



SCADA Systems

By

Dr. Mohammad Salah

**Mechatronics Engineering Department
Hashemite University**



Introduction

- **SCADA** systems are used to control dispersed assets where centralized data acquisition is as important as control (**i.e., SCADA is a method of monitoring and controlling large processes, often scattered over thousands of square kilometers.**
- These systems are used in distribution systems such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical utility transmission and distribution systems, and rail and other public transportation systems.
- **SCADA** systems integrate data acquisition systems with data transmission systems and **HMI** software to provide a centralized monitoring and control system for numerous process inputs and outputs.



Introduction

- **SCADA** systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in real time.
- Based on the sophistication and setup of the individual system, control of any individual system, operation, or task can be automatic, or it can be performed by operator commands.
- **SCADA** is not a full control system, but rather focuses on the supervisory level.
- **SCADA** is used for gathering, analyzing and to storage real time data.



Introduction

- **SCADA** systems consist of both hardware and software.
- Typical hardware includes an **MTU** placed at a control center, communications equipment (e.g., radio, telephone line, cable, or satellite), and one or more geographically distributed field sites consisting of either an **RTU** or a **PLC**, which controls actuators and/or monitors sensors.
- The **MTU** stores and processes the information from **RTU** inputs and outputs, while the **RTU** or **PLC** controls the local process.
- The communications hardware allows the transfer of information and data back and forth between the **MTU** and the **RTUs** or **PLCs**.



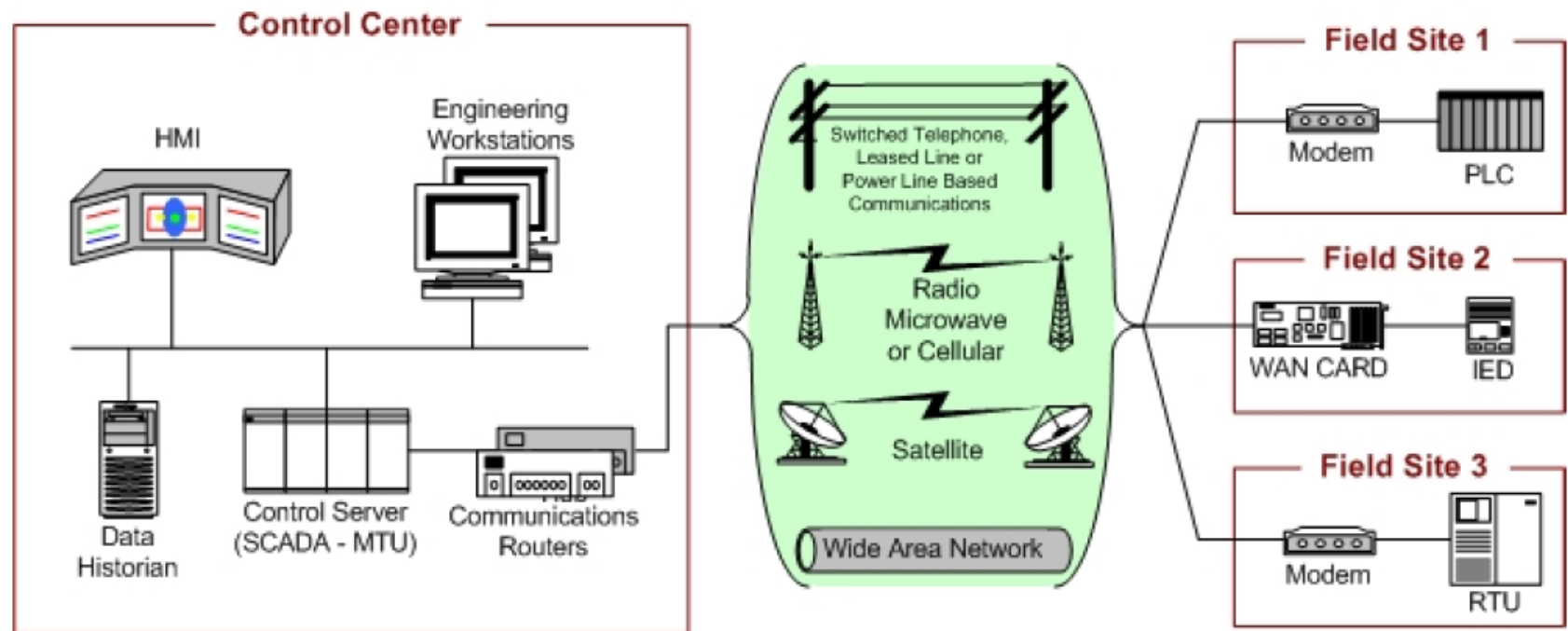
Introduction

- The software is programmed to tell the system what and when to monitor, what parameter ranges are acceptable, and what response to initiate when parameters change outside acceptable values.
- An **IED**, such as a protective relay, may communicate directly to the **SCADA** Server, or a local **RTU** may poll the **IEDs** to collect the data and pass it to the **SCADA** Server.
- **IEDs** provide a direct interface to control and monitor equipment and sensors.
- **IEDs** may be directly polled and controlled by the **SCADA** Server and in most cases have local programming that allows for the **IED** to act without direct instructions from the **SCADA** control center.



Introduction

- **SCADA** systems are usually designed to be fault-tolerant systems with significant redundancy built into the system architecture.





Introduction

- The control center houses a **SCADA** Server (**MTU**) and the communications routers.
- Other control center components include the HMI, engineering workstations, and the data historian, which are all connected by a LAN.
- The control center collects and logs information gathered by the field sites, displays information to the HMI, and may generate actions based upon detected events.
- The control center is also responsible for centralized alarming, trend analyses, and reporting.
- The field site performs local control of actuators and monitors sensors.



Introduction

- Field sites are often equipped with a remote access capability to allow field operators to perform remote diagnostics and repairs usually over a separate dial up modem or WAN connection.
- Standard and proprietary communication protocols running over serial communications are used to transport information between the control center and field sites using telemetry techniques such as telephone line, cable, fiber, and radio frequency such as broadcast, microwave and satellite.

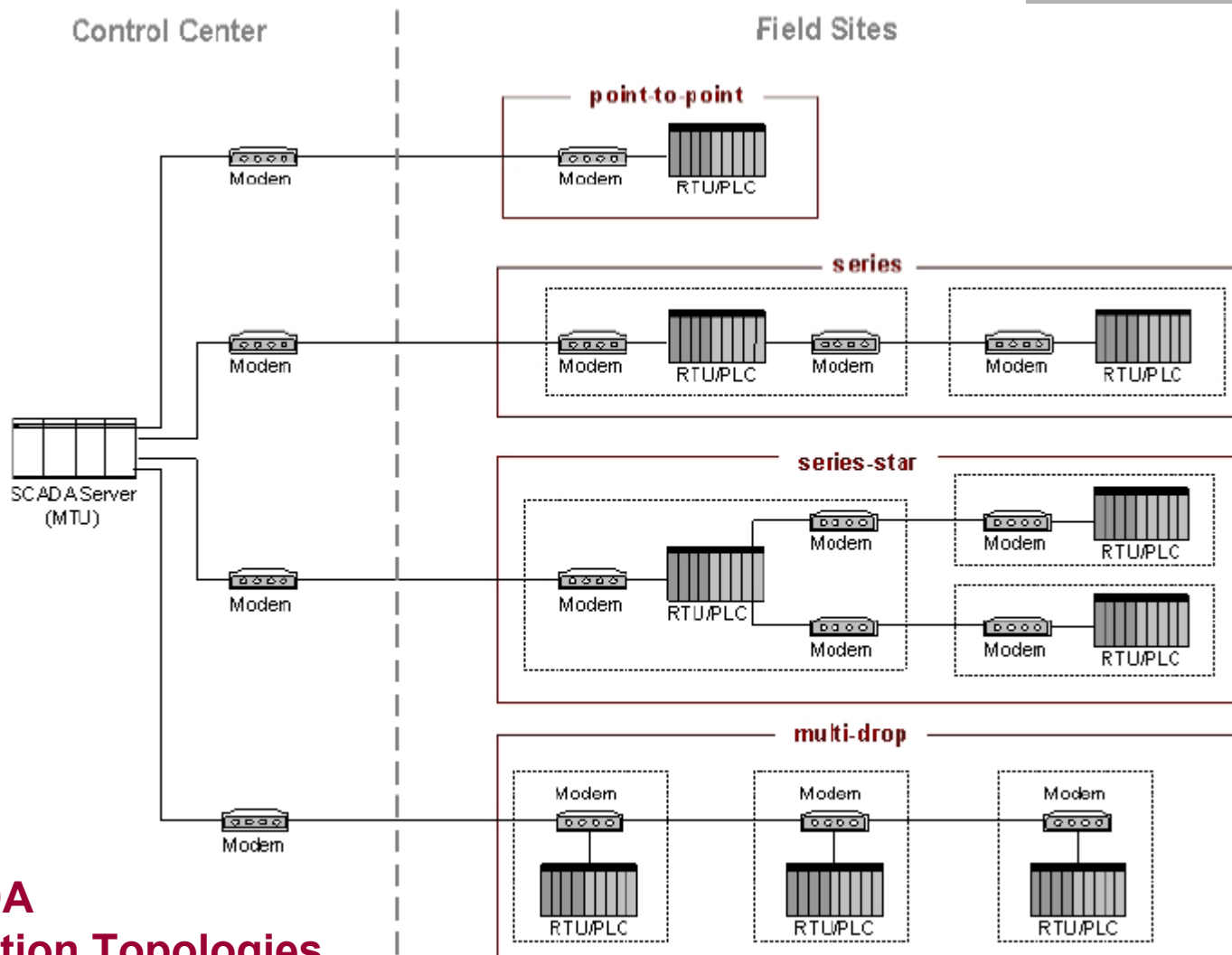


Introduction

- **MTU-RTU** communication architectures vary among implementations. The various architectures used, including point-to-point, series, series-star, and multi-drop.
- Point-to-point is functionally the simplest type; however, it is expensive because of the individual channels needed for each connection.
- In a series configuration, the number of channels used is reduced; however, channel sharing has an impact on the efficiency and complexity of **SCADA** operations.
- Similarly, the series-star and multi-drop configurations' use of one channel per device results in decreased efficiency and increased system complexity.



Introduction



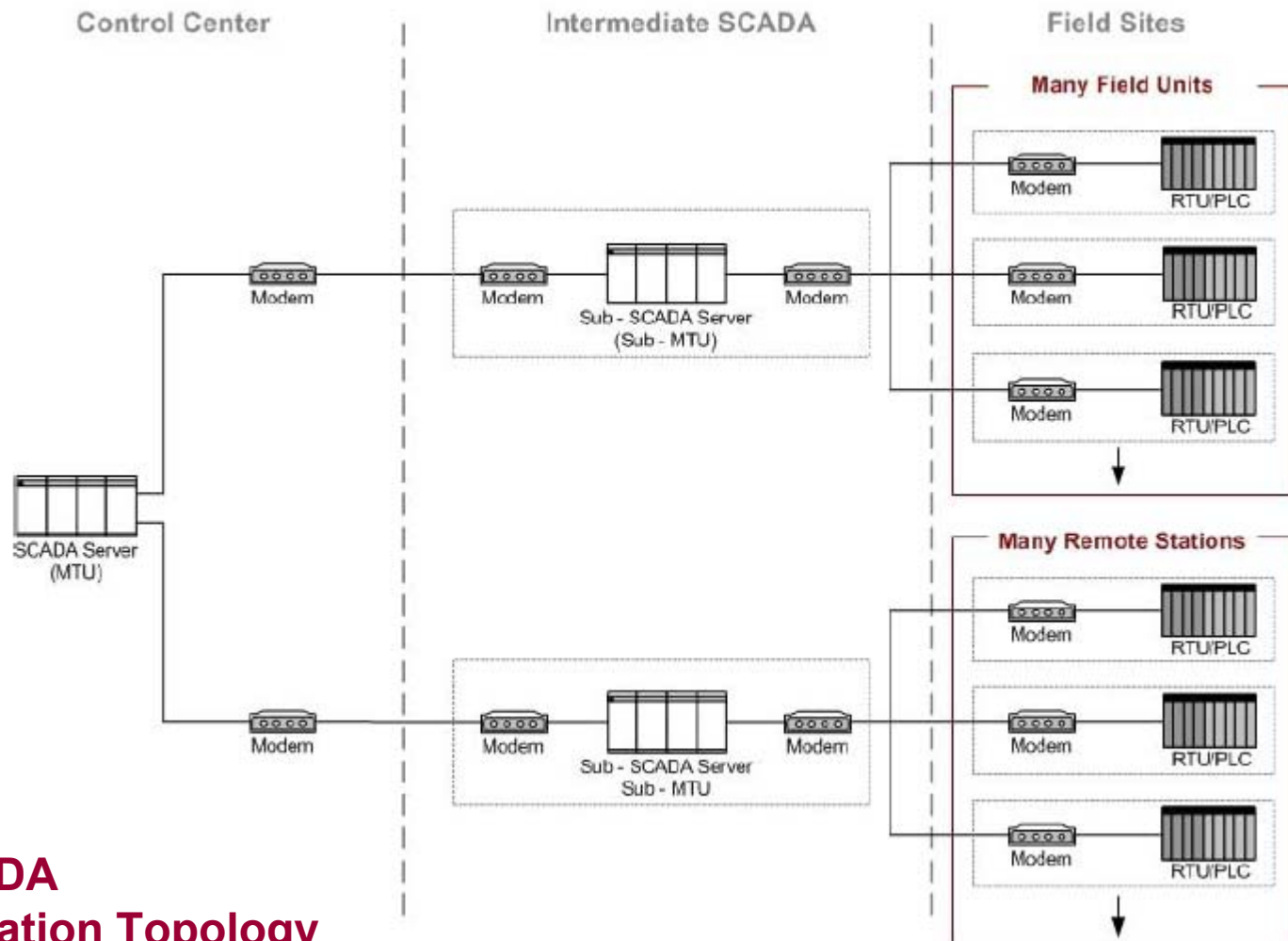


Introduction

- The four basic architectures can be further augmented using dedicated communication devices to manage communication exchange as well as message switching and buffering.
- Large **SCADA** systems, containing hundreds of **RTUs**, often employ **sub-MTUs** to alleviate the burden on the primary **MTU**. This type of topology is shown in the following figure.



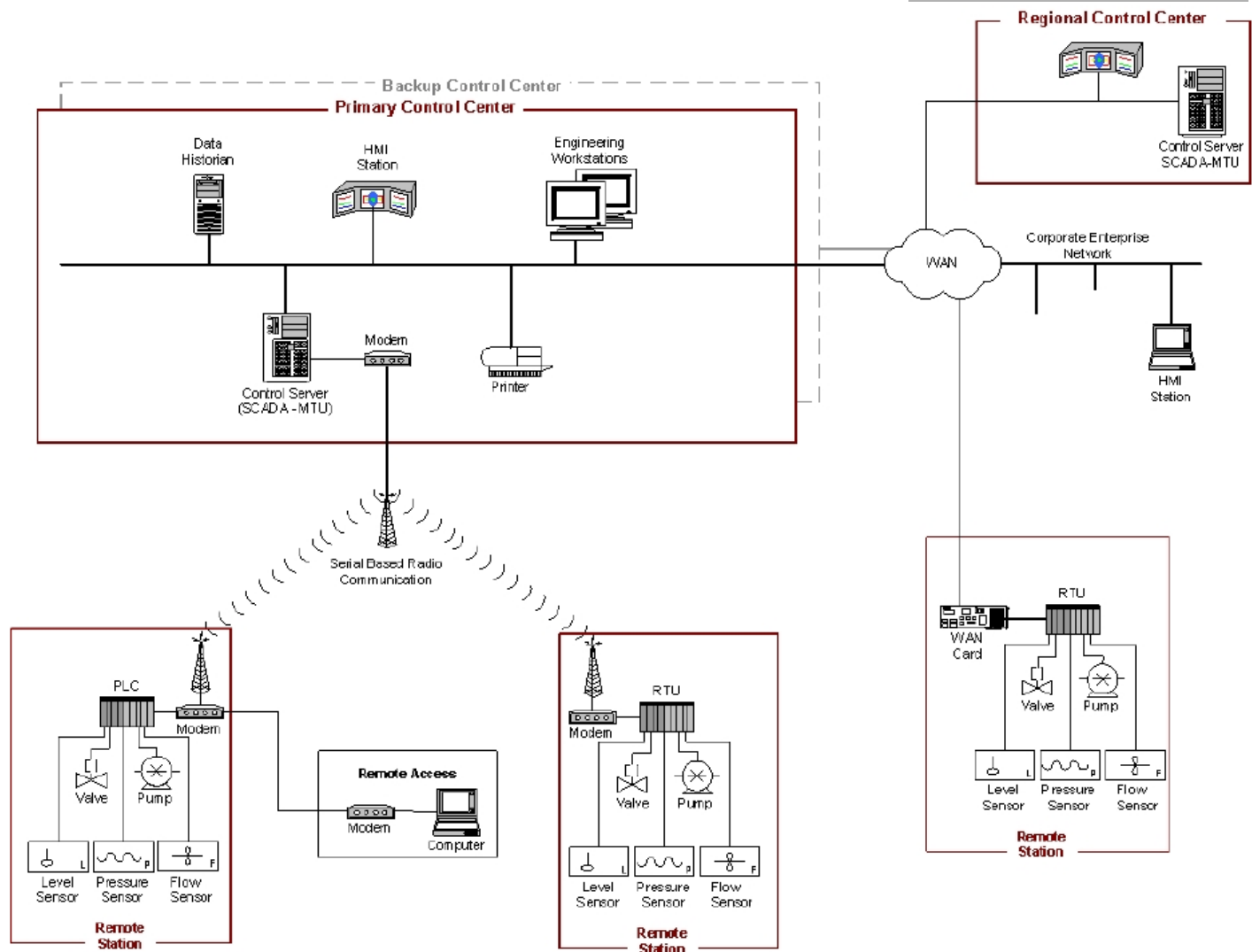
Introduction



**Large SCADA
Communication Topology**



Introduction



**SCADA System
Implementation
Example
(Distribution
Monitoring And
Control)**



Introduction

- This particular **SCADA** system consists of a primary control center and three field sites.
- A second backup control center provides redundancy in the event of a primary control center malfunction.
- Point-to-point connections are used for all control center to field site communications, with two connections using radio telemetry.
- The third field site is local to the control center and uses the wide area network (WAN) for communications.
- A regional control center resides above the primary control center for a higher level of supervisory control.



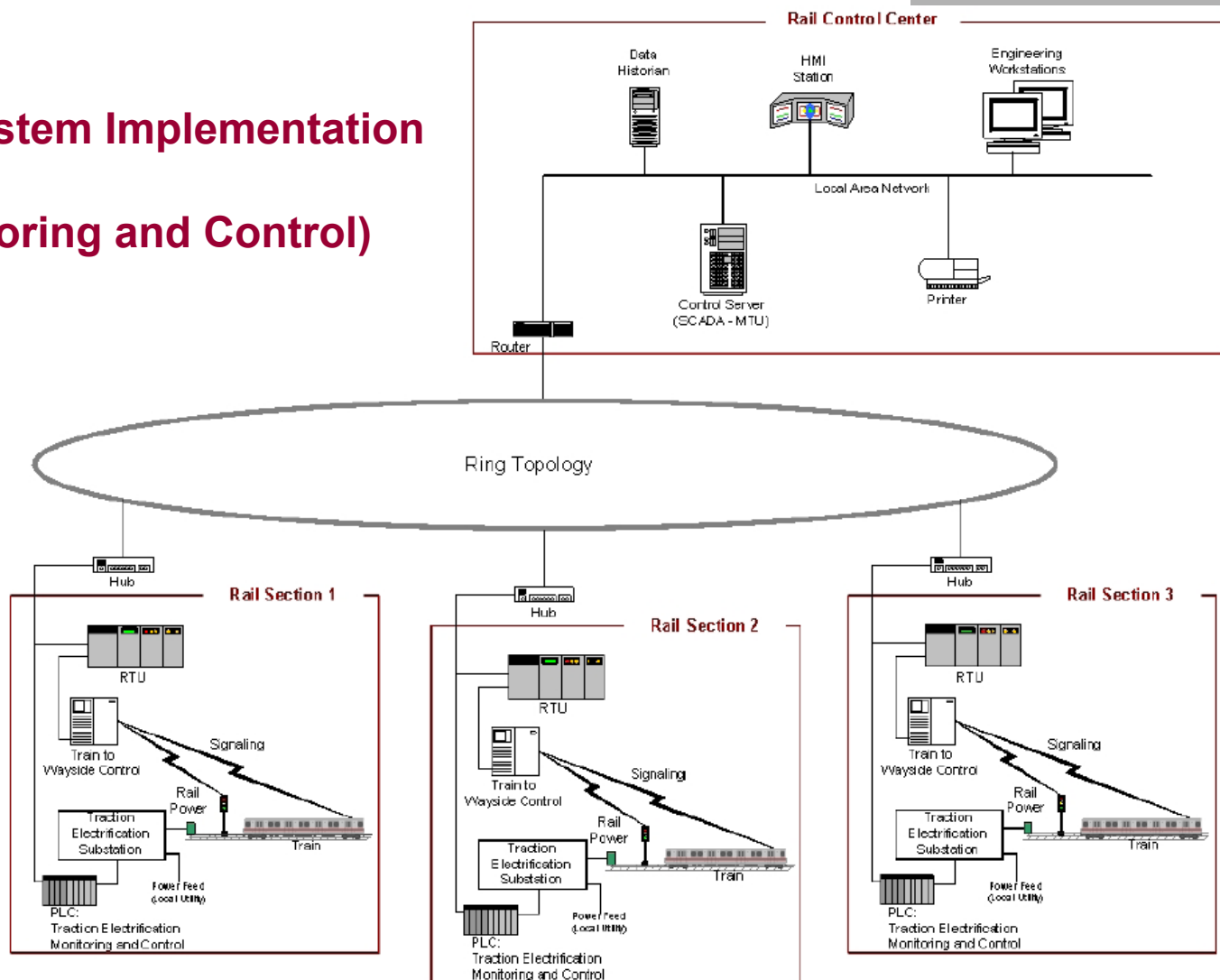
Introduction

- The corporate network has access to all control centers through the WAN, and field sites can be accessed remotely for troubleshooting and maintenance operations.
- The primary control center polls field devices for data at defined intervals (e.g., 5 seconds, 60 seconds) and can send new set points to a field device as required.
- In addition to polling and issuing high-level commands, the **SCADA** server also watches for priority interrupts coming from field site alarm systems.



Introduction

SCADA System Implementation Example (Rail Monitoring and Control)





Introduction

- The previous example includes a rail control center that houses the **SCADA** system and three sections of a rail system.
- The **SCADA** system polls the rail sections for information such as the status of the trains, signal systems, traction electrification systems, and ticket vending machines.
- This information is also fed to operator consoles at the HMI station within the rail control center.
- The **SCADA** system also monitors operator inputs at the rail control center and disperses high-level operator commands to the rail section components.



Introduction

- In addition, the **SCADA** system monitors conditions at the individual rail sections and issues commands based on these conditions (e.g., shut down a train to prevent it from entering an area that has been determined to be flooded or occupied by another train based on condition monitoring).



Introduction

- There are several common media of communication:
 - Fiber optics
 - Electrical cable.
 - Leased lines from a telephone utility.
 - Satellite telecommunications.
- The communications method used by most **SCADA** systems is called “master–slave”, where only one of the machines (in this case the MTU) is capable of initiating communication.
- The **MTU** talks to each **RTU** then returns to the first. This is called "scanning".
- The time required for the **MTU** to scan ALL its **RTUs** is called the **MTU** Scan Time (Scan Interval).
- Factors that determine scan interval are: number of **RTUs**, amount of data, data rate, and communications efficiency.



Introduction

Calculate a scan interval for a **SCADA** system that:

- Has 20 **RTUs**
- Every **RTU** has a point count of 180 status points, 30 alarm points, 10 meters (at 16 bits each), and 10 analog points (at 16 bits each).
- The **MTU** sends information to the **RTU** of 150 discrete control signals to valves and motors, 6 stepping motors (16 bits each), and 10 valve controller set points (16 bits each)
- Data rate for communication is 1200bps.
- Communication efficiency is 40%.

Solution

Total Points is 920, therefore the total amount of data is
 $20 \times 920 = 18,400\text{bits}$ and the data rate is
 $18,400\text{b}/1200\text{bps} \approx 15\text{sec}$ at 100% efficiency but at
40% efficiency, the scan interval is $15\text{sec}/0.4 \approx 38\text{sec}$.



Remote Terminal Units (RTUs)

- An **RTU** (sometimes referred to as a remote telemetry unit) as the title implies, is a standalone data acquisition and control unit, generally microprocessor based, which monitors and controls equipment at some remote location from the central station.
- Its primary task is to control and acquire data from process equipment at the remote location and to transfer this data back to a central station.
- It generally also has the facility for having its configuration and control programs dynamically downloaded from some central station.
- There is also a facility to be configured locally by some **RTU** programming unit.



Remote Terminal Units (RTUs)

- Although traditionally the **RTU** communicates back to some central station, it is also possible to communicate on a peer-to-peer basis with other **RTUs**.
- The **RTU** can also act as a relay station (sometimes referred to as a store and forward station) to another **RTU**, which may not be accessible from the central station.
- Small sized **RTUs** generally have less than 10 to 20 analog and digital signals, medium sized **RTUs** have 100 digital and 30 to 40 analog inputs.
- **RTUs**, having a capacity greater than this can be classified as large.