L16 – Industrial Control Networks

50.012 Networks

Jit Biswas

Cohort 1: TT7&8 (1.409-10)

Cohort 2: TT24&25 (2.503-4)

Introduction

- Todays lecture:
  - Networks off the mainstream: industrial control system networks
  - Historical context of such systems
  - Link Layer redundancy and Loop prevention (STP)
  - Recent trends: Ethernet, encapsulation, generalization

Industrial Control Networks

Industrial Control Networks

- Specialized networks to control
  - Industrial plant automation
    - Manufacturing, processing
  - Infrastructure systems
    - Transportation, water distribution, power distribution
- In general, cyber-physical systems
  - Combining cyber (i.e. networking) and physical (process)

Purpose of Industrial Control Networks

- Simplified, network consists of
  - Sensors
  - Actuators
  - Controllers
- Task of network:
  - Collection of distributed sensor signals
  - Distribution of sensor data among controllers
  - Delivery of control commands

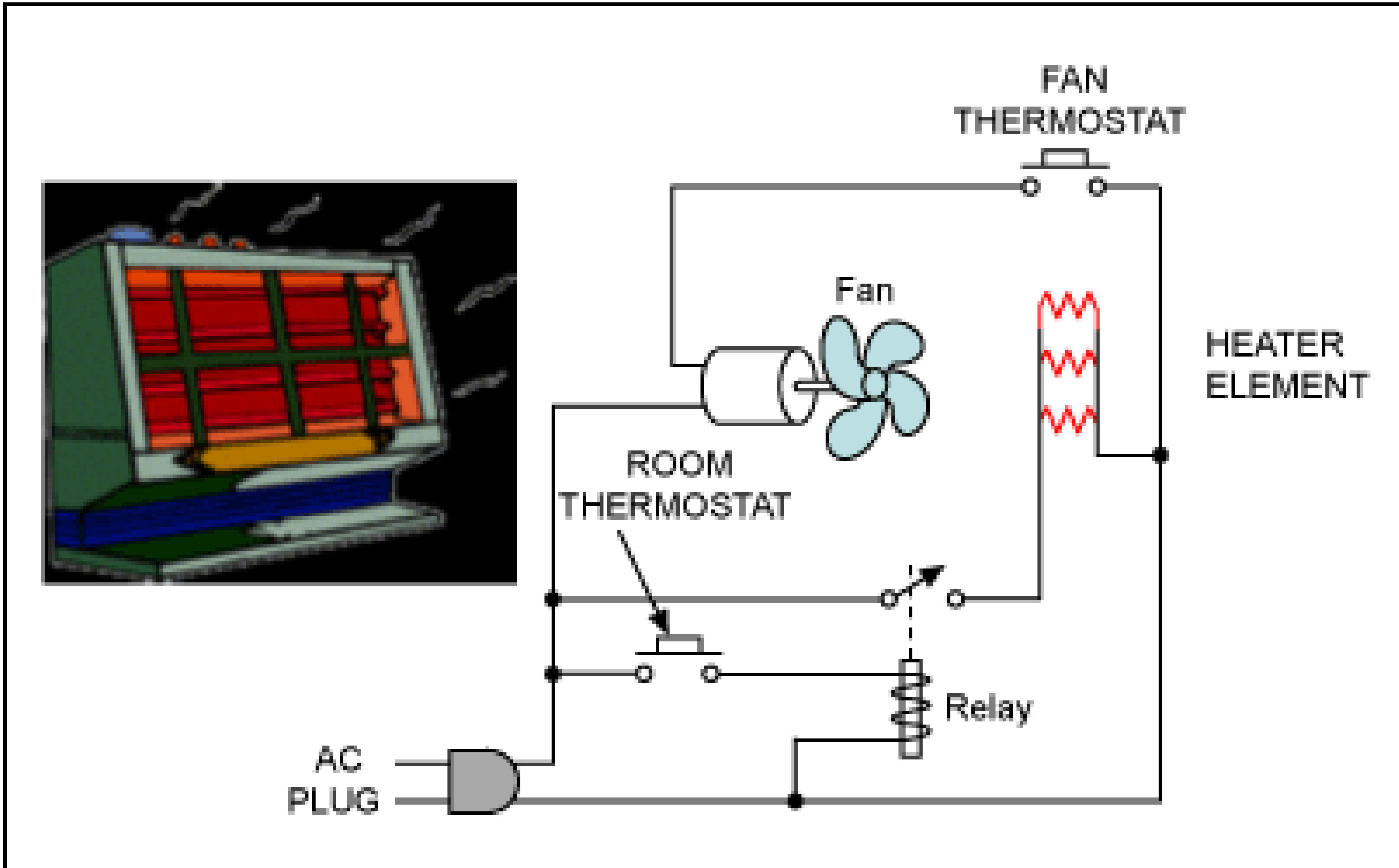
Challenges in Industrial Control Networks

- Used for continuous real-time control:
  - Real-time requirements (e.g., max delay)
  - Low tolerance to loss or errors
  - Predictable amount of traffic, static topology
- In addition:
  - Heterogeneous systems, growing over time
  - Multiple vendors, each speaking their own dialects
  - Constant availability requirements

Why Control Networks?

- Control systems started with mechanical controls
  - E.g. governors to regulate engine speed
  - Control actions taken manually by engineers
- Simple control automation introduced with electrical controllers
  - Naming depends on domain, but often called Programmable Logic Controllers (PLC)
- PLCs are connected to local sensors/actuators
  - Connections either analog (e.g. current based), RS-232, RS-485, proprietary bus systems
- Local view can make control inefficient, supervision hard, changes require local presence
  - How to mitigate this problem?

Simple Example of Process Control



A Household Electric Heater

https://www.maximintegrated.com/en/app-notes/index.mvp/id/4603

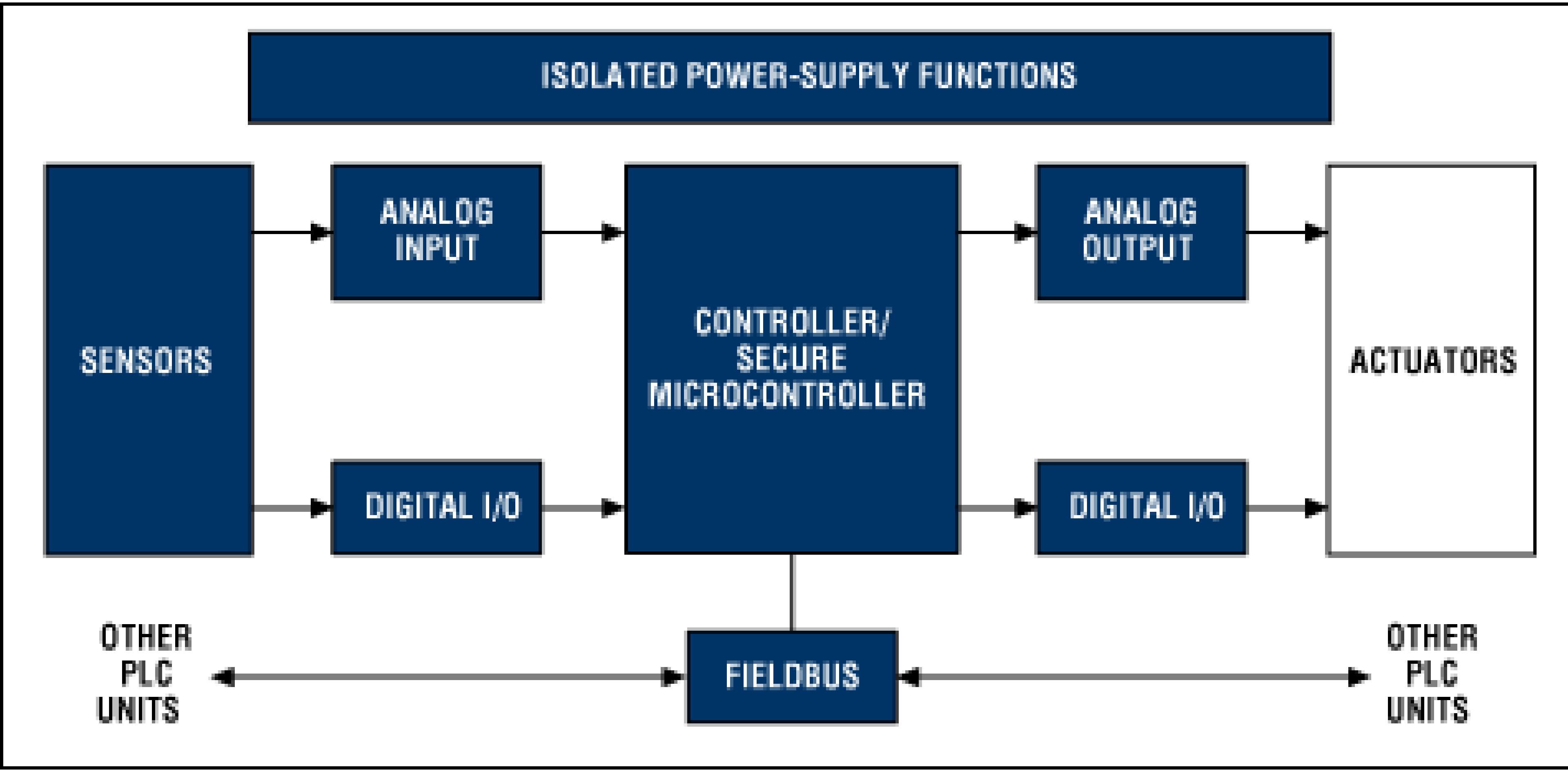
Programmable Logic Controllers

- PLCs control a wide array of applications from simple lighting functions to environmental systems to chemical processing plants. These systems perform many functions, providing a variety of analog and digital input and output interfaces:
  - signal processing;
  - data conversion; and
  - various communication protocols.

- All of the PLC's components and functions are centered around the controller, which is programmed for a specific task. Components of PLCs:
  - analog and digital I/Os
  - distributed control (e.g., a fieldbus)
  - Interface to sensors and actuators
  - CPU & power

- Ruggedized Processor
  - Ease of programming
  - Reliability
  - Field operation
  - Non-stop (decades)

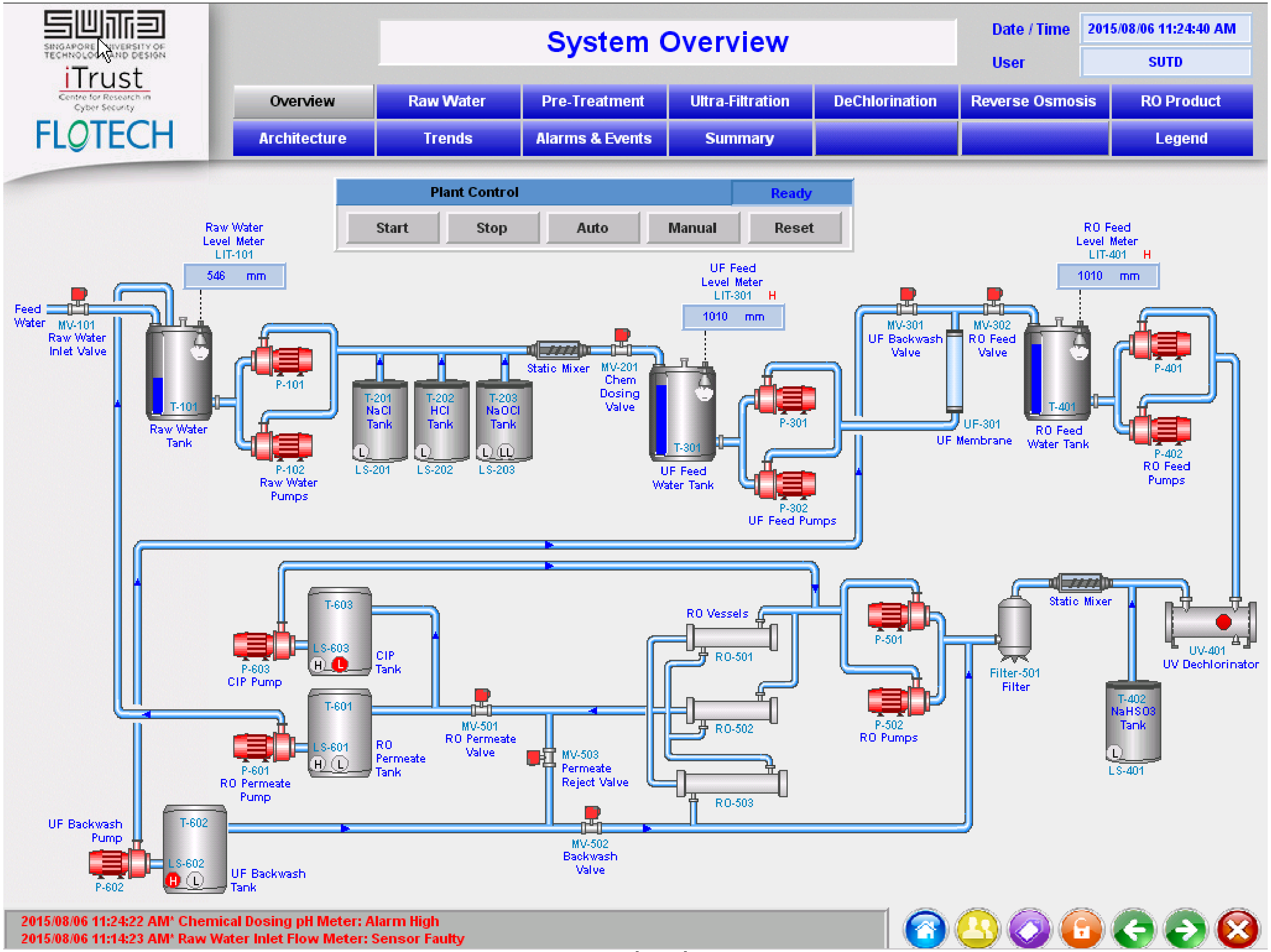
Simplified PLC Block Diagram



Supervisory Control and Data Acquisition (SCADA)

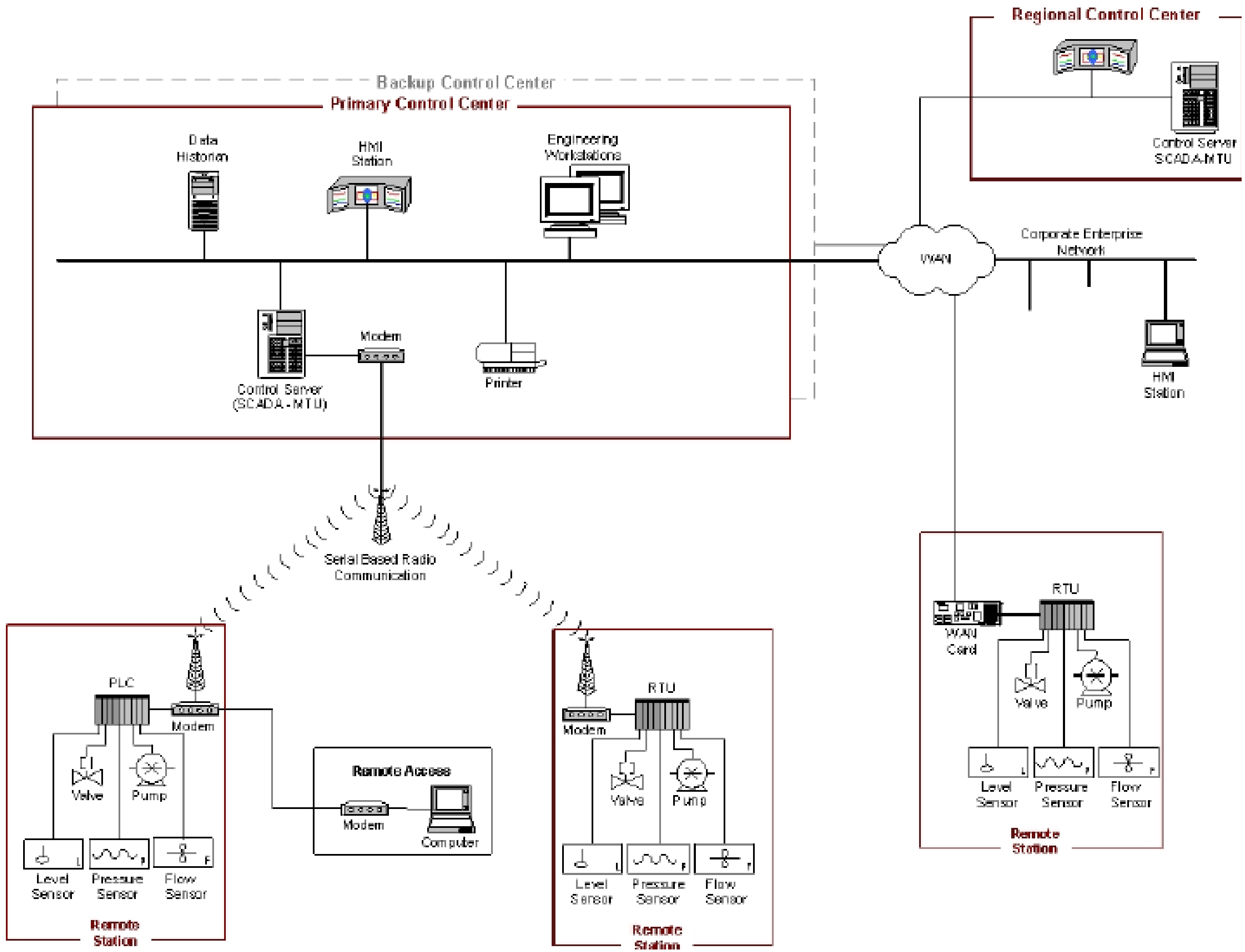
- On top of the basic control, SCADA systems can operate
- The SCADA system will supervise running systems and control actions by the PLCs
  - Visualizations to allow interpretation by human operators
  - SCADA can also take over control from local unit
  - SCADA will also connect to other business units to provide process data
  - Historian servers will store measured process data
- Problems:
  - How to connect remote sensors or actuators to SCADA?
  - How to connect multiple PLCs together to exchange data?

SCADA visualization example



Source: SWaT Testbed

Legacy SCADA networking

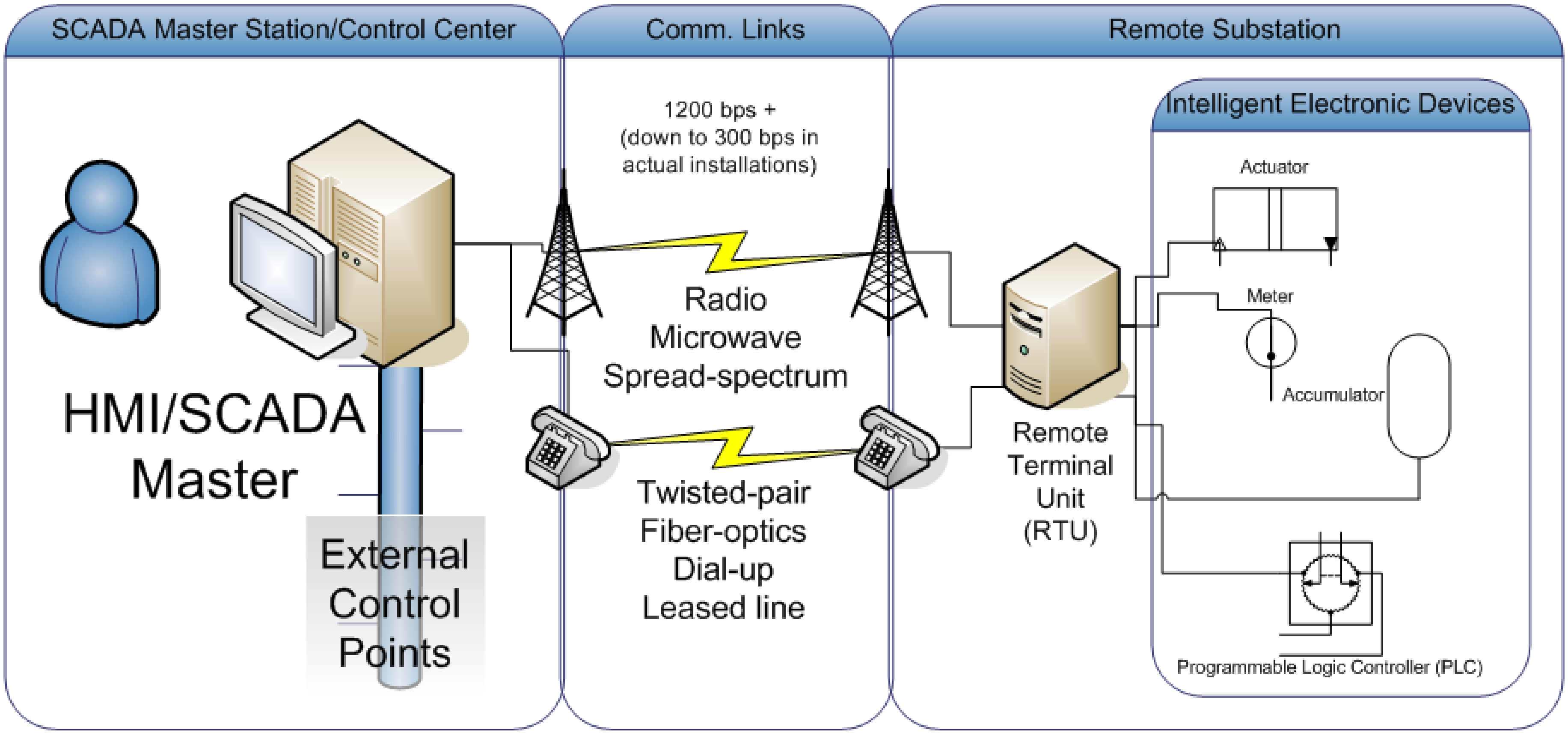


Source: Stouffer, Falco, Scarfone, "Guide to Industrial Control Systems (ICS) Security", NIST SP 800-82, 2011

Comments on legacy networking

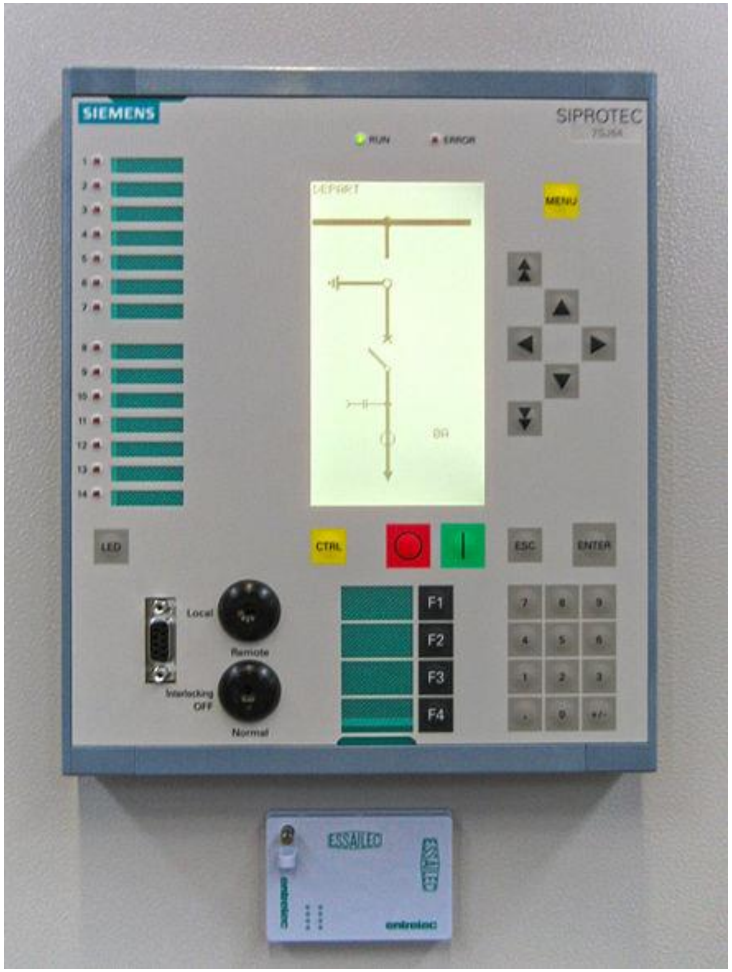
- Industrial components can have a long lifespan (30+ years)
  - This leads to range of technological generations in one system
- Large diversity in Layer communication standards on all layers
  - Analog (e.g. current based), RS-232, proprietary bus systems
  - Up-links via modems (phone lines), satellite, own lines
- Integration of new components into old comm. structure hard
- Heterogeneity is hard to manage, understand, expand
  - Proprietary solutions are often also more expensive. . .
- Likely solution to this problem:
  - Convert everything to run over Ethernet
  - Integrate all communication into few local networks
  - Use tunneling of legacy protocols over TCP/IP
  - But this standardization also increases security exposure

Example smart grid scenario for DNP3



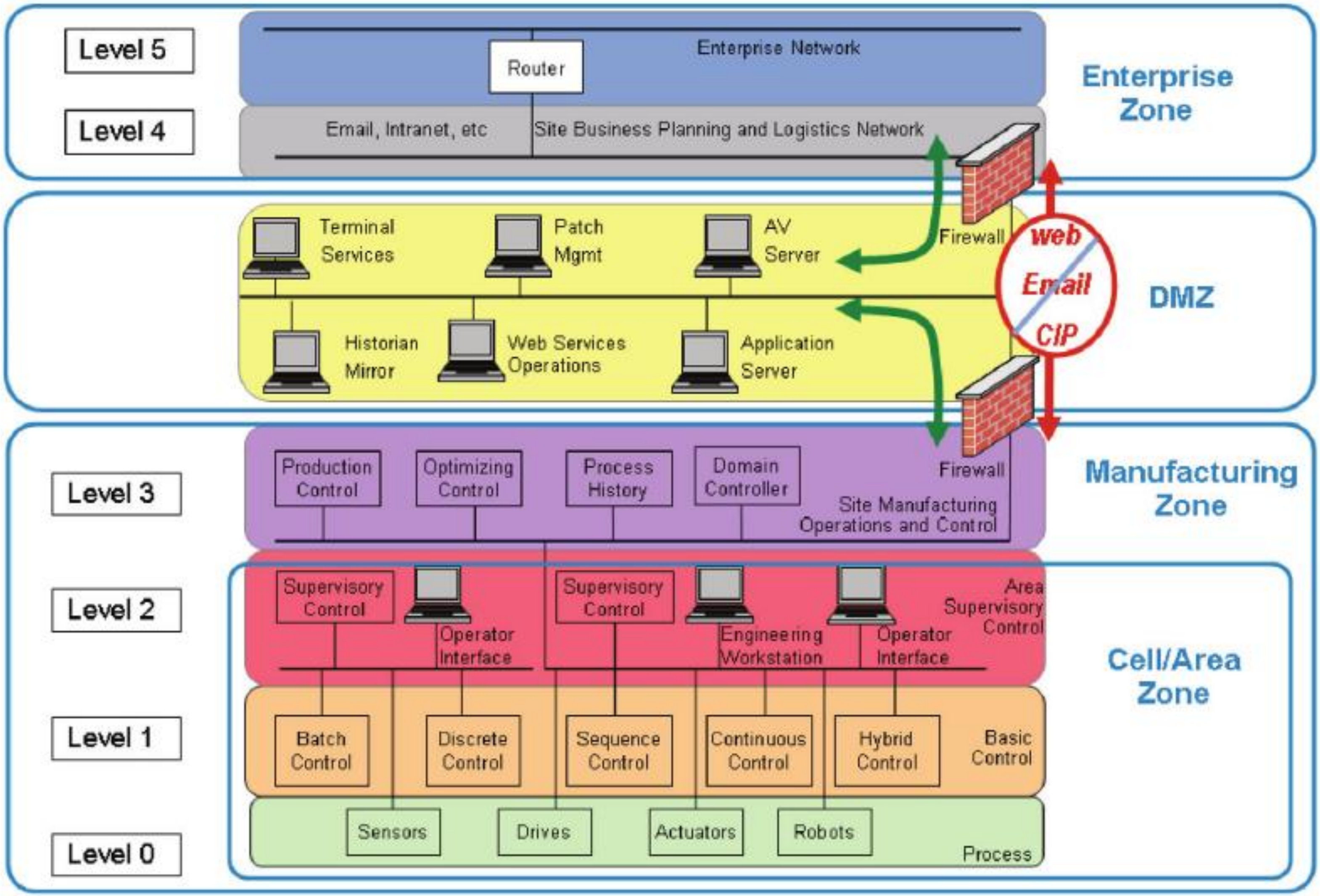
Typical RTU and IED

RTU: Remote Terminal Unit



IED: Intelligent Electronic Device

Future Networking Architecture



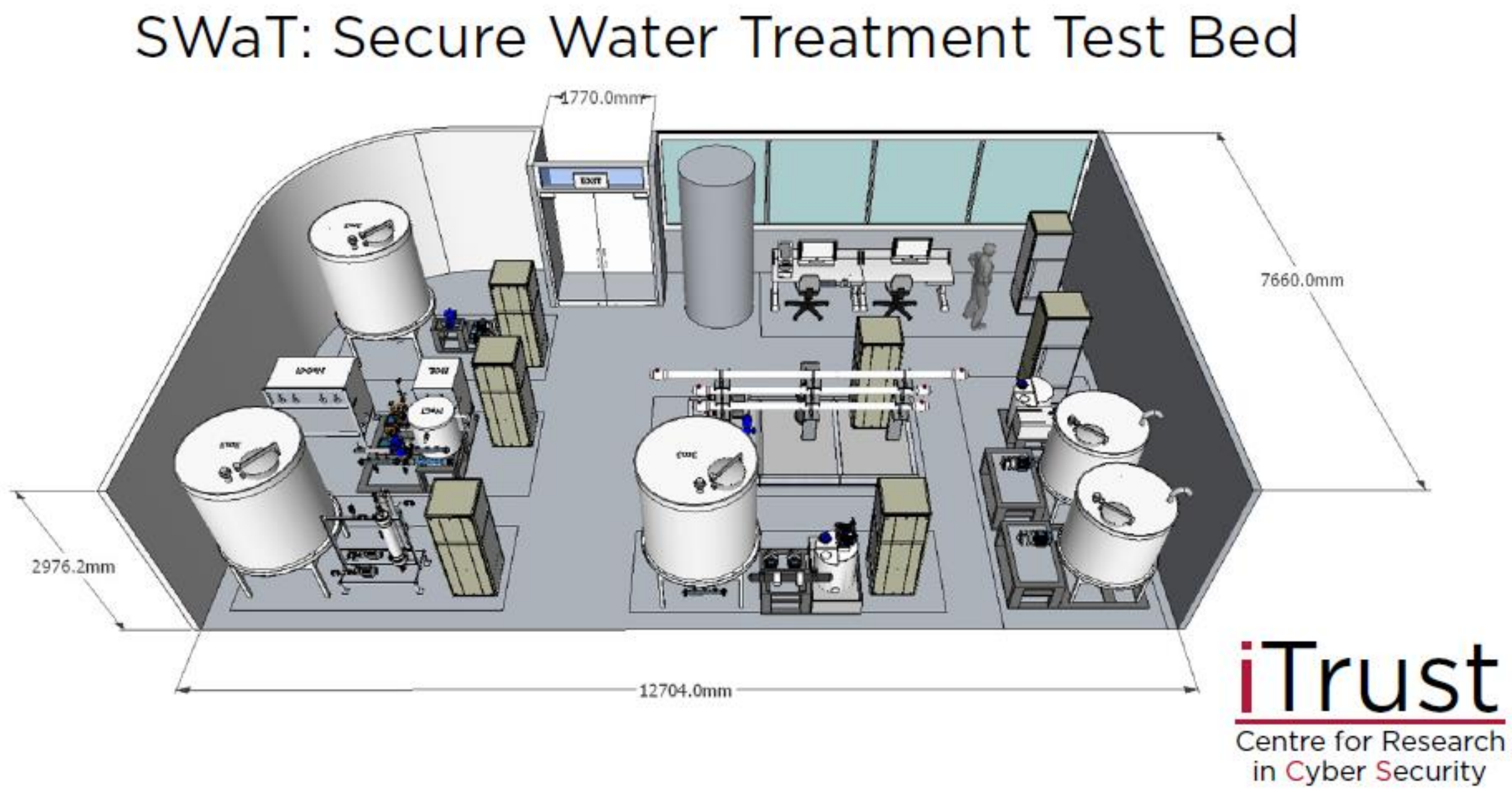
Source: Cisco, architecture for industrial control system security

DMZ

- In computer security, a DMZ or **demilitarized zone** (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.
- The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled. The DMZ functions as a small, isolated network positioned between the Internet and the private network.

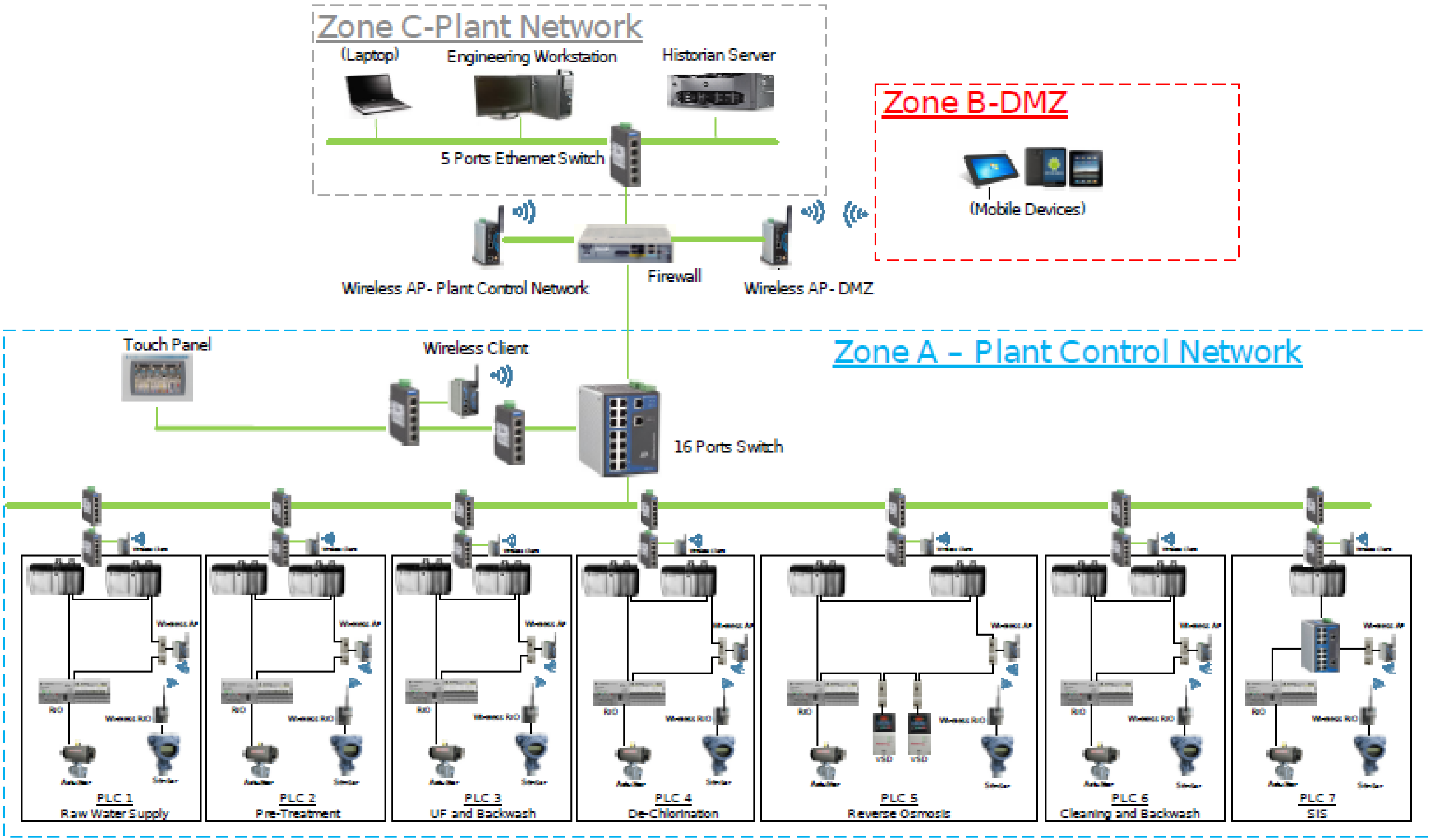
Source: Wikipedia

SwaT Testbed Physical Process



- Secure Water Treatment (SWaT) is a testbed at SUTD
- Realistic industrial process with control automation
- Operational since March 2015, used by iTrust security research

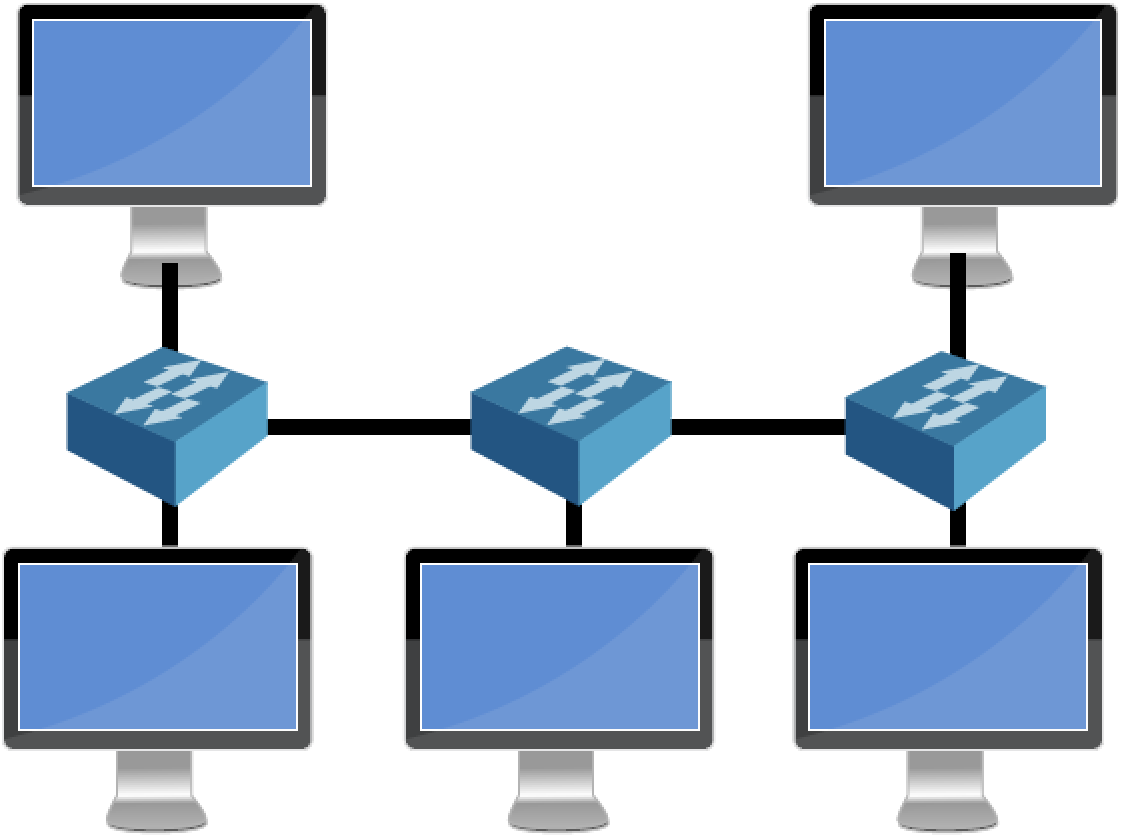
SWaT Testbed



Redundancy for Ethernet

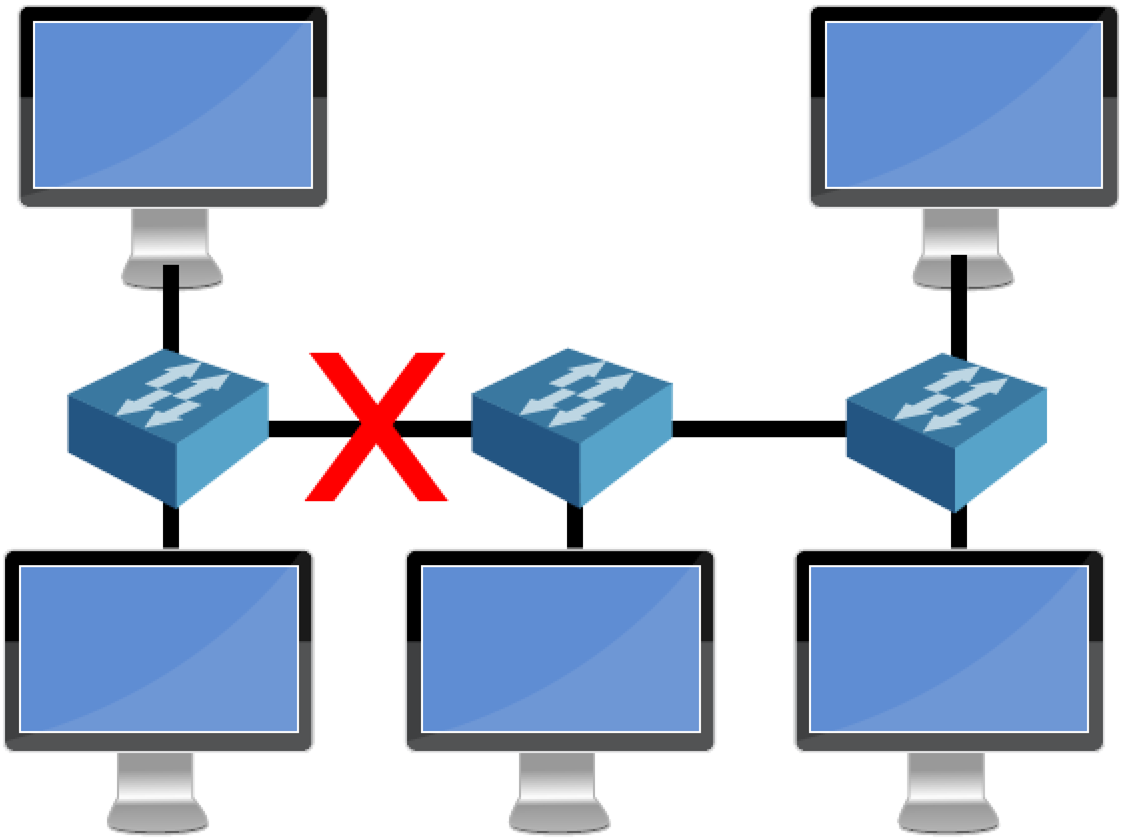
- So far, we have mostly discussed star topologies for Ethernet
  - Minimizes the number of links required
- What happens if one of those links fails?
  - The connection will be lost
- How to introduce redundancy?
  - Just adding another switch will create loops

Link Layer Loops



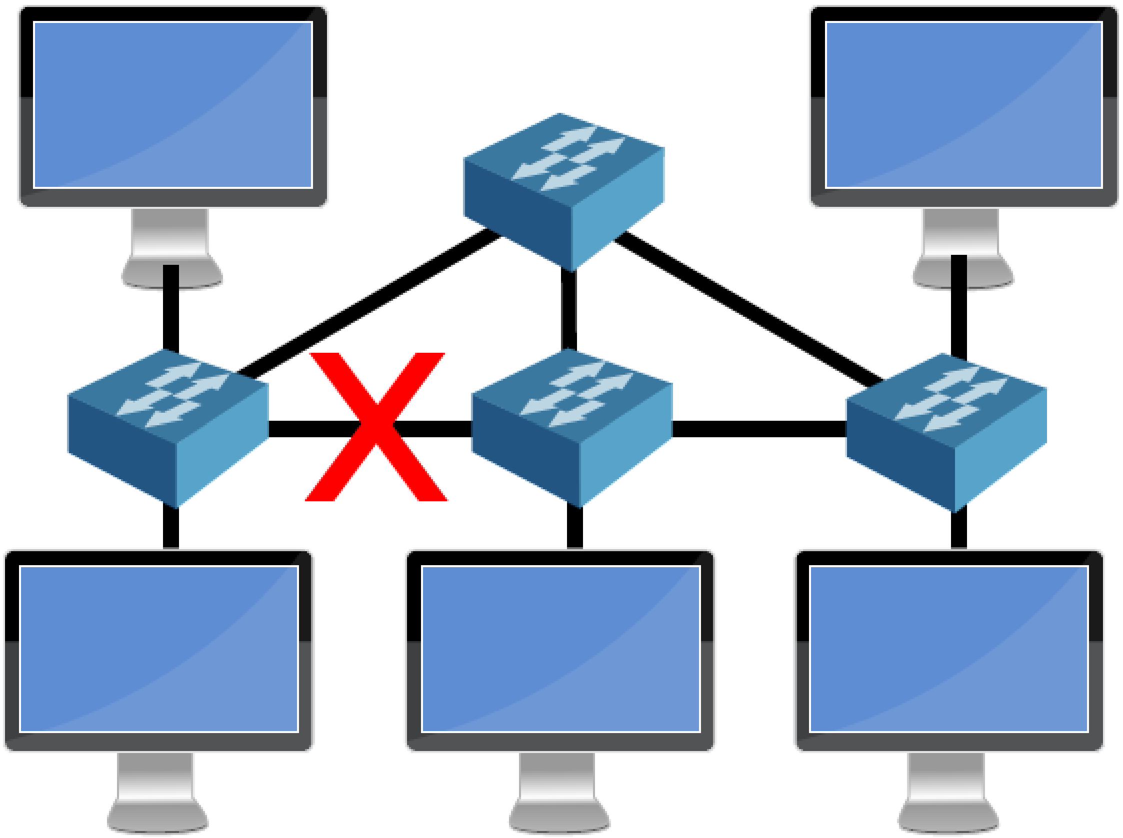
Normal star topology setup

Link Layer Loops



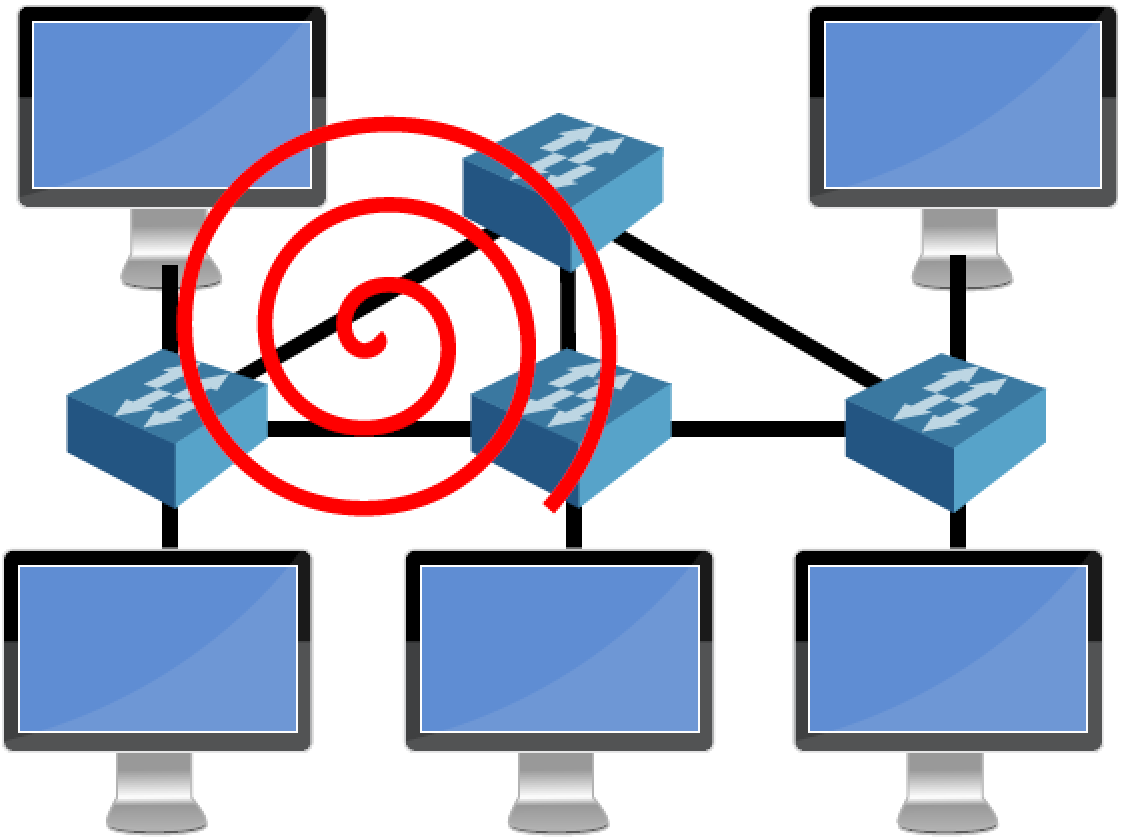
Link failure disconnects network

Link Layer Loops



Could we just add a redundant switch?

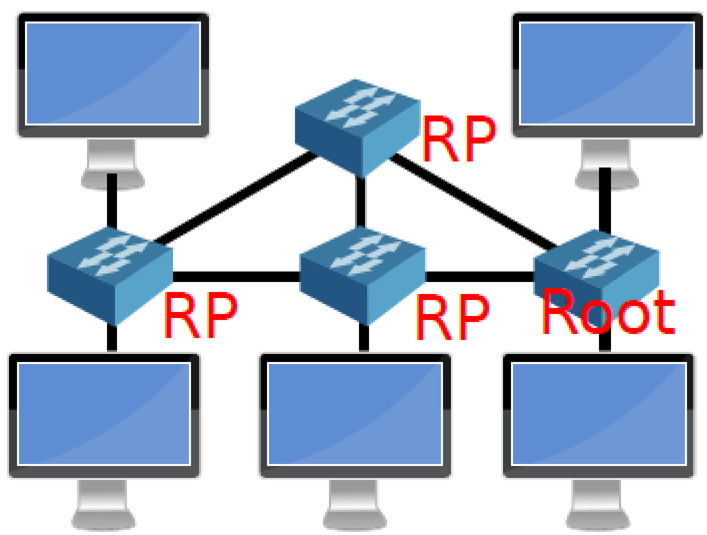
Link Layer Loops



In normal operations, that can lead to link layer loops

Spanning Tree Protocol (STP)

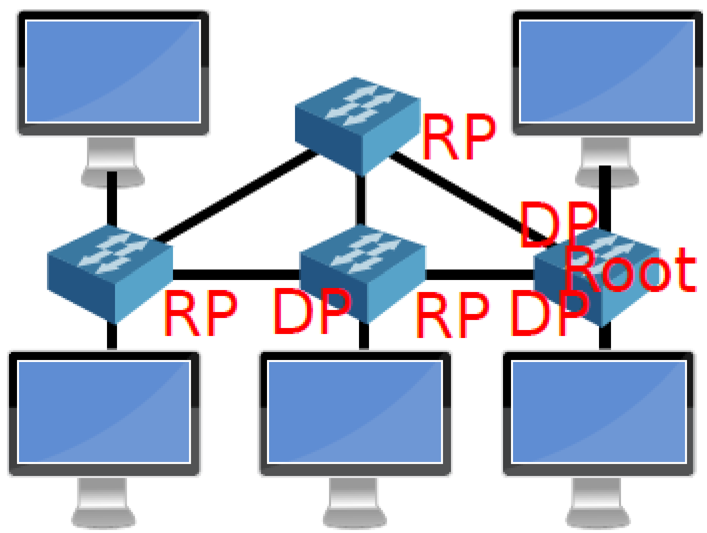
- Protocols such as STP can be used to detect and prevent link layer loops
- All switches communicate with each other via STP
- One switch is a root switch, used as reference to build spanning
- tree
- STP ensures that all switches stay connected to the root switch
  - all unnecessary connections are temporally disabled



All switches determine Root Ports (RP)

Spanning Tree Protocol (STP)

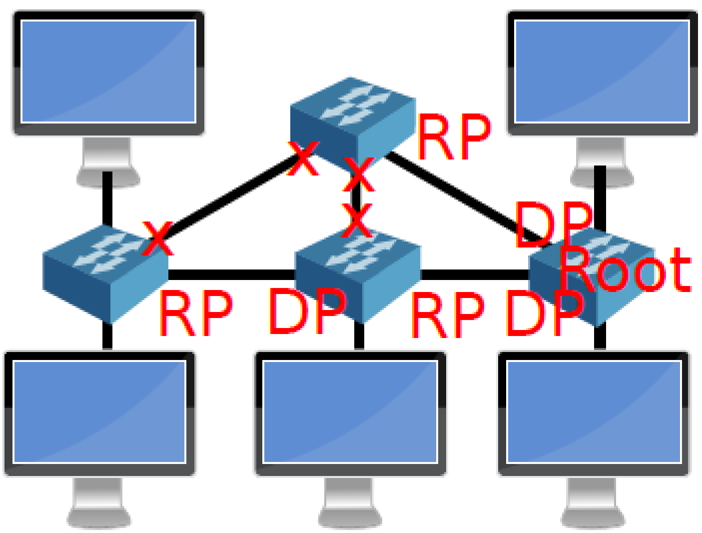
- Protocols such as STP can be used to detect and prevent link layer loops
- All switches communicate with each other via STP
- One switch is a root switch, used as reference to build spanning
- tree
- STP ensures that all switches stay connected to the root switch
  - all unnecessary connections are temporally disabled



Corresponding ports are Designated Ports (DP)

Spanning Tree Protocol (STP)

- Protocols such as STP can be used to detect and prevent link layer loops
- All switches communicate with each other via STP
- One switch is a root switch, used as reference to build spanning
- tree
- STP ensures that all switches stay connected to the root switch
    - all unnecessary connections are temporally disabled

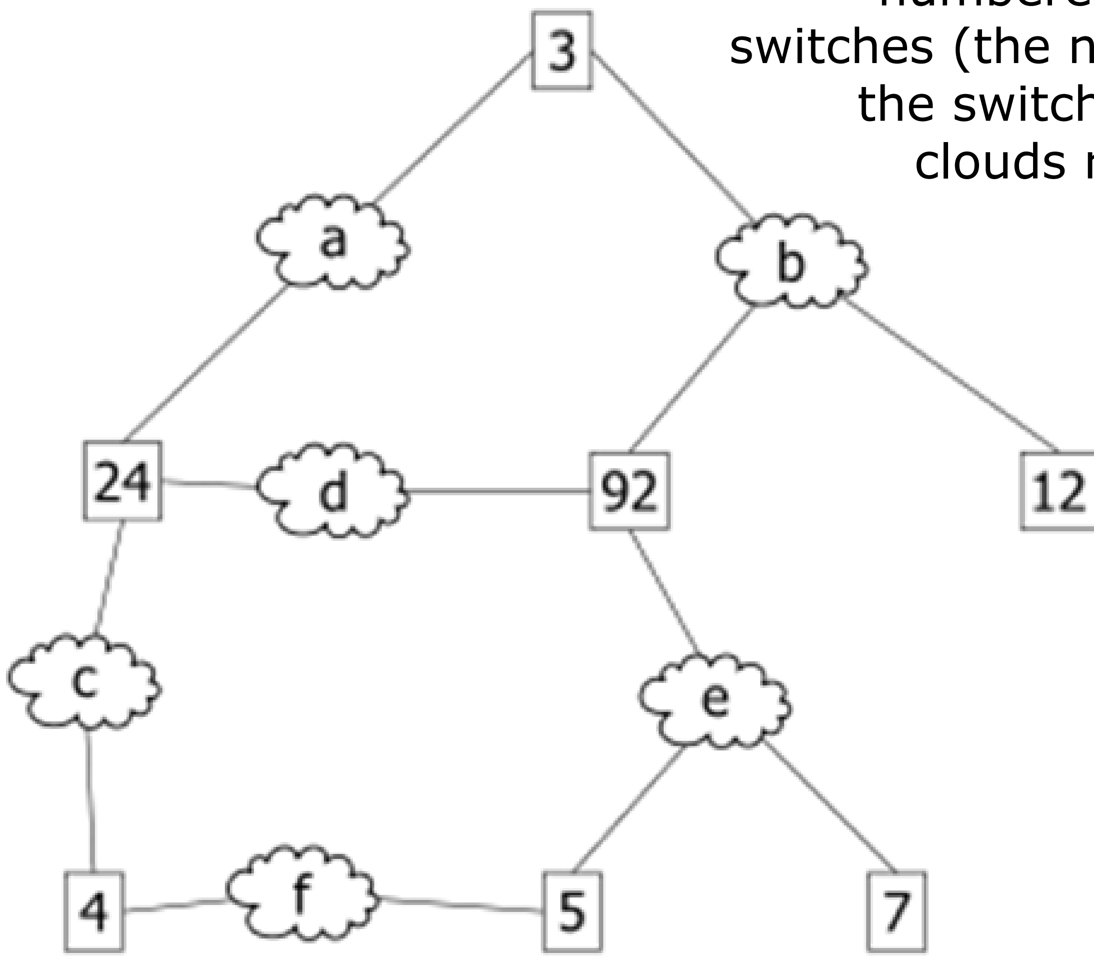


All non-RP/DP ports to other switches are closed temporarily

Spanning Tree Protocol-1

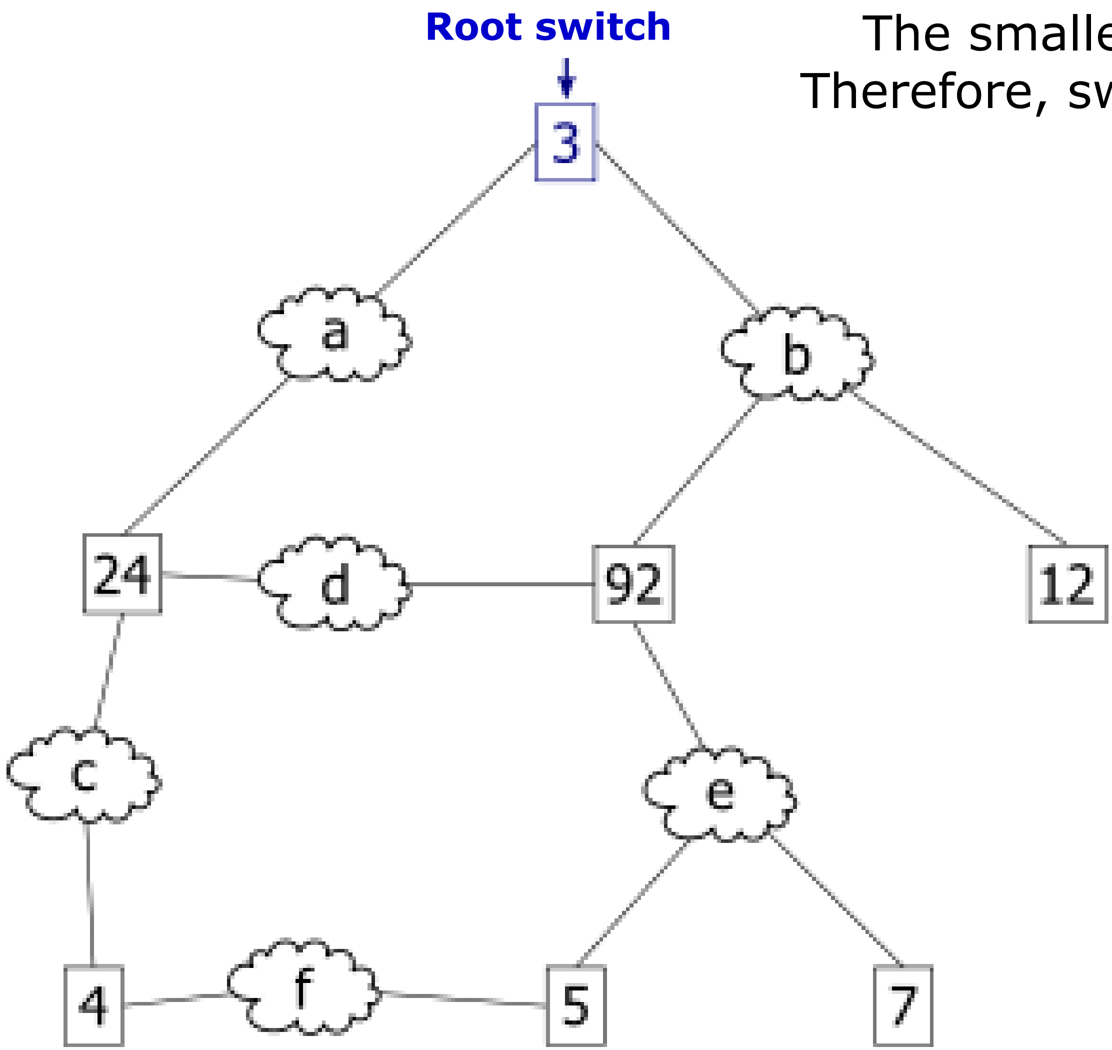
SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

An example network. The numbered boxes represent switches (the number represents the switch ID). The lettered clouds represent network segments.

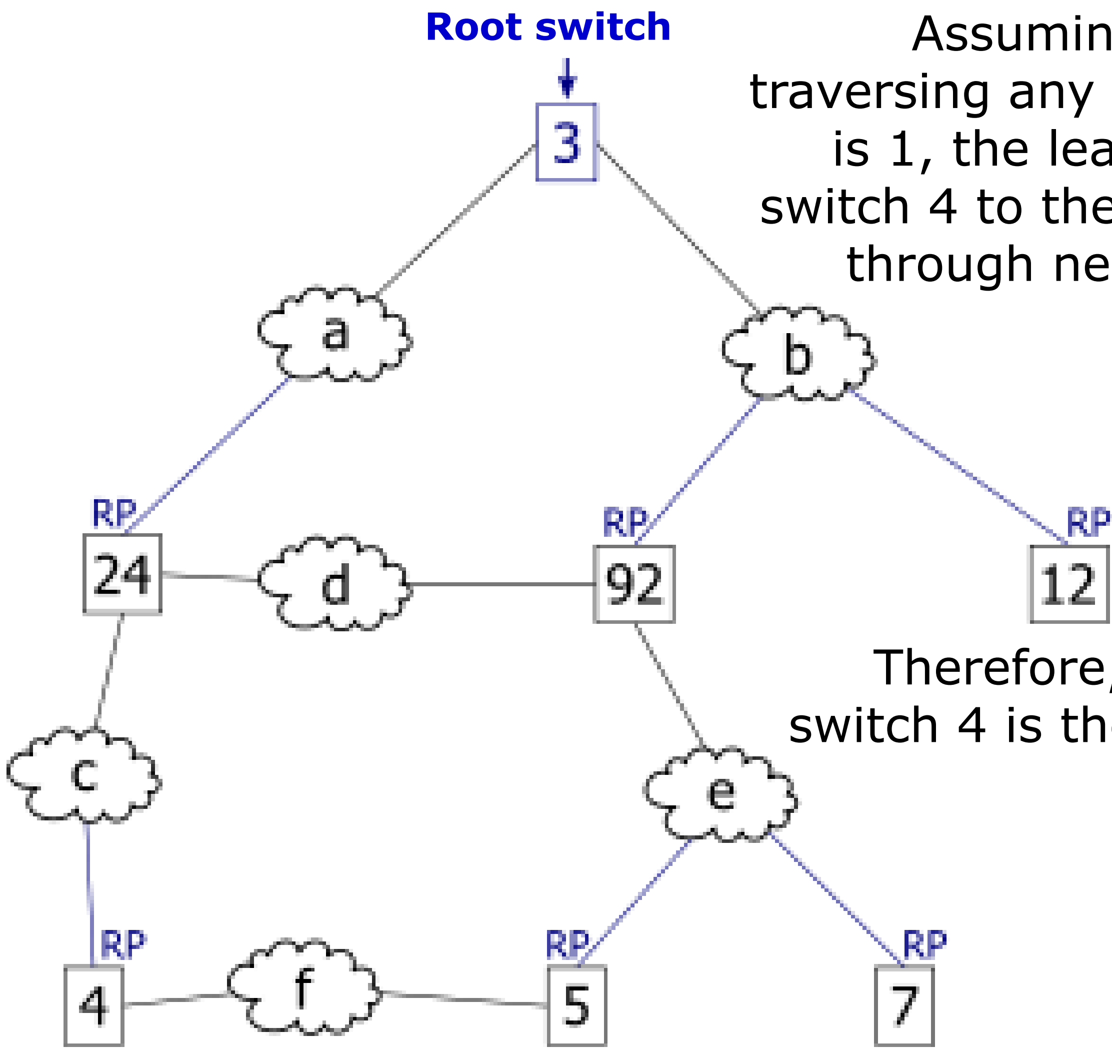


Spanning Tree Protocol-2

The smallest switch ID is 3. Therefore, switch 3 is the root switch.



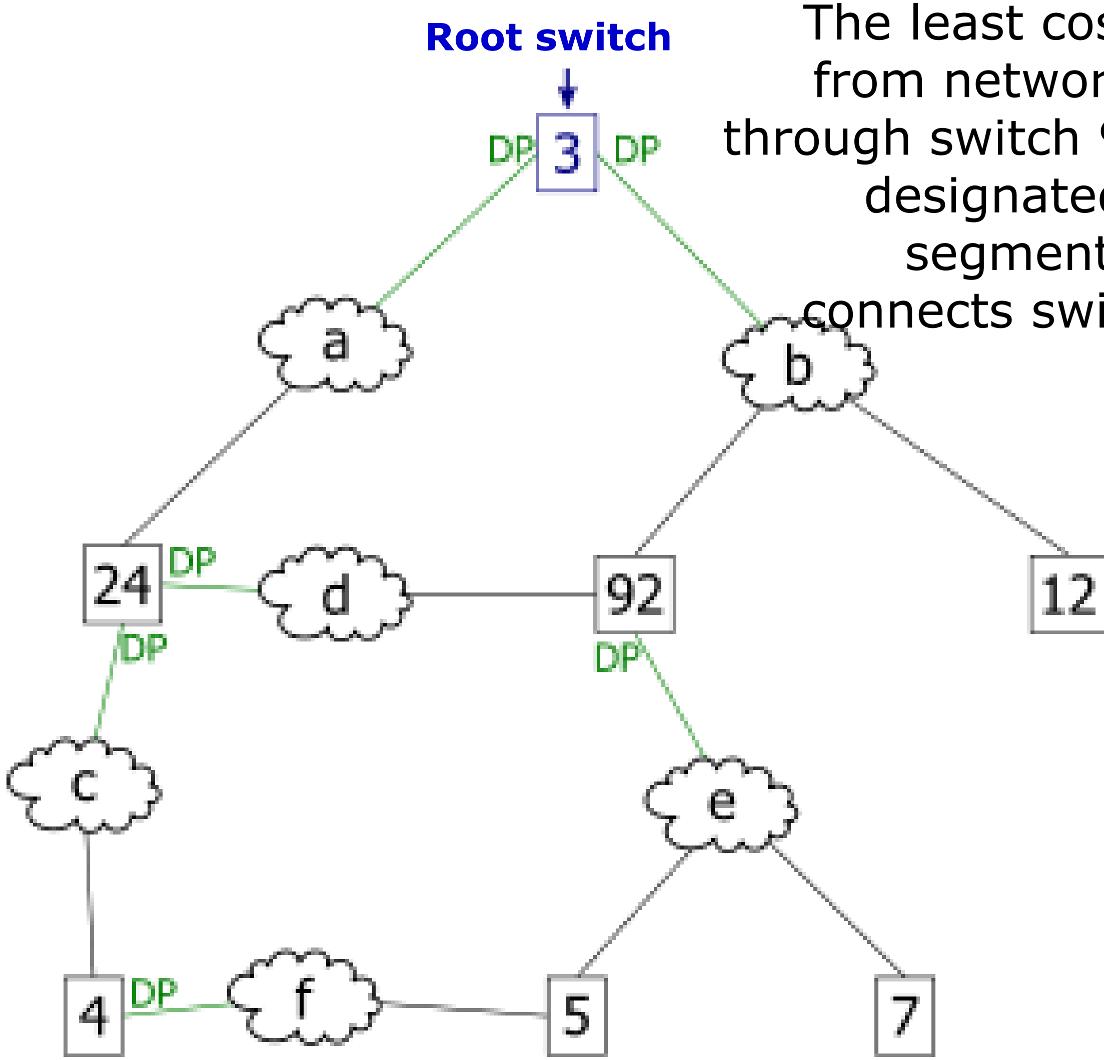
Spanning Tree Protocol-3



Assuming that the cost of traversing any network segment is 1, the least cost path from switch 4 to the root switch goes through network segment c.

Therefore, the root port for switch 4 is the one on network segment c.

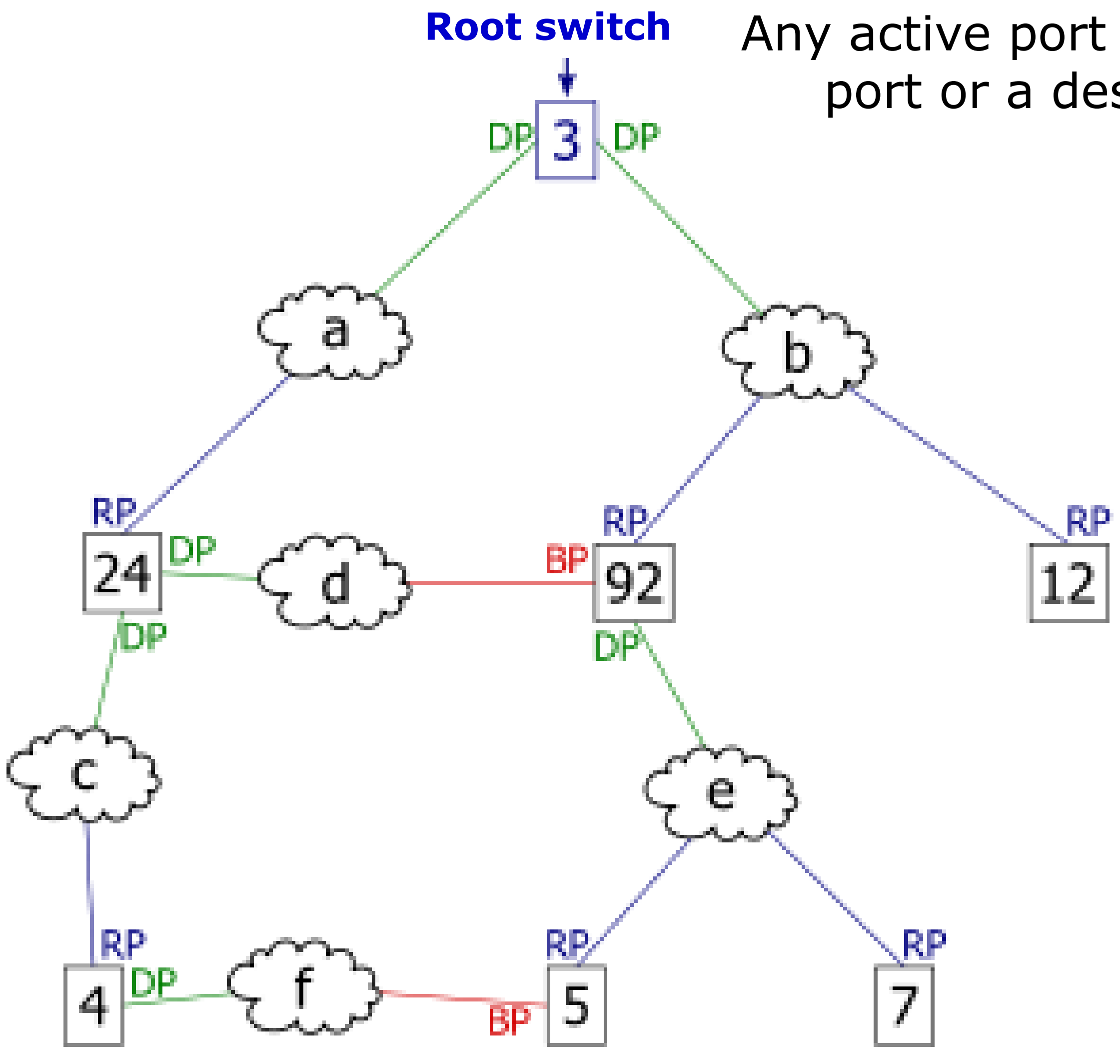
Spanning Tree Protocol-4



The least cost path to the root from network segment e goes through switch 92. Therefore, the designated port for network segment e is the port that connects switch 92 to network segment e.

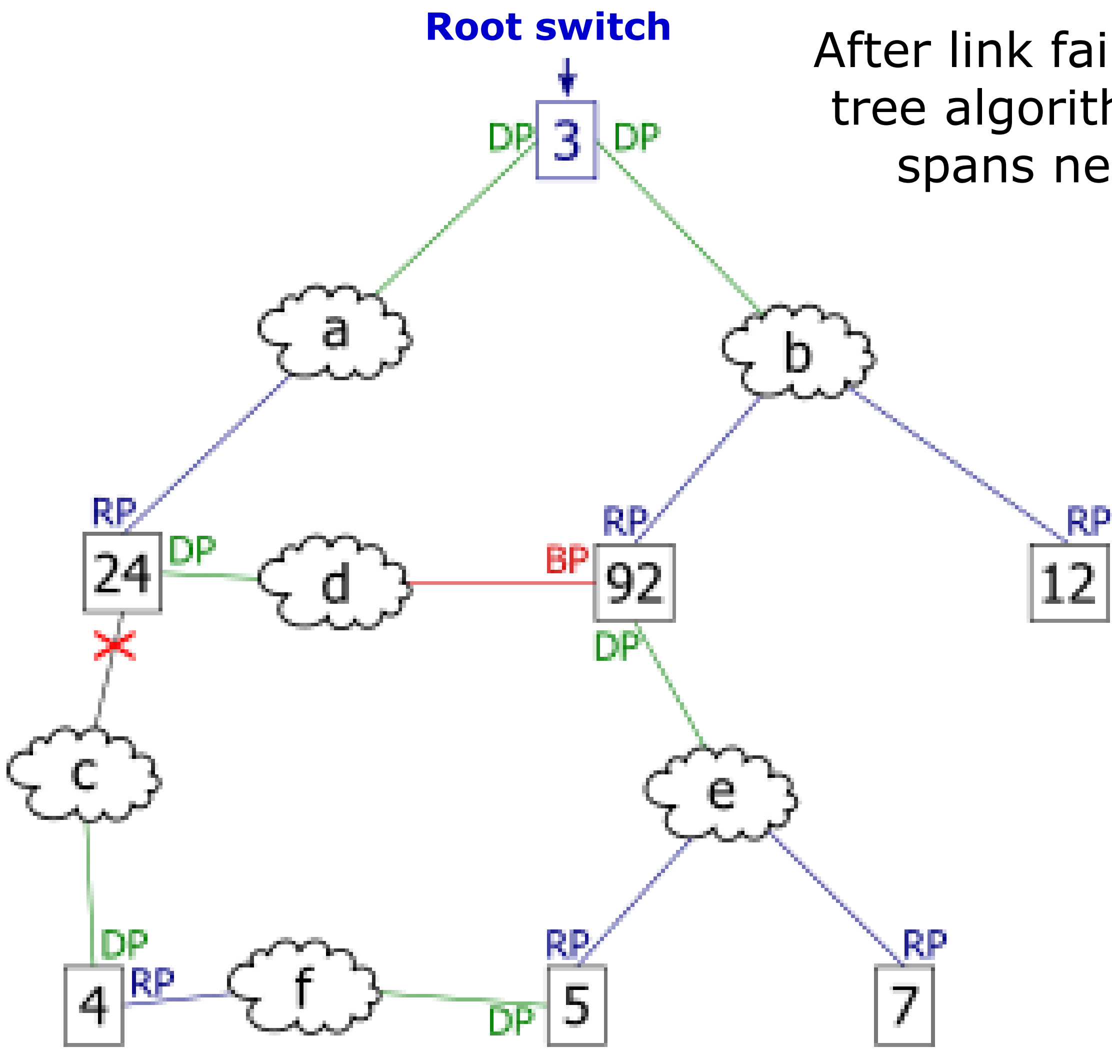
Spanning Tree Protocol-5

Any active port that is not a root port or a designated port is a blocked port.



Spanning Tree Protocol-6

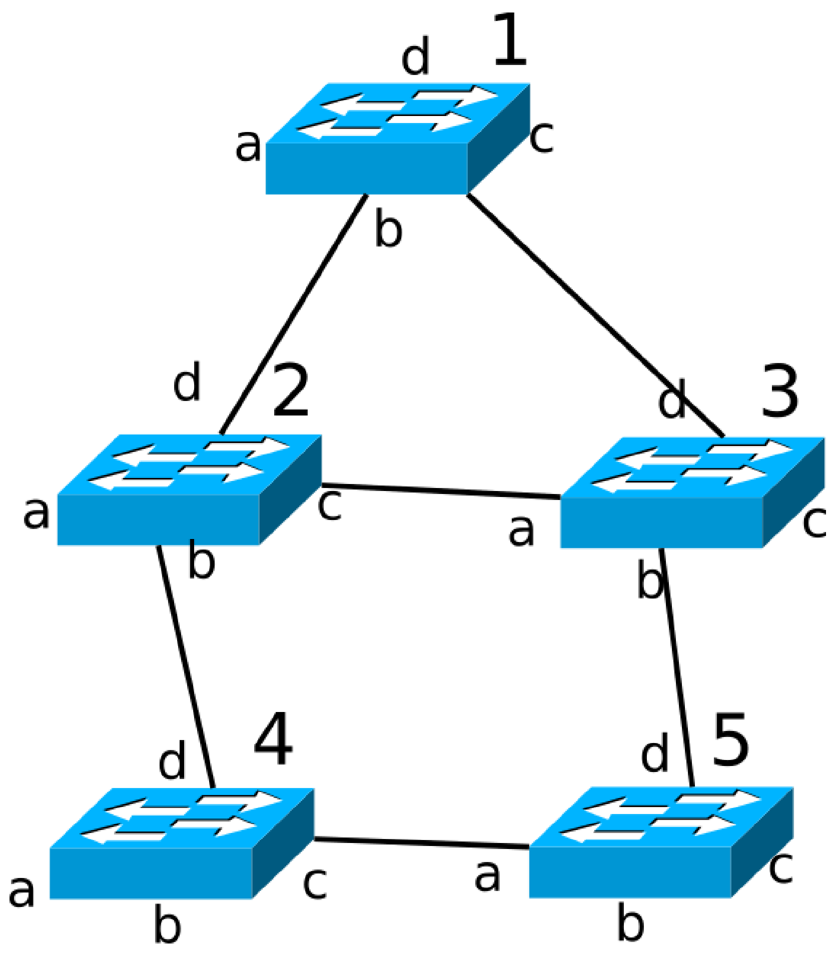
After link failure the spanning tree algorithm computes and spans new least-cost tree.



Activity 13: Shortest Spanning Tree algorithm

In the figure five switches (aka bridges) are shown, labelled 1 through 5. The ports on each switch are labelled a, b, c and d as shown.

1. Taking switch 1 to be the Root (R), use the STP algorithm build a spanning tree for this network. Assume that the links 2c-3a and 4c-5a are disabled while the remaining links belong to the spanning tree. Assign labels to each port as either RP, DP or BP based on whether the port is a Root Port, Designated Port or Blocked Port.
2. Assume that the link 2b-4d fails, thereby isolating switch 4. Reassign labels using the STP so that every port on every switch can be reached.



Submit on eDimension

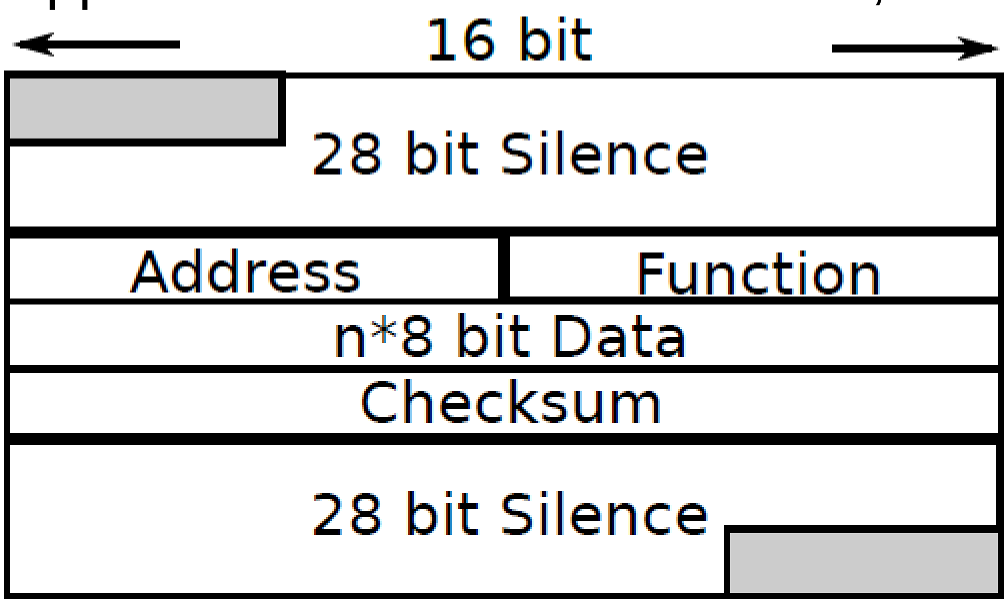
Protocols for Control Networks

Protocols for Control Networks

- A large number of industrial protocols exist:
  - Modbus
  - DNP3
  - DeviceNet, ControlNet, CompoNet (AB/Rockwell)
  - ProfiBus
- These usually specify several layers (from PHY to application)
- The devices talking these standards are old and will not be replaced in near future
- How to integrate all of them?

Modbus

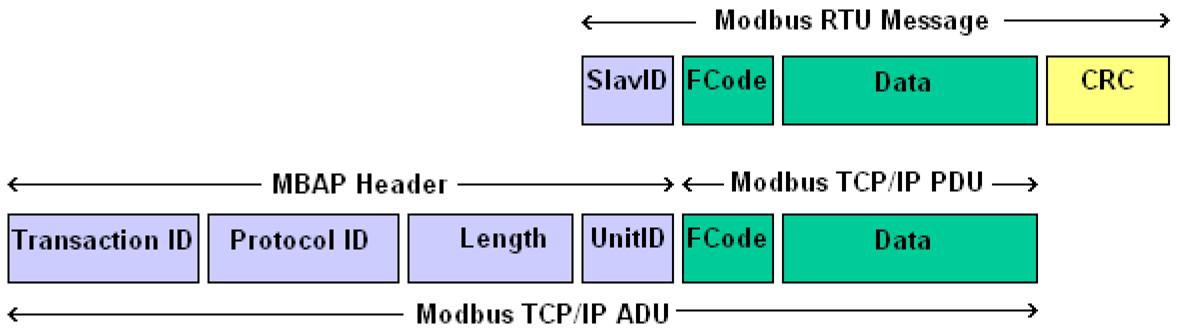
- Modbus is a very simple and common automation protocol
- Implements a basic remote memory access (read/write) between master and slaves
- Approximately Link-layer and above protocol
- Often implemented on a 2 wire bus (RS-485)
  - RS-485 defines the Physical layer
- Modbus supports two modes: ASCII based, or *RTU mode*



Modbus header (RTU mode)

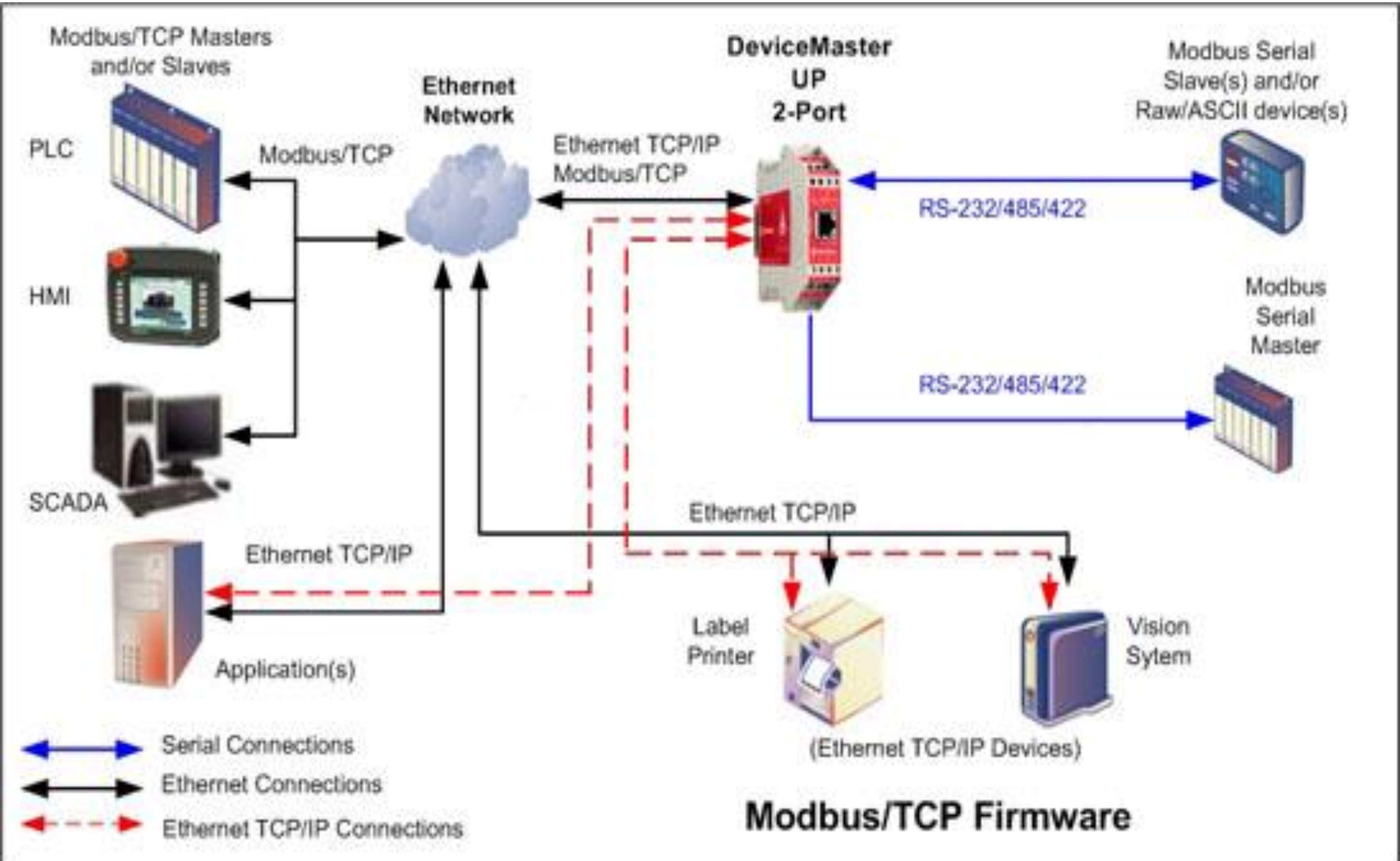
Transport over TCP / IP

- To unify the physical layer, industrial protocols are encapsulated in TCP/IP
- So-called gateway-devices will talk the proprietary protocol to the legacy device, and put the data content into a TCP stream to the identified target gateway.
- Examples for this: ModBus/TCP



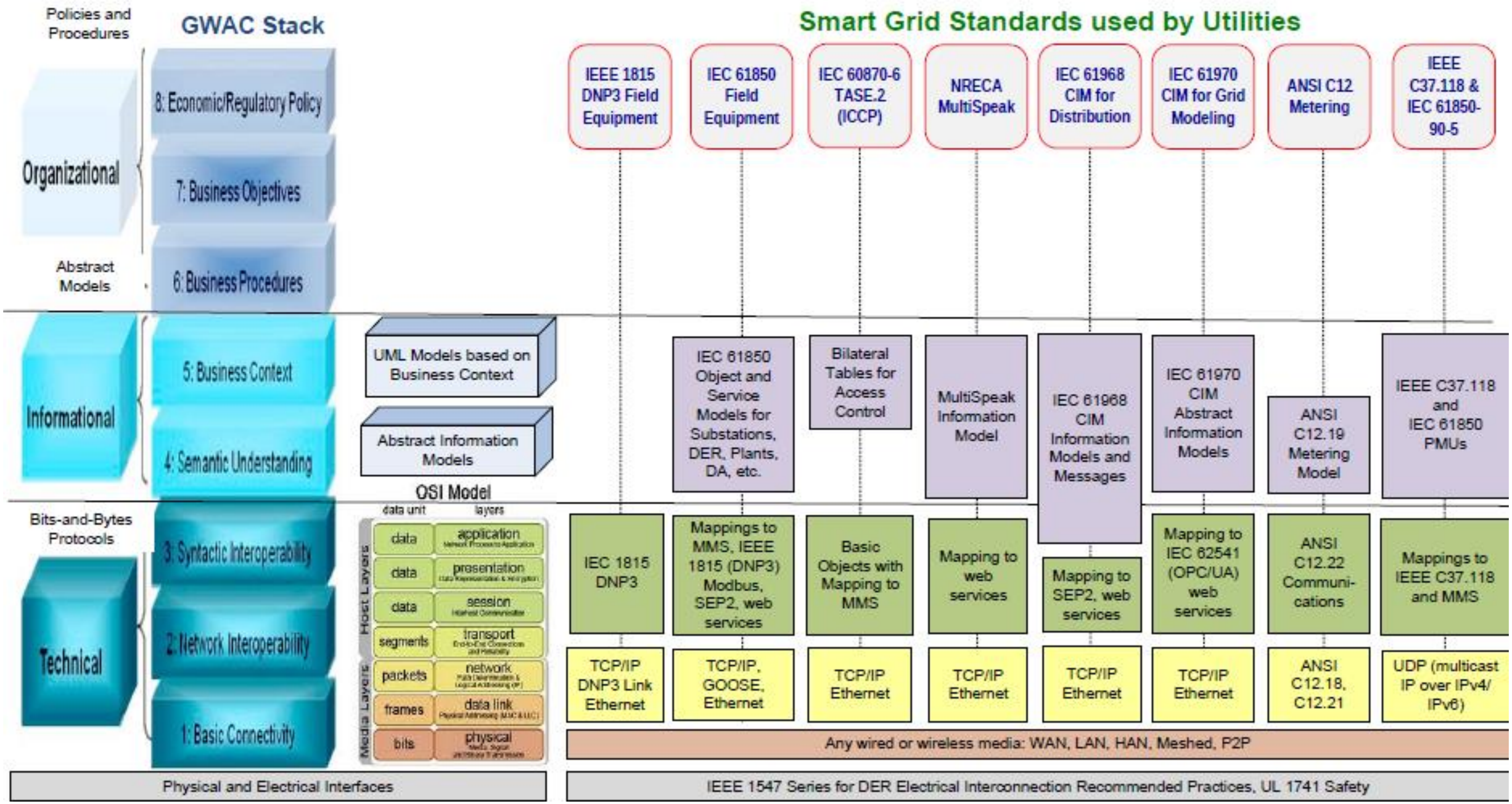
Source: simplymodbus.ca

Example Modbus/TCP setup



Source: Comtrol.com

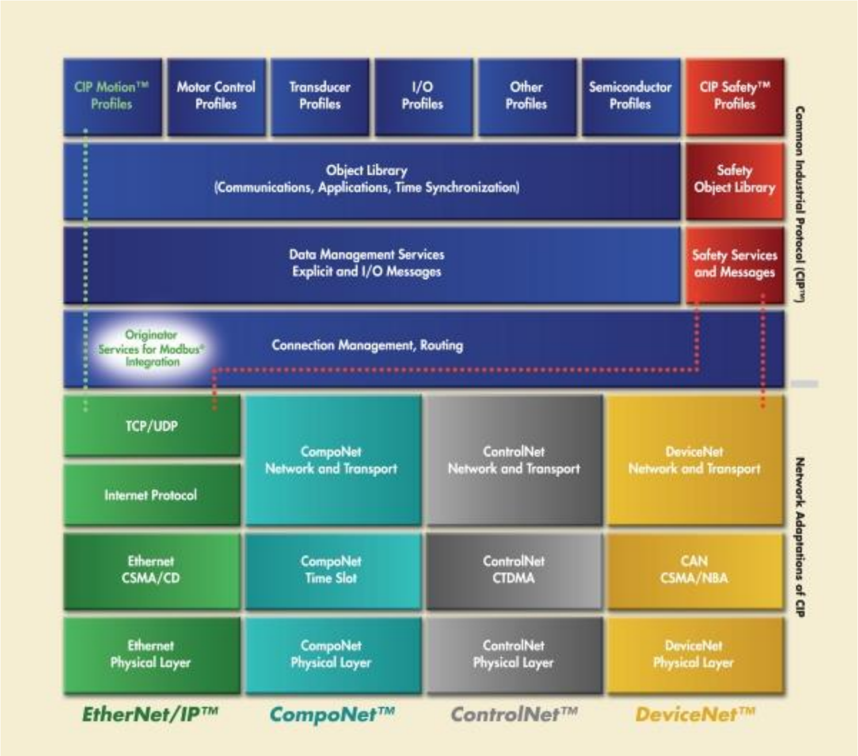
Example: Smart Grid Standards over IP



Source: Frances Cleveland, fcleve@xanthus-consulting.com

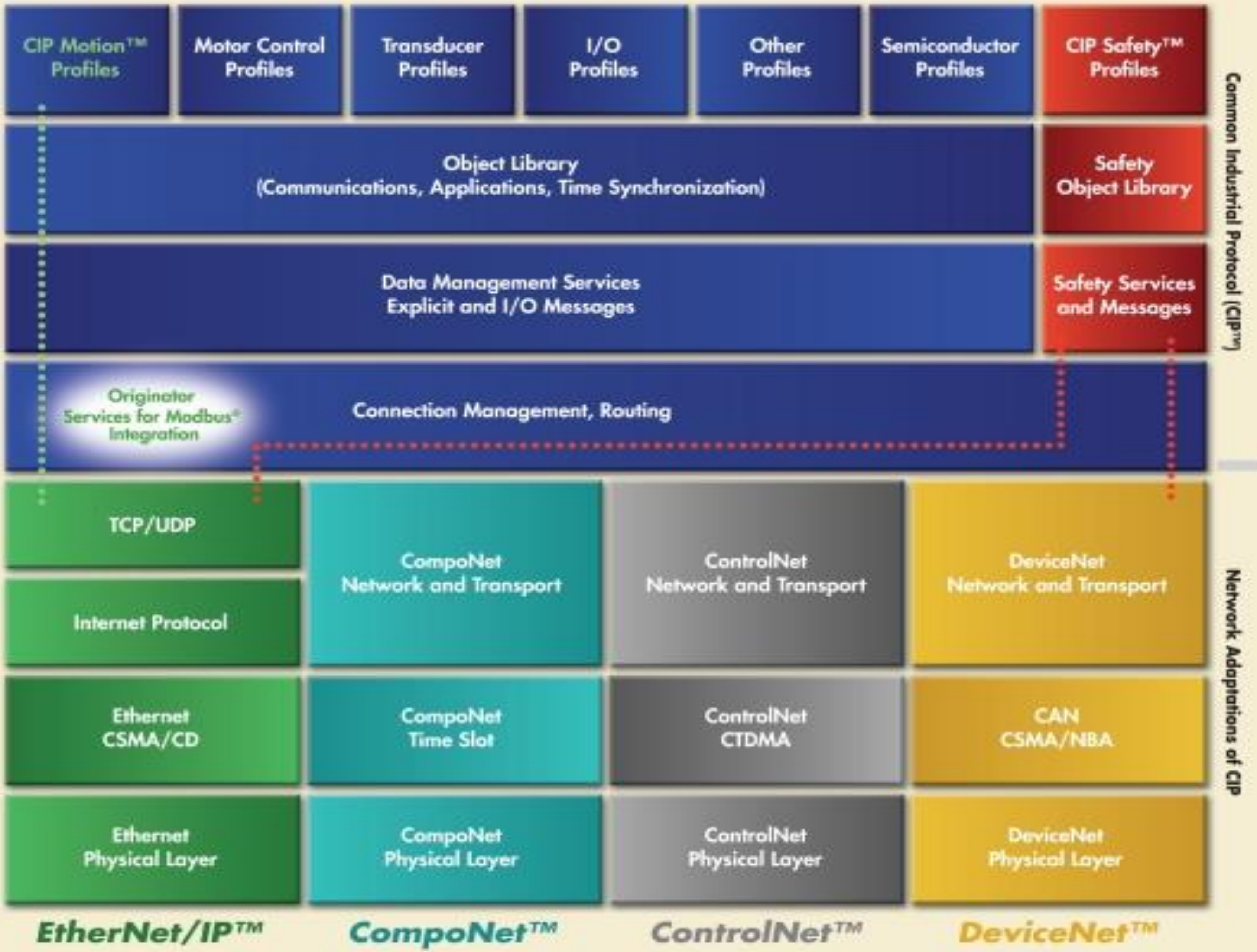
Common Industrial Protocol (CIP)

- Standardization efforts on the application layer resulted in CIP
- CIP run on top of custom transport
  - CIP over CAN: DeviceNet
  - CIP over ControlNet (coaxial)
  - CIP over CompoNet (2-wire bus)
  - CIP over TCP/IP: EthernetIP



Common Industrial Protocol (CIP)

- CIP contains a suite of messages and services for the collection of manufacturing automation applications – control, safety, synchronization, motion, configuration and information.
- It allows users to integrate manufacturing applications with enterprise-level Ethernet networks and the Internet.
- Supported by hundreds of vendors around the world
- Media-independent. CIP provides a unified communication architecture throughout the manufacturing enterprise.
- It is used in EtherNet/IP, DeviceNet, CompoNet and ControlNet.
- ODVA is the organization that supports network technologies built on the Common Industrial Protocol (CIP). These also currently include application extensions to CIP: CIP Safety, CIP Motion and CIP Sync



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® Integration
Connection Management, Routing
Common Industrial Protocol (CIP™)
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
Network Adaptations of CIP
EtherNet/IP™
CompoNet™
ControlNet™
DeviceNet™

Conclusion

- In industrial control and automation
  - A large set of legacy communication standards and protocols exist
  - There is a trend towards unifying everything on top of TCP/IP
- Resulting protocols are for example:
  - Modbus/TCP
  - Ethernet/IP (really: CIP over TCP/IP)
- Integration allows shared commercial off-the-shelf infrastructure
  - But also increases exposure to remote attacks