UNIT II IOT Protocol

Standardization for IoT – Efforts – M2M and WSN Protocols – SCADA and RFIDProtocols – Issues with IoT Standardization – Unified Data Standards – Protocols – IEEE802.15.4–BACNet Protocol– Modbus – KNX – Zigbee– Network layer – APS layer – Security.

SCADA

Supervisory control and data acquisition is One of the IoT pillars to represent the whole industrial automation arena.

IEEE created standard specification called Std C37.1™, for SCADA & automation systems in 2007. In recent years, network-based industrial automation has greatly evolved. With the use of **intelligent electronic devices (**IEDs), or IoT devices in our terms, used in substations and power stations. The processing is now distributed and the functions that used to be done at control center can now be done by IED i.e. M2M between devices.

The ISA100 was developed by the standards committee of the Industrial Society for Automation formed to define procedures for implementing wireless systems in the automation and control environment with a focus on the field level.

OPC, which stands for Object Linking and Embedding (OLE) for Process Control standard specification developed by an industrial automation industry task force (IAITF) . The standard specifies the communication of real- time plant data between control devices from different manufacturers.

OPC was designed to provide a common bridge for Windows- based software applications and process control hardware.

In recent years, network-based industrial automation has greatly evolved with the use of intelligent electronic devices (IEDs), or IoT devices in our terms, in substations and power stations.

The processing is now distributed Functions that used to be done at control center can now be done by IED i.e. M2M between devices Due to restructuring of electric industry, traditional vertically integrated electric utilities are replaced by many entities such as

- GENCO (Generation Company),
- TRANSCO (Transmission Company),
- DISCO (Distribution Company),
- ISO (Independent System Operator), etc.

What is Supervisory Control and Data Acquisition (SCADA) System?

SCADA (supervisory control and data acquisition) is a category of industrial control systems (ICS) that remotely gathers data in real time from industrial processes in order to supervise and control equipment and conditions. SCADA tools enable organizations to control and monitor their industrial devices and make data-driven decisions regarding their industrial processes. SCADA can be used to manage almost any type of industrial process via a graphical

user interface (GUI). Both SCADA and ICS fall under the broader category of operational technology (OT).

- It is a computer-based industrial control system to inspect real-time data.
- It is a software application to monitor & control the whole industrial process through its graphical representation.
- SCADA collects various data in real-time from remote locations to control process & plant equipment.
- The large-scale industry consists of a huge number of processes, but monitoring and controlling each and every process is very complex since each piece of equipment issues or produces different outputs.
- It enables operators to optimize operations, detect abnormalities or faults, and make informed decisions to improve efficiency, productivity, and safety.

Components of a SCADA system

SCADA systems gather real-time data to help with the remote management of industrial sites in order to enhance industrial efficiency and output. A SCADA system requires both hardware and software components. The most common hardware devices in a SCADA system include the following:

- **Field devices (sensors and actuators).** A sensor is a device that detects inputs from industrial processes. It functions like a gauge or meter, displaying the status of a machine. An actuator controls the mechanisms of the various processes. It acts like a switch, dial or control valve to control a device. Both sensors and actuators are controlled and monitored by SCADA field controllers.
- **SCADA field controllers.** These elements are microcomputers that interface directly with sensors and actuators and send data to the human-machine interface (HMI). They also send control commands to the field devices to which they are attached. Field controllers come in two varieties:
- **Remote telemetry units.** RTUs, also called remote terminal units or remote telecontrol units, interface with field devices such as sensors, actuators and valves to collect telemetry data and transform it into useful information for human consumption. RTUs are often placed in remote locations, and can be programmed to suit different environmental conditions and applications. They can then initiate specific actions based on specific triggers.

- **Programmable logic controllers.** A PLC is a small digital computer typically used to control industrial processes based on certain inputs, as well as the standards and instructions provided for a specific process or application. PLCs can monitor and control many types of complex , automated and repeatable processes on a constant basis.
- **SCADA supervisory computers.** These control all SCADA processes and are used to gather data from field devices. They also send commands to those devices in order to control industrial processes.
- **Communication infrastructure**. Communication infrastructure enables SCADA supervisory systems to communicate with field devices and field controllers. This infrastructure enables SCADA systems to collect data from field devices and to control those devices.

SCADA software is HMI software. It consolidates and presents data from SCADA field devices, PLCs and RTUs for human consumption. HMI software usually includes a GUI that enables operators to understand, control, analyze and modify the status of SCADA-controlled equipment and processes.

The HMI provides a human-friendly way to interpret data, react to alarms and make data-driven decisions. For example, the SCADA system might send a notification to a user's phone that a device is not working properly. The operator can then decide to stop the device via the HMI. The HMI sends the appropriate command to the PLC or RTU, which then forwards the command to the malfunctioning device and causes it to stop.

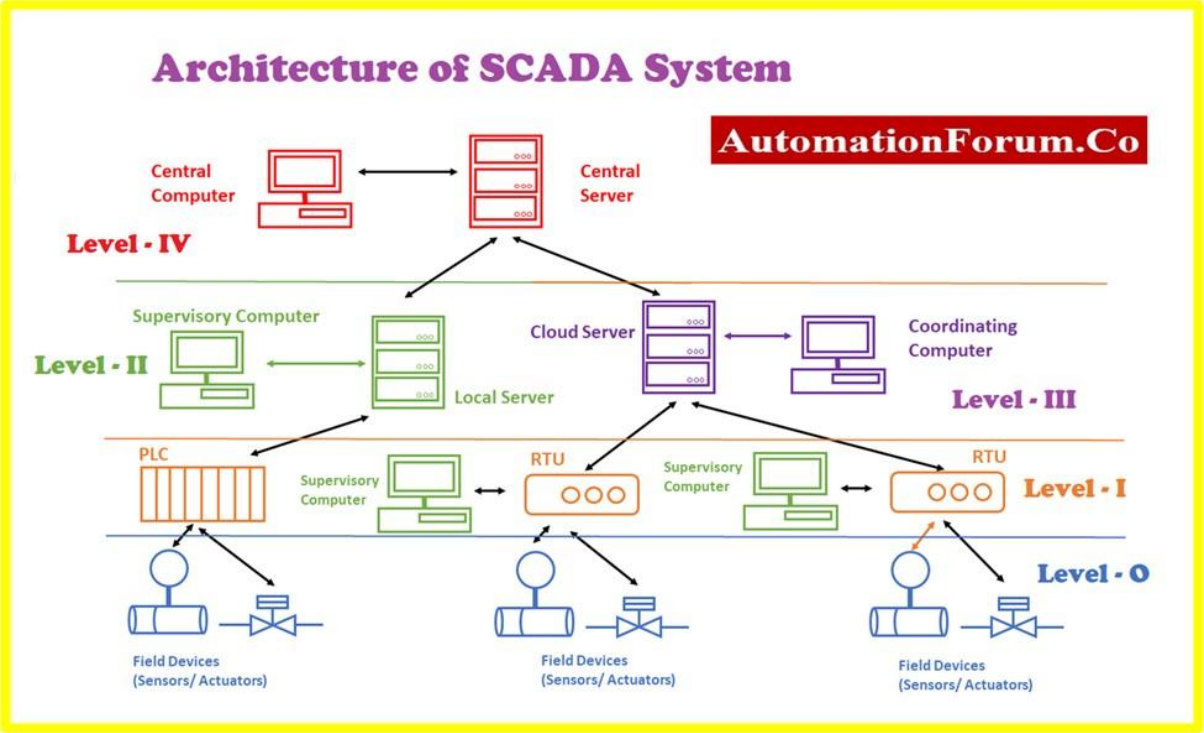
Features of SCADA systems

Most SCADA systems include the following features:

- **Data acquisition** is a foundation of SCADA systems. Sensors collect data and deliver it to field controllers, which, in turn, feed data to SCADA computers. The information is then delivered to an HMI device to support human analysis and decision-making.
- **Remote control** through the control of field actuators is based on the data acquired from field sensors.
- **Networked data communication** enables all SCADA functions. Data collected from sensors must be transmitted to SCADA field controllers that communicate with the SCADA supervisory computers. Remote control commands are transmitted back to actuators from the SCADA supervisory computers.
- **Data presentation** is achieved through HMIs, which represent current and historical data to the operators running the SCADA system.

- **Real-time and historical data** are both important parts of the SCADA system. Users can use live data for real-time equipment tracking and maintenance, and historical data to track current performance against historical trends and determine what -- if any -- improvements are required.
- **Alarms** alert SCADA operators to potential problems or significant conditions. Alerts can be configured to notify operators when processes are blocked, when systems fail or when other aspects of SCADA processes must be stopped, started or adjusted.
- **Reporting** on SCADA system operations can include reports on system status, process performance and reports customized to specific uses

Architecture of SCADA System



- Generally, the SCADA system is an integrated system for monitoring and controlling the entire process plant.
- SCADA is a pure software application provided on top of the hardware unit. A supervisory system gathers data on the process and sends the command control to the process. The SCADA is a kind of Remote Terminal Unit RTU.
- The SCADA system makes use of Local & Wide Area Networks, both these networks comprise internet protocols to enable data communication between the master station and ground or field devices.
- The sensor is the physical equipment connected to the PLC or RTU. The RTUs convert the sensor signals to digital data and send digital data to the master.

1. **Level 0 (Sensors & Actuators)**

- Level 0 is considered as a ground or field level.
- At this level, these field devices such as Sensors or Actuators usually interact with the physical environment. These devices function as technicians in a supervision system.
- This level consists of various types or classes of sensors and actuators.
- Basically, A sensor is a sensing device to sense the physical changes in process parameters and generates equivalent electronic signals.
- For example, we use RTD, or Thermocouple to measure the temperature of a process. Likewise, the SCADA system uses various sensors like Flow sensors, pressure sensors, LDR, and many more.
- But an actuator is an output device that makes some physical change in a system when an electrical or electronic signal is applied to it.
- For example, we make use of a solenoid valve to regulate fluid flow using an electrical method.

2. **Level I (Programming Devices)**

- Various programming devices such as Programmable Logic Controller, and Remote Terminal Units are the members of this category.
- The main objective of these devices is to monitor and control ground or field-level devices such as sensors and actuators.
- A SCADA system is made up of Local Area Networks (LAN), Wide Area Networks (WAN), or a combination of both networks.
- To build the SCADA system
    1. Local Area Network is used only for PLC
    2. Wide Area Networks are used only for RTU

3. **Level II (Local Control and Human Machine Interface)**

- Level II consists of supervisory computers, here various programming devices such as Programmable Logic Controller, and Remote Terminal Unit that controls the ground or field level devices are linked to these supervisory computer systems.
- Supervisory computers are a type of computer system that enables SCADA software for functioning; these may be linked to a specific machine or some machines that are similar to each other within that manufacturing unit.
- These Supervisory computers furnish actual instructions and commands for plant operation.

- These Supervisory computers can be easily operated by respective plant operators, supervisors, & technicians to observe and control production errors.

4. **Level III (Coordination)**

- Coordination is the second top level of the SCADA System.
- In this level-III Coordination is used to coordinate the computers that come under this level.
- Generally, these computers are linked to various control systems of the plant.
- Coordination aims to collect process data from various sections of plants in one place.
- At this level, various activities such as planning, scheduling, and managing event time are done by the plant in charge or section manager.

5. **Level IV (Central Control)**

- Central Control is the topmost level of the SCADA System.
- Here, a central computer is linked to various equipment or machines .
- Generally, this level is governed by the management team of the plant.
- The management team has a right to make decisions by using the data and information that are collected and stored.
- Through this Central Control level, the management team can visualize each and every action and operation of the plant.

Difference Between PLC and SCADA

Essential parts of industrial automation, PLC (programmable logic controller) and SCADA (supervisor control and data acquisition) have various uses even if they are While SCADA is a software-based system for supervisor level process monitoring and control, PLCs are mostly utilized for hardware-level control of machines. The following table shows their variations:

Aspect	**PLC**	**SCADA**
Full Form	Programmable Logic Controller	Supervisory Control and Data Acquisition
Nature	Hardware-based	Software-based
Primary Function	Controls processes in industries like motors, machines, etc.	Supervises, monitors, and controls plant operations
Components	Processor, I/O Modules, Programming Device, and Power Supply	MTU (Master Terminal Unit), RTU (Remote Terminal Unit), HMI (Human Machine Interface)
Types	Fixed (Compact) and Modular	Monolithic, Distributed, Networked, and IoT

Input/Output Representation	Represented as NO (Normally Open), NC (Normally Closed), and coil contacts	Represented as images
Component Identification	Components are identified by addresses	Components are identified by names
Control Scope	Operates at a machine or equipment level	Supervises at the plant or process-wide level
Complexity	Handles real-time, low-level process control	Manages high-level process visualization and data analysis
Data Logging	Limited or none	Extensive, includes trends and historical data
Communication	Communicates with field devices directly	Interfaces with multiple PLCs and other systems
Cost	Relatively lower	Higher due to software and integration capabilities

Advantages of SCADA

The SCADA system offers numerous advantages, including:

1. Enhances operational efficiency and output quality.
2. Reduces system failures and enhances uptime.
3. Minimizes the need for frequent maintenance.
4. Simplifies complex processes, requiring less manual intervention.
5. Enables the monitoring of large-scale system parameters.
6. Automates processes, decreasing the need for human labor.
7. Facilitates quicker identification and resolution of faults.
8. Provides accurate fault identification and location.
9. Records vast amounts of operational data for analysis.
10. Presents data in various formats as per user needs.
11. Supports thousands of sensors for effective monitoring and control.
12. Offers operators real-time data simulations for better decision-making.
13. Ensures quick reactions to changing conditions.
14. Easily adapts to additional resources or expanded systems.
15. Provides detailed on-screen displays of operational status.
16. Allows integration of new control units and sensors as required.
17. Operates effectively under critical conditions.

Disadvantages of SCADA

Despite its benefits, SCADA systems have some limitations:

1. The system relies on interdependent modules and hardware units.
2. Needs skilled operators, analysts, and programmers for maintenance.
3. Involves significant initial investment.
4. Reduces the need for manual labor, potentially increasing unemployment rates.
5. Limited to specific hardware devices and compatible software.

Applications of SCADA

SCADA systems are widely used in various industries and applications, including:

Turbines and Generators: Monitoring and controlling equipment performance.

Power Generation and Distribution: Monitoring and controlling power plants, transmission, and distribution systems.

Public Transport: Managing train systems, traffic lights, and other transportation infrastructure.

Water and Sewage Systems: Controlling water treatment, distribution, and reservoir management.

Manufacturing: Supervising and automating factory processes.

Industrial and Building Systems: Managing heating, cooling, and other building operations.

Communication Networks: Overseeing data and signal transmission systems.

Oil and Gas Industries: Monitoring pipelines, refineries, and storage facilities.

Traffic Control Systems: Managing urban and intercity traffic signals.

RFID in IoT

RFID (Radio Frequency Identification) is a type of wireless communication that uses electromagnetic or electrostatic coupling in the radio frequency spectrum to uniquely identify an object, animal, or human.

It is a technology used for automatically identifying and recording data about an object via a tiny, uniquely identifiable microchip tag connected to the object. A built-in antenna on the RFID tag interacts with a scanning device that can remotely read the tag's data.

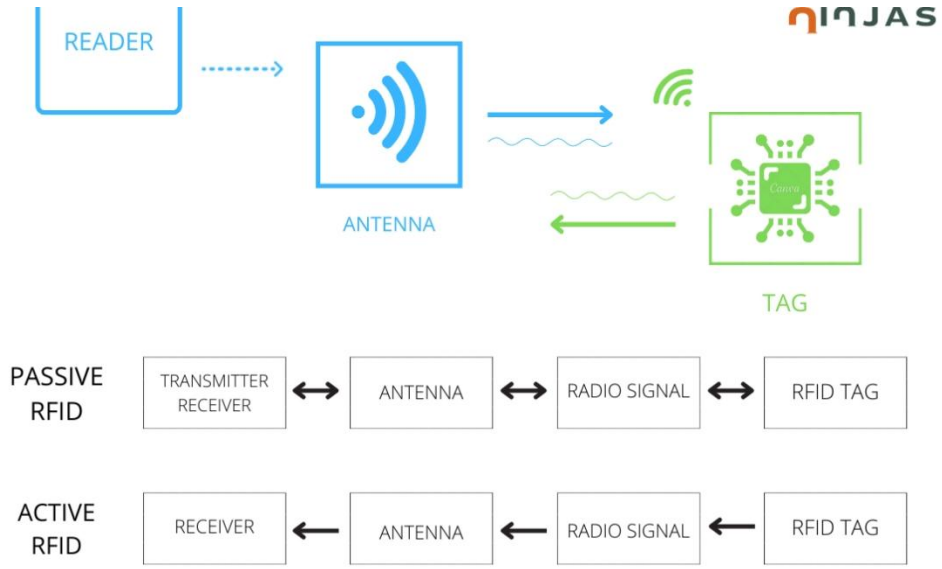
The scanning device scans the tag when it comes in range. After that, the data is sent from the scanning equipment to an application program. With the help of the application, the user will store and send it wherever he desires

Working of RFID

RFID, or radio frequency identification, is a technique for automatically identifying and capturing data about an object that has been stored in a small microchip tag attached to the

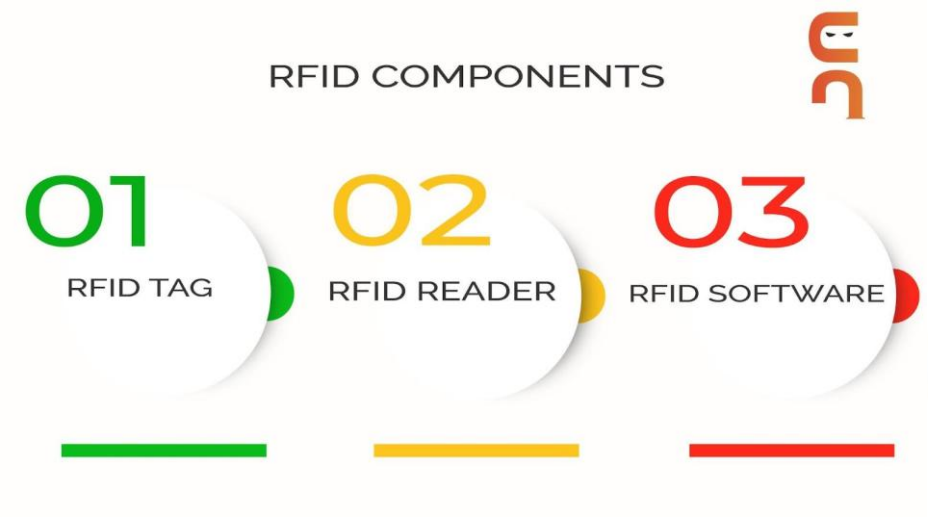
object. An antenna built into the RFID tag communicates with a scanning device that reads the data remotely. This data is then transferred from the scanning device to the data-housing enterprise application software. Each RFID tag has a unique identification number.

RFID can be used to track and control asset and personnel movement. RFID tags can be found on the back of library books and even in the new biometric passports. It simplifies the management of assets contained in boxes or pallets.



Components of RFID

Radio Frequency Identification technology consists of three main components:



1. **The RFID tag**: The RFID tag comprises an integrated circuit, a substrate, and an antenna. If the tag has an active power source and thus can support a sensor, it is called an active RFID tag. If the tag doesn't have an active power source, it is called a passive RFID tag.

2. **The RFID reader:** It is a device that reads RFID tags and gathers data about the connected object. It can be both wired and wireless. It can use many technologies to communicate with the software, including USBs and Bluetooth connections.

3. **The RFID software**: The software monitors and tracks the object connected to the RFID tags. It can be called data exchange and management software.

Applying RFID to IoT Devices

RFID tags are helpful in cameras, GPS, and other smart sensors when used in IoT. They can aid in the identification and location of objects. It is a low-cost way to make household objects "smart," similar to the popular Google Nest products. RFID tags are being used by some healthcare systems to track patients and their medical records. RFID is used in transportation systems to read passenger data, control traffic, and update transportation systems.

Role of RFID in IoT

Radio Frequency Identification technology is one of the three main components of IoT, along with the Savant system and the Internet. Thus, it has had wide-ranging implications for IoT development as a whole.

RFID technology has a wide range of applications in the Internet of Things. RFID tags are generally used to enable ordinary things to interact with one another and with the central hub and report their status. These features serve as the building blocks for an IoT system. To put it another way, RFID technology allows IoT to connect items to a network and will enable them to produce and deliver data.

Types of RFID

There are many kinds of RFID, each with different properties, but perhaps the most fascinating aspect of RFID technology is that most RFID tags have neither an electric plug nor a battery. Instead, all of the energy needed to operate them is supplied in the form of radio waves by RFID readers. This technology is called passive RFID to distinguish it from the(less common) active RFID in which there is a power source on the tag.

- **UHF RFID (Ultra-High Frequency RFID)**. It is used on shipping pallets and some driver's licenses. Readers send signals in the 902-928 MHz band. Tags communicate at distances of several meters by changing the way they reflect the reader signals; the reader is able to pick up these reflections. This way of operating is called backscatter.
- **HF RFID (High-Frequency RFID).** It operates at 13.56 MHz and is likely to be in your passport, credit cards, books, and noncontact payment systems. HF RFID has a

short-range, typically a meter or less because the physical mechanism is based on induction rather than backscatter.

- **Passive RFID:** Passive RFID tags does not have their own power source. It uses power from the reader. In this device, RF tags are not attached by a power supply and passive RF tag stored their power. When it is emitted from active antennas and the RF tag are used specific frequency like 125-134KHZ as low frequency, 13.56MHZ as a high frequency and 856MHZ to 960MHZ as ultra-high frequency.
    - No need embedded power
    - Tracking inventory
    - Has unique identification number
    - Sensitive for interference
    - Semi-passive RFID

- **Active RFID:** In this device, RF tags are attached by a power supply that emits a signal and there is an antenna which receives the data. means, active tag uses a power source like battery. It has it's own power source, does not require power from source/reader.
    - Embedded power: communication over large distance
    - Has unique identifier /identification number
    - Use other devices like sensors
    - Better than passive tags in the presence of metal

There are also other forms of RFID using other frequencies, such as LF RFID (Low-Frequency RFID), which was developed before HF RFID and used for tracking.

BACnet Protocols

BACnet, which stands for "Building Automation and Control Networks," is a widely used communication protocol specifically designed for building automation and control systems. It enables interoperability and communication between various devices and systems in buildings, such as heating, ventilation, air conditioning (HVAC), lighting, access control, fire detection, and more. BACnet is essential for creating integrated and efficient building automation systems.

Here are some key features and details about the BACnet protocol:

Open Standard: BACnet is an open, vendor-neutral protocol standardized under the ANSI/ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning