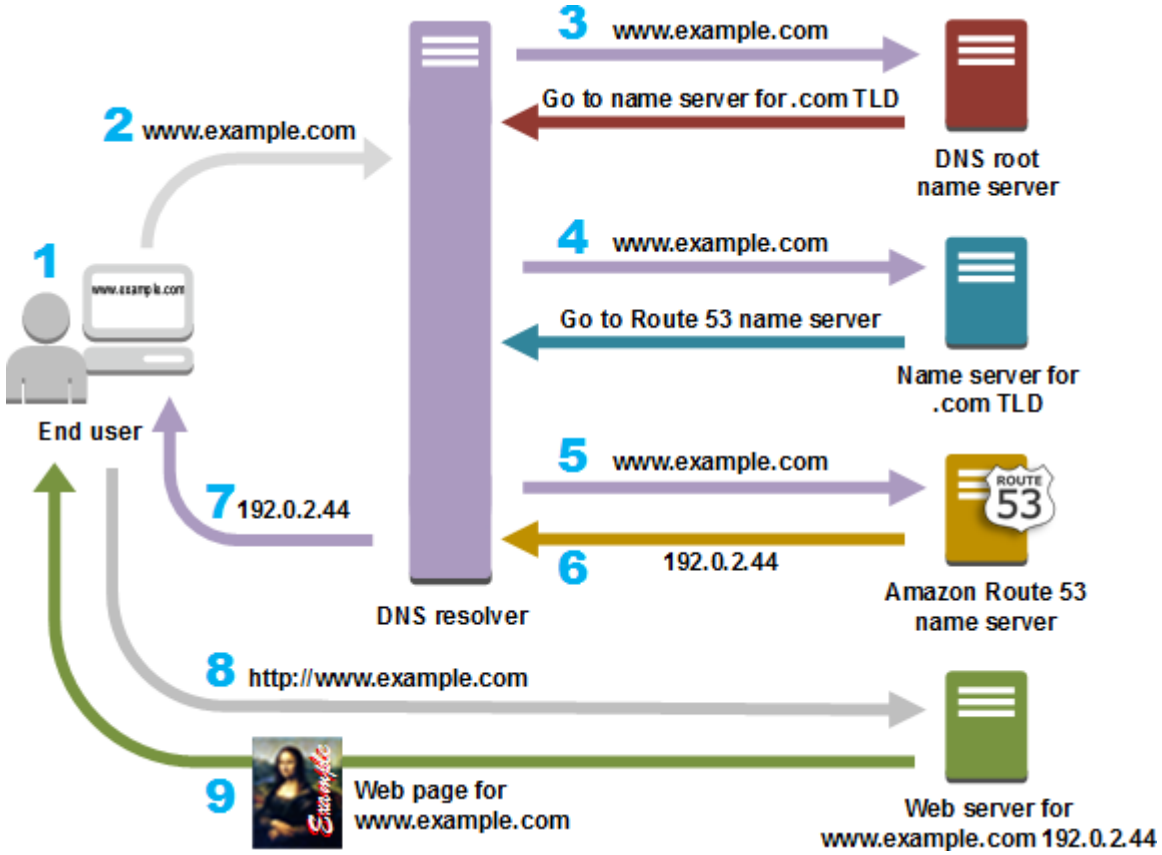
+ Critical Infrastructure Security Attacks

Attacks on different Layers

- **Application Layer Attacks**
  - Virus/Worm
  - Password Attack
  - Information Sniffing
  - DNS Attack
  - SNMP (Simple Network Management Protocol) Attack
  - FTP Bounce Attack
  - Operating System and Application Weakness

DNS Protocol

- **Step 1:** Request information
- **Step 2:** Ask the recursive DNS servers
- **Step 3:** Ask the root name servers
- **Step 4:** Ask the TLD (Top-Level Domain) name servers
- **Step 5:** Ask the authoritative DNS servers
- **Step 6:** Retrieve the record
- **Step 7:** Receive the answer



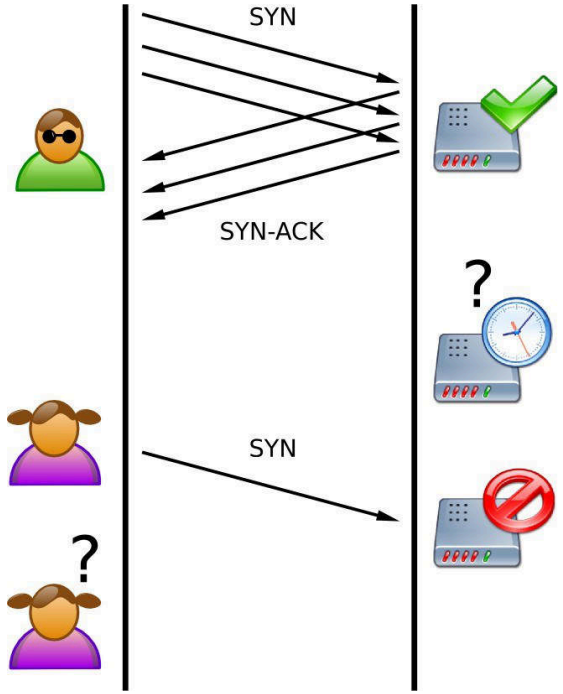
https://aws.amazon.com/route53/what-is-dns/

DNS Attacks

- A DNS attack is an exploit in which an attacker takes advantage of vulnerabilities in the domain name system (DNS).
  - **Cache Poising:** the attacker corrupts a DNS server by replacing a legitimate IP address in the server's cache with that of another, rogue address in order to redirect traffic to a malicious website.
  - **DNS Amplification:** the attacker takes advantage of a DNS server that permits recursive lookups and uses recursion to spread his attack to other DNS servers
  - **Fast-flux DNS:** Quickly associating multiple IP addresses with same domain
  - **DDOS**

Attacks on OSI Layers

- **Transport Layer Attacks**
  - **SYN Attack**
    - It is also DOS attack. It depends on three way hand shake.
    - A SYN flood attack works by not responding to the server with the expected
  - **SSL Man-in-the-Middle Attacks**
  - **Land Attack**
    - It is a Layer 4 Denial of Service (DoS) **attack** in which, the attacker sets the source and destination information of a TCP segment to be the same.
  - **UDP Flood Attack**
  - **Port Scan Attack**



Attacks on OSI Layers

- **Network Layer Attack**
  - IP Spoofing
    - Create IP packet with false IP address.
    - Packet crafting is not an easy task. It involve Packet assemble, Packet editing, Packet Replay, and Packet Decoding
  - Routing Attacks
  - ICMP (Internet Control Message Protocol) Attacks
    - PING Flood (ICMP Flood)
  - Ping of Death Attack
    - Send large size malformed ping packet. Normal size is 56 to 64 bytes.
  - Teardrop Attack
    - It is DoS attack which involves sending fragmented packets to a target machine which fails to reassemble.

Attacks on different Layers

- **Data Link Layer Attacks**
  - **ARP Spoofing**
  - **DHCP Attack**
  - **Media Access Control (MAC) Address spoofing**
    - MAC spoofing is a technique for changing a factory-assigned Media Access Control address of a network interface on a networked device.

Non-malicious program errors

- **Buffer overflows**
  - Over-spilling the allocated capacity of the buffer (or when parameter values are passed into a routine on a Web server)
- **Incomplete mediation**
  - Passing incorrect data to a program to cause system failure
- **Time-of-check to time-of-use errors**
  - Mediation-type flaw with “bait and switch” - something is changed between the initial check and the actual use (i.e. Checks one action but actually performs another)
- **These three vulnerabilities can be used in conjunction with one another for a multi-step approach**

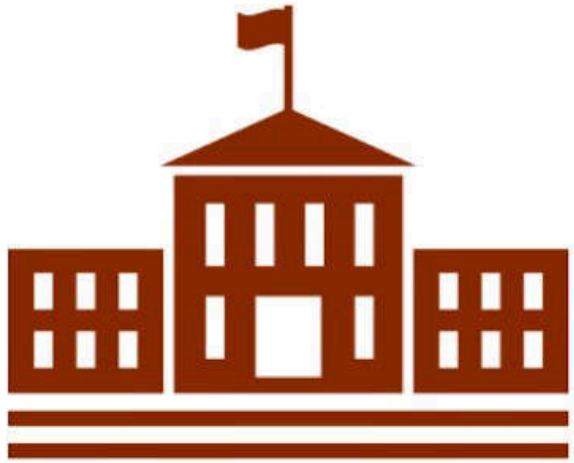
Industrial Network Design, Architecture and Protocols

Industrial Network

Industrial Network

any network that supports the interconnectivity of and communication between devices that make up or support an ICS.

Industrial Network



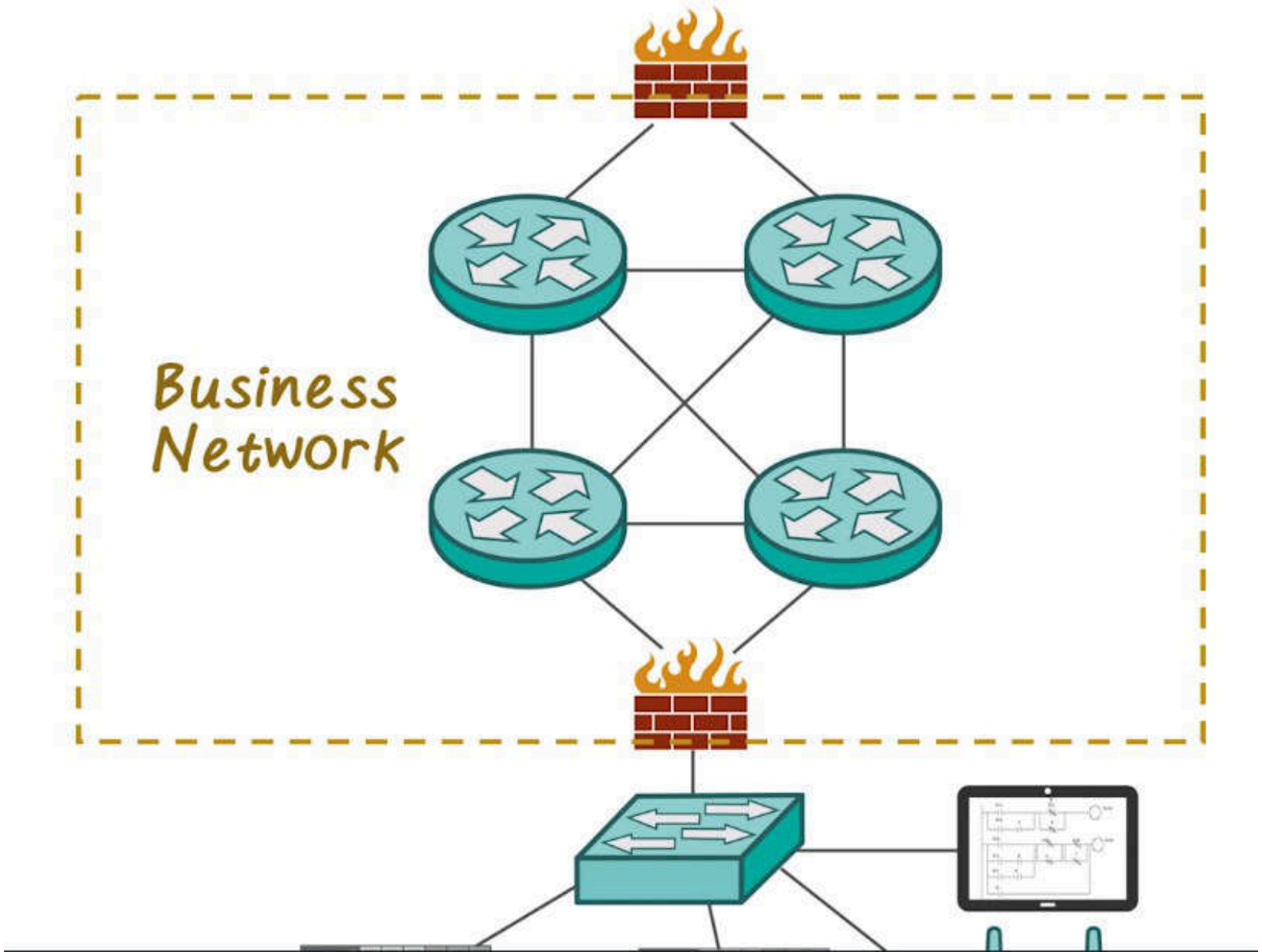
LAN

Local Area Network

WAN

Wide Area Network

Industrial Network



Industrial Network

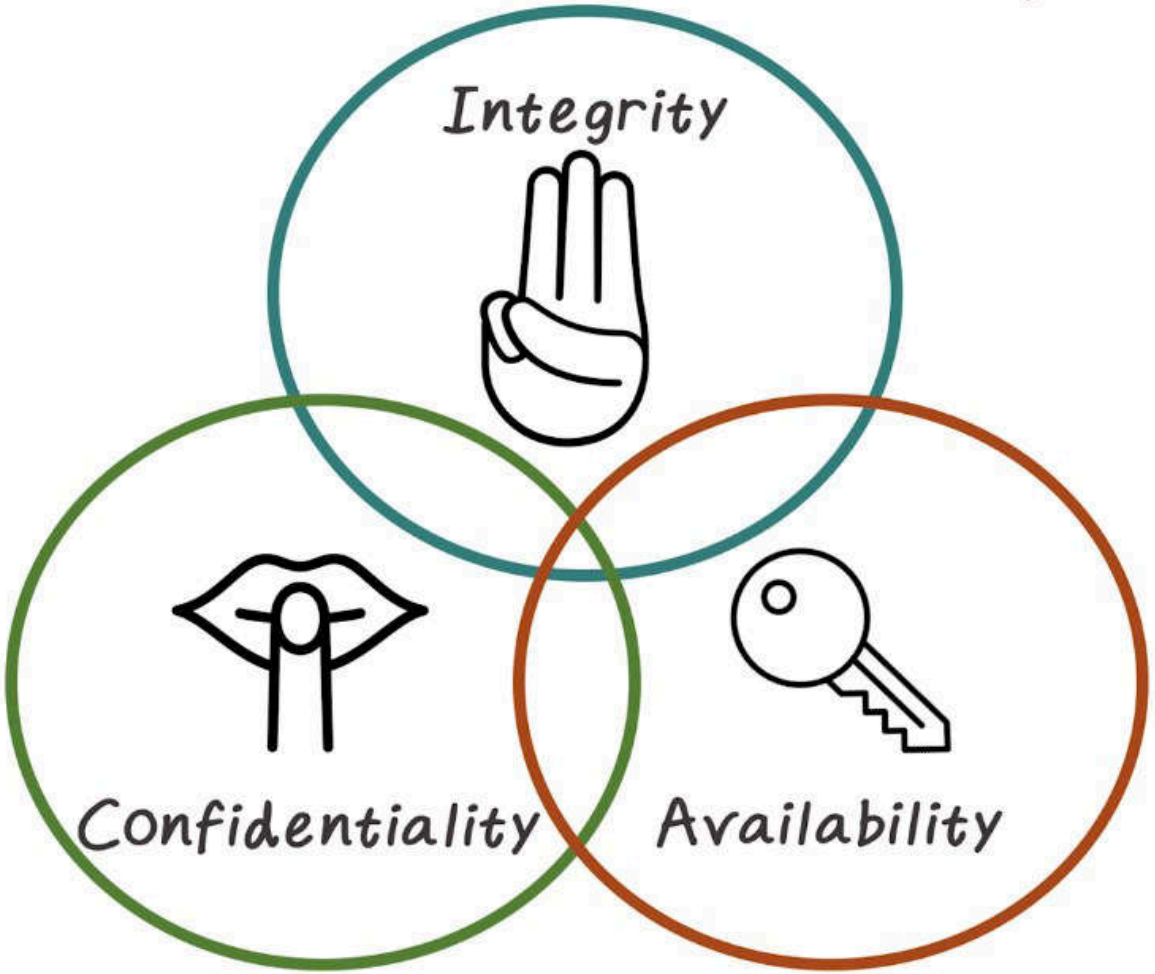
BUSINESS NETWORK

highly interconnected

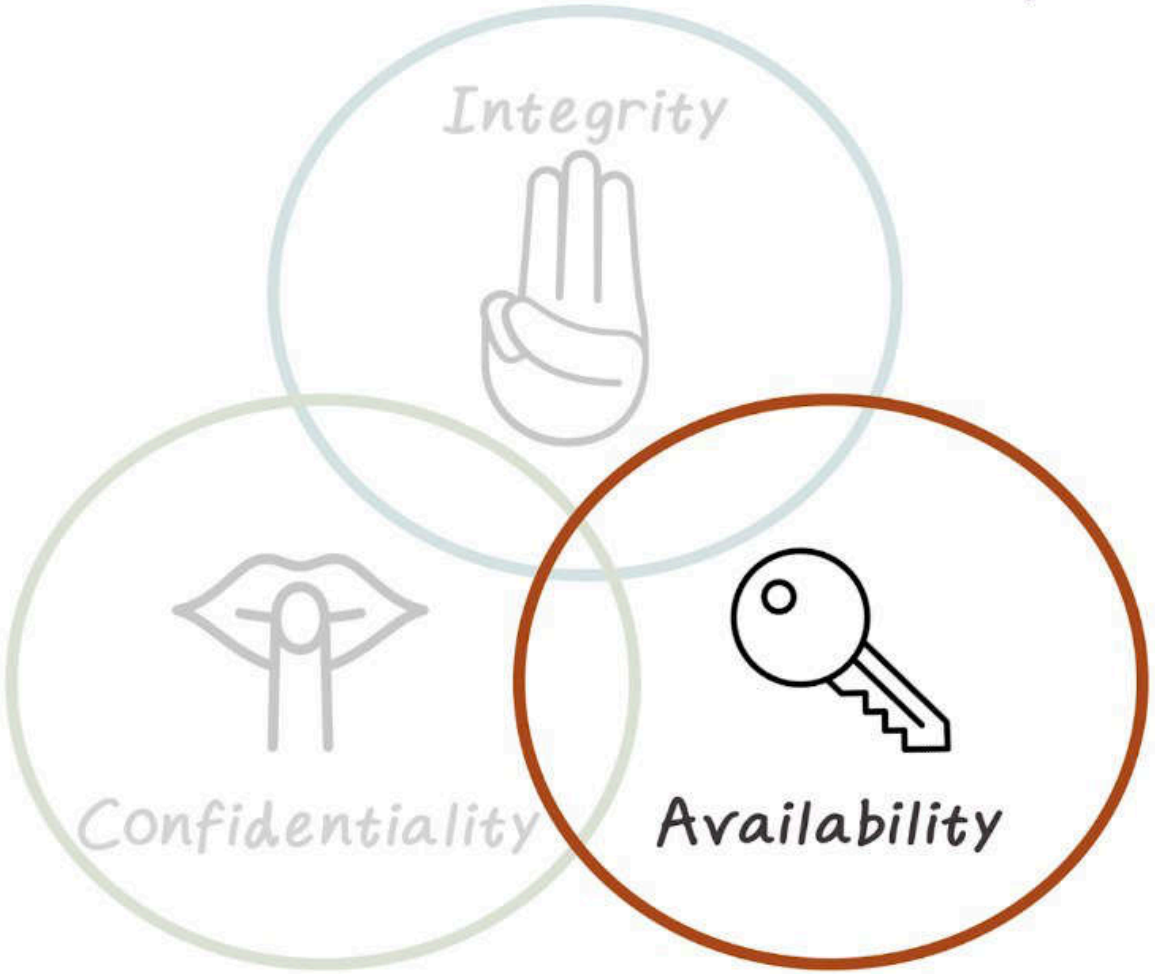
has various wireless connectivity options

extremely dynamic in nature

Industrial Network



Industrial Network



Industrial Network

Function	Industrial Network (control & process areas)	Industrial Network (supervisory areas)	Business Network
Real-time operation			
Reliability/ Resiliency			
Bandwidth			
Sessions			
Latency			
Network			
Protocols			

Industrial Network

Function	Industrial Network (control & process areas)	Industrial Network (supervisory areas)	Business Network
Real-time operation	Critical	High	Best effort
Reliability/ Resiliency			
Bandwidth			
Sessions			
Latency			
Network			
Protocols			

Industrial Network

Function	Industrial Network (control & process areas)	Industrial Network (supervisory areas)	Business Network
Real-time operation	Critical	High	Best effort
Reliability/ Resiliency	Critical	High	Best effort
Bandwidth			
Sessions			
Latency			
Network			
Protocols			

Industrial Network

Function	Industrial Network (control & process areas)	Industrial Network (supervisory areas)	Business Network
Real-time operation	Critical	High	Best effort
Reliability/ Resiliency	Critical	High	Best effort
Bandwidth	Low	Medium	High
Sessions			
Latency			
Network			
Protocols			

Industrial Network

Function	Industrial Network (control & process areas)	Industrial Network (supervisory areas)	Business Network
Real-time operation	Critical	High	Best effort
Reliability/ Resiliency	Critical	High	Best effort
Bandwidth	Low	Medium	High
Sessions	Few, explicitly defined	Few	Many
Latency			
Network			
Protocols			

Industrial Network

Function	Industrial Network (control & process areas)	Industrial Network (supervisory areas)	Business Network
Real-time operation	Critical	High	Best effort
Reliability/ Resiliency	Critical	High	Best effort
Bandwidth	Low	Medium	High
Sessions	Few, explicitly defined	Few	Many
Latency	Low, Consistent	Low, Consistent	N/A, retransmissions are acceptable
Network			
Protocols			

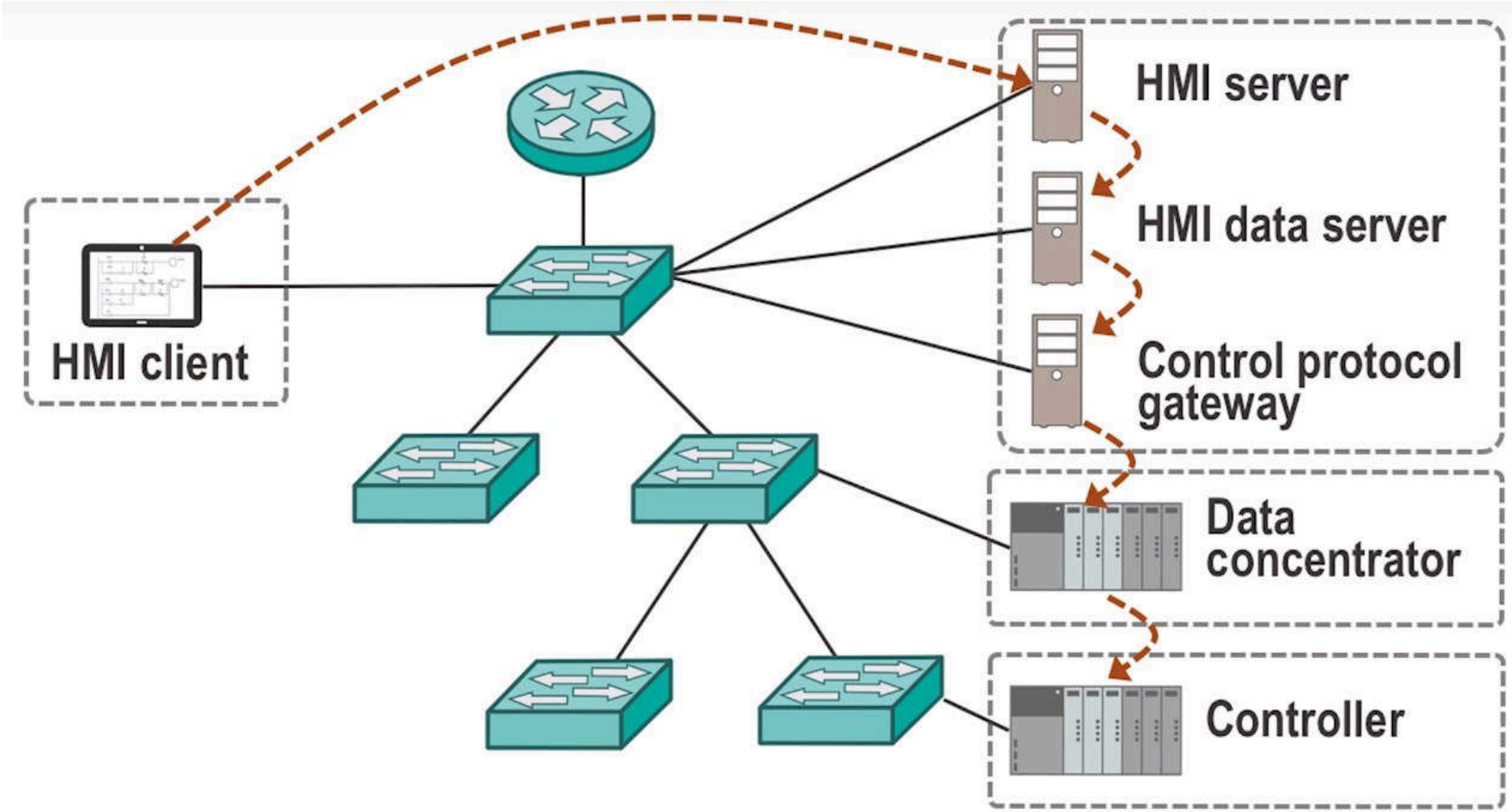
Industrial Network

Function	Industrial Network (control & process areas)	Industrial Network (supervisory areas)	Business Network
Real-time operation	Critical	High	Best effort
Reliability/ Resiliency	Critical	High	Best effort
Bandwidth	Low	Medium	High
Sessions	Few, explicitly defined	Few	Many
Latency	Low, Consistent	Low, Consistent	N/A, retransmissions are acceptable
Network	Serial, Ethernet	Ethernet	Ethernet
Protocols			

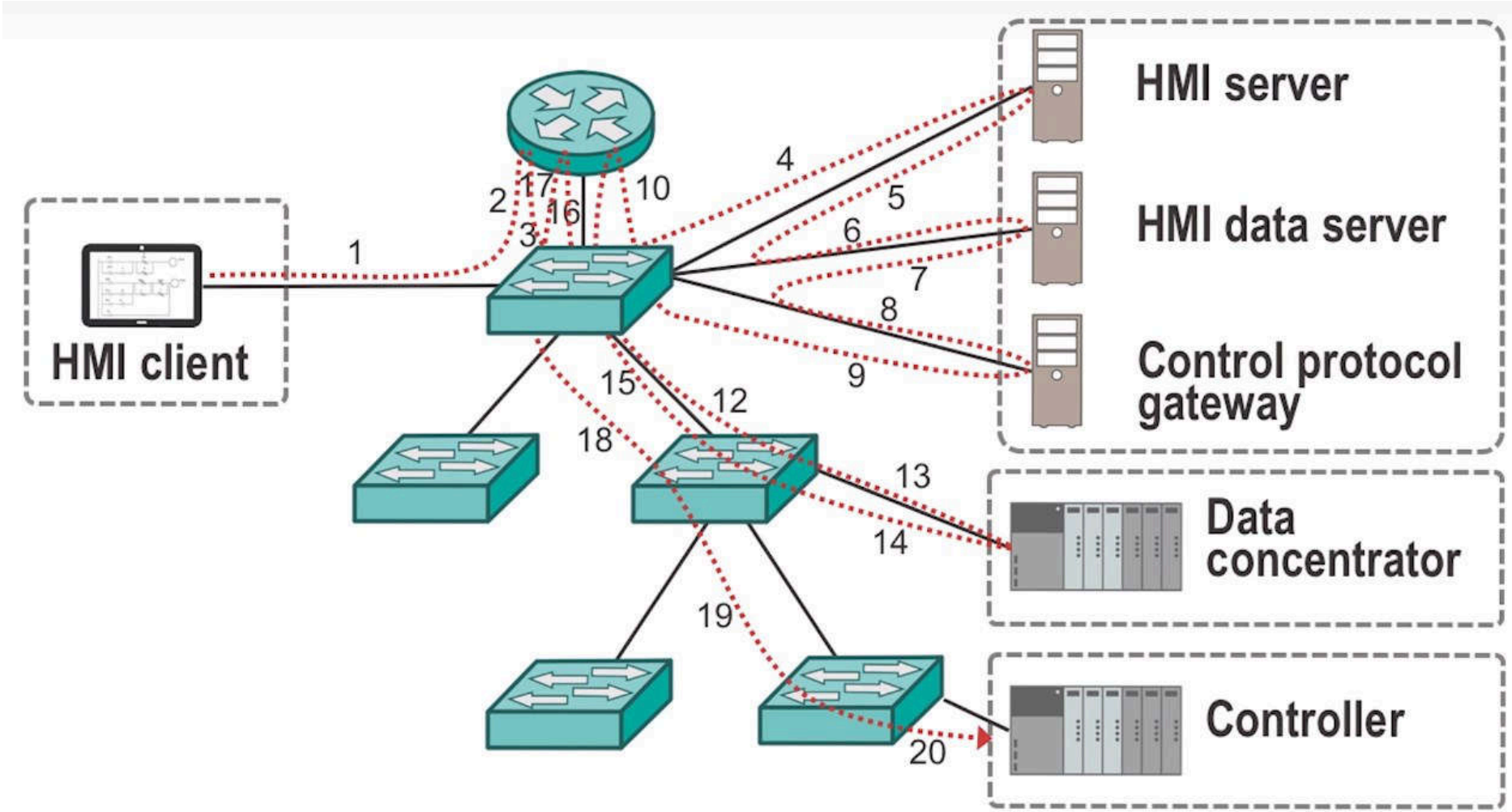
Industrial Network

Function	Industrial Network (control & process areas)	Industrial Network (supervisory areas)	Business Network
Real-time operation	Critical	High	Best effort
Reliability/ Resiliency	Critical	High	Best effort
Bandwidth	Low	Medium	High
Sessions	Few, explicitly defined	Few	Many
Latency	Low, Consistent	Low, Consistent	N/A, retransmissions are acceptable
Network	Serial, Ethernet	Ethernet	Ethernet
Protocols	Real-time, Proprietary	Never real-time, Open	Non real-time, Open

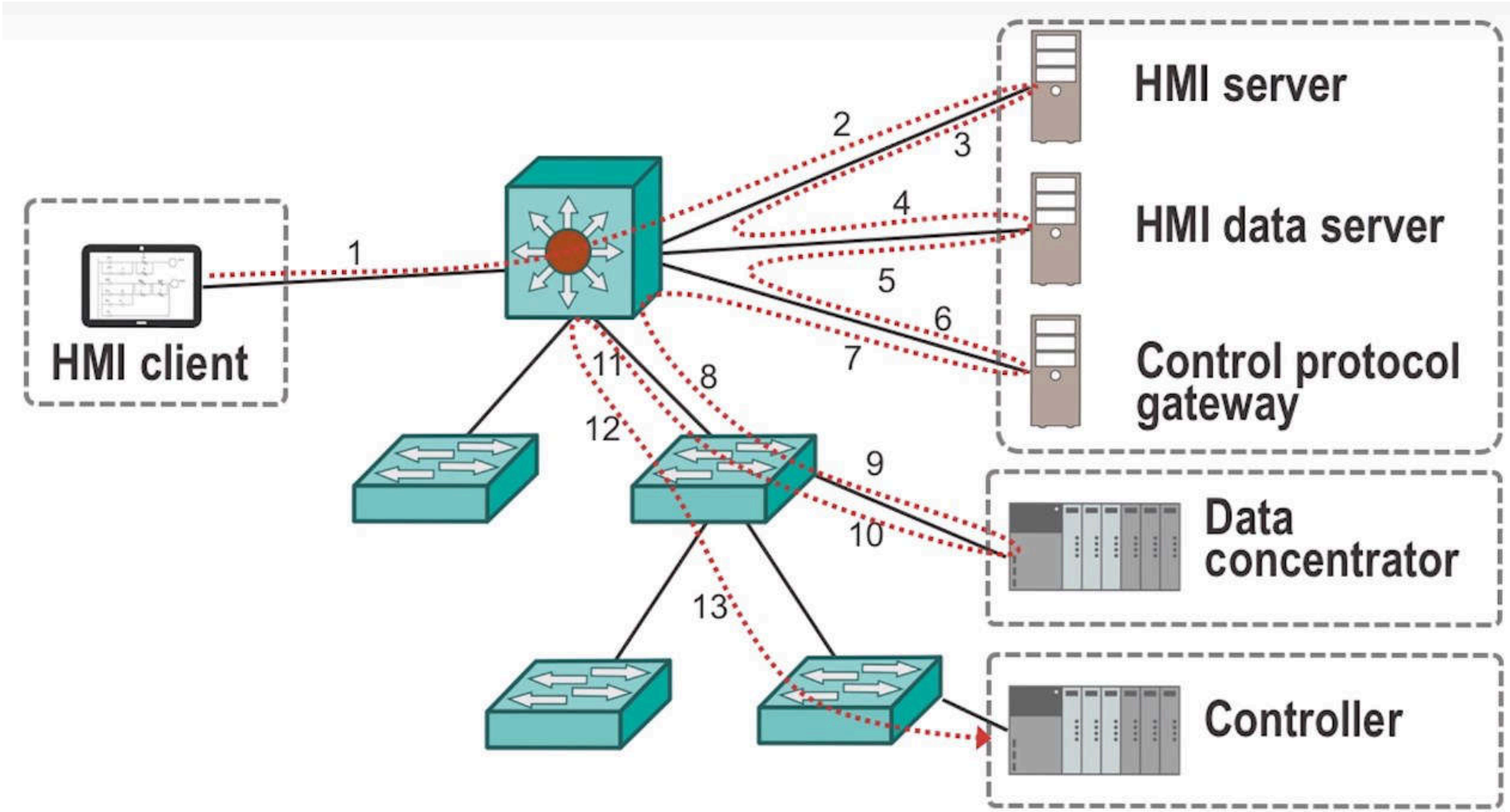
Industrial Network (Latency)



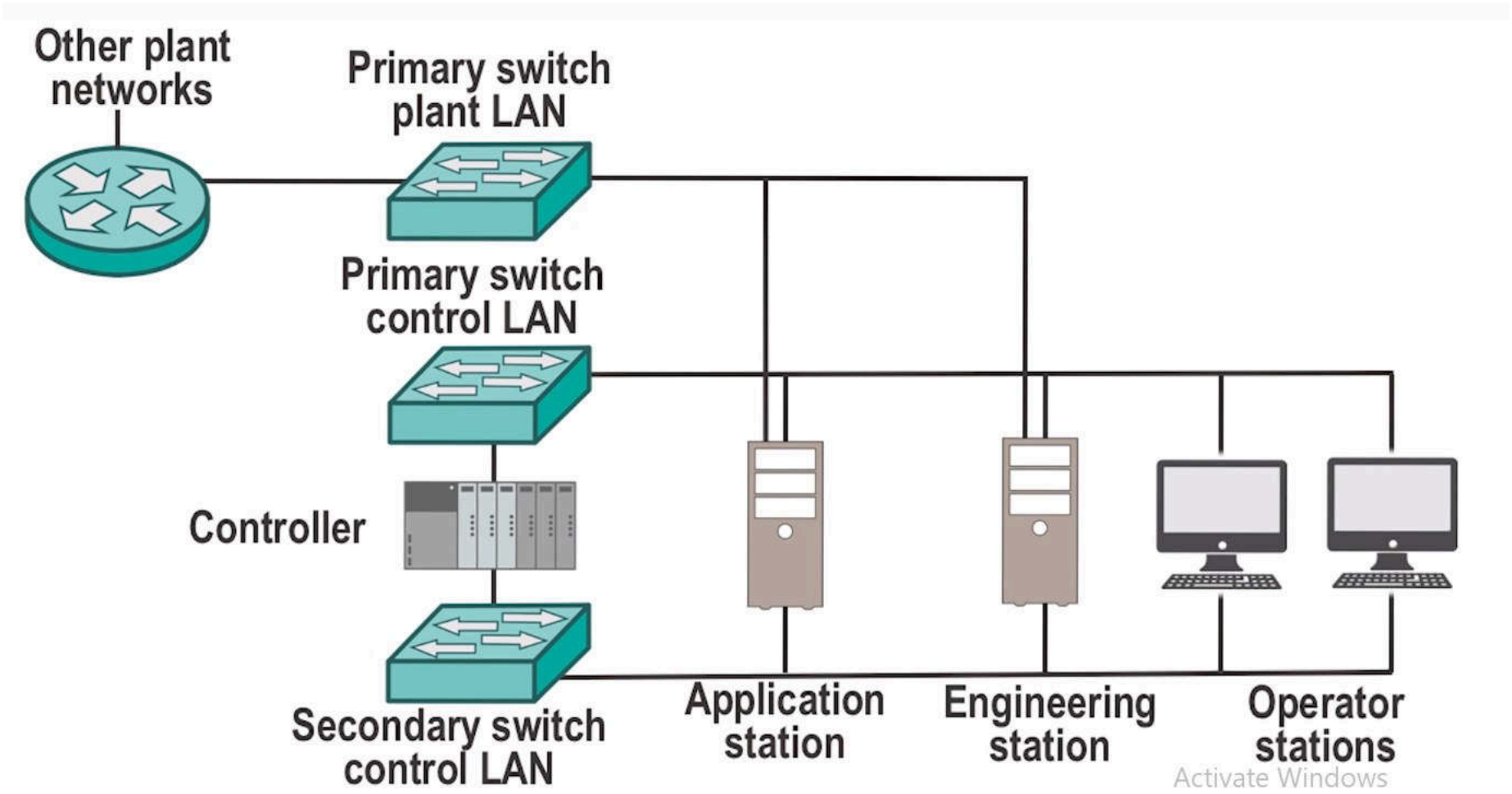
Industrial Network



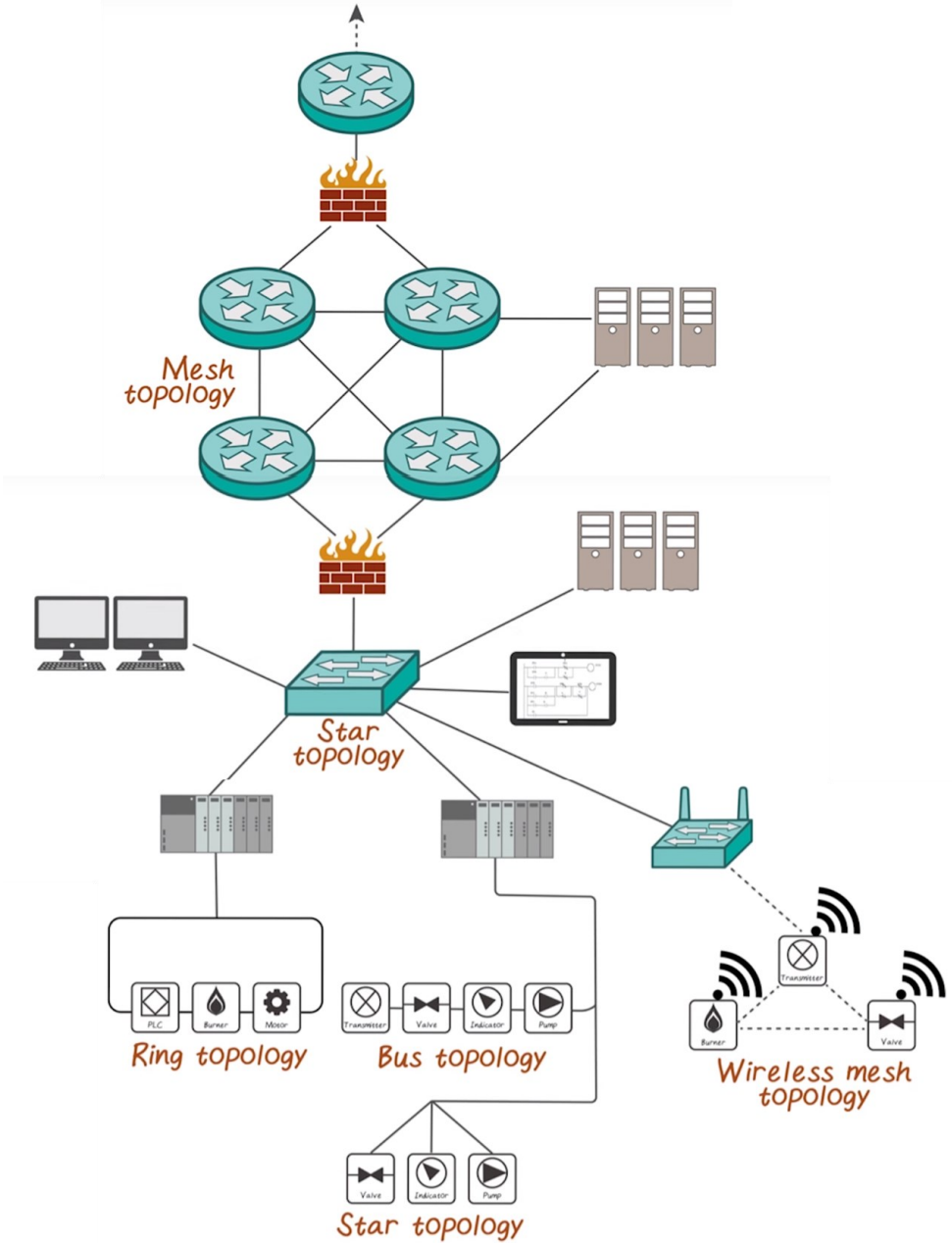
Industrial Network



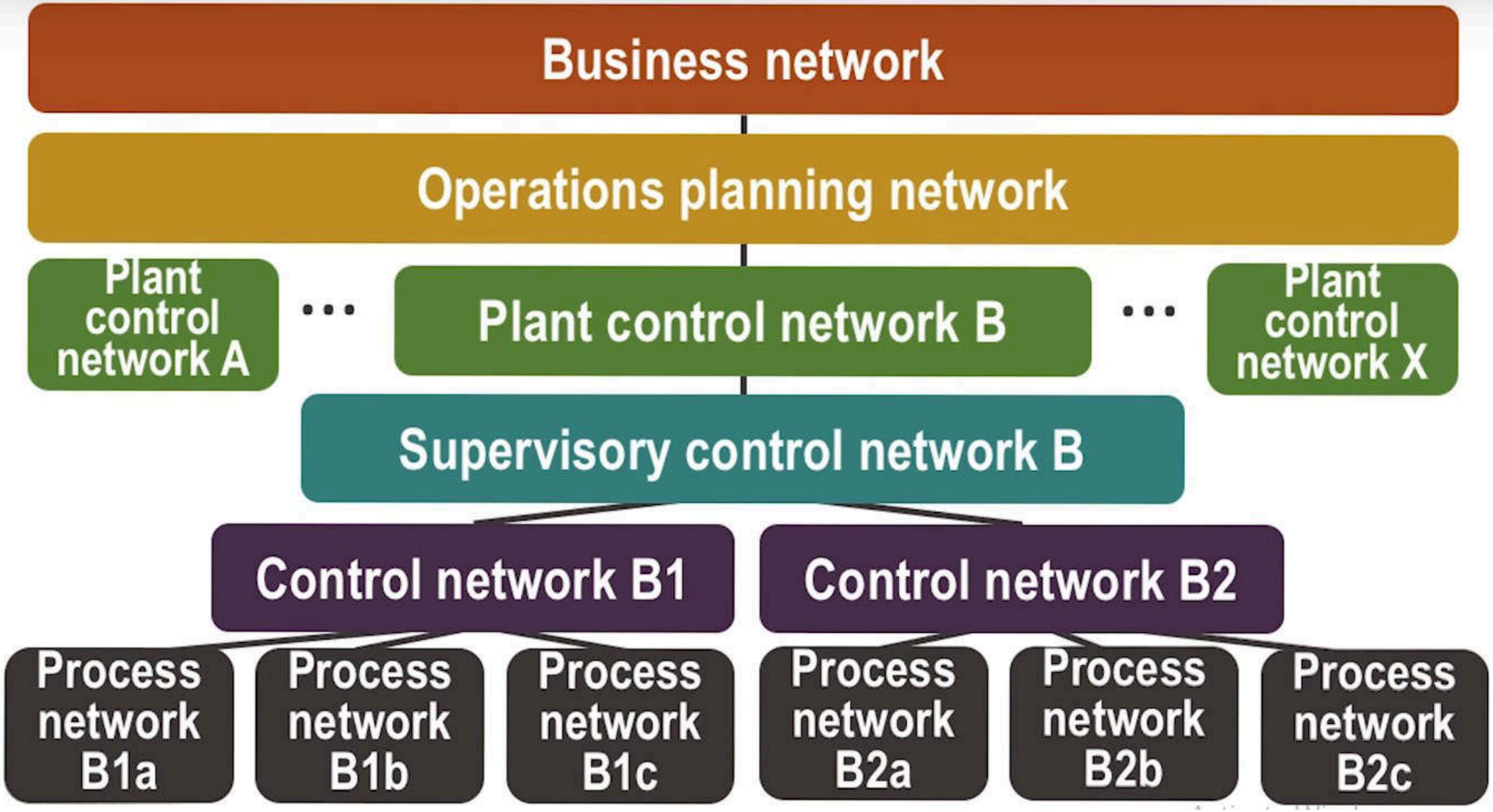
Redundancy



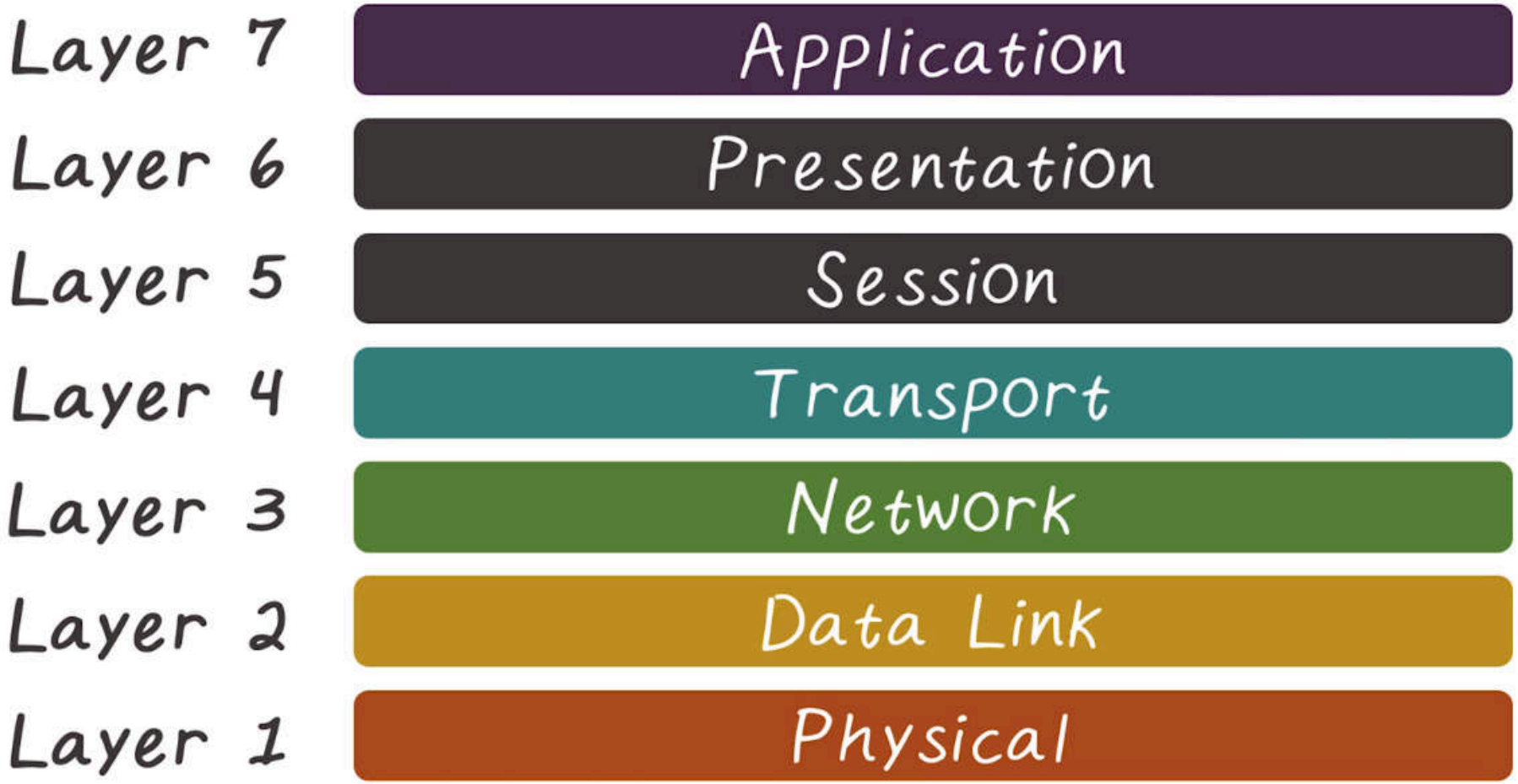
Network Topologies



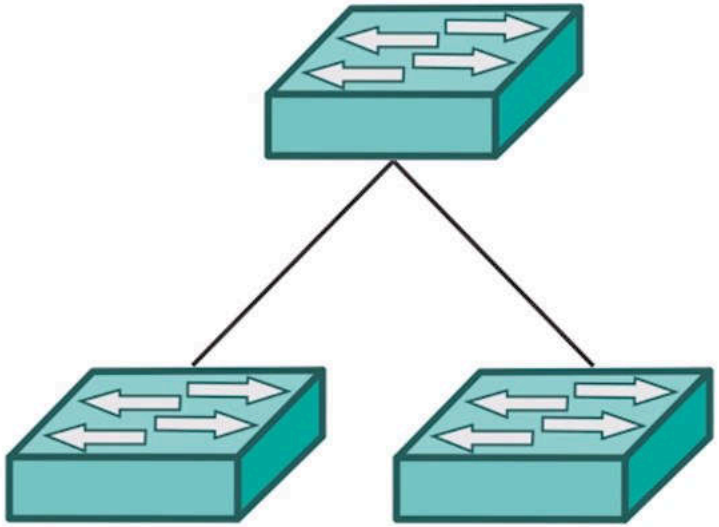
Network Segmentation

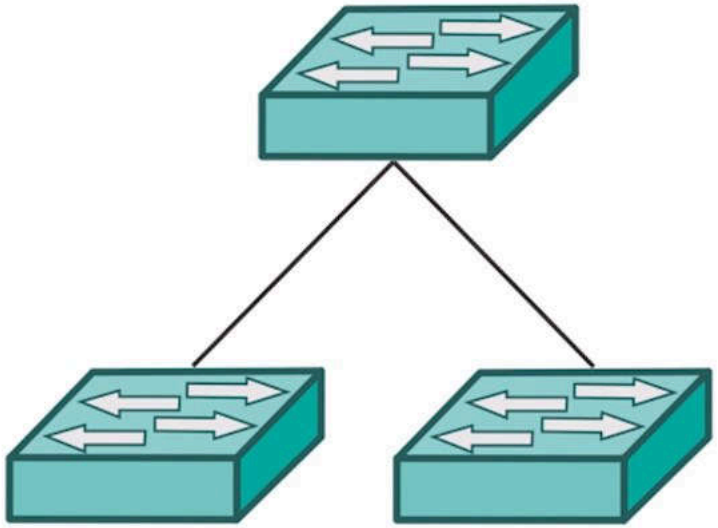


Higher Layer Segmentation

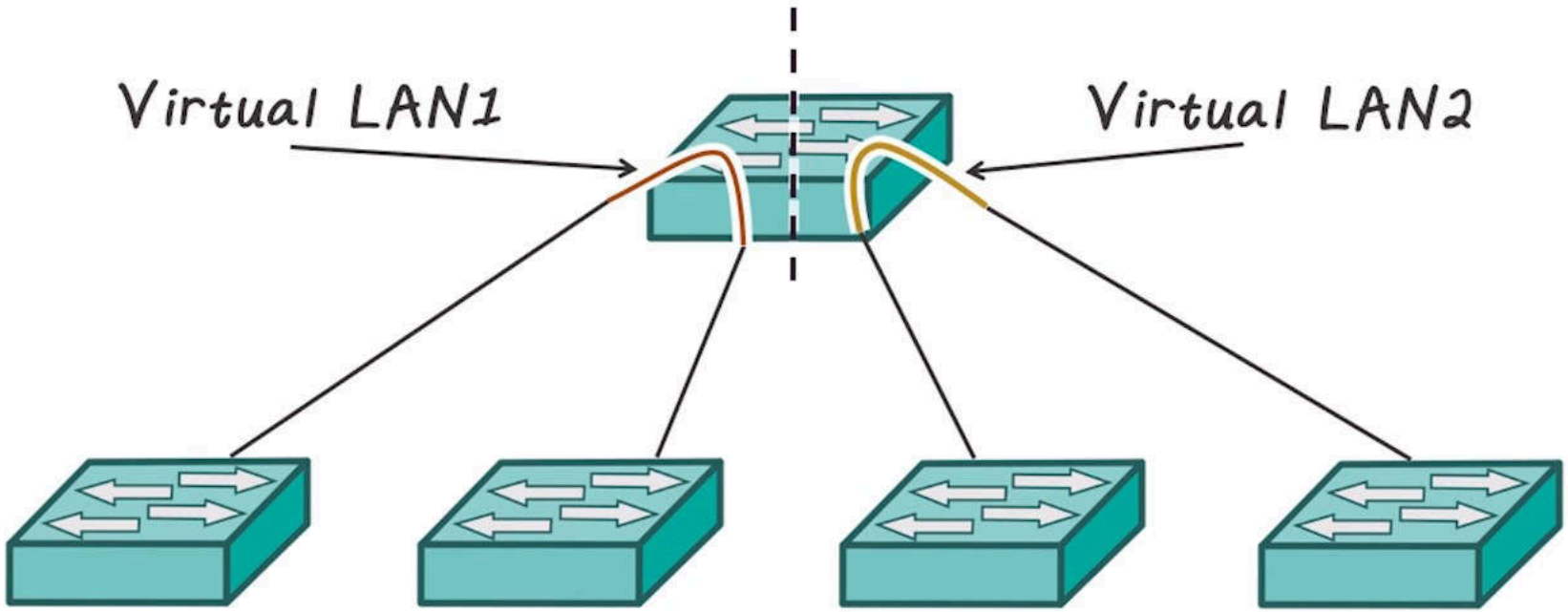


Physical vs. Logical Segmentation



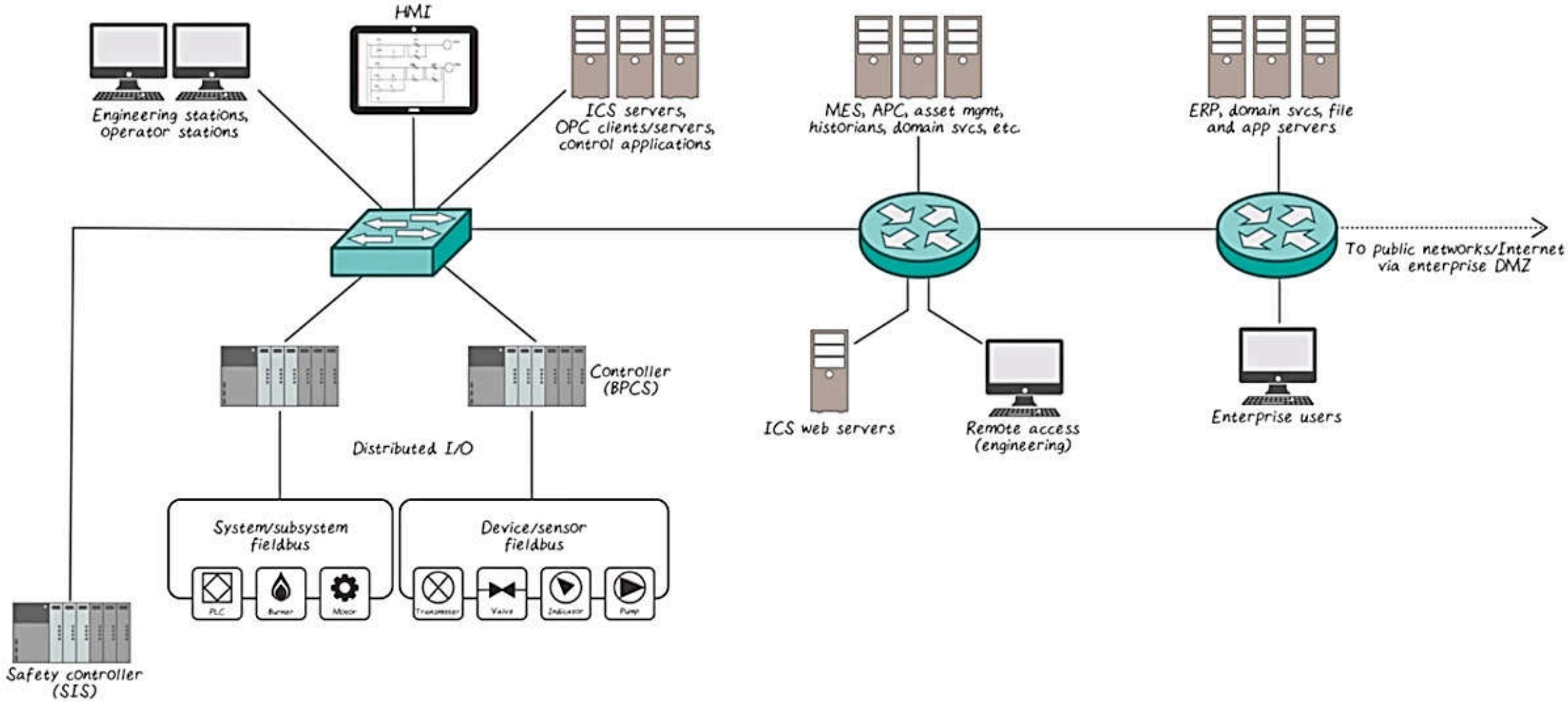


Physical vs. Logical Segmentation

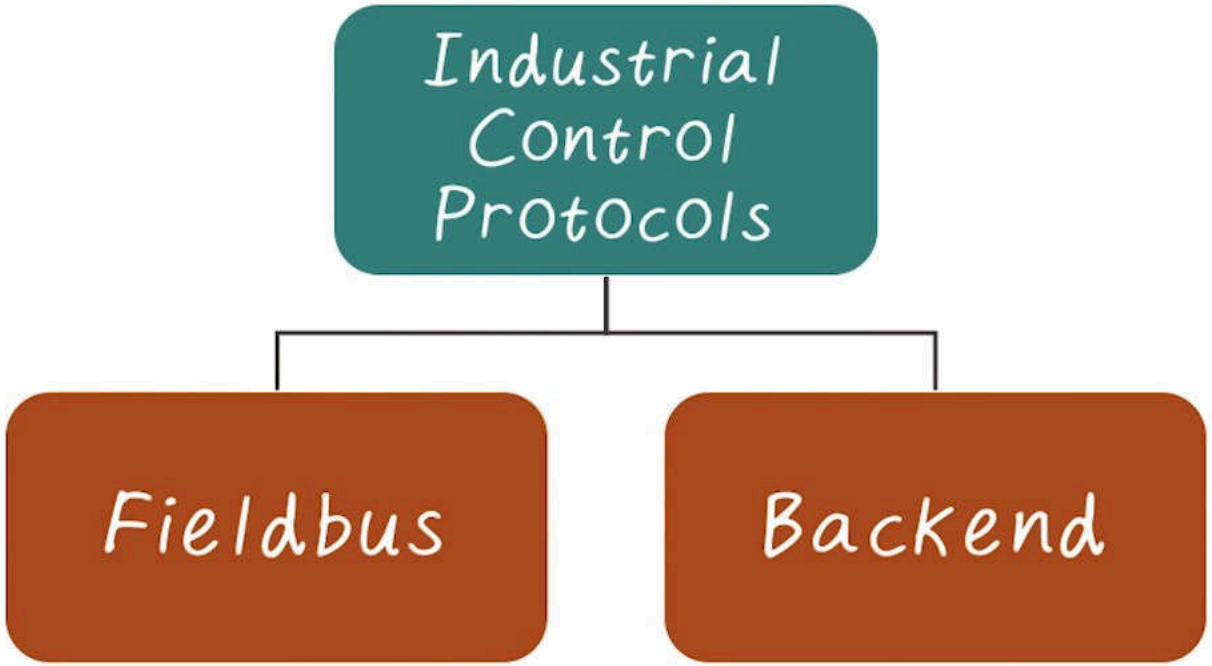


Now Comes Protocols

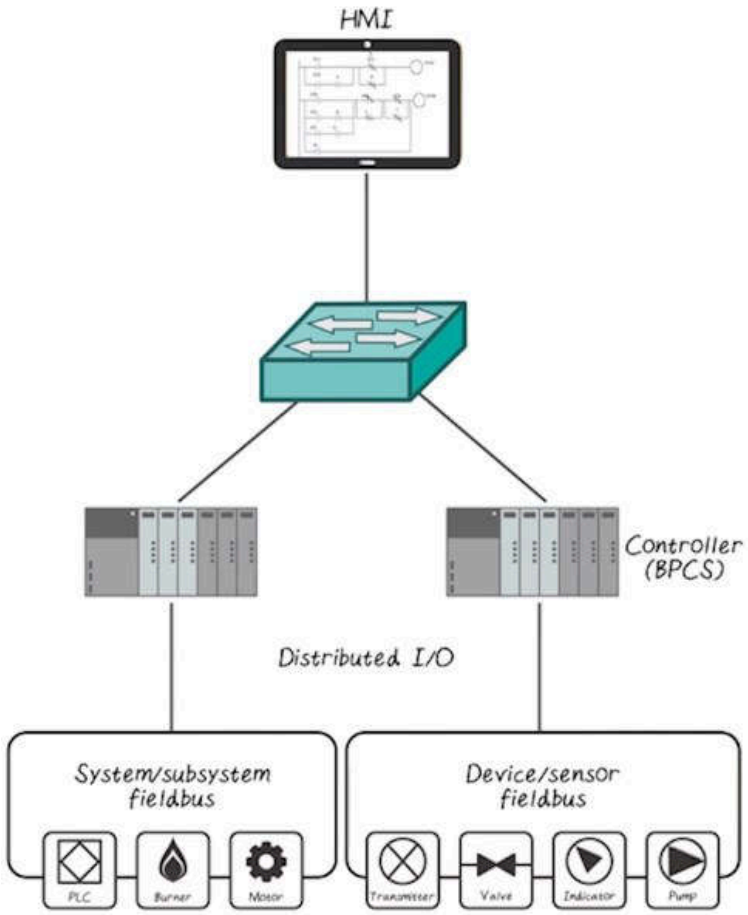
Protocol Overview

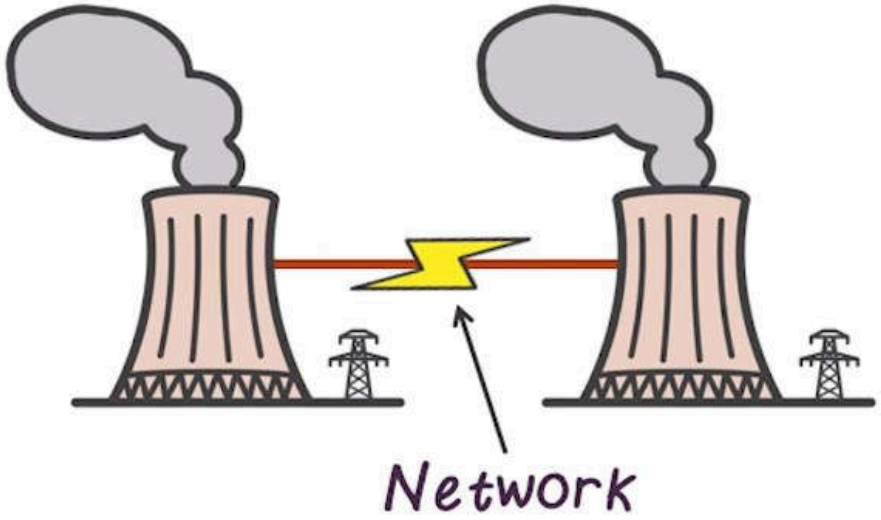


Protocol Overview

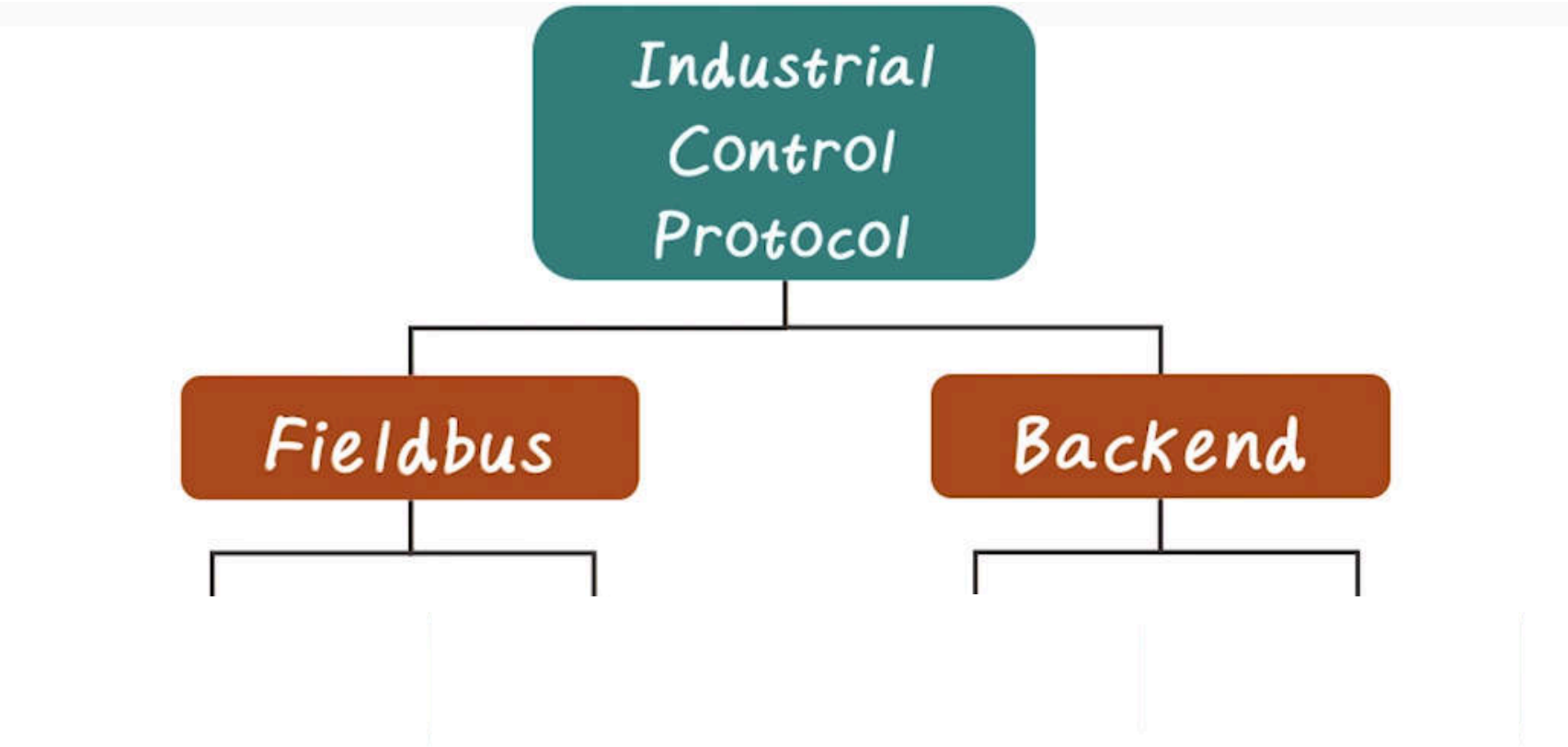


FieldBus vs Backend Protocols

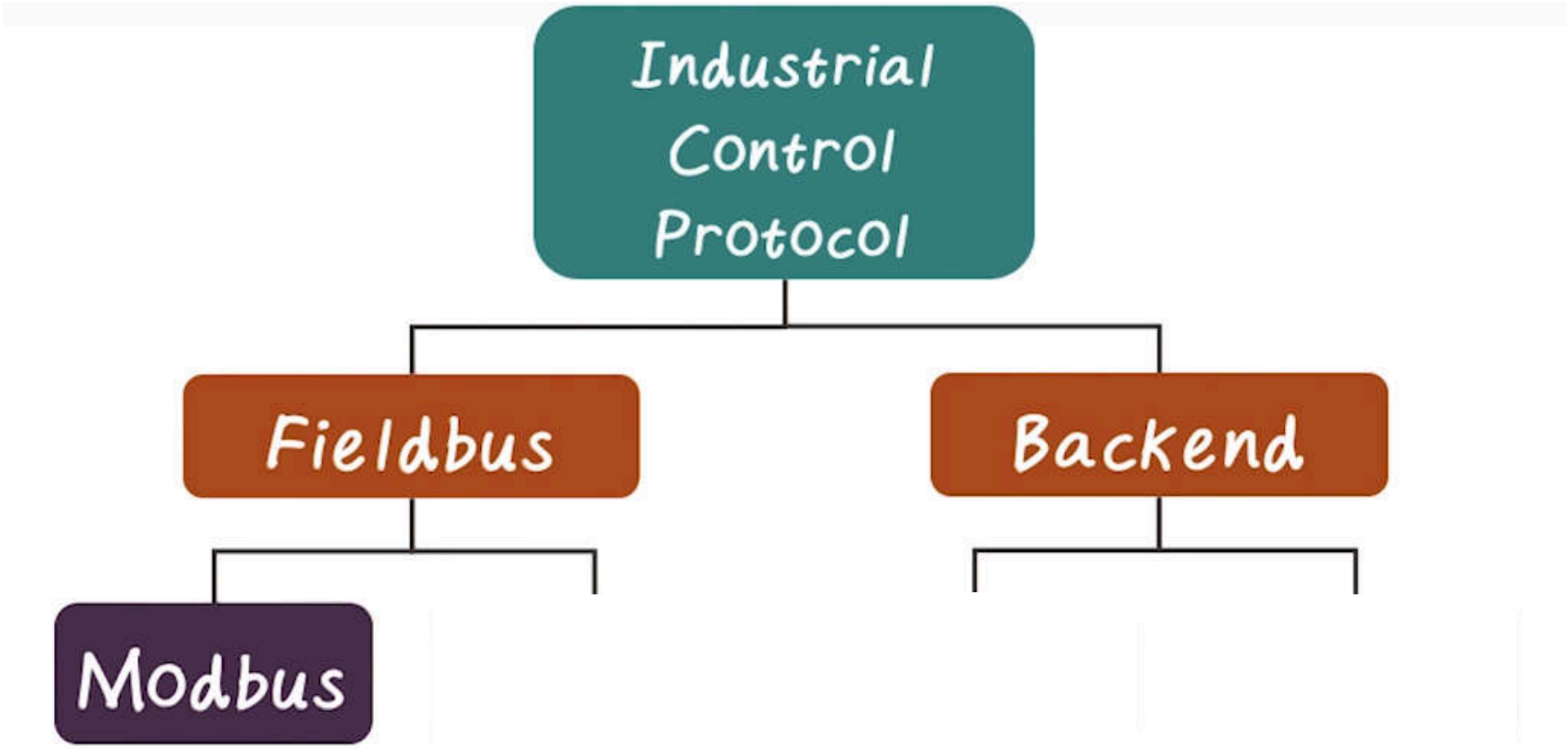




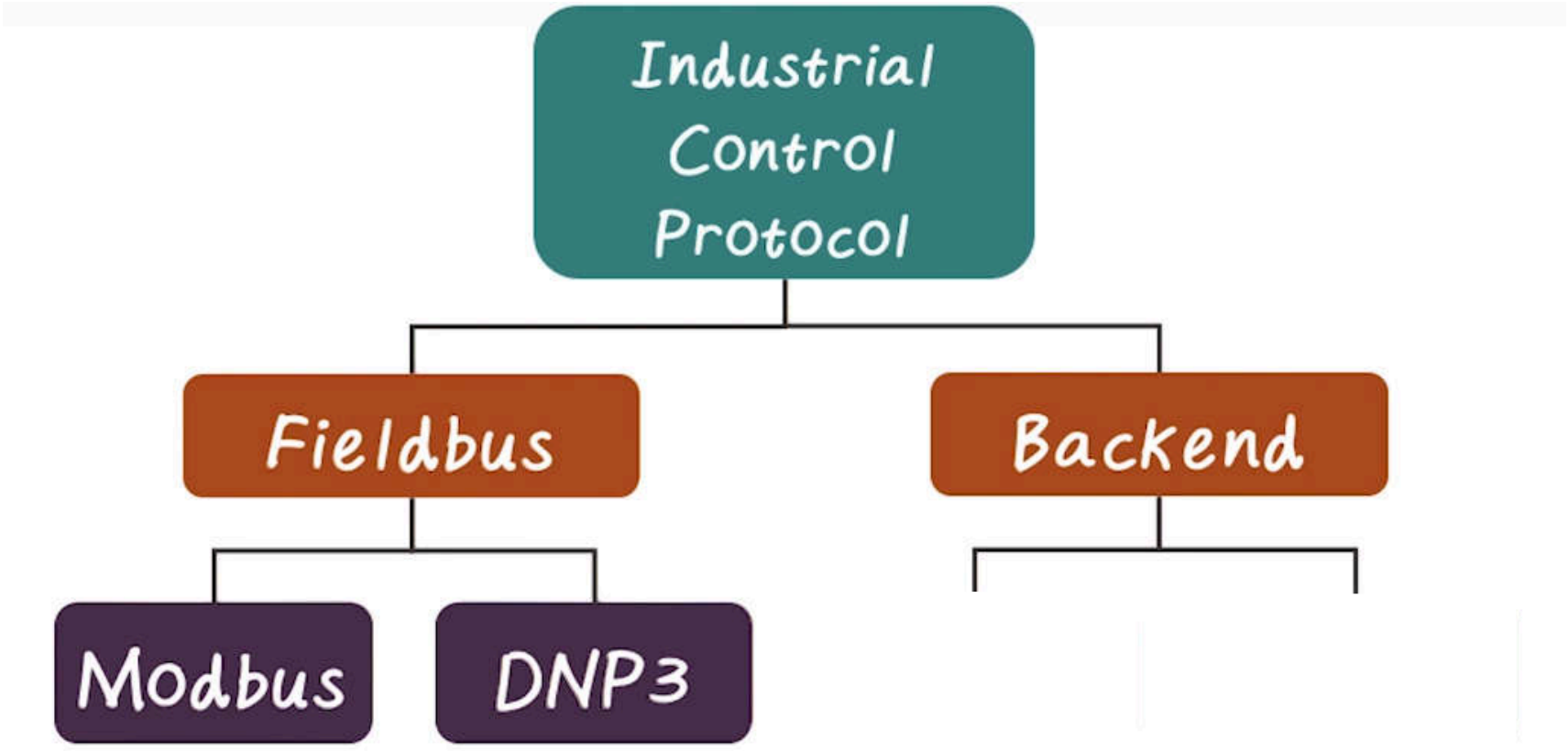
FieldBus vs Backend Protocols



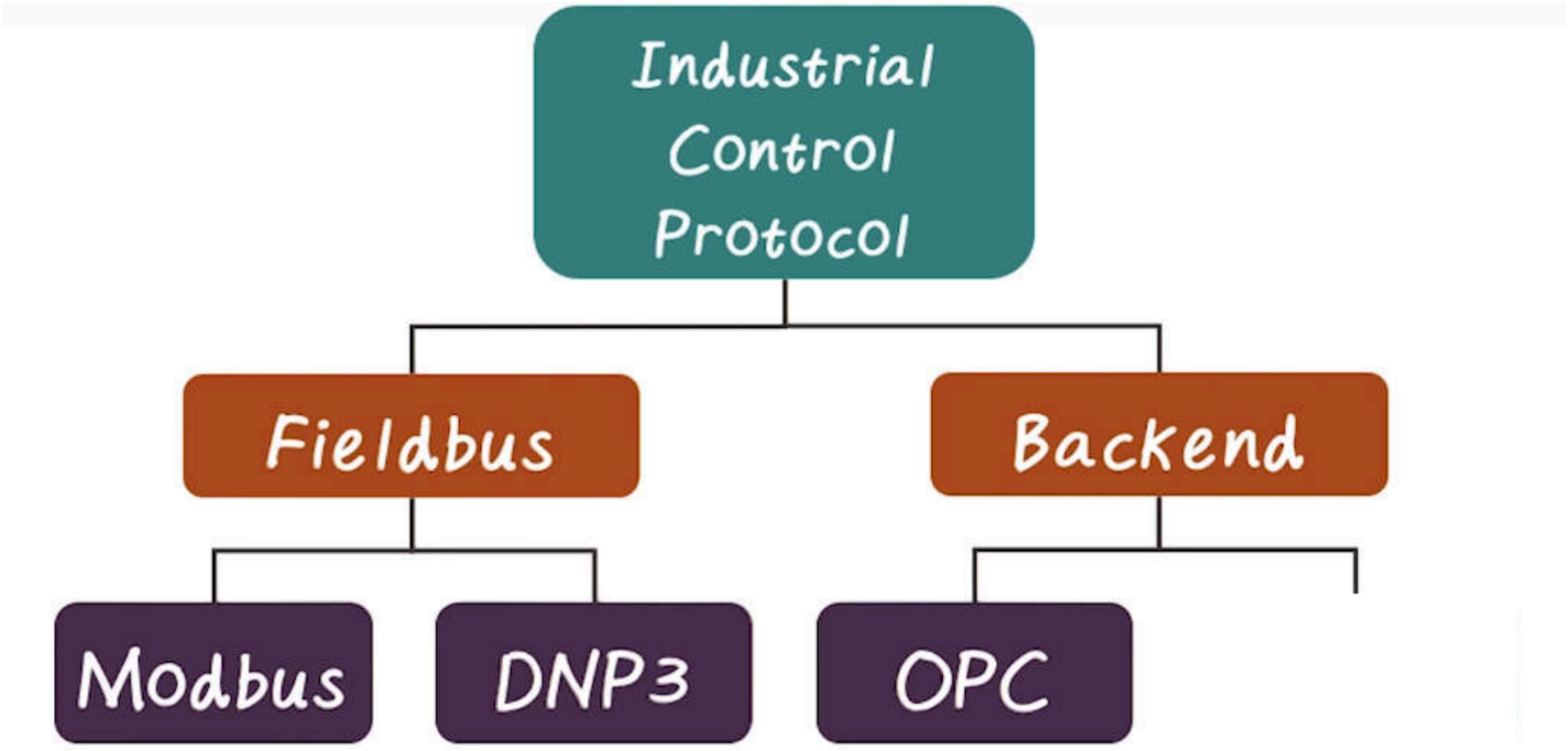
FieldBus vs Backend Protocols



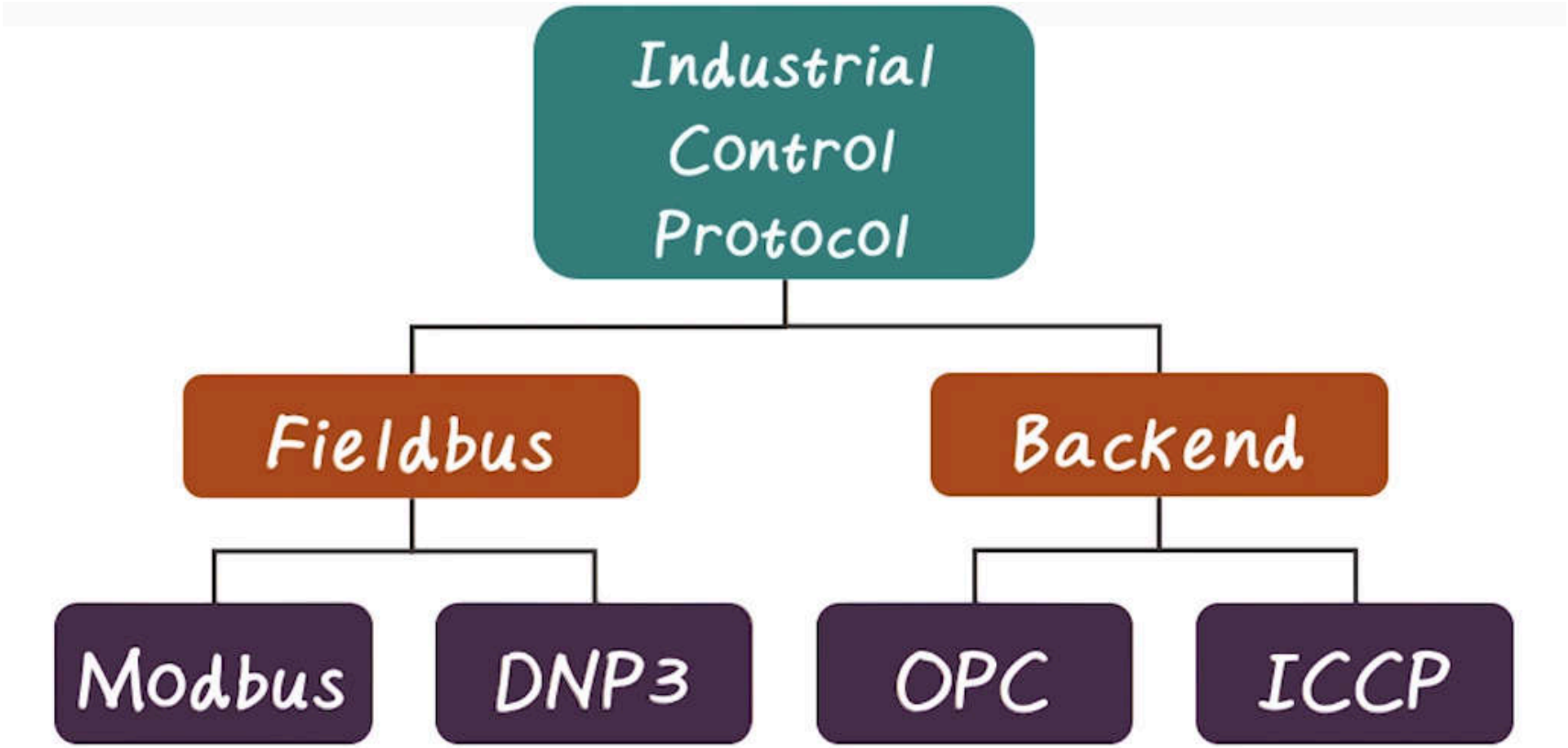
FieldBus vs Backend Protocols



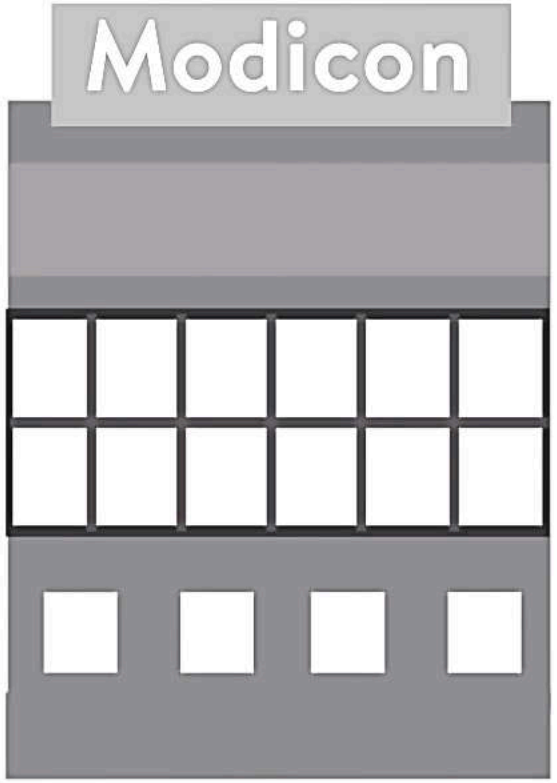
FieldBus vs Backend Protocols



FieldBus vs Backend Protocols



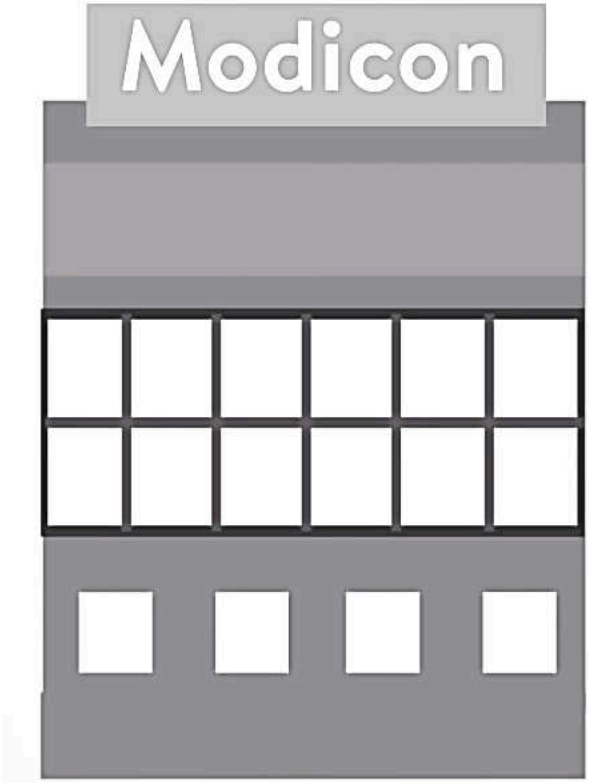
Modbus



Modbus

1979

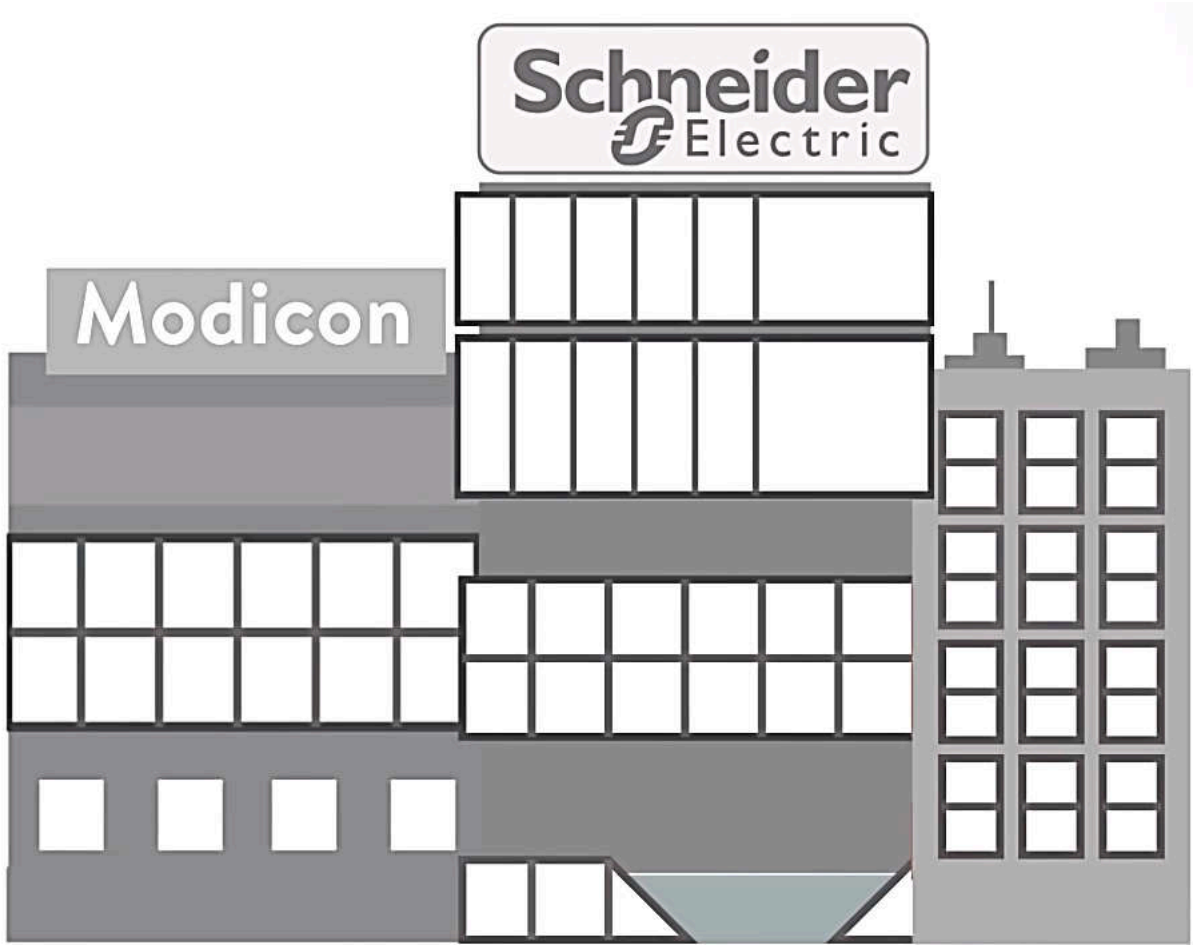
Modbus



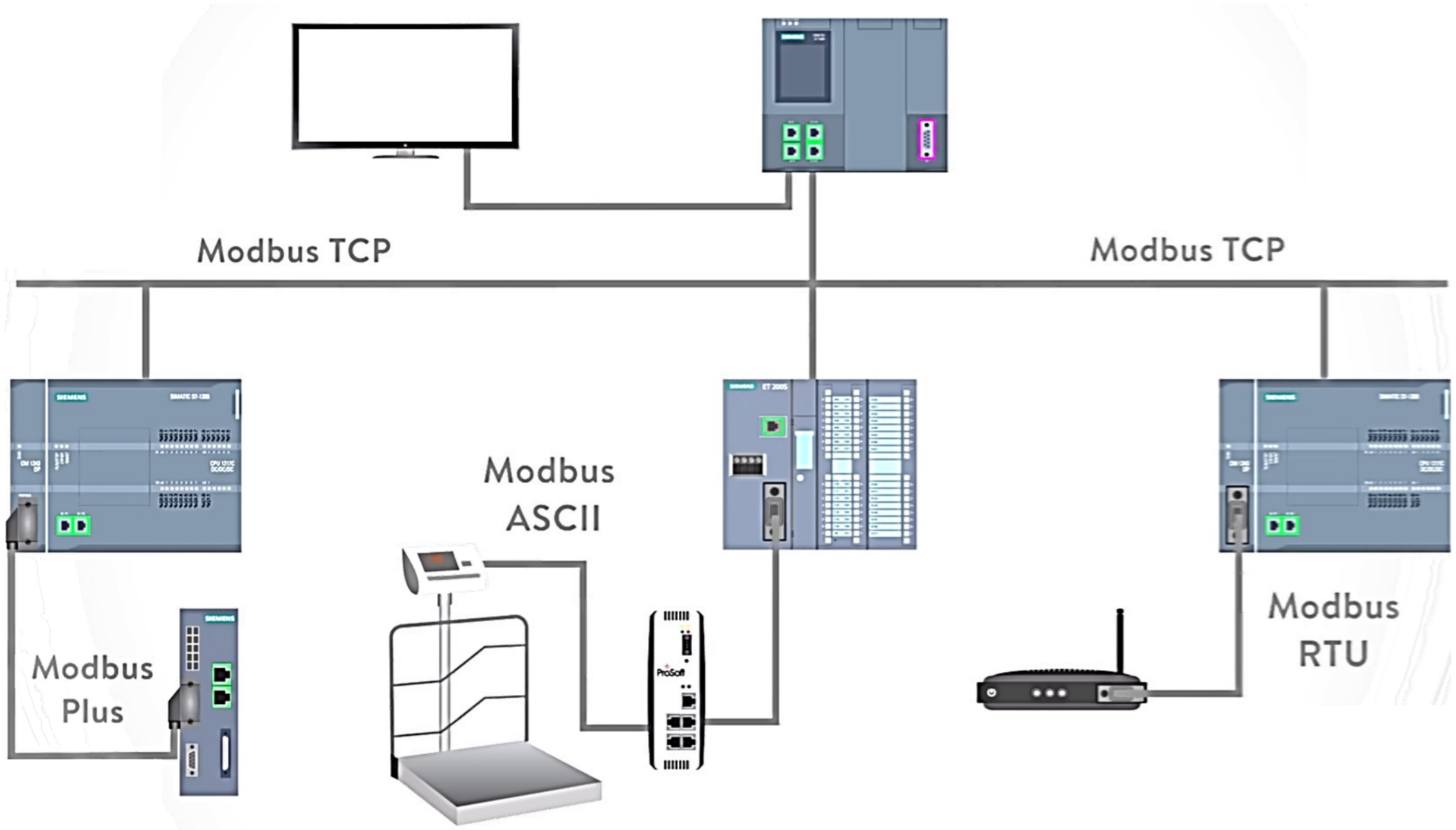
Modbus

1979

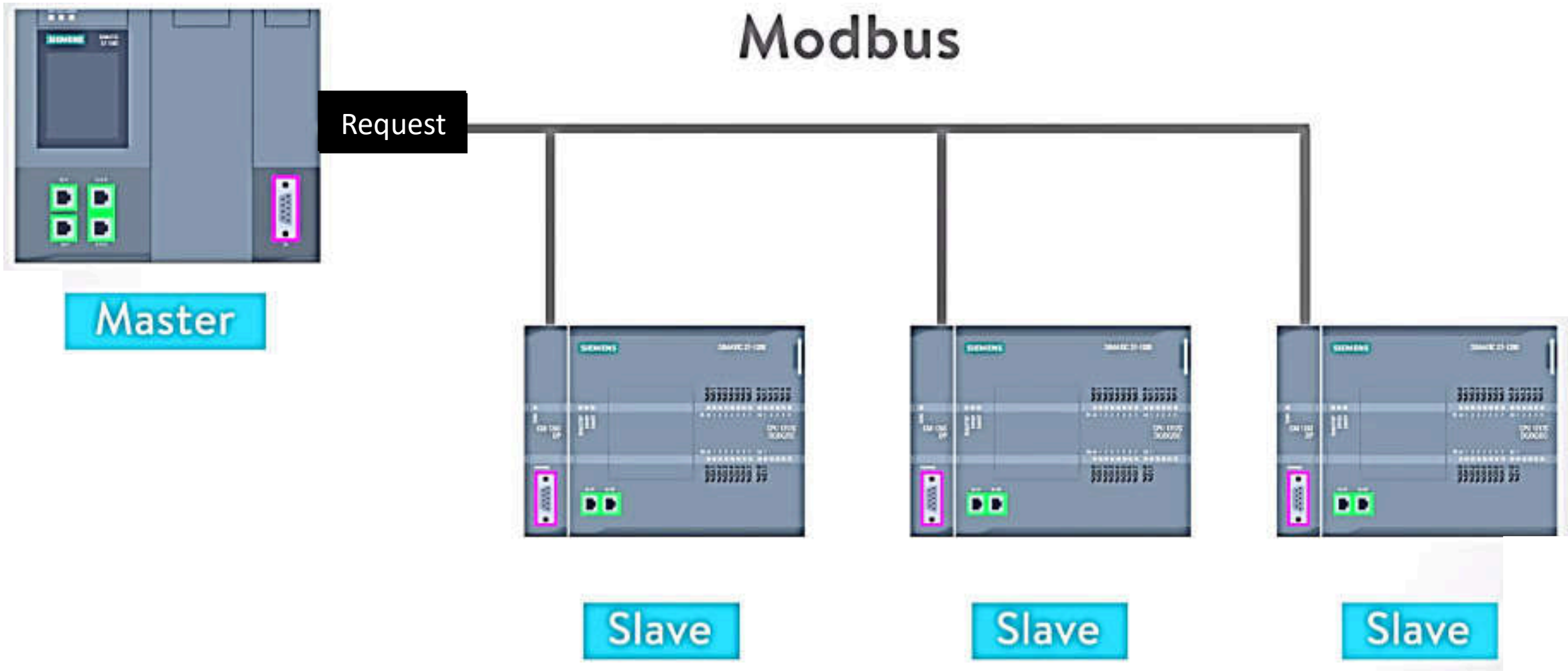
Modbus



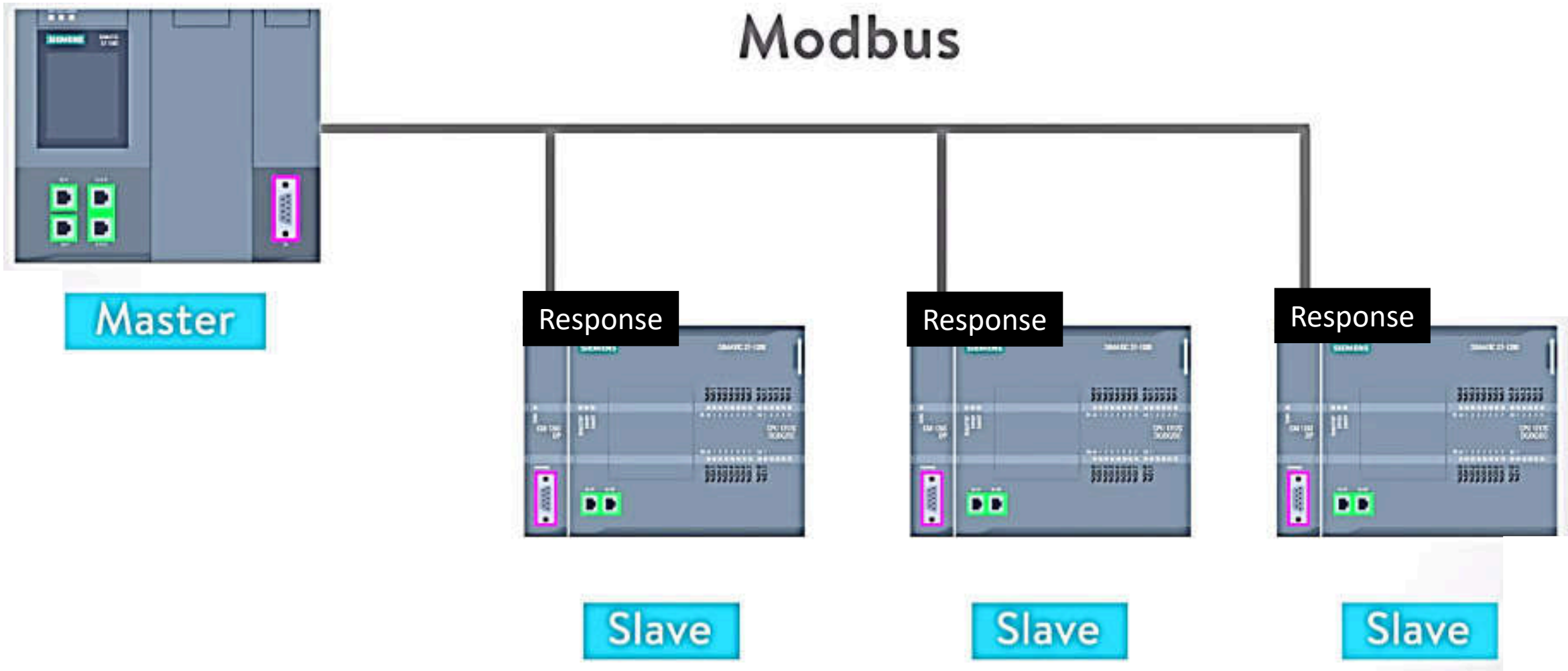
Modbus Variants



Modbus Protocol



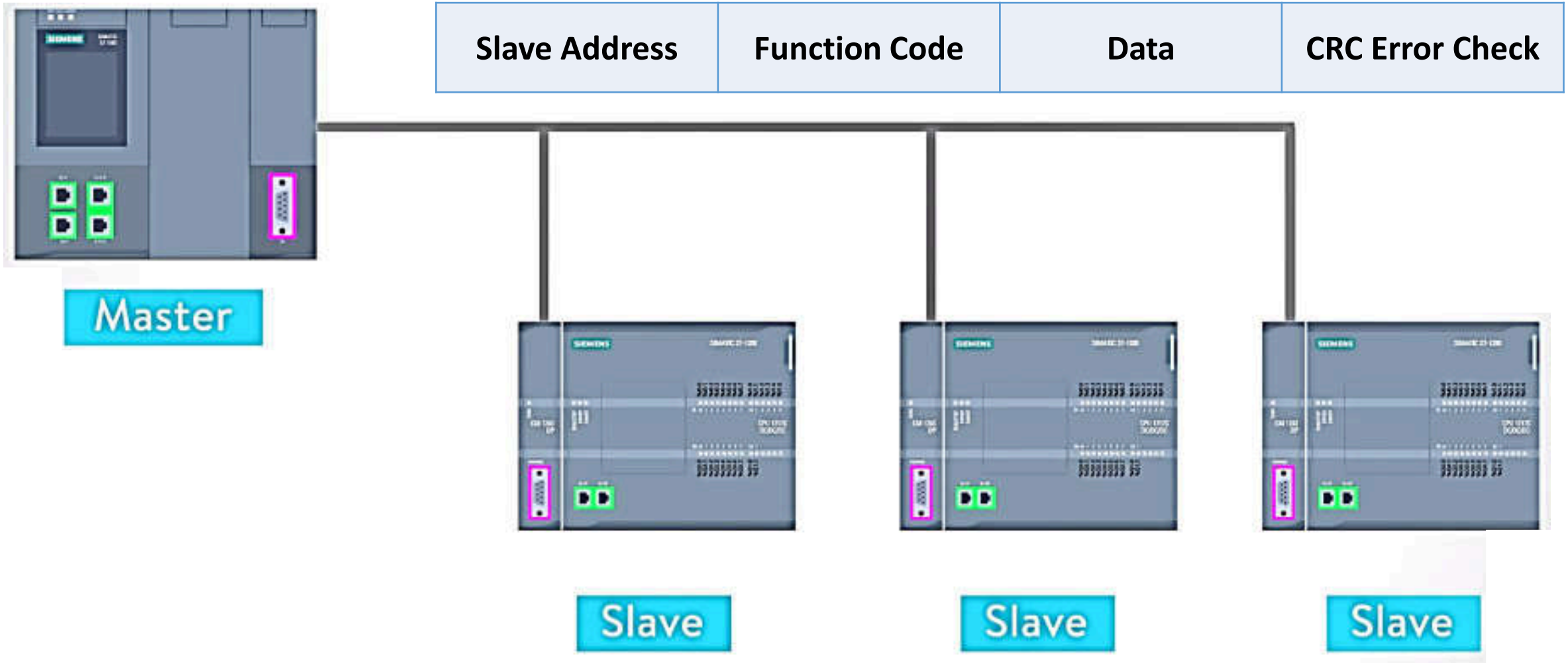
Modbus Protocol



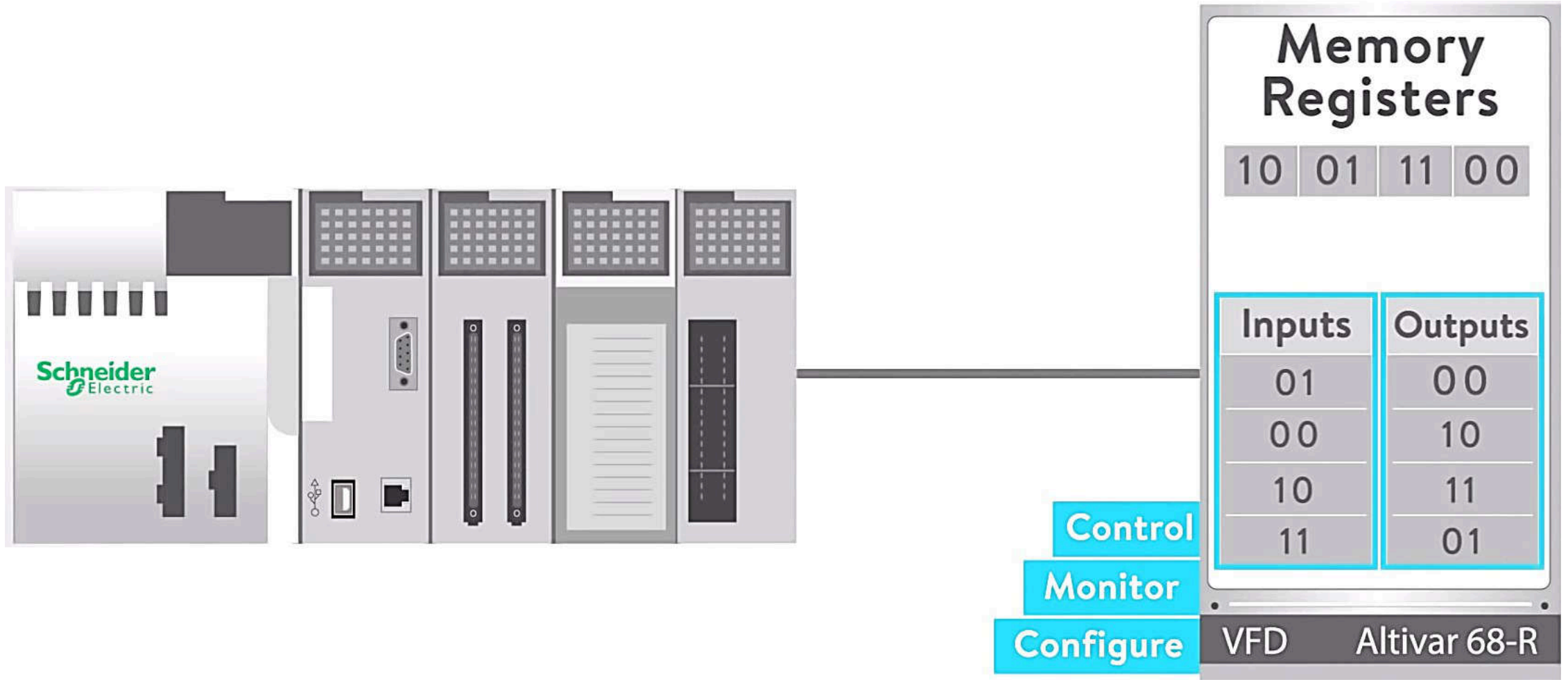
Modbus Protocol

Request Message

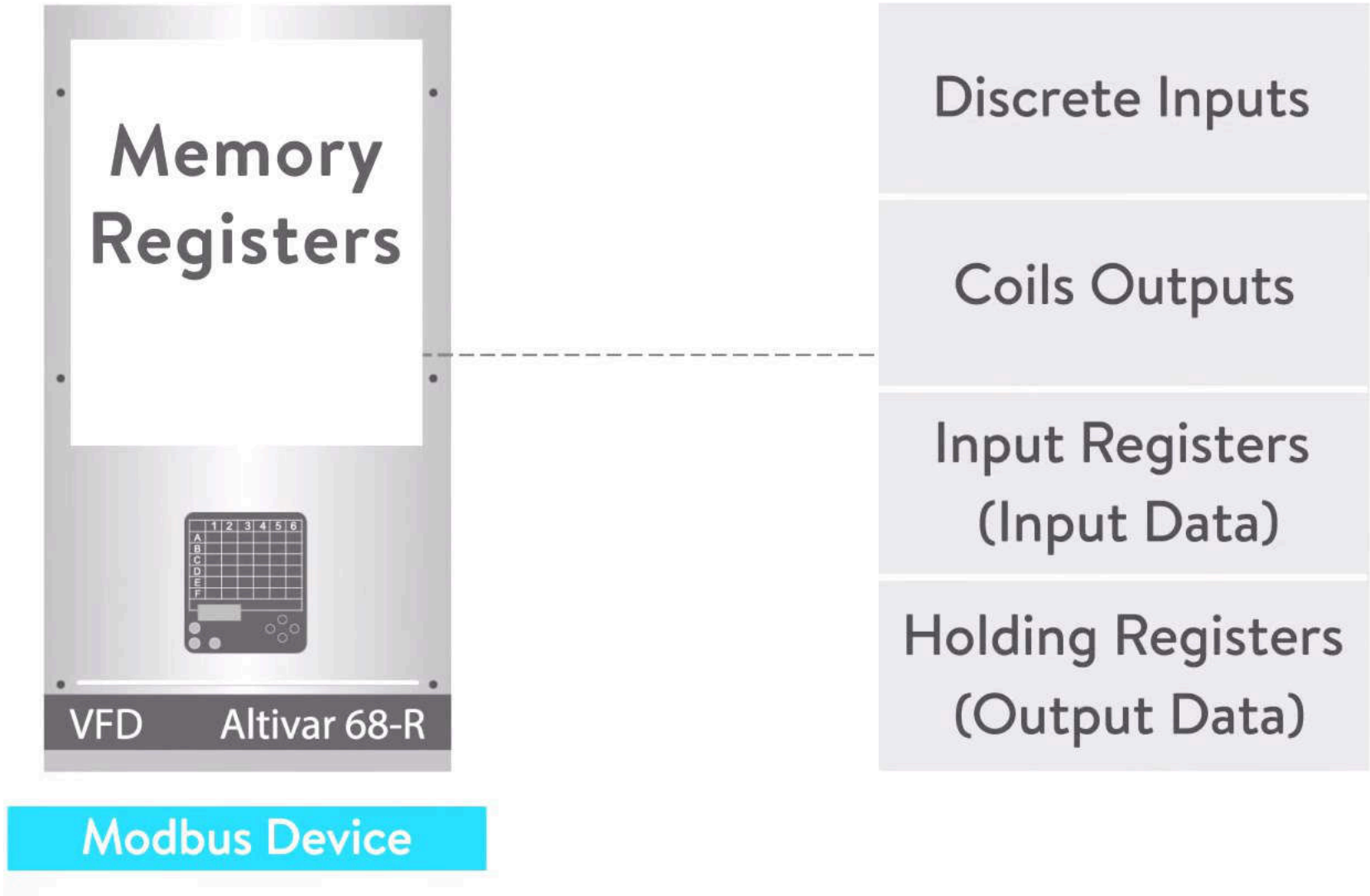
Slave Address	Function Code	Data	CRC Error Check



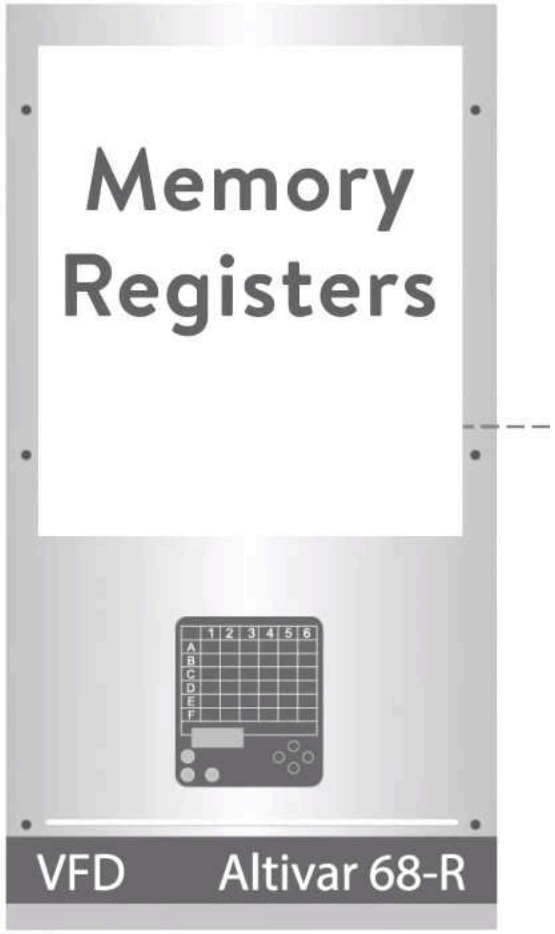
Modbus Protocol



Modbus Protocol



Modbus Protocol



Modbus Device

Function Code	Action	Table name
01 (01 hex)	Read	Discrete output coils
05 (05 hex)	Write single	Discrete output coil
15 (0F hex)	Write multiple	Discrete output coils
02 (02 hex)	Read	Discrete output contacts
04 (04 hex)	Read	Analog input contacts
03 (03 hex)	Read	Analog output holding registers
06 (06 hex)	Write single	Analog output holding register
16 (10 hex)	Write multiple	Analog output holding registers

Request Message

Slave Address	Function Code	Data	CRC Error Check

Modbus Protocol

MODBUS RTU

Application Data Unit (ADU) – max. 256 bytes

Start	Slave address	Function code	Data	CRC	End
>28 bits	1 byte	1 byte	n x 1 byte - max. 252 bytes (Continuous)	2 bytes	>28 bits

Protocol Data Unit (PDU)

MODBUS ASCII

Application Data Unit (ADU) – max. 510 bytes

Start	Slave address	Function code	Data	LRC	End
1 char (1 byte)	2 chars (2 bytes)	2 chars (2 bytes)	n x 2 x 1 chars - max. 2x252 chars (504 bytes max.)	2 chars (2 bytes)	2 chars (CR+LF)

Protocol Data Unit (PDU)

Modbus Protocol

MODBUS RTU

Application Data Unit (ADU) – max. 256 bytes

Start	Slave address	Function code	Data	CRC	End
>28 bits	1 byte	1 byte	n x 1 byte - max. 252 bytes (Continuous)	2 bytes	>28 bits

Protocol Data Unit (PDU)

MODBUS over TCP/IP

Modbus Application Protocol (MBAP) header | **Modbus RTU ADU**

Transaction ID	Protocol ID	Length	Unit ID	Slave addrs	Func code	Data	CRC

Modbus over TCP/IP ADU

Modbus Security Concerns

Lack of authentication

Modbus Security Concerns

Lack of authentication

Lack of encryption

Modbus Security Concerns

Lack of authentication

Lack of encryption

Lack of message checksum (Modbus/TCP only)

Modbus Security Concerns

Lack of authentication

Lack of encryption

Lack of message checksum (Modbus/TCP only)

Lack of broadcast suppression
(serial Modbus variants only used in a multidrop topology)

Modbus Security Recommendations

Monitor communication with ICS-aware intrusion detection system

Modbus Security Recommendations

Monitor communication with ICS-aware intrusion detection system

Whitelisting

Modbus Security Recommendations

Monitor communication with ICS-aware intrusion detection system

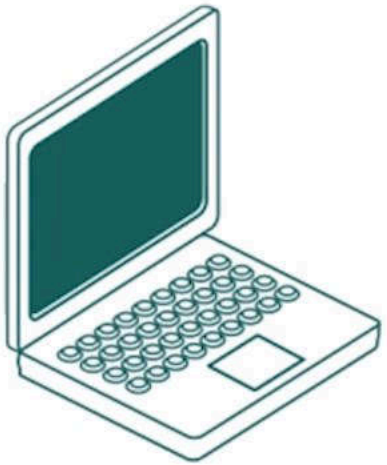
Whitelisting

Application aware firewall

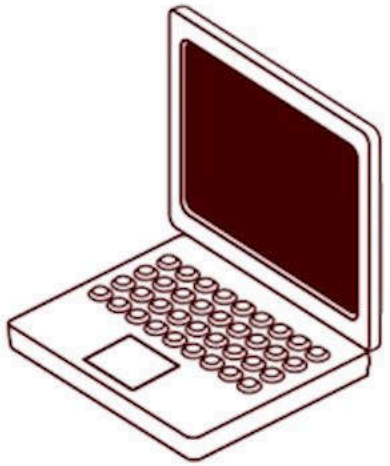
DNP3

The Distributed Network Protocol began as a serial protocol much like Modbus.

Designed for use between "master stations" or "control stations" and slave devices called "outstations."



Master station



Slave/outstation

NEXT CLASS

Thanks a lot

If you are taking a Nap, **wake up**.....Lecture Over