SIU Southern Illinois University CARBONDALE

Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 6: Industrial Network Components

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

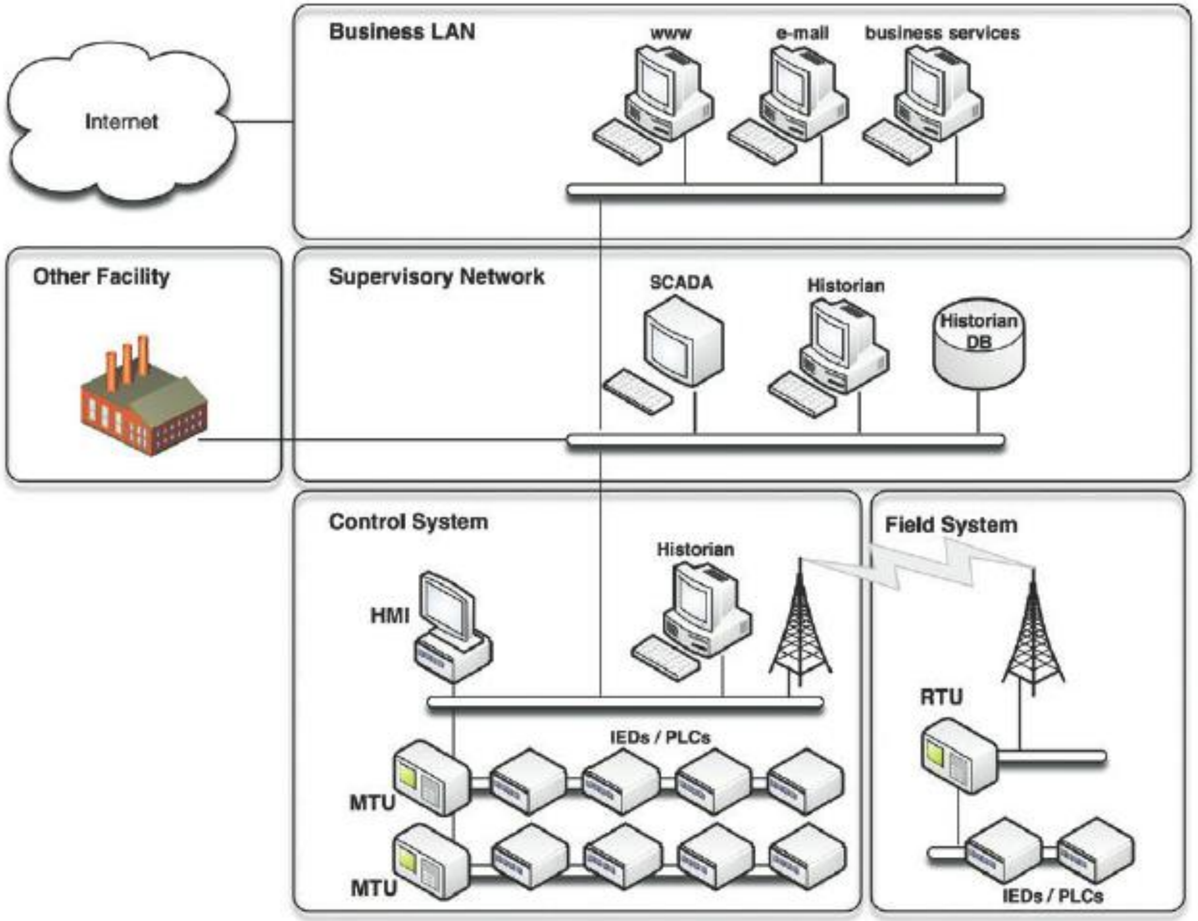
EMAIL: AYDEGER@CS.SIU.EDU

Outline

ICS Components

Different ICS Types

Recall: Sample Industrial Automated Control System Network



Industrial Network Components/Assets

Intelligent Electronic Devices (IEDs)

Programmable Logic Controllers (PLCs)

Remote Terminal Units (RTUs)

Human Machine Interface (HMI)

Supervisory Management Workstations

Data Historians

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

IED Functions

Protection

- Ex: detecting faults at a substation

Control

- Ex: provide a visual display and operator controls on the device front panel

Monitoring

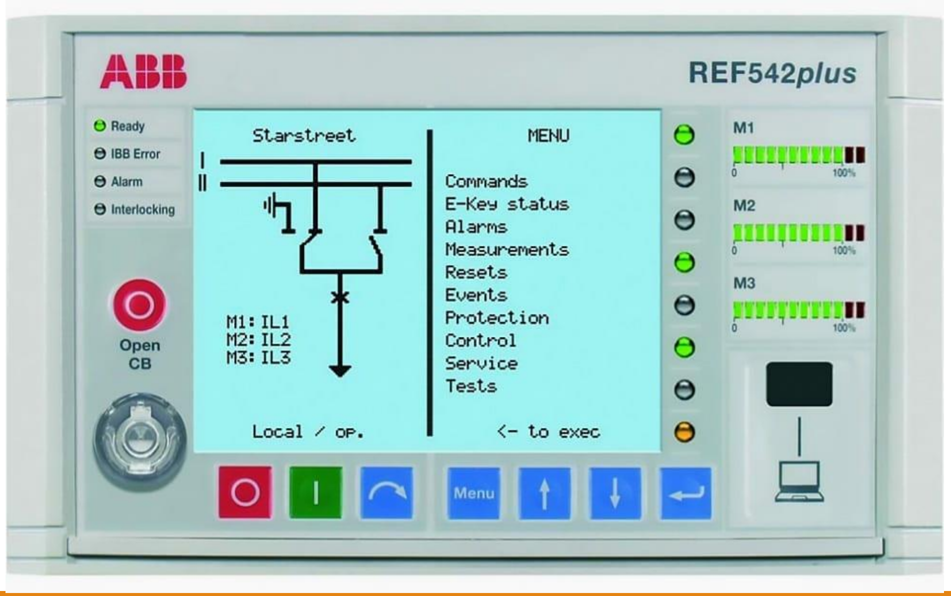
- Ex: report on the circuit breaker condition and record events

Metering

- Ex: may track power metrics

Communications

- Ex: to communicate with supervisory components



Programmable Logic Controller (PLC)

Specialized computer used to automate functions within industrial networks

Materially hardened

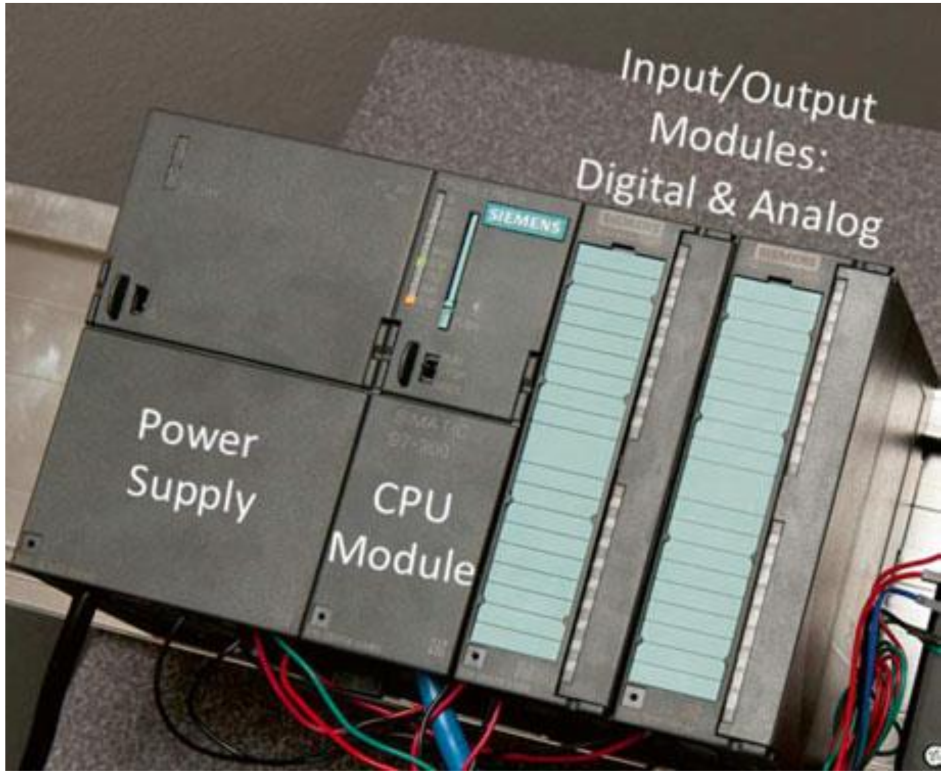
- May be <u>specialized</u> for specific industrial uses with multiple specialized inputs and outputs
- Making them <u>suitable for deployment</u> on a production floor
  - 10-15 years of deployment, maybe even longer

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

PLC Components

- Power supply
- Central processing unit (CPU)
- Communications interface
- Input/output (I/O) module(s)
  - Digital or analog



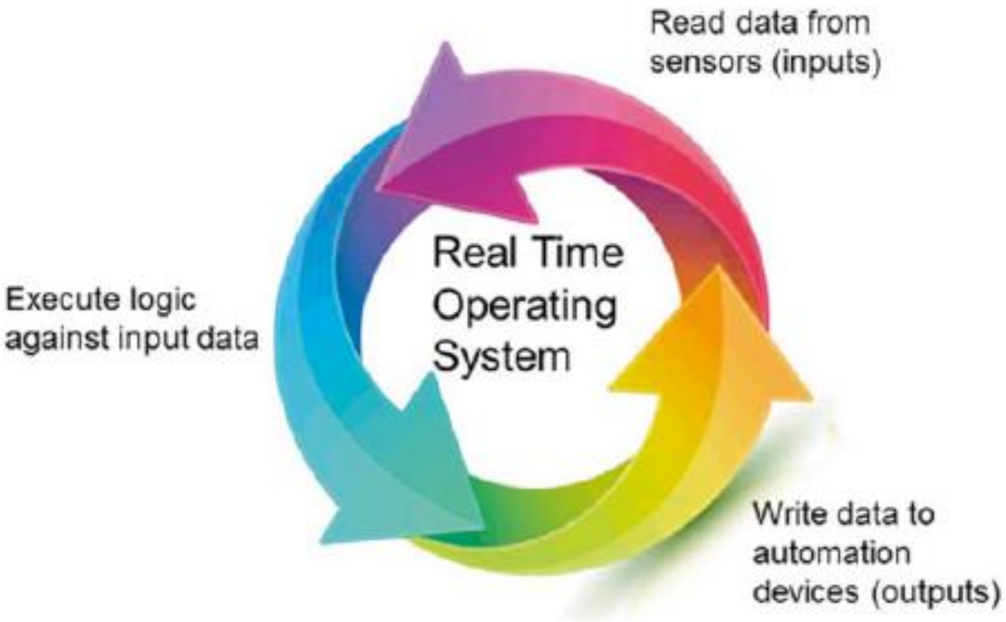
Siemens S7-300 PLC

PLC Cycle

Read

Execute

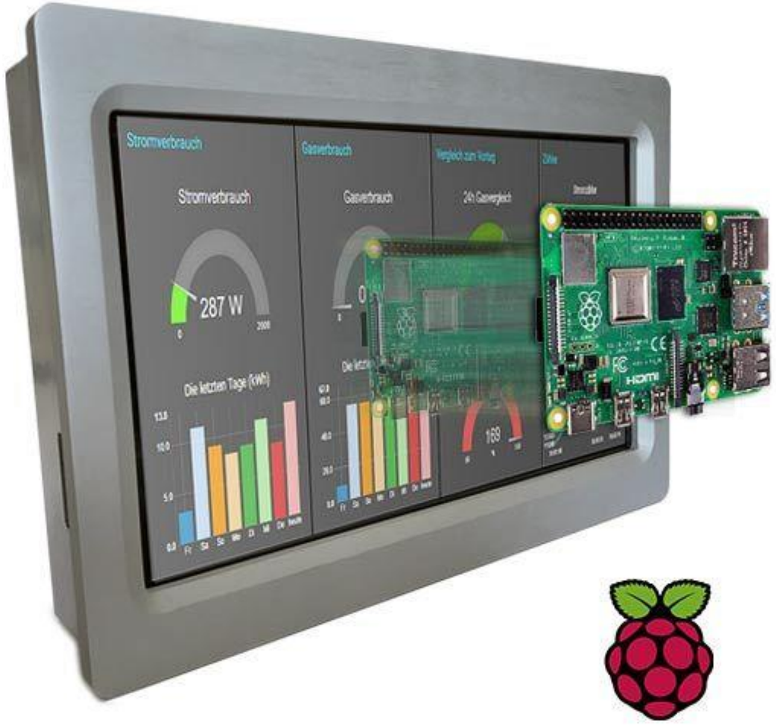
Write


Read data from sensors (inputs)
Real Time Operating System
Execute logic against input data
Write data to automation devices (outputs)

PLC Examples

Industrial Solutions based on Open Source Hardware

- Industrial Compact PLC based on Arduino
- PLC Raspberry Pi



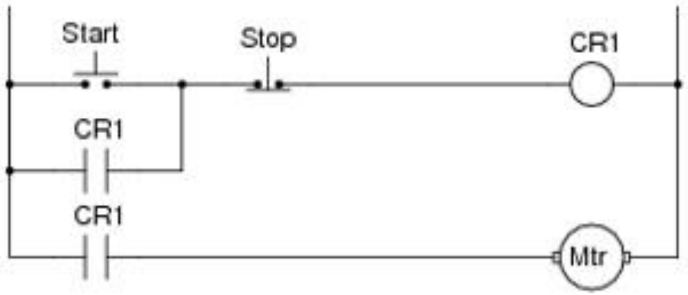
https://www.industrialshields.com/

Ladder Logic

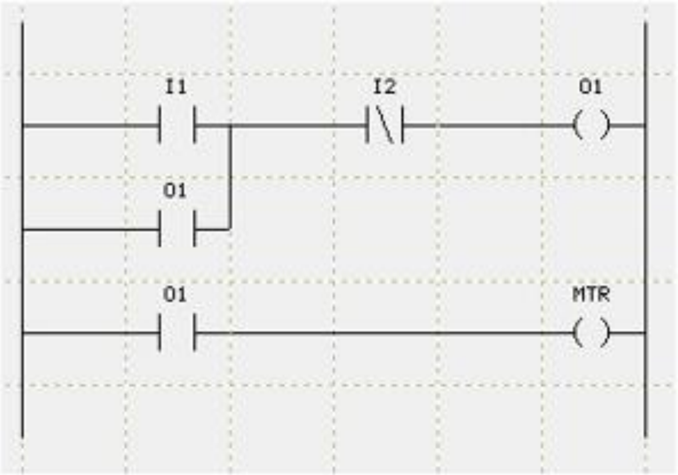
Simplistic programming language that is well suited for industrial applications

Relay-based logic and can be thought of as a set of connections between inputs and outputs

Motor Control PLC Ladder Logic



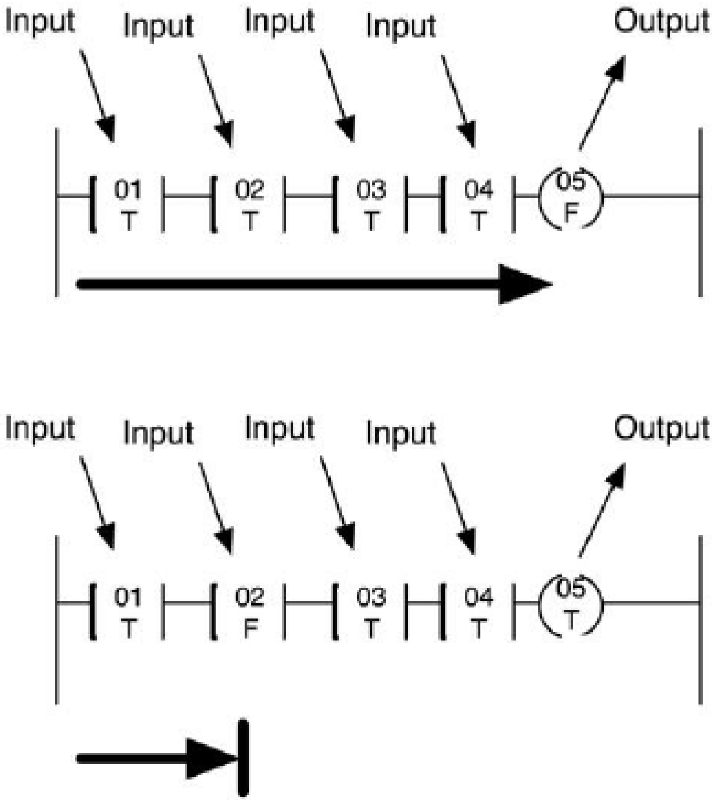
Motor Control Relay Logic



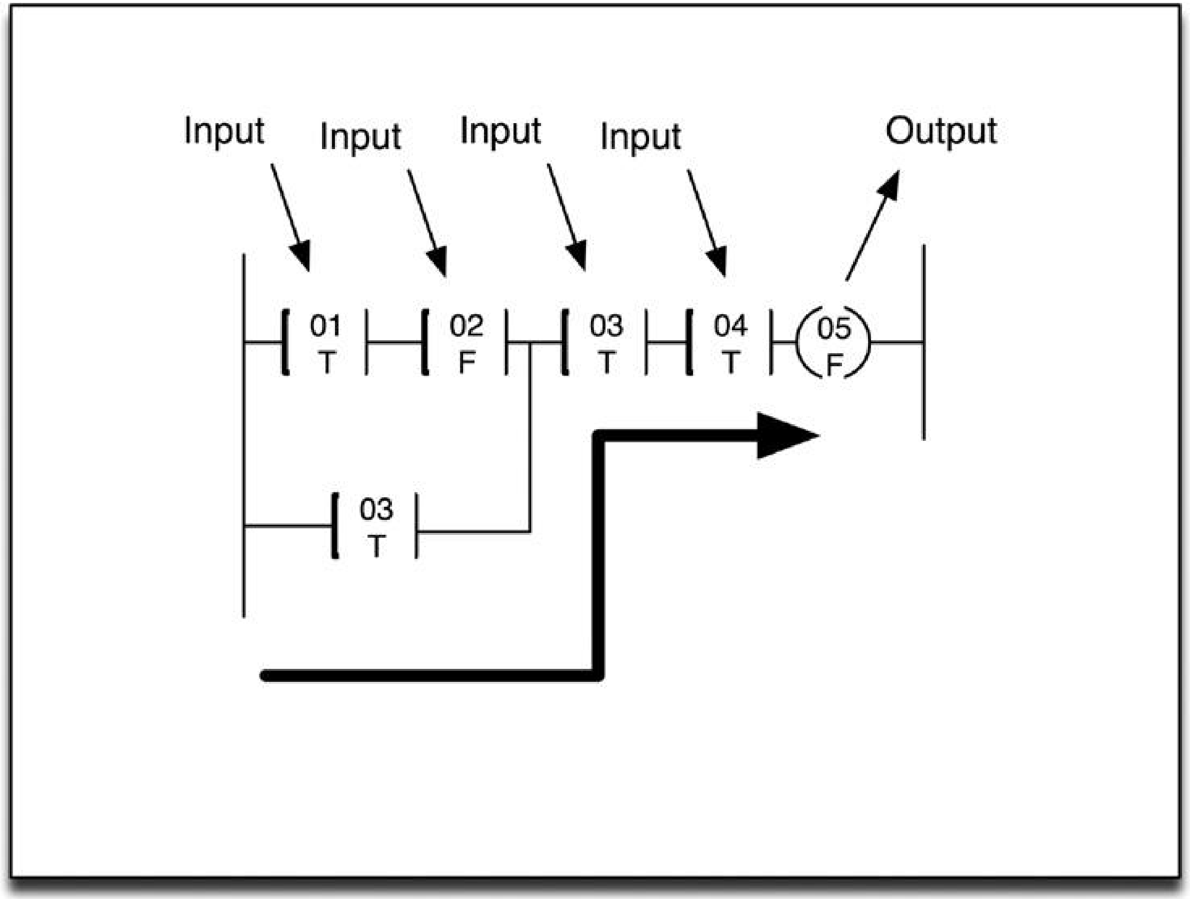
How Ladder Logic Works?

By looking at inputs from digital or analog devices such as sensors that are connected to the outside world and comparing them to set points

- If a set point is satisfied, the input is considered “true,” and if it is not it is considered “false”



Example of “or” Condition in Ladder Logic



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

Remote Terminal Unit (RTU)

Monitor field parameters and transmit that data back to a central monitoring station:

- Either to a Master Terminal Unit (MTU), or a centrally located PLC, or directly to an HMI system

Either poll-based or event-based, or programmed to take independent actions

Include remote communications capabilities:

- Consisting of a modem, cellular data connection, radio, or other wide area communication capability

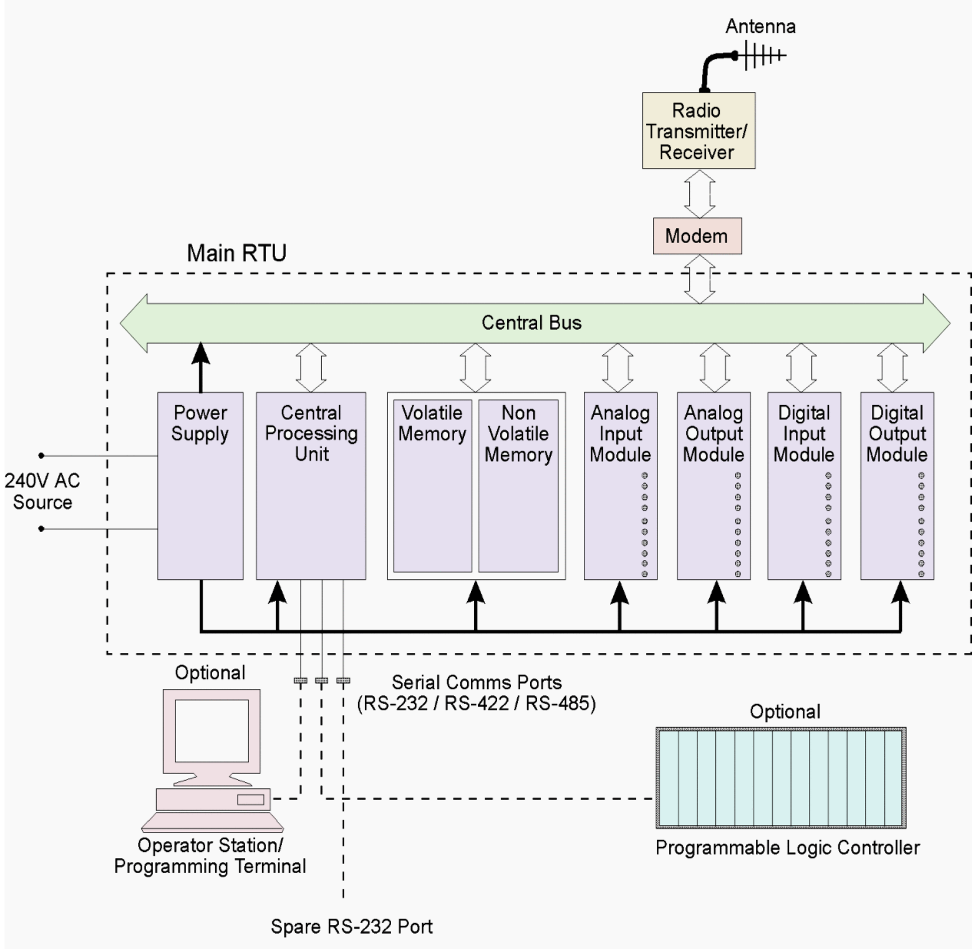
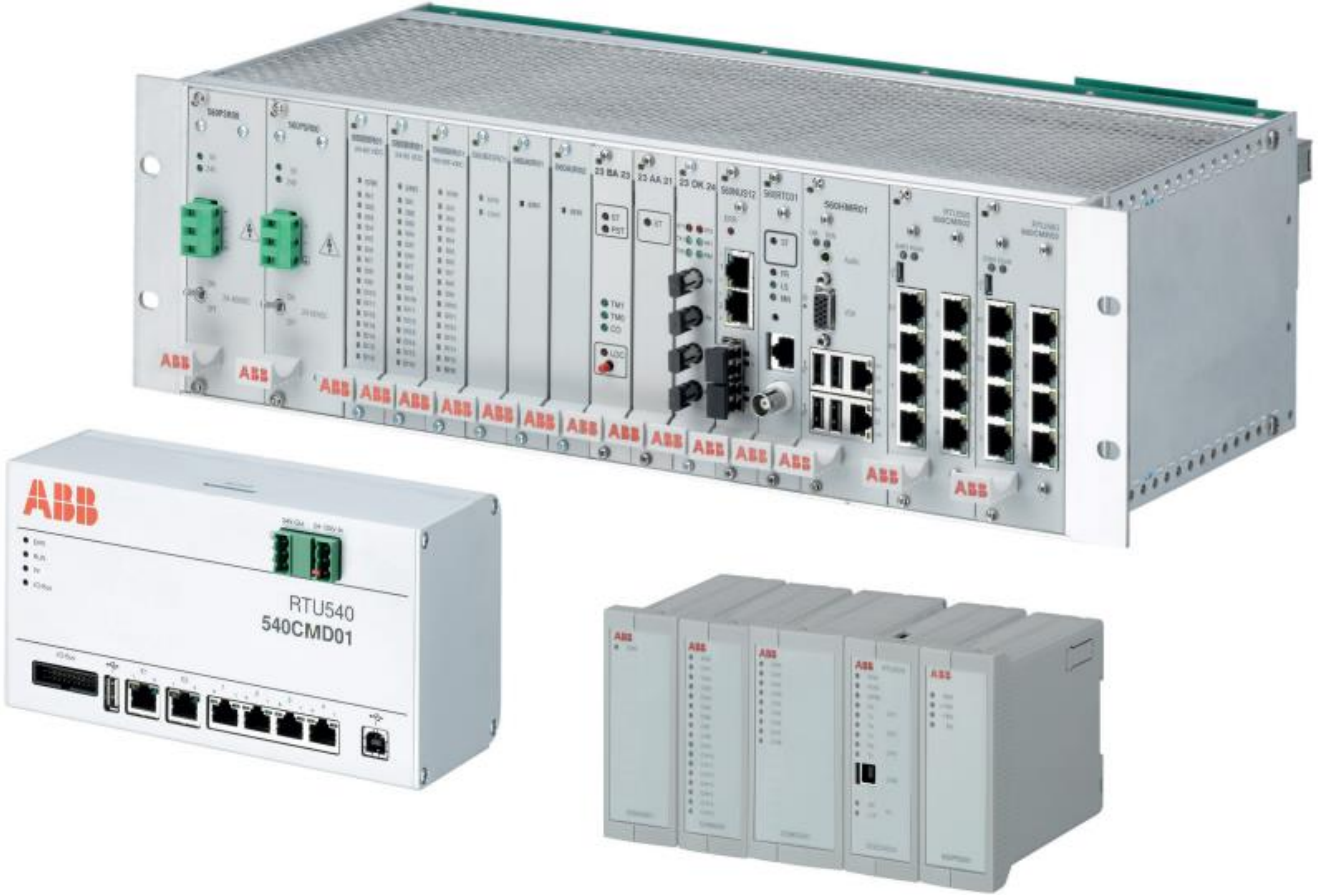


ABB RTU Example

RTU500 Series



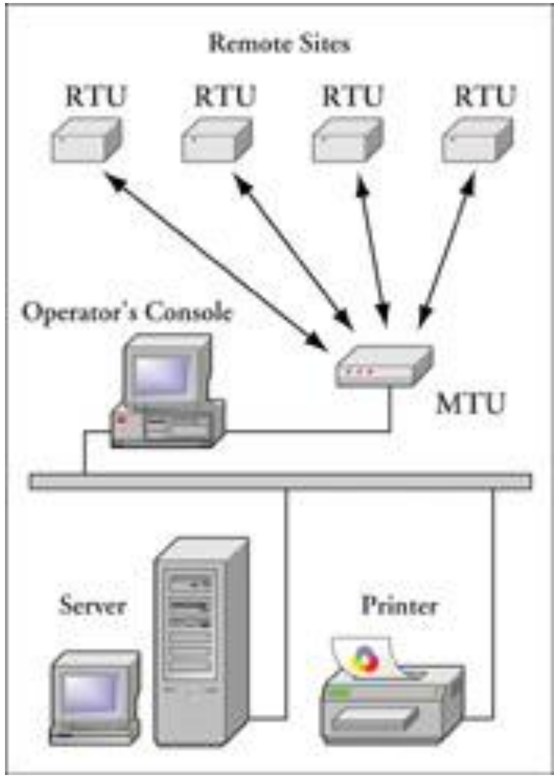
Master Terminal Unit

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



PLC – RTU

RTUs and PLCs continue to overlap in capability and functionality,

- With many RTUs integrating programmable logic and control functions, RTU can be thought of as a remote PLC

RTUs tend to be used more for wide geographic telemetry, while PLCs are best suited for local area control

Tetragenics MiniMote 6 RTU and AutomationDirect's DirectLogic PLC

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

HMI

Allow interaction with control processes

Act as a bridge between the human operator and the complex logic

- Allowing the operator to function on the process rather than on the underlying logic
- Performs functions and controls many functions across distributed complex processes from a centralized location

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

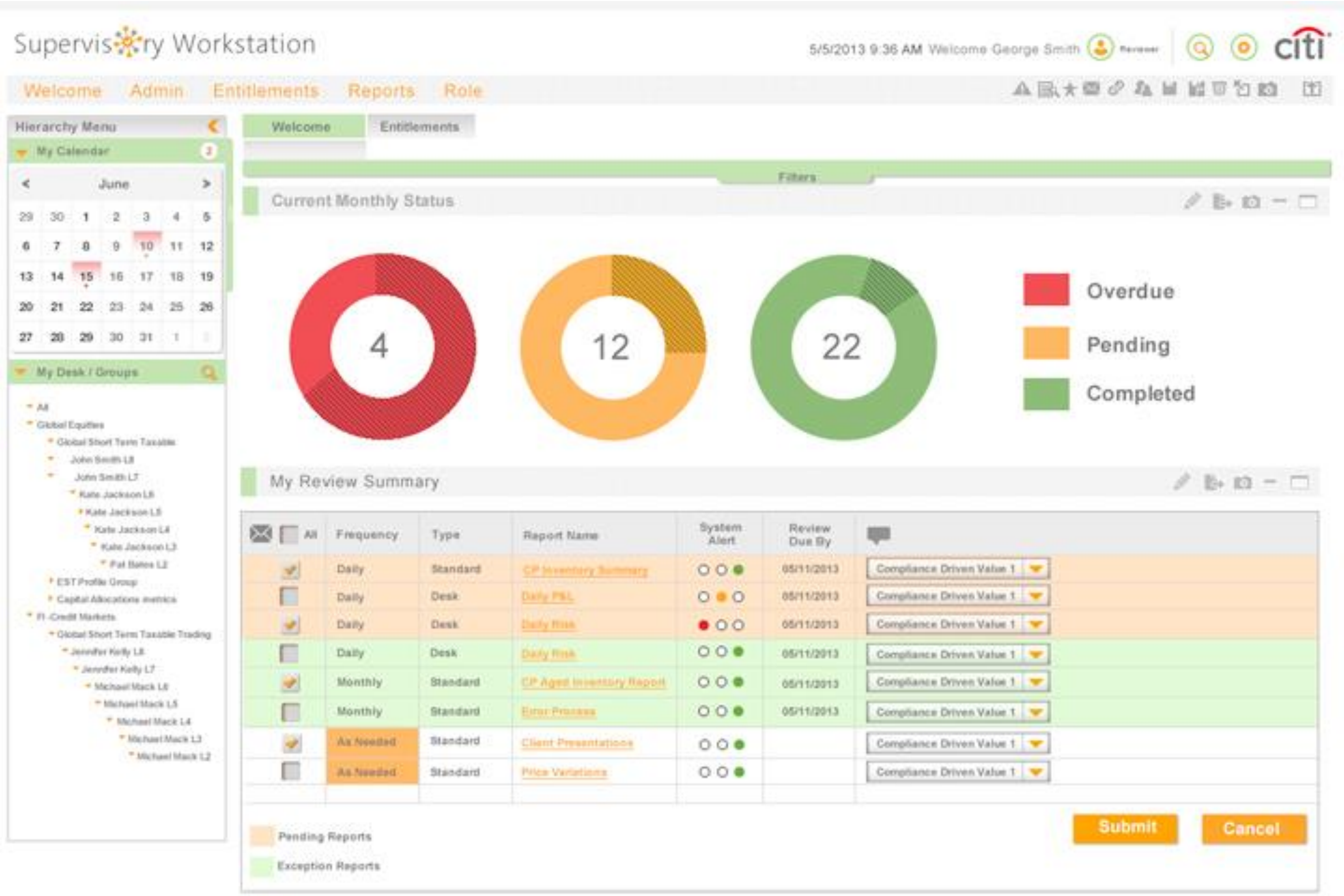
Presents them for supervisory purposes

Read-only system

- Different than HMI

Can be employing an HMI or Data Historian

Supervisory Workstations



☐ All	Frequency	Type	Report Name	System Alert	Review Due By	
☑	Daily	Standard	CP Inventory Summary	○ ○ ●	05/11/2013	Compliance Driven Value 1 ▼
☐	Daily	Desk	Daily P&L	○ ● ○	05/11/2013	Compliance Driven Value 1 ▼
☑	Daily	Desk	Daily Risk	● ○ ○	05/11/2013	Compliance Driven Value 1 ▼
☐	Daily	Desk	Daily Risk	○ ○ ●	05/11/2013	Compliance Driven Value 1 ▼
☑	Monthly	Standard	CP Aged Inventory Report	○ ○ ●	05/11/2013	Compliance Driven Value 1 ▼
☐	Monthly	Standard	Error Process	○ ○ ●	05/11/2013	Compliance Driven Value 1 ▼
☑	As Needed	Standard	Client Presentations	○ ○ ●		Compliance Driven Value 1 ▼
☐	As Needed	Standard	Price Variations	○ ○ ●		Compliance Driven Value 1 ▼

🟧 Pending Reports

🟩 Exception Reports

Other Assets

Anything connected to network (any kind of network) within ICS

- RFID cards

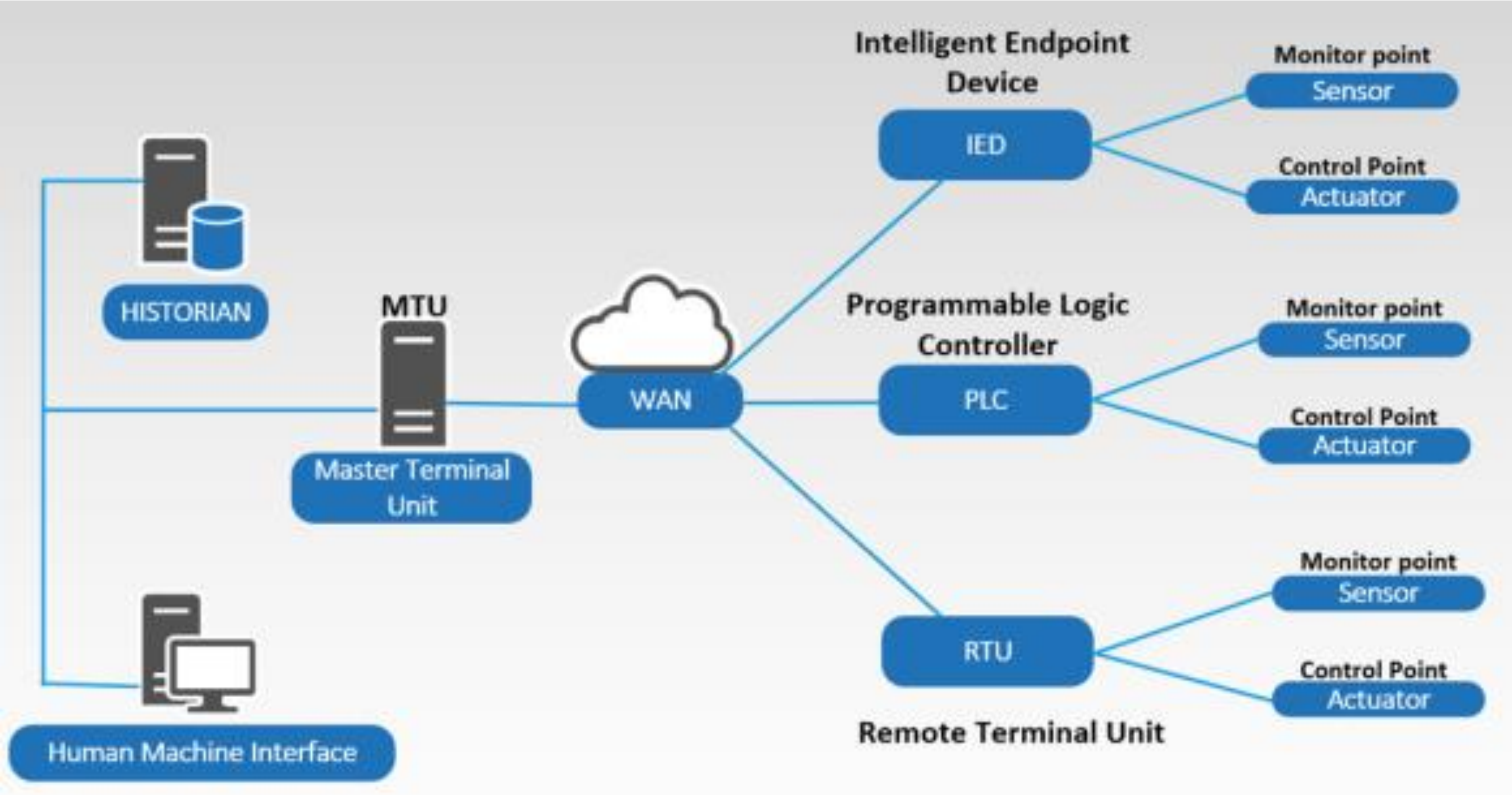
Capable of transporting data

- Such as USB

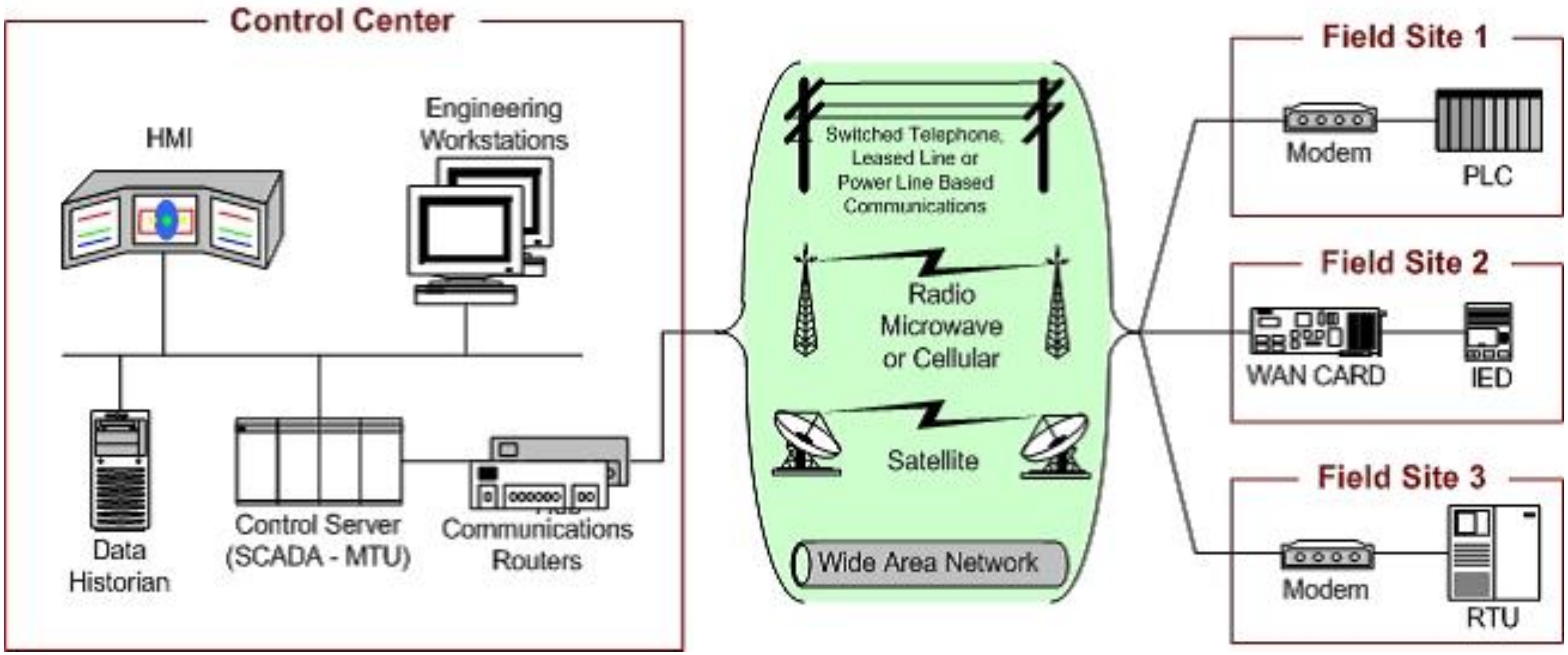
Suggestion: Detect and Disable interfaces unless required

- Example: commercial off-the-shelf (COTS) microprocessor with many capabilities
    - Even the capabilities you do not need or request

Abstract Topology Example for ICS



Abstract Model for ICS



Types of ICS

Process Control System

Safety Instrumented System

Distributed Control System

Building Automation System

Supervisory Control and Data Acquisition (SCADA)

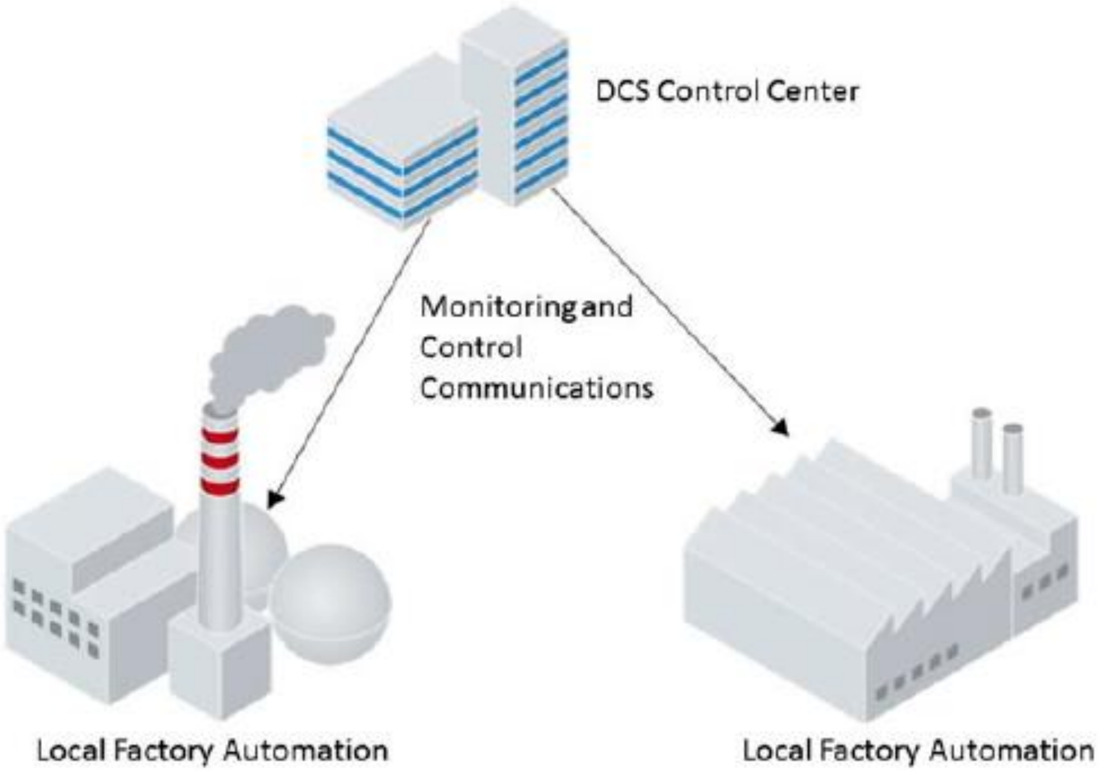
Energy Management System

Distributed Control System

Controls multiple automation processes at a single site (or plant)

Examples:

- The control processes at oil refineries
- Drinking water and wastewater treatment plants
- Car assembly lines



SCADA

Collects data and monitors automation across geographic areas

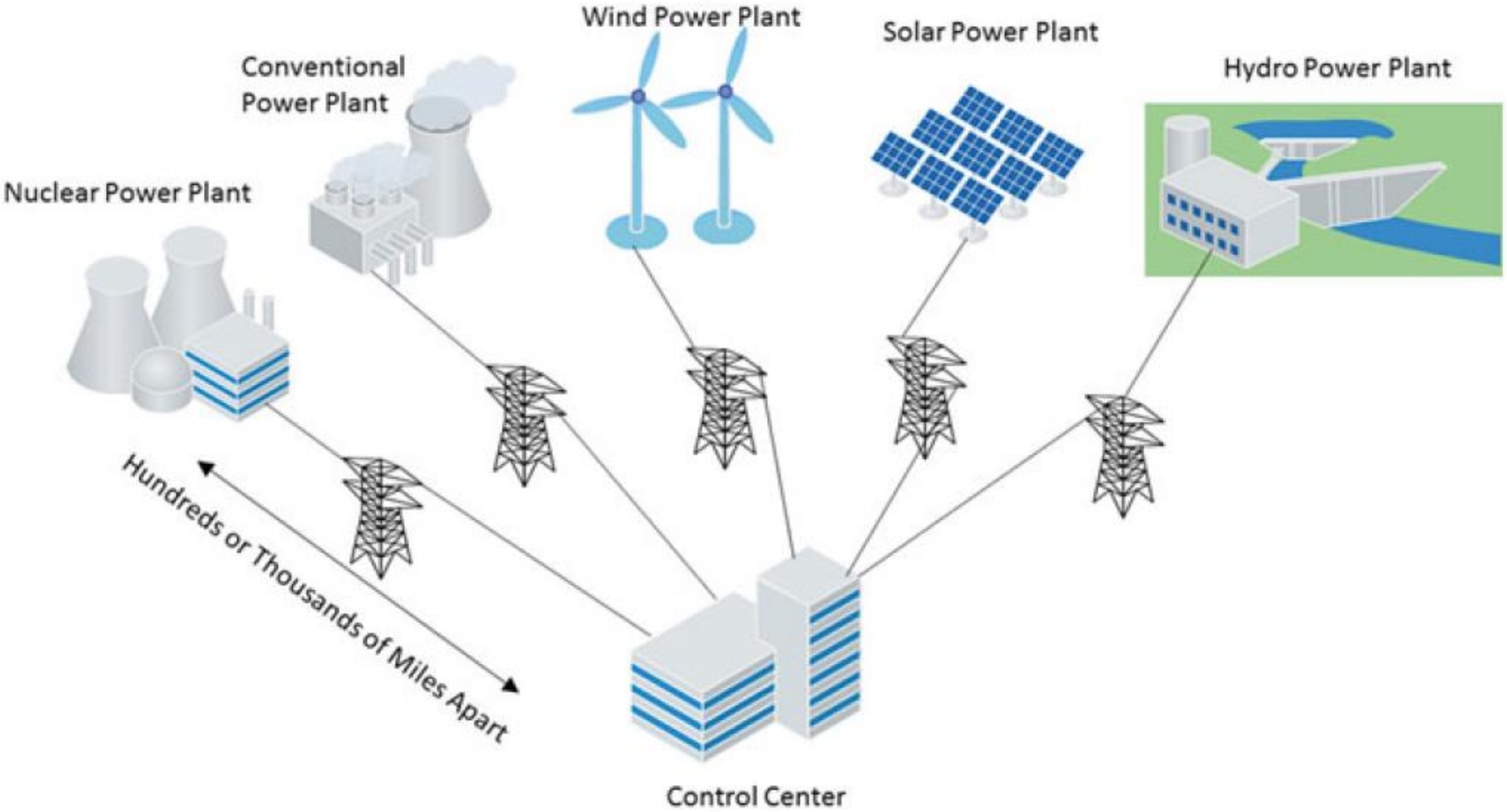
- Can be thousands of miles apart

The SCADA control center monitors and manages remote field controllers (such as RTUs and IEDs) at several energy production plants

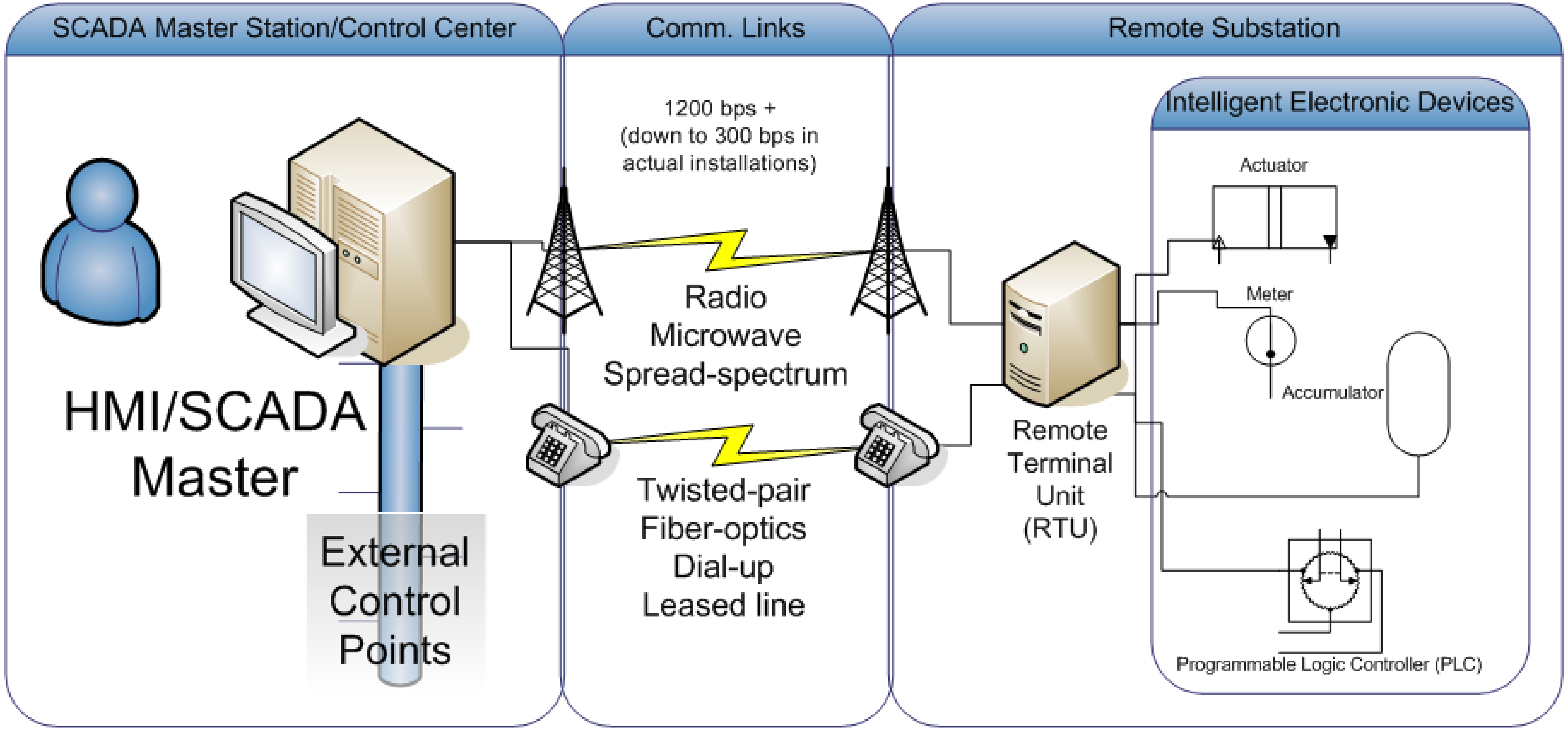
A SCADA system may supervise one or more DCSs at distant geographic locations

The SCADA control center may poll the controllers <u>less frequently</u> than a DCS and may only want status information such as <u>when an alarm or event occurs</u>

SCADA Example



SCADA Example



Why do we need to know all these?

How Cyber attack starts?

- Usually from one of the parts of ICS

Security of IED? RTU? PLC?

- Cyber
- Physical ?

Security of Data Historian?

- Databases
- Access control to user interface

Smart Grid Research Lab Example