SWAYAM NPTEL COURSE ON

MINE AUTOMATION AND DATA ANALYTICS

By

Prof. Radhakanta Koner

Department of Mining Engineering

Indian Institute of Technology (Indian School of Mines) Dhanbad

Module 06

Automated tracking and VR systems

Lecture 14 A

Automated Communication and Tracking Technologies: SCADA

CONCEPTS COVERED

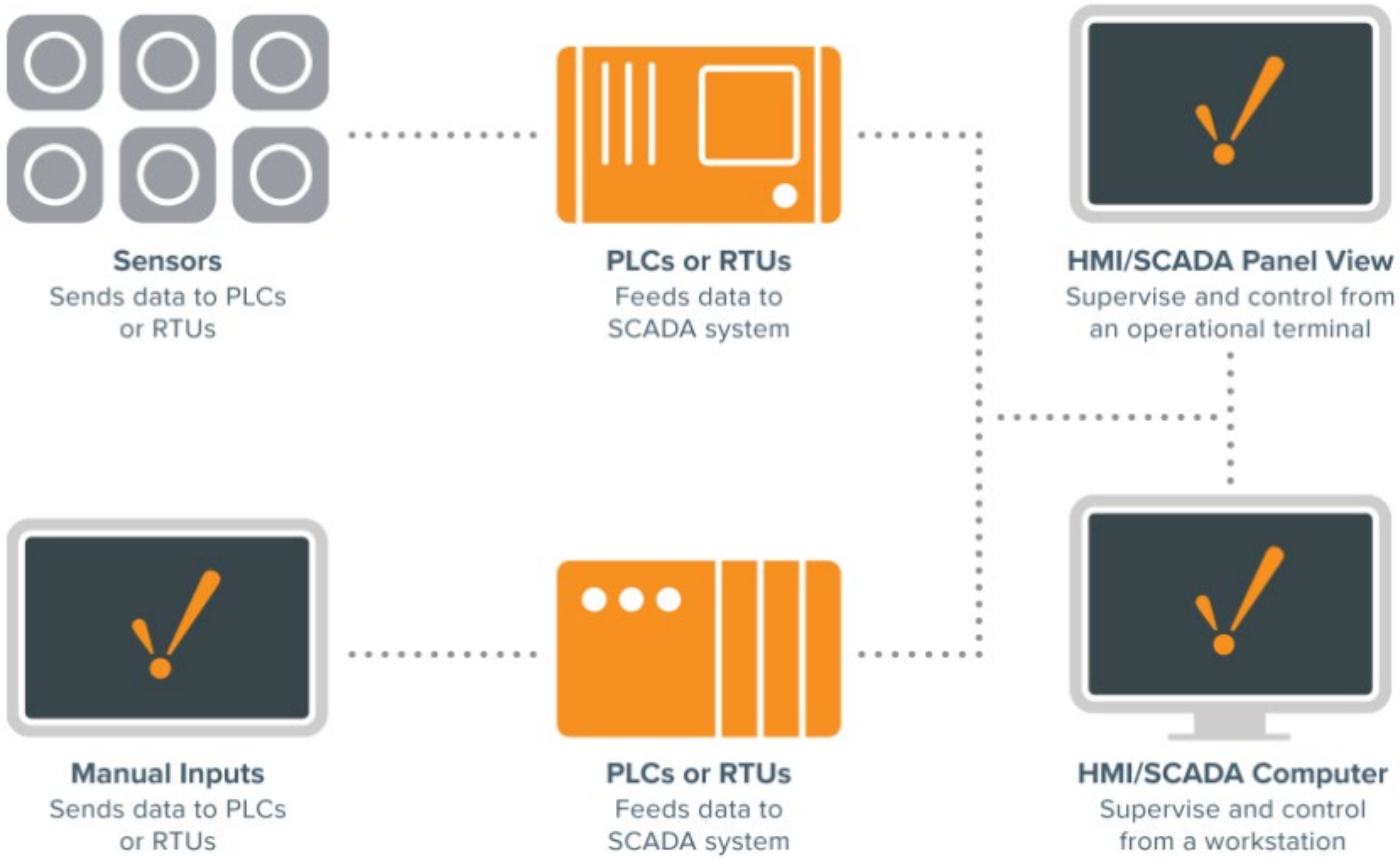
- Introduction to SCADA
- SCADA Architecture
- Evolution of SCADA
- SCADA Components
- SCADA Communication Protocols
- Fundamental of Control of SCADA System

Introduction

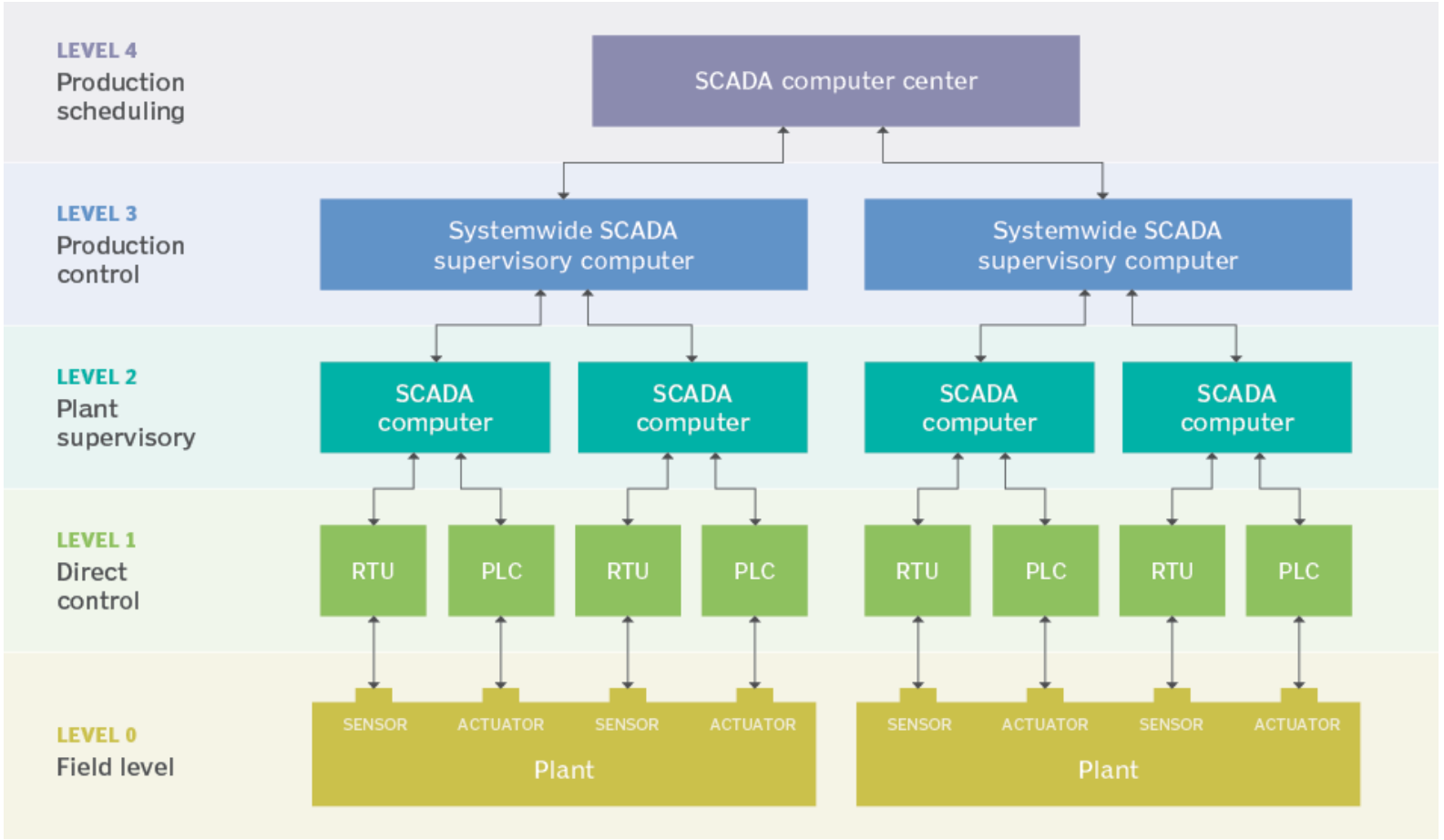
Supervisory control and data acquisition (SCADA) is a system of software and hardware elements that allows industrial organizations to

- **Control industrial processes locally or at remote locations**
- **Monitor, gather, and process real-time data**
- **Directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software**
- **Record events into a log file**

A Basic SCADA Diagram



SCADA Architecture



Level 0

The field level includes field devices, such as sensors, used to forward data relating to field processes and actuators used to control processes.

Level 1

The direct control level includes local controllers, such as PLCs and RTUs, that interface directly with field devices, including accepting data inputs from sensors and sending commands to field device actuators.

Level 2

The plant supervisory level includes local supervisory systems that aggregate data from level controllers and issue commands for those controllers to carry out.

Level 3

The production control level includes systemwide supervisory systems that aggregate data from Level 2 systems to produce ongoing reporting to the production scheduling level, as well as other site or regionwide functions, like alerts and reporting.

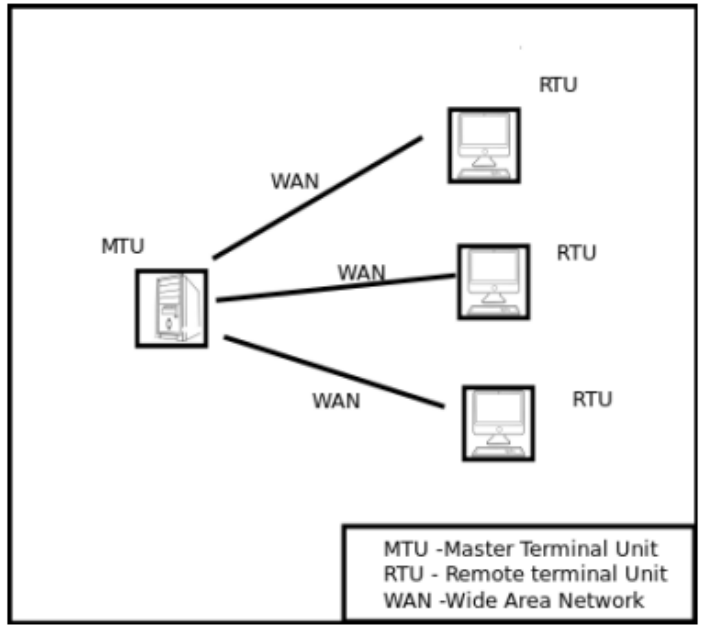
Level 4

The production scheduling level includes business systems used to manage ongoing processes.

Evolution of SCADA

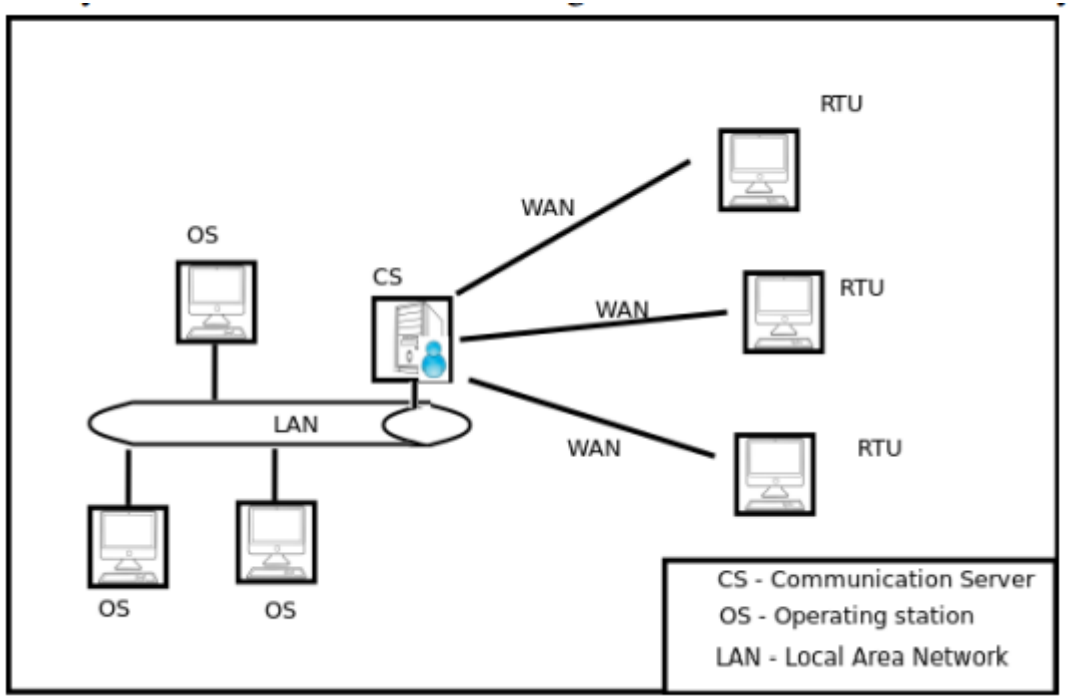
First generation: Monolithic systems

SCADA systems implemented in the 1960s and 1970s usually incorporated RTUs at industrial sites connected directly to mainframe or minicomputer systems, usually also on-site or connected over a wide area network.



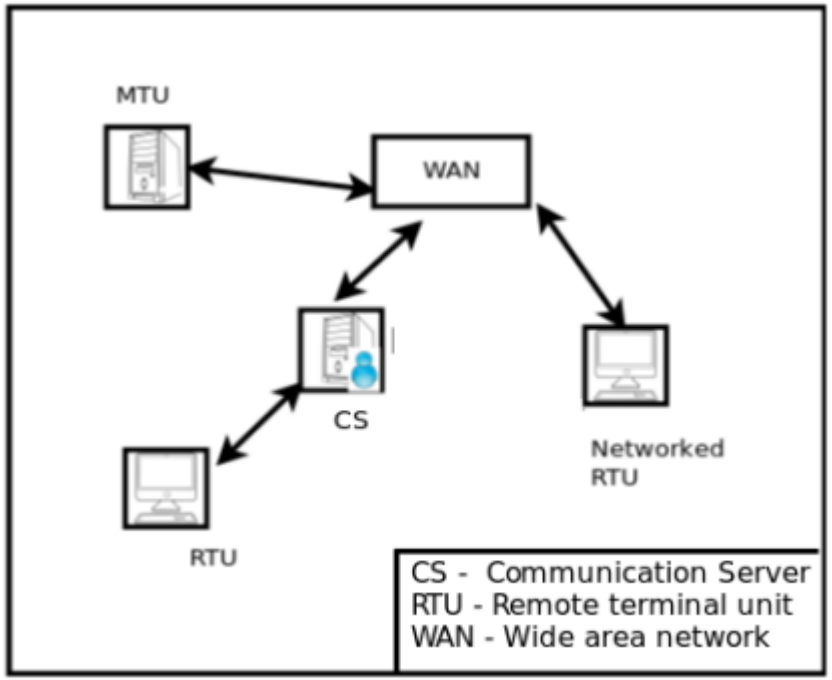
Second generation: Distributed systems

SCADA systems took advantage of wide availability of proprietary local area networks and smaller, more powerful computers during the 1980s to enable greater sharing of operational data at the plant level and beyond. However, the lack of open networking standards prevented interoperability across SCADA product vendors.

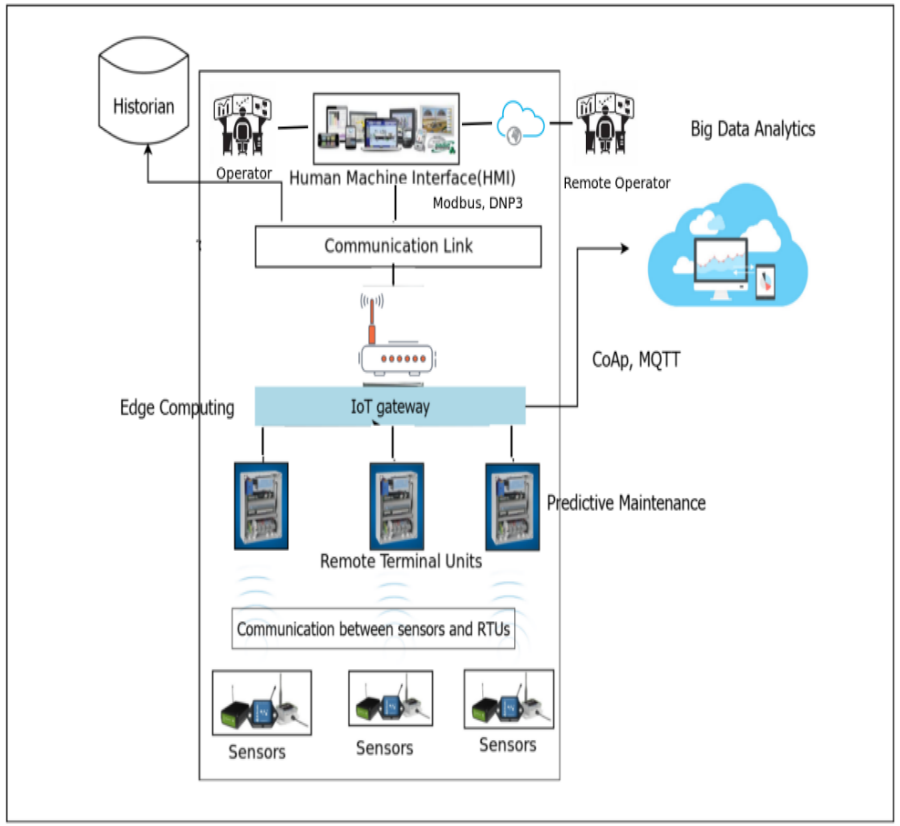


Third generation: Networked systems

SCADA systems depended on greater interoperability provided by industry acceptance and incorporation of standard network protocols during the 1990s. SCADA systems could be scaled more easily, as enterprises were able to integrate systems across their own industrial infrastructure while using a wider variety of devices and systems.

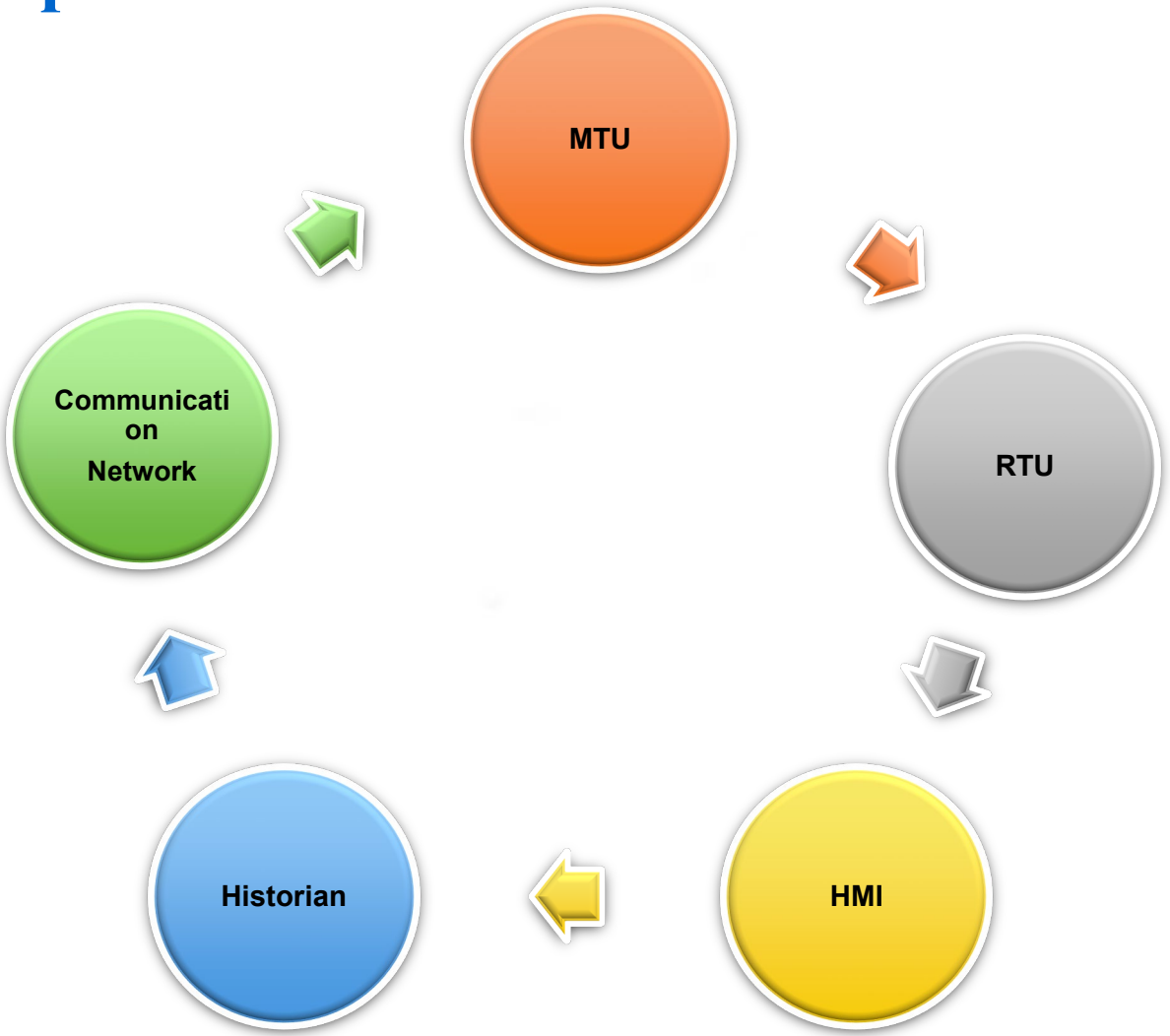


Fourth generation: Web or IIoT-based systems



SCADA systems began appearing in the early 2000s as SCADA vendors embraced web software development tools to enable transparent interoperability and access via universally available interfaces, like web browsers running on handheld devices, laptops, and desktop computers.

SCADA Components

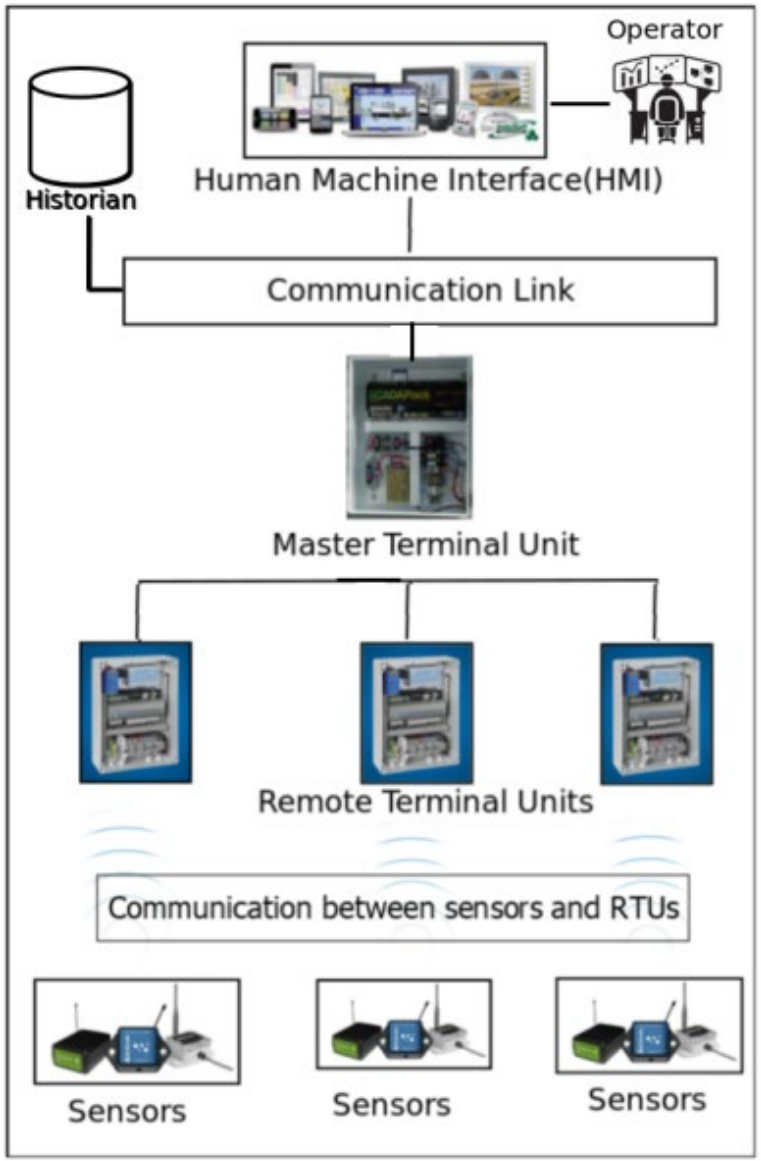


Remote Terminal Units (RTU)

1) RTU is responsible for collecting real-time data and information from sensors that are connected to the physical environment using link LAN/WAN.

2) RTUs forward information to MTU.

3) These are additionally in charge of conveying the present status data of physical devices associated with the system.



Master Terminal Unit (MTU)

1) **MTU is the central monitoring station.**

2) **It is in charge of controlling and commanding the RTU machine over communication links.**

3) **It also responds to messages from RTU and processes and stores them for succeeding communication.**

Human Machine Interface (HMI)

1) HMI provides a communication interface between SCADA hardware and software components.

2) It is responsible for controlling SCADA operational information, for example, controlling, observing, and communication between several RTU and MTU in the form of text, statistics, or other comprehensible content.

Central database (Historian)

1) Historian is used for accumulating two-way communication data, events, and alarms between SCADA control centers.

2) It can be described as a centralized database or a server located at a distant location.

3) The historian is queried to populate graphical trends on the HMI.

Communication network

1) The communication network provides communication services between various components in the SCADA network framework.

2) The medium utilized can be either wireless or wired. Presently, wireless media is generally utilized as it interfaces geologically circulated areas and less available zones to communicate effortlessly.

SCADA Communication Protocols

Modbus

- Modbus transmission protocol developed by Gould Modicon for their Modicon programmable controller.
- Most commonly used protocol for connecting electronic devices due to being openly published and easy to use.
- Used for interactions between MTU and RTUs.
- Modbus/TCP is an enhanced variation focusing on reliable communication over the Internet and Intranet.
- Modbus Plus protocol proposed to overcome master terminal vulnerability issues.

Distributed Network Protocol (DNP)

- **Distributed Network Protocol (DNP) is based on the Enhanced Performance Architecture (EPA) model, which is a streamlined type of OSI layer architecture developed by Harris, Distributed Automation Products.**
- **DNP3 protocol was developed to achieve open and standards-based interoperability between RTUs, MTU, and Programmable Logic Controllers (PLCs).**

Distributed Network Protocol (DNP)

- Core components of the DNP3 protocol include data link layer conventions, transport functions, application conventions, and a data link library.
- A user layer is added to the EPA architecture responsible for tasks such as multiplexing, data fragmentation, prioritization, and error checking.

IEC 60870-5 Protocol

- The International Electro-Technical Commission (IEC) 60870-5 protocol also follows the Enhanced Performance Architecture (EPA) model.
- An additional top layer representing the application layer is included in the EPA architecture to indicate functions related to the telecontrol framework.
- Variations of the telecontrol framework, such as T101, T102, T103, T104, define diverse specifications, data objects, and function codes at the application convention level.
- For efficient transmission, the DNP3 layer stack adds a pseudo-transport layer, but it is not utilized in IEC 60870-5.

Foundation Fieldbus Protocol

- Foundation Fieldbus utilizes a four-layer stack comprising the user, application, data link, and physical layers.
- Foundation Fieldbus architecture follows the OSI layer model, with the user layer added as an additional top layer of the application layer.
- The user layer serves as a gateway between software programs and field devices, facilitating easy process integration.
- Foundation Fieldbus offers features such as multifunctional devices, open standards, and decreased wire costs, setting it apart from other protocols.

Apart from these traditional communication protocols, in IIoT-based SCADA other IoT protocols are

Zigbee

- Zigbee, an IEEE 802.15.4 based communication protocol, was developed by the Zigbee Alliance and standardized in 2003, with a revision in 2006.
- The communication range of Zigbee is between 10 to 100 meters line-of-sight, depending on environmental characteristics.

- **Zigbee architecture comprises three types of devices: Fully Functional Devices (FFDs) which act as routers, Reduced Functional Devices (RFDs), and a coordinator.**
- **Zigbee enables Wireless Personal Area Networks (WPAN) and provides a communication protocol with low-power digital radios.**
- **It operates as a low data rate, low-power, and low communication range wireless ad hoc network, secured by 128-bit symmetric encryption keys, with a data rate of 250 kbps.**

Bluetooth Low Energy (BLE)

- Bluetooth Low Energy (BLE) aims to decrease power consumption compared to classic Bluetooth technology.
- BLE shares the same protocol stack as classic Bluetooth but supports quick transfer of small data packets with a 1 Mbps data rate. It does not support data streaming.
- BLE follows a master-slave architecture, where the master acts as a central device connecting to multiple slaves, making the devices power-efficient.

- Energy is conserved by keeping the slave nodes in sleep mode by default and waking them periodically to send data packets to the master node and receive control packets from the slave node.
- BLE is reported to be 2.5 times more energy efficient than Zigbee.

LORA

- LoRa, a long-range communication protocol, was initially developed by Cycleo of Grenoble, France, and later acquired by Semtech in 2012.
- It supports long-range communication up to 10 km and data rates less than 50 kbps while maintaining low power consumption.
- LoRa is particularly suitable for non-real-time applications that require fault tolerance.
- It operates in the physical layer combined with Long Range Wide Area Network (LoRaWAN) in the upper layers.

Fundamental of Control

SCADA systems make extensive use of electronic technology, the technology cycles are very short, and recommendations regarding specific types of hardware, software, communications protocols, etc. needs to upgrade as and when technology advances.

General control

Control consists of monitoring the state of a critical parameter, detecting when it varies from the desired state, and taking action to restore it. Control can be discrete or analog, manual or automatic, and periodic or continuous.

- The process variable is the parameter that is to be controlled
- Devices that measure process variables are transducers or sensors
- The setpoint is the desired value of the process variable.
- The control output

The process variable is the parameter that is to be controlled

- Examples of process variables in deep metal mine system are the temperature, humidity, air velocity etc.
- To be controlled, the process variable must be capable of being measured and that measurement converted into a signal that can be acted on by the controller.

Devices that measure process variables are transducers or sensors

In many cases, the process variable sensor consists of a direct measurement device, called an element and a separate signal processor called a transmitter. An example of this would be temperature measurement using a resistive temperature detector (RTD), as the element and a temperature transmitter, which converts the varying resistance value of the RTD into a current or voltage proportional to the temperature.

The setpoint is the desired value of the process variable

- Normally preset into the control system by an operator, or derived as an output of another control calculation.
- The error signal is the difference between the process variable and the setpoint and is the basis for control action.
- The controller is the device that processes the error signal, determines the required control action, and provides a control output to the process.

The control output

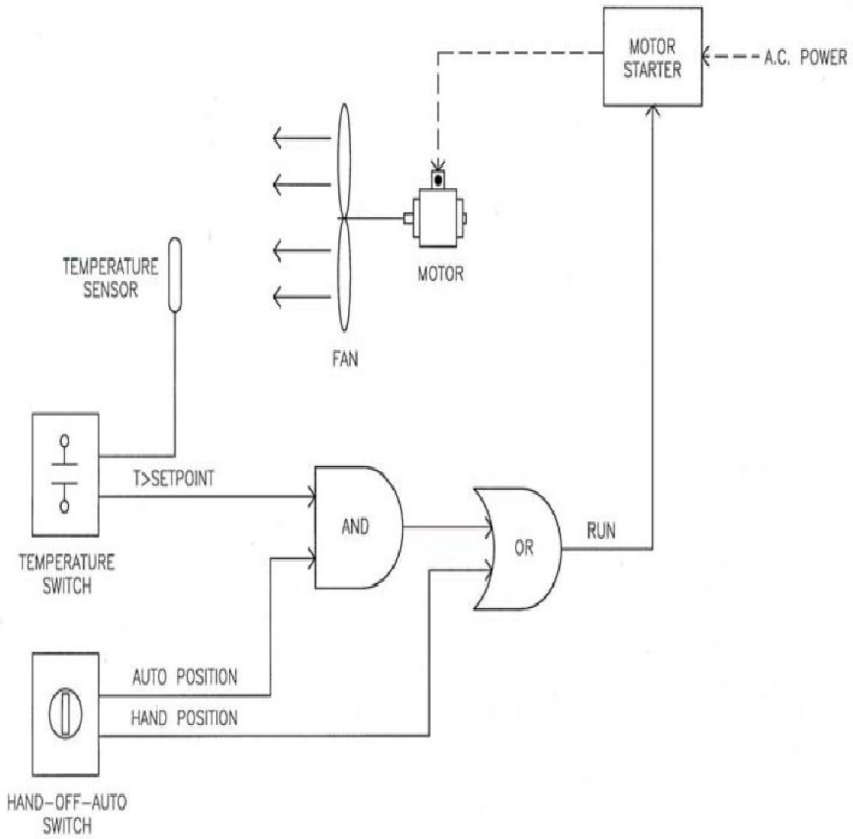
- usually must act on the system through another device to effect the desired control action, such as varying the position of a valve, the speed of a motor, or the current through a heating element.

- The device that converts the control output into control action is the actuator.

Discrete control

Discrete control deals with systems in which each element can only exist in certain defined states. An example of discrete control would be starting an exhaust fan when the temperature in a space exceeds a preset value and stopping the fan when the temperature falls below a lower preset value. The temperature (process variable) is either within the acceptable range, or outside of it.

The fan control relay (actuator) is either on or off. This type of control is implemented with logic diagrams and circuits. In discrete control, even though some of the parameters actually have a continuous range of values, the only information used by the control system is whether their value is greater than, less than, or equal to some desired value.



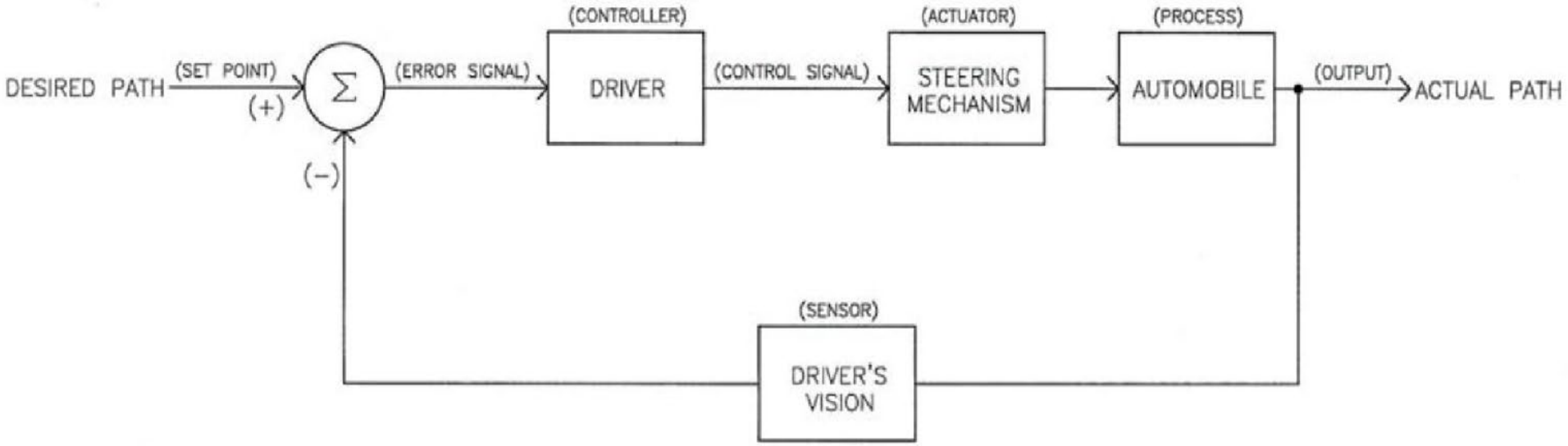
- **The devices used to sense system conditions in discrete control are typically electrical switches, with contacts that are open when the variable is in one state and closed when it is in the other.**

- **Similarly, the control action is typically produced by control relays, which open or close contacts in the control circuits of motors, valve actuators, or other devices.**

Analog control

Analog control deals with systems in which variables can have a continuous range of values, rather than simply discrete states. Basic analog control consists of the process of measuring the actual output of a system, comparing it to the desired value of that output, and taking control action based on the difference to cause the output to return to the desired value.

This process can be as simple as the driver of an automobile comparing the speedometer reading (process variable) to the speed limit (setpoint) and adjusting the position of the accelerator pedal (control action) to speed up or slow down the vehicle accordingly.



Analog control system block diagram

Classes of analog controllers

Analog controllers can be classified by the relationship between the error signal input to them and the control action they produce:

A. Proportional (P)

- **Controllers in proportional (P) control systems generate an output proportional to the error signal.**
- **An essential feature of P control is that the error signal must remain non-zero to prompt a control action.**
- **Consequently, P control alone cannot restore the process to the setpoint after an external disturbance.**

- **The steady-state offset, a non-zero error signal inherent in P controllers, is a defining characteristic.**
- **The adjustable parameter determining the proportionality of the controller's response is known as the gain.**
- **Higher gains result in larger control actions for a given error signal and faster system response.**

B. Proportional plus Integral (PI)

- Controllers in proportional-integral (PI) control systems generate a control action proportional to the error signal plus the integral of the error signal.
- The addition of the integrator enables the controller to eliminate steady-state offset and return the process variable to the setpoint value.
- The adjustable parameter controlling the integration constant of the PI controller is known as the reset, as it effectively resets the error signal to zero.
- An engine governor operating in isochronous mode, maintaining a constant RPM over the full load range, utilizes PI control to achieve this control behaviour.

C. Proportional plus Integral plus Derivative (PID)

- Controllers in proportional-integral-derivative (PID) control systems incorporate a component of control action proportional to the derivative of the error signal, representing the rate of change of the error signal.
- This control mode enables the controller to anticipate changes in the process variable by increasing control action for rapid changes, which is particularly beneficial for systems requiring fast response times or those inherently unstable without control.
- The adjustable parameter controlling the derivative component in a PID controller is known as the rate.

Control loops

- The complete control scheme required to control a single process variable or a group of related process variables is called a control loop.
- The control loop includes the relevant part of the process, the process variable sensor and associated transmitter(s), the input signals, the controller, the control output signal, and the actuator.
- The process of adjusting the gain, reset, and rate parameters to obtain effective and stable response of the system to changes in the setpoint or external disturbances is called loop tuning, and is an essential aspect of control system startup and commissioning.

Types of controllers

- Control can be implemented using either individual standalone controllers, known as single-loop controllers, or by combining multiple control loops into a larger controller.
- Single-loop controllers have provisions for a process variable input signal, a control output signal, setpoint adjustment, tuning of the PID control parameters, and typically include some type of display of the value of the process variable and the setpoint.

REFERENCES

- Army - Coe Technical Manuals (Tm) Tm 5-601 Supervisory Control And Data Acquisition (Scada) Systems For Command, Control, Communications, Computer, Intelligence, Surveillance, And Reconnaissance (C4isr) Facilities.
- https://www.techtarget.com/whatis/definition/SCADA-supervisory-control-and-data-acquisition
- Yadav, Geeta & Paul, Kolin. (2020). Architecture and Security of SCADA Systems: A Review, https://www.researchgate.net/publication/338500163_Architecture_and_Security_of_SCADA_Systems_A_Review

CONCLUSION

- Provided an overview of Supervisory Control and Data Acquisition (SCADA) systems.
- Explored the structural framework of SCADA systems, including hardware and software components.
- Traced the historical development and advancements in SCADA technology over time.
- Discussed the key elements that comprise a SCADA system, such as sensors, actuators, and control interfaces.
- Explored the various protocols used for communication between SCADA components.
- Introduced the basic principles and methodologies involved in controlling SCADA systems for monitoring and management purposes.


THANK YOU