SIU Southern Illinois University
CARBONDALE

Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 7: Industrial vs. Business Network

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

EMAIL: AYDEGER@CS.SIU.EDU

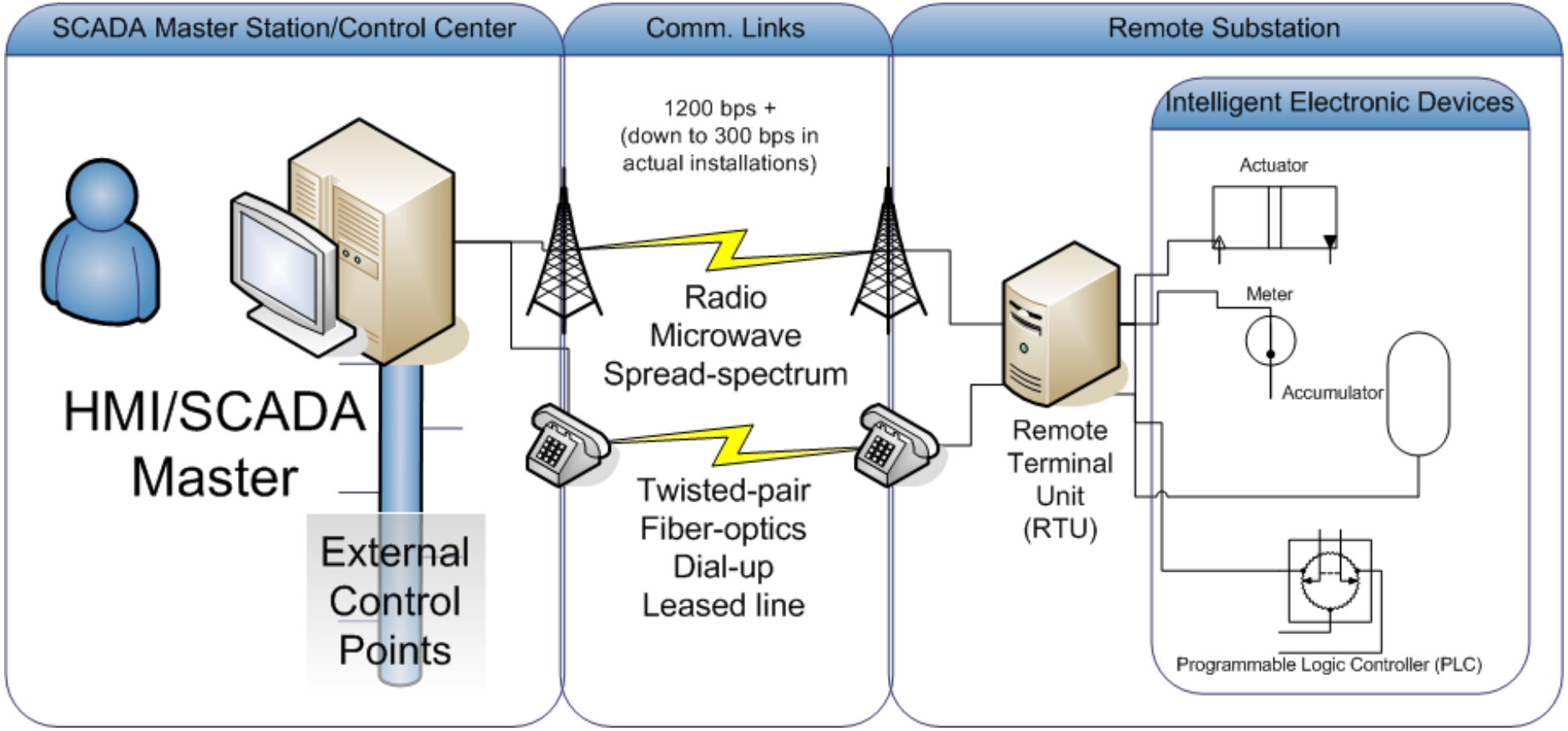
Outline

Details about SCADA Network

- Network Topology
- Network Segmentation

Operational Technology

Recall: SCADA Example



ICS Network Architecture

ICS Network; Any network that supports the interconnectivity of and communication between devices that make up or support an ICS

Various options depending on the application

Two distinct networks:

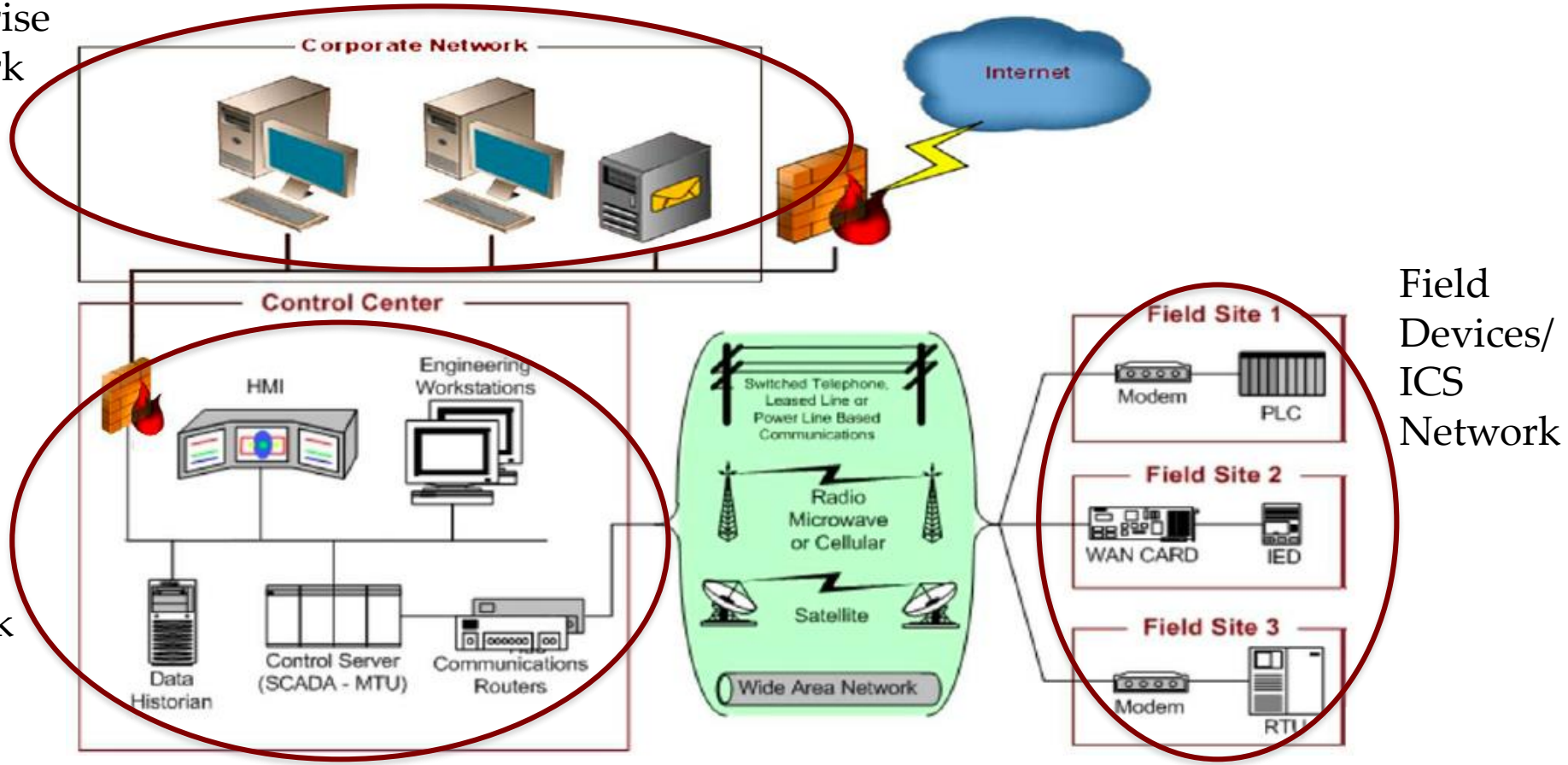
- Industrial control and automation
- Supervisory control or SCADA

These connect to Business/Enterprise Networks which then connects to Internet

- TCP/IP based networks
- They have different requirements

Enterprise vs SCADA

Enterprise Network



SCADA Network

Field Devices/ ICS 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

Network Topologies

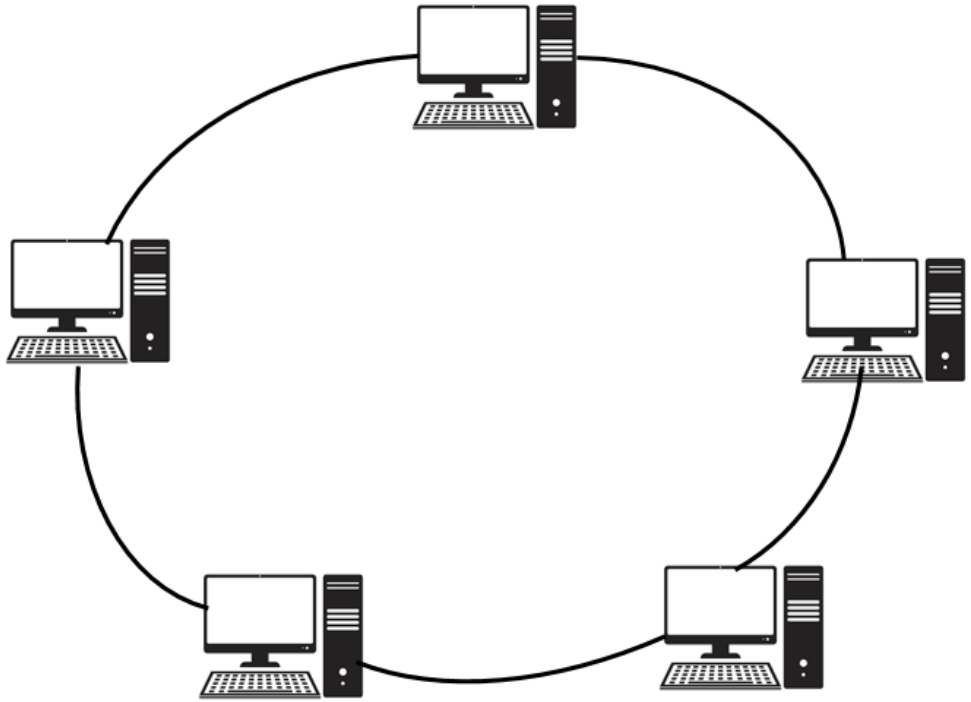
Ring

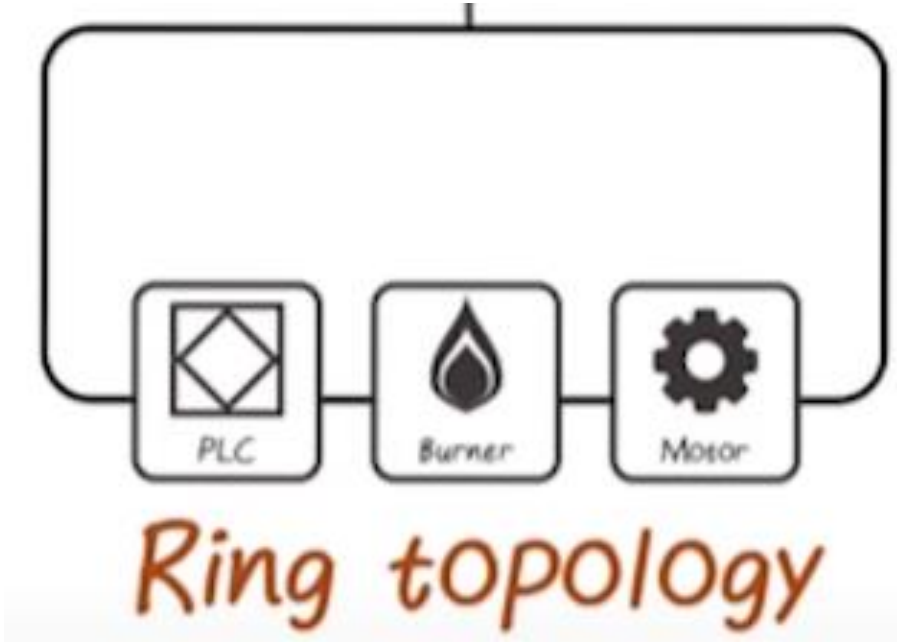
Bus

Star

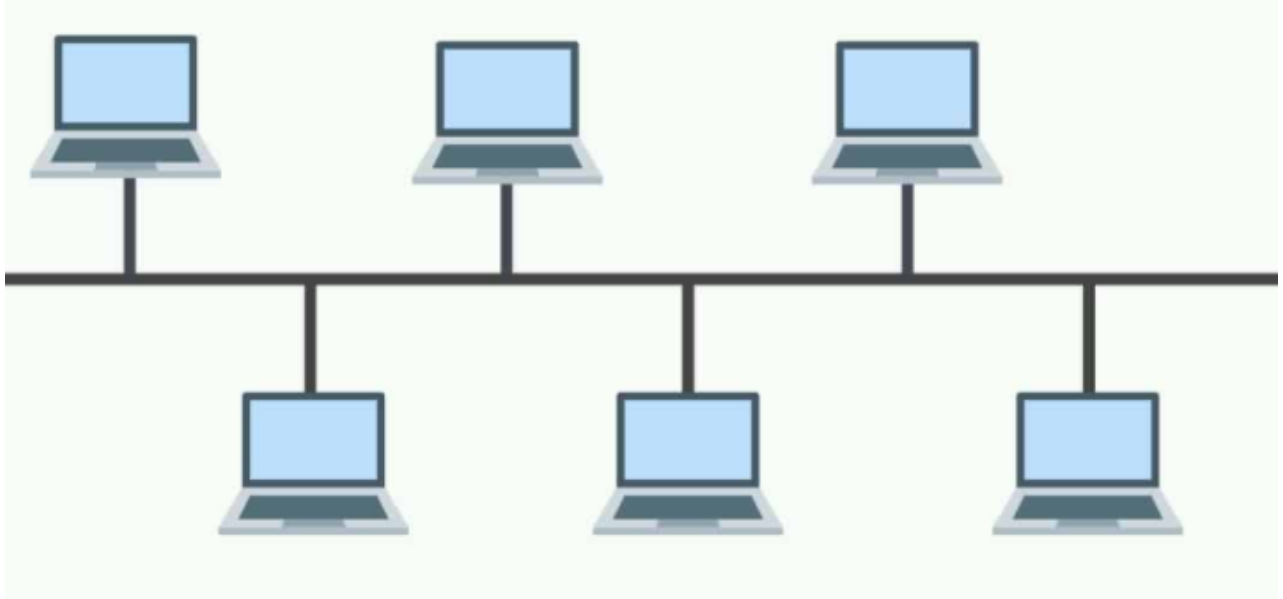
Wireless Mesh

Ring Topology

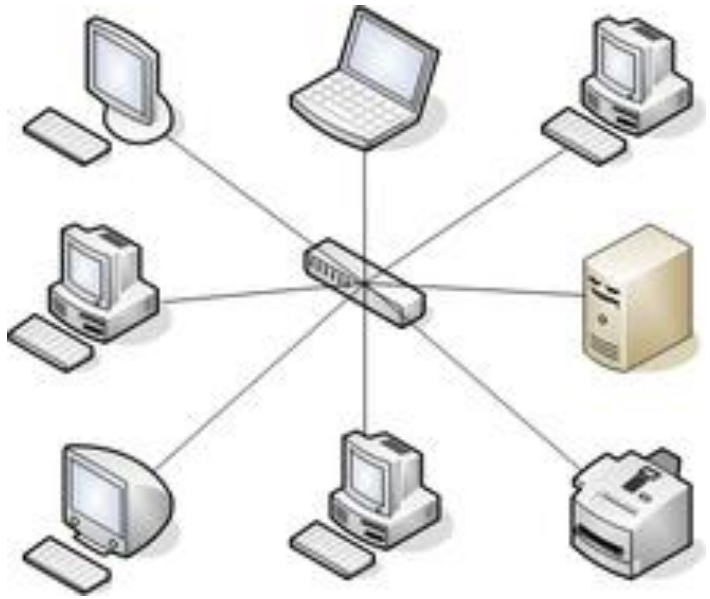


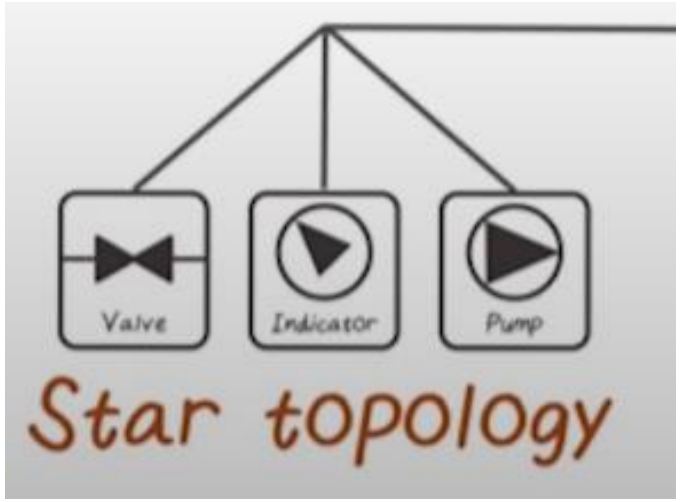


Bus Topology

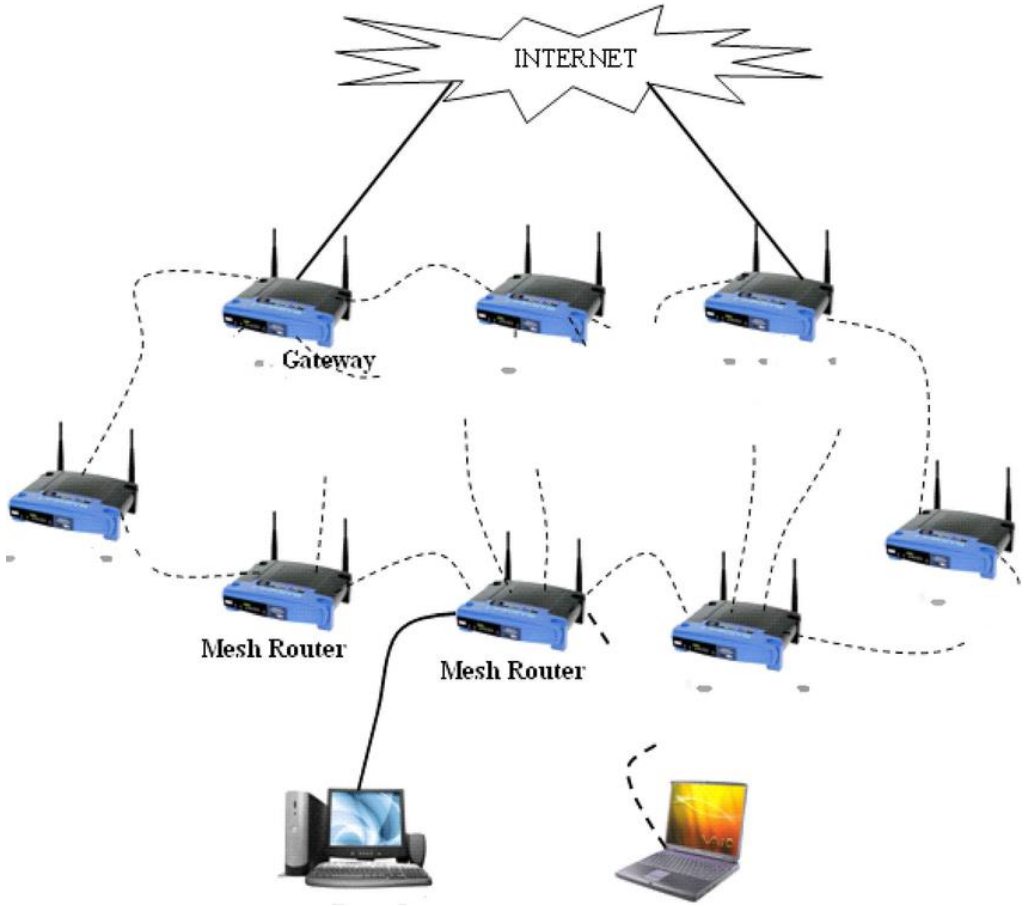


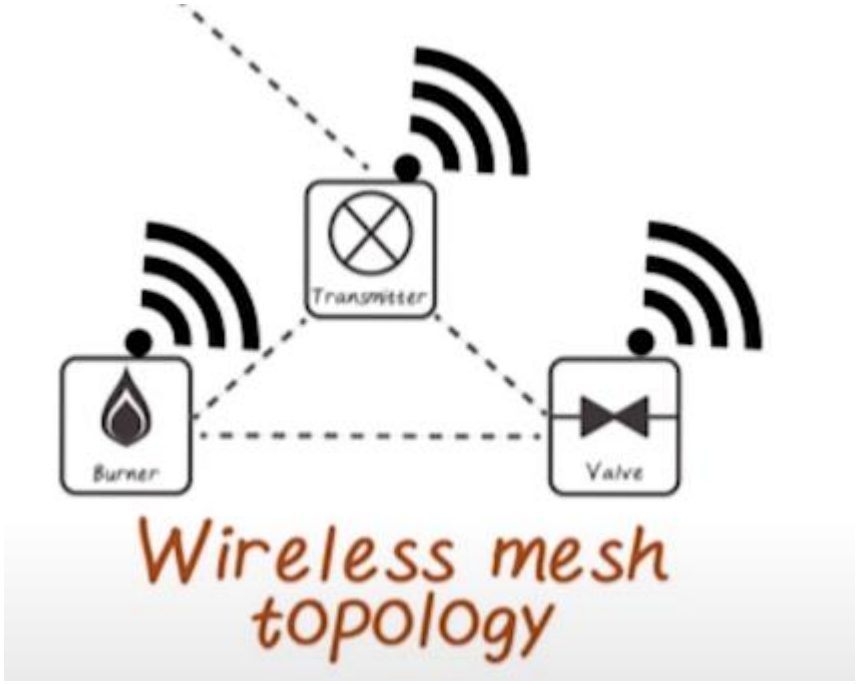
Star Topology



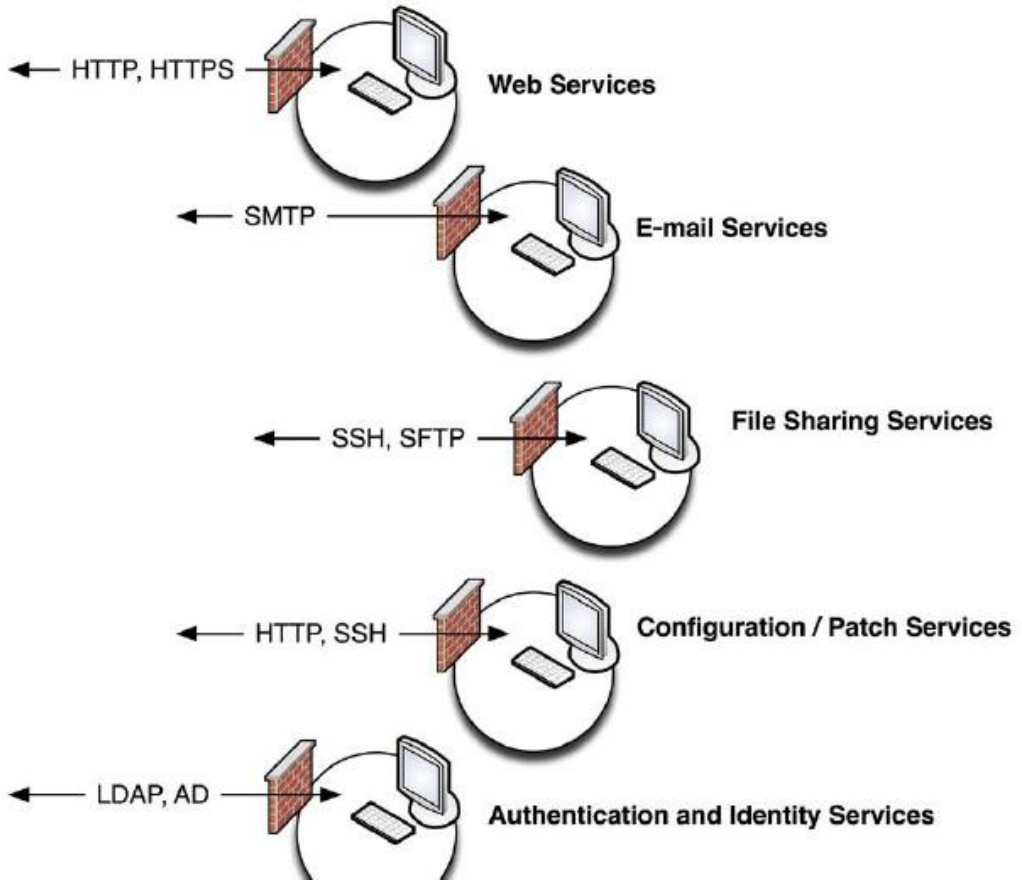


Wireless Mesh Topology

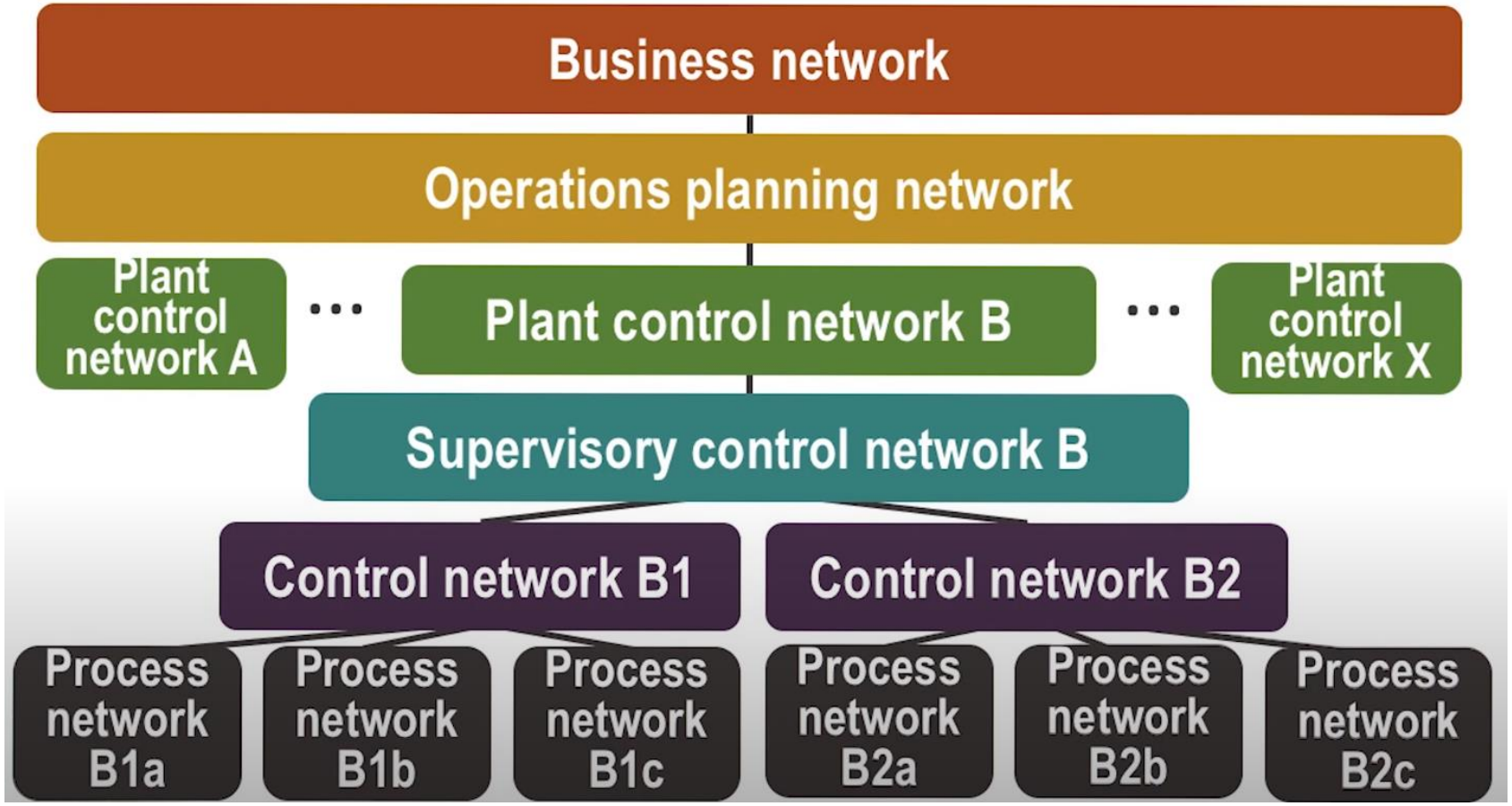




Network Segmentation/Isolation of Systems



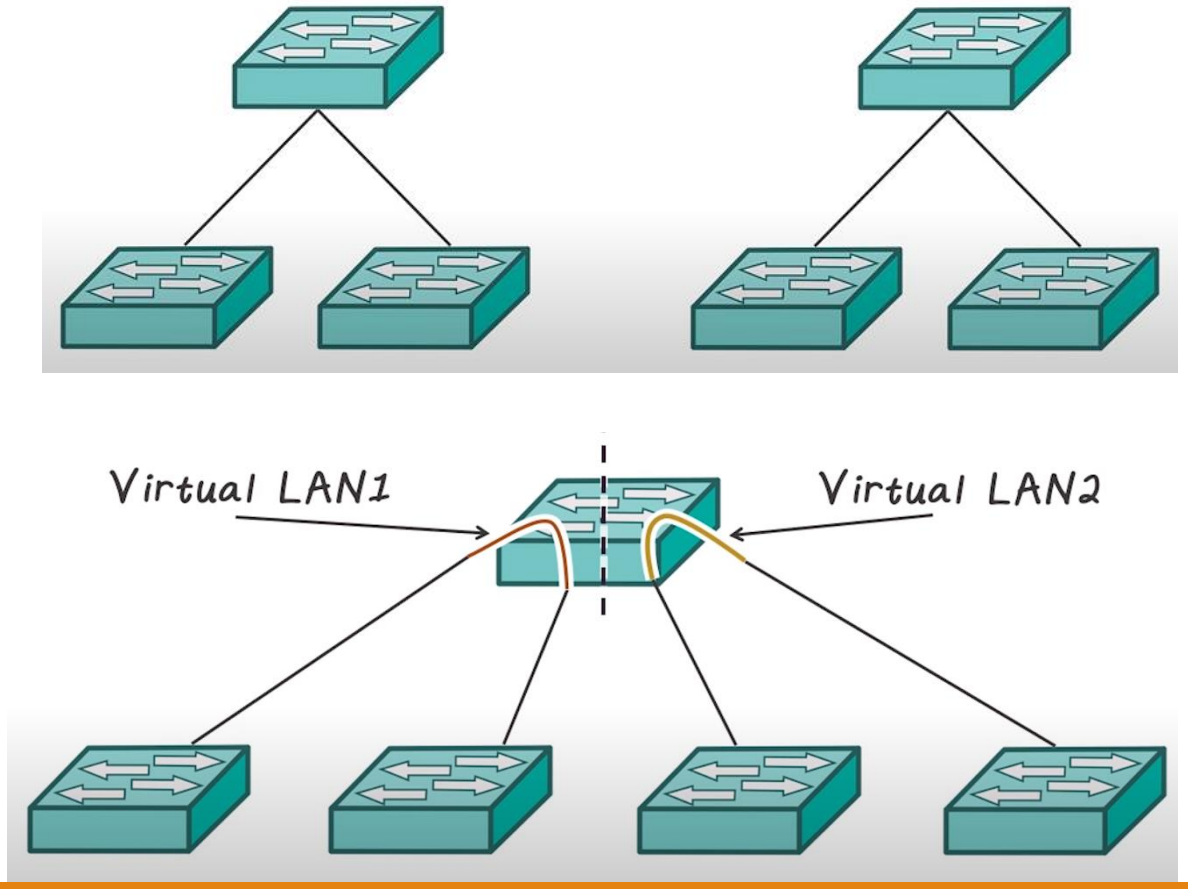
ICS Network's Segmentation



Segmentation by Layers

Segmentation/ Segregation	Provided By	Management	Performance	Network Security	ICS Protocol Support	OT Applicability
Physical Layer	Air Gap Data Diode	None	Good	Absolute	N/A	High
DataLink Layer	VLAN	Moderate	Good	Very Broad	High	High
Network Layer	Layer 2 Switch (via VLAN interfaces only) Layer 3 Switch Router	Low	Moderate	Broad	High	High
Application Layer	Application Proxy/IPS "Next Generation" Firewall/IPS Content Filter	High	Poor	Very Specific	Low	Low

Physical vs. Logical Segmentation



Network Metrics

Latency

Jitter

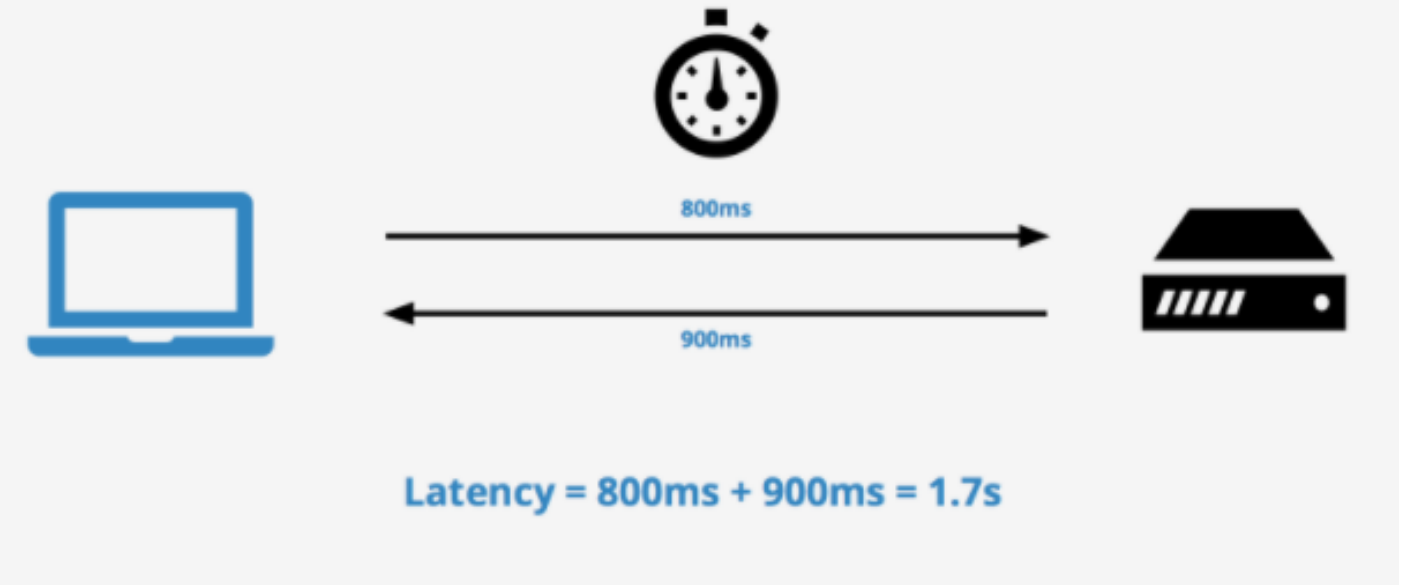
Bandwidth

Throughput

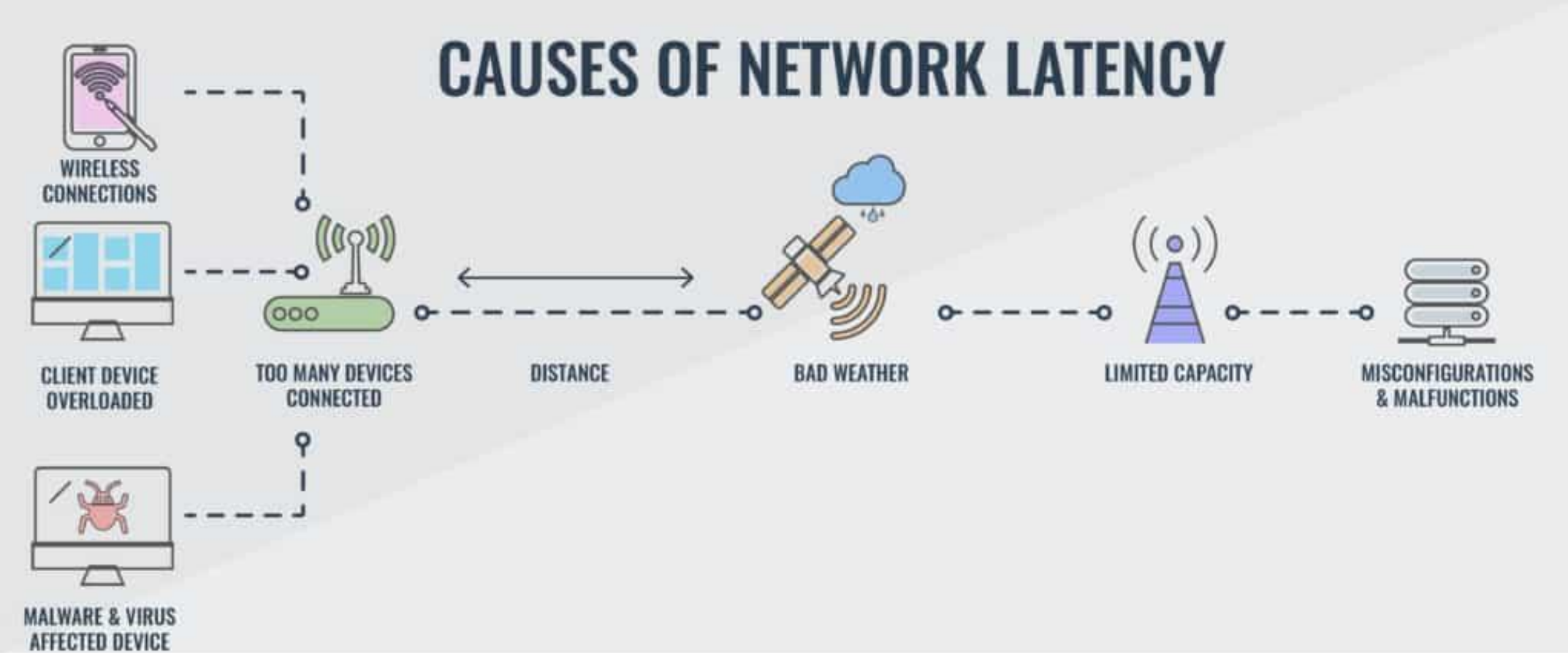
Latency

Time it takes for a packet to travel from source to destination

- Usually calculated as round trip time (RTT)



Potential Causes of Increased Latency

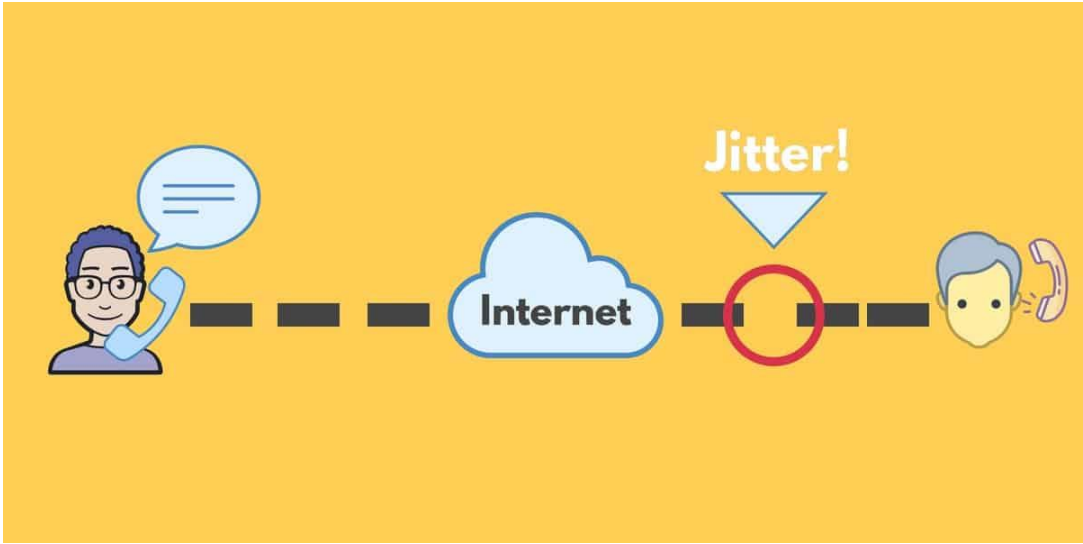


Jitter

Jitter, or network jitter, is the variance in time delay between data packets over a network

It is a disruption in the normal sequence of sending data packets

The technical term for jitter “packet delay variance”



Bandwidth and Throughput

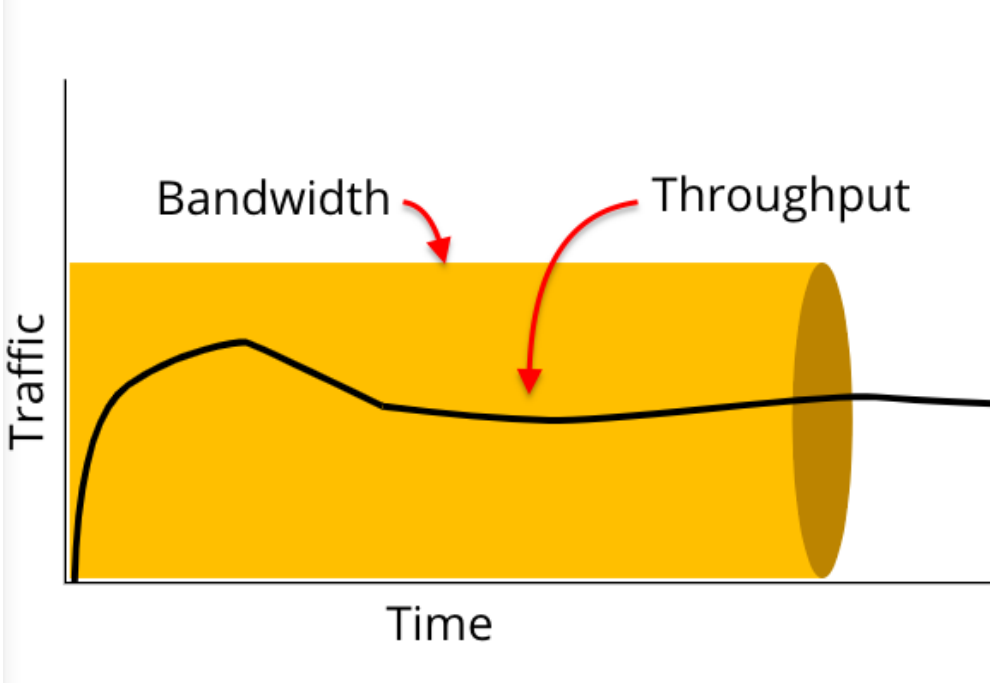
Bandwidth:

Amount of data can be transferred in a given period of time

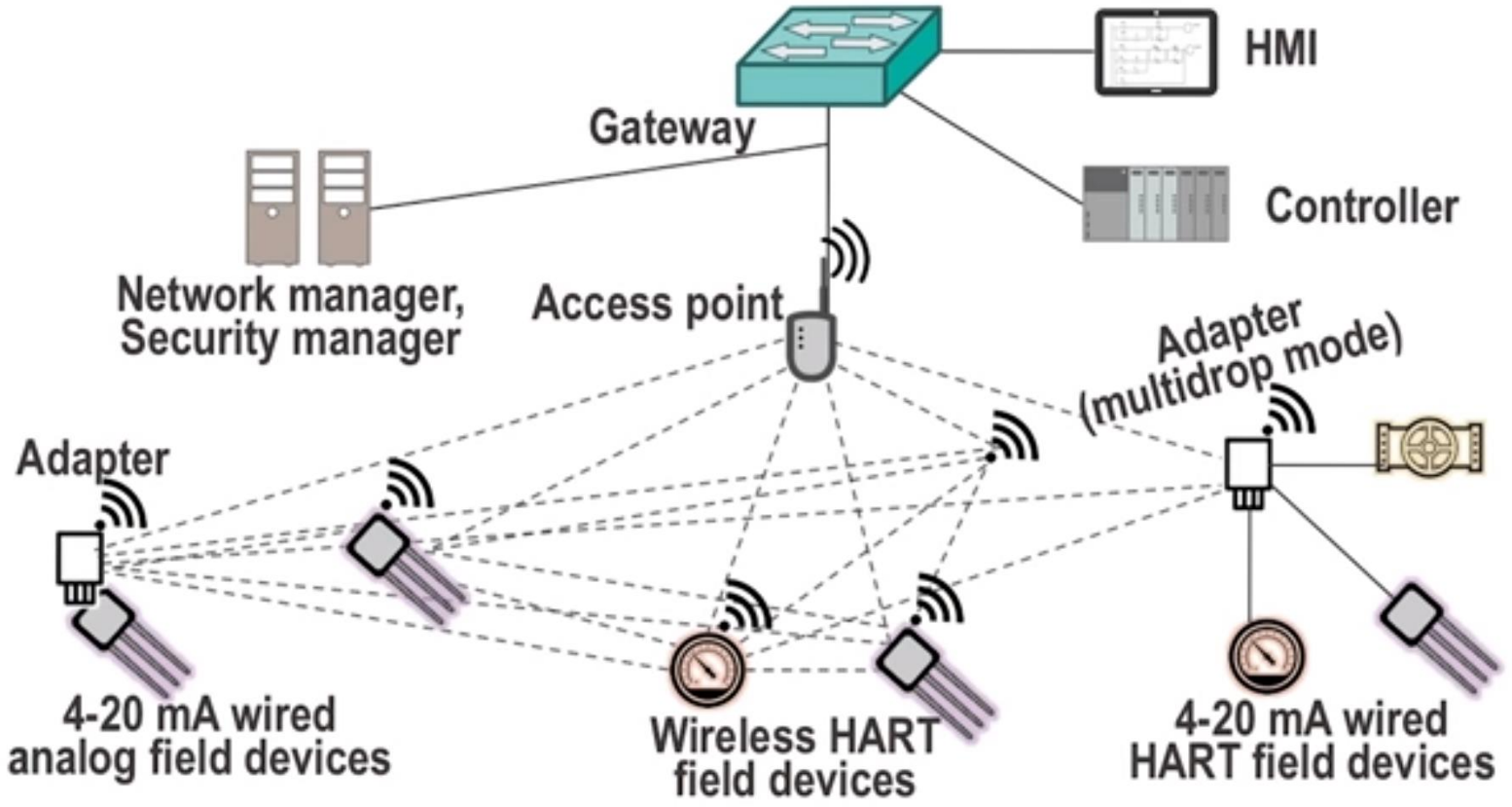
- Maximum rate

Throughput:

The rate of successful message delivery over a communication channel



Wireless ICS



Wireless Protocols

Bluetooth

Microwave

Satellite

Zigbee

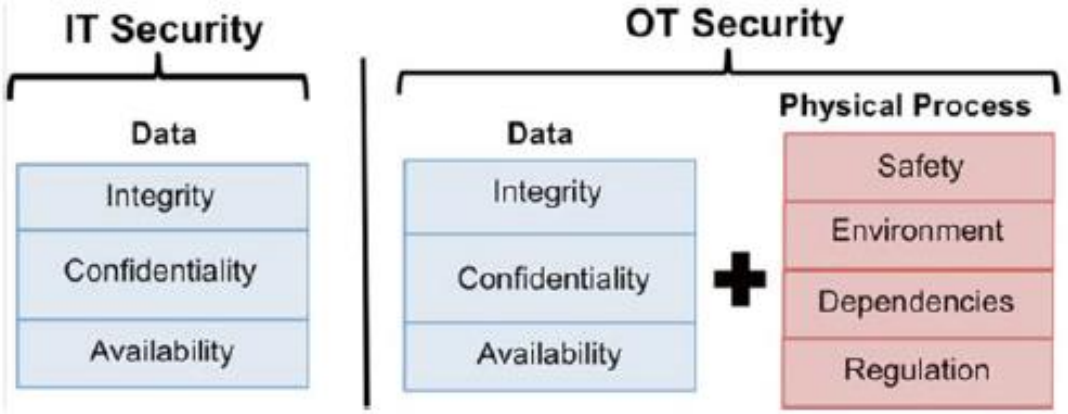
Z-wave

WirelessHART

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

OT's Real-Time Performance Example

IEC 61850 communication latency requirements

Functions	Message type	Delay (ms)
Fault isolation and protection	Type 1A/P1	3
	Type 1A/P2	10
Routine automation functions	Type 1B/P1	100
	Type 1B/P1	20
Measurement readings	Type 2	100
	Type3	500

Performance overhead for cryptographic operations (2.8 GHz AMD processor in a publisher/ subscriber architecture)

Algorithm	Pub (ms)	Sub (ms)	Total (ms)
128 bit AES	0.04	0.03	0.07
SHA-256	0.01	0.01	0.02
2048 bit RSA	59.00	2.04	61.04
1024 bit DSA	4.10	9.80	14.90