Unit-3

IoT: Design Methodology.

3.1) Steps
3.2) Basics of IoT Networking
3.3) Networking components
3.4) Internet structure
3.5) Connectivity technology
3.6) IoT communication models and IoT communication APIs
3.7) Sensor Networks
3.8) Four pillars of IoT :-
- 3.8.1) M2M
- 3.8.2) SCADA
- 3.8.3) WSN
- 3.8.4) RFID

3.1> IOT: Design methodology: steps:-

- The designing IoT systems can be a complex and challenging task.
- The role of IoT designer is to design IoT system keeping specific products/services in mind.

- IoT Design methodology that includes
1. Purpose and Requirements Specificatn
2. Process Specificatn
3. Domain model Specificatn
4. Informatn model Specificatn
5. Service Specifications
6. IoT level Specificatn
7. Functional view specificatn
8. Operational view specificatn
9. Device and component Integratn
10. Appln Development.

- The proposed methodology have reduced design, testing and maintenance time, better interoperability and reduced complexity of IoT system.

5.2) Basics of IoT Networking:
- An IoT or a very complex system involving sensors, actuators, networks, local area, wide area, internet & diff. servers, diff. algorithms, ML and so on.
- All these executing together to make the system fun or one single entity.
- An IoT based system consist of physical objects and that are fitted with diff. sensors.
- These sensors are fitted things, sensors actuators & diff. other devices.
- These components become diff. nodes in the n/w or individual nodes in the n/w.
- IoT is basically internet based IoT. So the flow of info is through the internet or some other wide area n/w.
- Finally, it is arrive at the intended destination node for further processing.
- These diff. protocols that are used for something diff. purposes in IoT. The IoT comm^n protocol concept already explained in previous unit also.

details about these protocols.

- When we talk about IoT n/w we consider following points.
  1. N/w arch. is comm^n bet^n IoT devices, n/w and the outside world.
  2. Correct choice of comm^n tech. indicates the IoT devic n/w requirement and costs.
  3. IoT based appl^n single n/w paradigm is not sufficient to address all the needs of IoT device.
  4. Complexity of n/w, in that we have to consider the issues like
     - Growth of n/w.
     - Interfacing among devices
     - N/w mgmt.
     - Heterogeneity in n/w
     - Protocol standardizat^n with n/w.

3.3) Networking Components: -

- The following fig. shows the IoT based networking component.
- We have diff. things. These things can be diff. physical obj.s which are fitted with diff. sensors. for example things like telephones, lightning systems,

cameras, diff. other scanner sensors like the temp. sensor & so on.

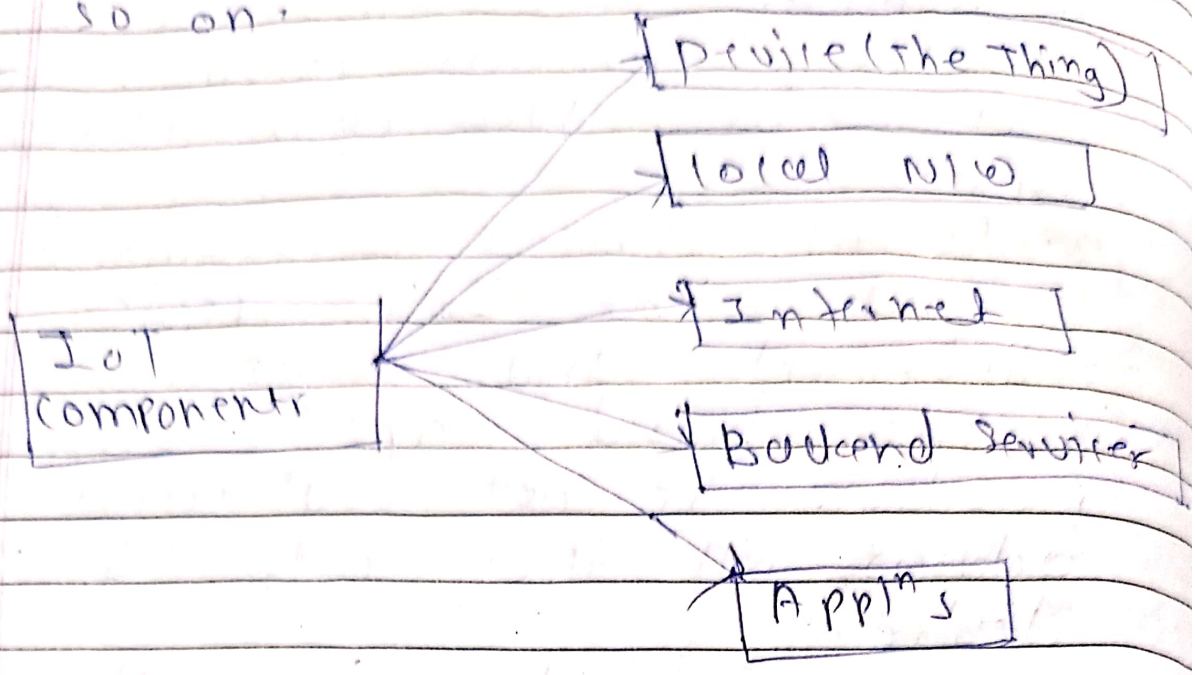

Fig. Basic IoT components

- These things are able to communicate with one another with the help of wireless technologies like Zigbee, Bluetooth wi-fi and so on.

- Functional components of IoT:- For building IoT system following functional component are important.

1. Component for interaction & comm^n with other IoT devices.
2. Component & processing & analysis

4. operations.
3. Components for internet infrastructure
4. Components for handling internet services & applications.
5. Components to integrate application service.
6. User interface to access IoT.

3.4) Internet structure:-

Internet is interconnected world wide computers in the form of a network. The user can access the knowledge from other computers. The internet is also defined as a network of networks.

- Structure of the internet:-

The structure of internet is divided into 3 parts:-

1.) Internet Addressing:-

- computer connected to the internet means that the systems are connected to computers worldwide network. It is necessary to that each machine/device has it's own or unique address.

2.) Protocol stack & Packets:-

- As the device is connected to the internet with a unique address. The next thing, what is the procedure to communicate the device with the system at another end?
- If you are using ISP facility then the message will be communicated via phone like ISP.

3. Complete Infrastructure:-
- The framework of the internet consists of multiple interconnected large n/ws. That large n/ws is called as Network service provider. The internet structure is built up of packets & routers. Addresses are embedded in the headers of packets.

3.5) Connectivity Technology:-
- In this sect^n we will discuss diff. connectivity technologies used in IoT system. As we know that IoT this communicat^n we need some protocols.
- The following fig. shows the structure of diff. protocols used

in various layer. We will discuss the protocols in each layer short.

(a) Appln Layer:

In this layer, protocols define how the data can be sent over the nw with the lower layer protocols using the appln interface. The protocols HTTP, CoAP, Web socket, XMPP, MQTT, DDS, and AMQP are used in appln layer.

1) HTTP:-
- HTTP stands for Hypertext Transfer Protocol (HTTP)
- Forms foundatn of WWW.
- HTTP follows a request-response model
- HTTP uses URI to identify HTTP resources.

2) CoAP
- CoAP stands for constrained Appln Protocol.
- CoAP is used for Machine to Machine applns.
- CoAP uses client-server architecture.

3) Web socket:-
- Web socket is a TCP type of commn protocols.
- Web socket allows full-duplex

comm^n over single socket

4) mqtt:
- mqtt stands for message queue telemetry transport
- mqtt is a light-weight messaging protocol
- mqtt is suited for constrained environment where devices have limited processing.

5) xmpp:
- xmpp stands for Extensible messaging and presence protocol (xmpp)
- xmpp used for appl^n such as, multi-party chat and voice/video calls.

6) DDS:-
- DDS stands for Data distribution service.
- Like mqtt, DDS uses publish subscribe model.
- DDS Provides Quality-of-service control & configurable reliability.

7) AMQP:-
- AMQP stands for Advanced messaging queuing protocol.
- AMQP is used for business messaging

b) Transport Layer: -

- Transport layer protocols provide end-to-end message transfer capability idenpedat of the underlying nlw.
- Transport layer protocol provides comm^n either conn^n oriented or conn^n less.

1) TCP: -

- TCP stands for Transmission control Protocol.
- TCP is conn^n oriented protocol that means it establishes the conn^n prior to the comm^n that occurs betn the computing devices in a nlw.
- TCP is reliable protocol as it follows the flow and error control mechanism.

2) UDP: -

- UDP stands for User Datagram Protocol.
- UDP transfers data quickly or conn^n establishment phase faster time.
- UDP is less reliable as compared TCP b'coz it is conn^n less protocol and does not support retransmission of data or removal of duplicate packets

c) N/w layer: -
- N/w layer is responsible for sending datagram's from source n/w to destn n/w. Host addressing scheme is managed by IP addresses.

1) IPV4:
- IPV4 stands for Internet Protocol version 4
- IPV4 is connⁿ less proto(s) doesn't guarantee delivery of packets.

2) IPV6: -
- IPV6 stands for Internet prot version.
- IPV6 is a successor of IPV4. It uses 128 bits for an IP address.

3) 6LowPAN: -
- 6LoWPAN stands for IPV6 Low power Wireless Personal Area N/w.
- It operates 2.4 GHz frequency and data rate is 250 kb/s.

d) Link Layer: -
- Link layer proto(s) is determine that how the data is physically sent over the n/w through physical medium.

- The physical medium can be a copper wire, pair cable, radio wave or coaxial cable etc.

1) Ethernet:
- Eternet is the most popular physical layer LAN tech.
- A standrard Ethernet n/w can transmit dates at a rate up to 10 megabits per second.

2) WinMAX:-
- WinMAX stands for worldwide Inter-operability for Microwave Access.
- Data rate is 1.5 mb/s to 1 Gb/s.

3) LR-WPAN:-
- 802.15.4 - WPAN stands for low Rate - Wireless Personal Area N/W.
- Data Rate of 40 kb/s to 250 kb/s can be achieved using WPAN standrads.

4) Wi-Fi:-
- 802.11 - Wifi most popular protocol for wireless Area N/W.
- Data rate of 1 mb/s to 6.75 Gb/s can be achieved using these standard.

5) 2G | 3G | LTF - Cellular:-
- These standards provide Comm^n over cellular n/w.

- Data rates of 9.6 kbps for 2G devices upto 100 mbps for 4G devices can be achieved using these standards.

3.6> IoT communicatn models & IoT commn APIs :-

- **IoT commn models :-**

In IoT commn can be carried in diff. ways. So following sectn describes diff. commn model in detail.

1> **Request - Response commn model**

- As per name Request-Response commn model, the client sends request to to server and the server responds to the request.
- When the server receives a request, it processes the request, retrieves resources, prepares the response, and then sends the response to the client.

2> **Publish - Subscribe commn model**

- Publish - Subscribe commn model has 3 elements publishers, brokers & consumers.

- publishers are the source. So the once the data is recived from publisher, broker sends the data to all subscribed consumer.
- In this model publisher are not aware about the consumer.

3) Push-Pull comm^n model:-
- In Push-Pull comm^n model, in which the data producers push the data to queues and the consumers pull the data from the queues.
- In this comm^n model, queues are used to separate out the single producer consumer comm^n.
- In this queues also act as a buffer.
- Queues used in such situations when there is a mismatch betn the rate at which the producers push data and the rate at which the producers push data and the rate at which the consumers pull data.

4) Exclusive pair comm^n model:-
- Exclusive pair comm^n model is a bidirectional, fully-duplex comm^n.
- It uses a persistent conn^n betn the client and server. It means once the client sends a request to close the conn^n.

- Once the connⁿ is setup client and server can send messages to each other.
- Exclusive pair is a stateful commⁿ model and the server is aware of all the open connⁿs.

3.6.1 IOT commⁿ APIS:-

In this section we will study two commⁿ APIs that are mostly used in IOT based applⁿ. Before that we will see what is API.

- What is an IOT API?
- The applⁿ program or programming interface, or API, is the together the connected "things" of the "Internet of Things."
- IOT APIs are provide the interactⁿ betⁿ an IOT device and the internet and/or other elements within the n/w.

- REST - based commⁿ APIs
- Representational state Transfer is a set of architectural style by which you can design Web services and Web APIs.
- These APIs focus on a system's

resources and how resource state is addressed and transferred.
- REST APIs follow the request-response comm^n model described in previous segⁿ.
- Most of the APIs works over HTTP which consists of HTTP command.

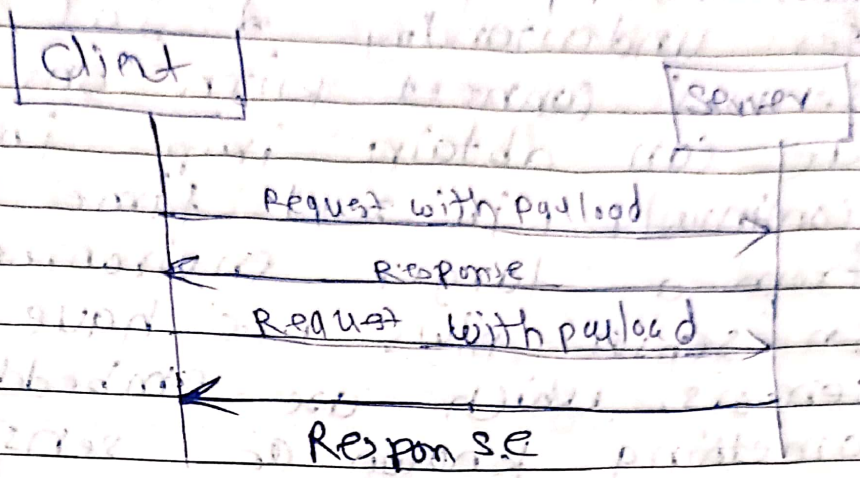

Fig. client-server comm^n using REST

REST based APIs follows the following characteristics :-

1) client - server
2) stateless
3) cache - able
4) Layered System
5) Uniform Interface
6) code on demand.

3.7> Sensor Networks:-

- Sensor network is a very imp. technology and one of the most imp. enablers of IOT that is used for building IOT.
- Sensors, transducers, actuators these are all very important things for understanding of IOT system.
- Sensors connect with one another we can obtain imp. info continously, in real time remotely from a larger environment.
- In sensor n/ws we have individual sensors, which are embedded in something known as sensor device or sensor nodes, or sometimes also known as sensor nodes.
- One device communicates with another device, that device communicates with another device the third device with a fourth fourth with the first and so on.
- As we know that we have diff. types of topologies, we can have all sorts of topologies that we have already heard of in n/ws.

3.7.1> Wireless Sensor n/w:-

- A wireless Sensor n/w (WSN) is

a distributed device with sensors deploy over an area.
In WSN sensor nodes are capable of wireless together with one another and measuring the condition of their surrounding environment.

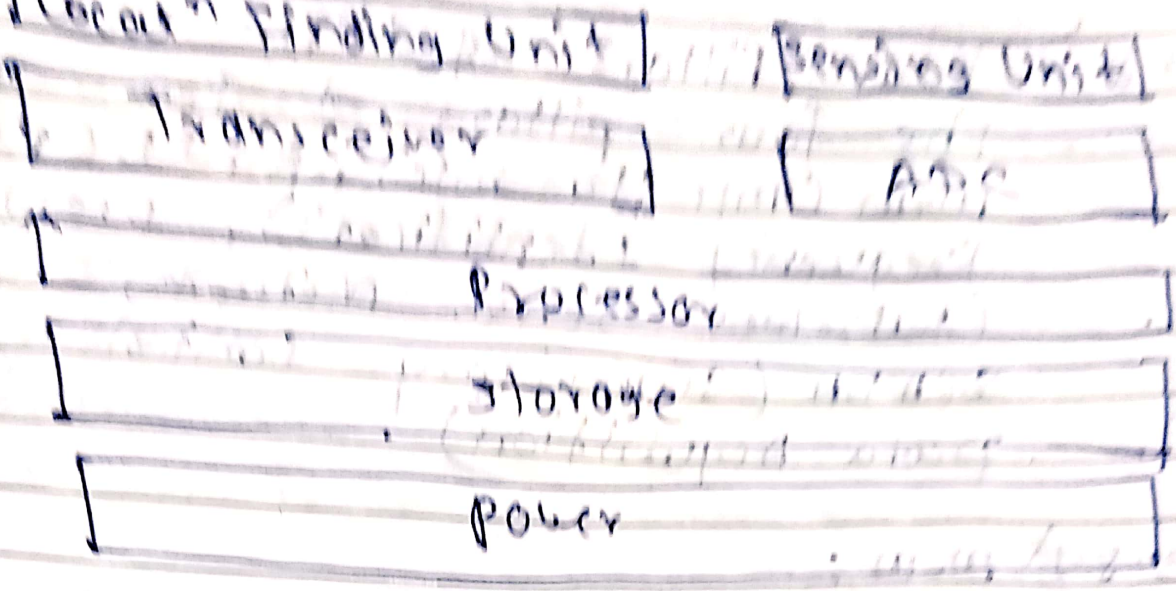

Fig. Basic components of wireless Sensor Node.

- In WSN we have diff. units
- In WSN the first thing required is sensing unit. The sensing unit basically sense the particular physical phenomena.
- Then next unit is processing unit. It is used to process info which is sensed by sensor
- Then a next unit is the analog digital converter.

- So, these are the different units and we have other optional units such as the locating systems for example GPS etcetera.

3.8) Four Pillars of IOT:-
- The four pillars of IoT are M2M (mic to mic), RFID (Radio frequency Identificat^n), WSN (Wireless Sensor Network) and SCADA (Supervisory control & Data Acquisition).

3.8.1) M-M :-
- M2M literally means mic to mic communicat^n
- M2M enables flow of data betn mic which monitors data by means of sensors.
- At other end gathered data is extracted the info & process it
- M2M also called as a subset of IOT.
- For example if your train is cancled due to poor weather, a smart alarm clock would determine the extra time you'll need to reduce diff.

route, and wake you up early enough so that you're not late for work.
- Another example M2M is smart Home, a connected thermostat can automatically switch the heating on when room temp. falls below a certain point.
- key features of M2M comm system are given below:
(a) Low Mobility (b) Time controlled
(c) Time Tolerant (d) Packet Switched
(e) Online small data transmission
(f) Monitoring
(g) Low Power Consumption

3.8.2) RFID:
- Second pillar of IoT is RFID that is Radio frequency Identification
- This RFID tag is a simplified, low-cost, disposable contactless smart card.
- RFID tags include a chip that stores a static number (ID) and attributes of the tagged obj.
- An RFID system involves hw known as readers and tags as well as RFID sw or RFID middleware.

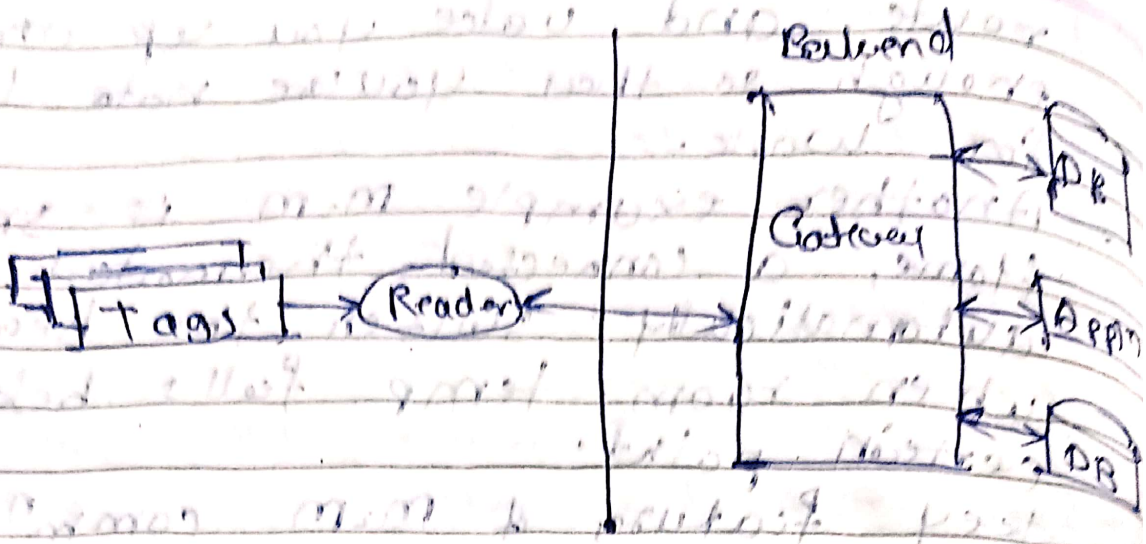

Fig. A General Overview of RFID Ar

- Firstly items tags are scanned by reader. Secondly, in backend transmitted data coming through antenna are being recognized by RFID based system PC.
- The working example of RFID appl?:-
- A RFID base Attendance system RFID system is used to maintain and checking database for members of an institution.
- The basic idea involves each person of the institution having ID card.
- RFID is considered as a non specific short range device. It can use frequency bands without

of license.

3.8.3> WSN :-
- Wireless Sensor N/w to sense and gathers data using sensors which are spatially distributed.
- WSN collect this data into a centralized locatn with the help of wired / wireless connn.

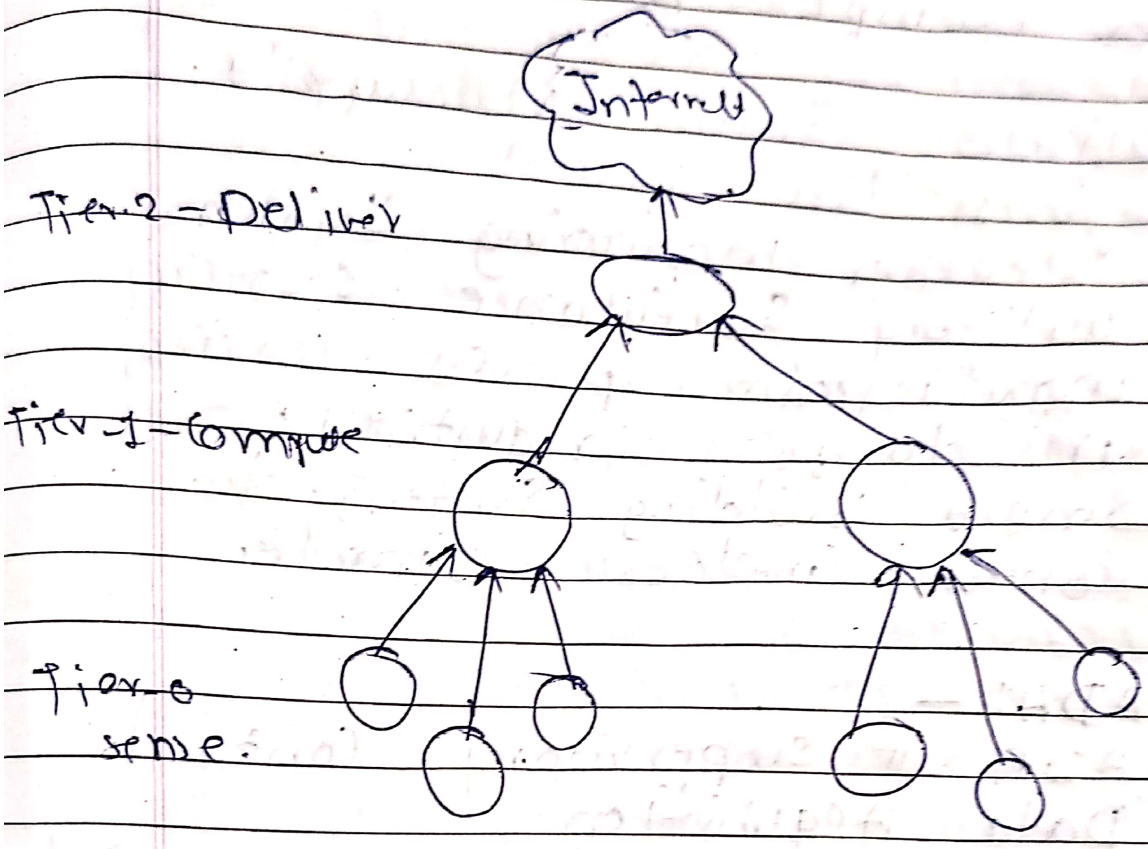

Fig. Sensor n/w. arch.

- Recently with the development of WSN, it led to distributed wireless sensor & actuator n/w's that are capable. Obsrvi

the physical world.
- Based on observation it makes the decision & performed the appropriate action.
- wireless sensor n/w consist of 3 elements, sensors, wireless modules & open source API.
- The development of WSNs was motivated by military appln's for example battlefield surveillance

- Wireless Sensor N/W appl^n's:-
1. forest fire detect^n
2. Weather monitoring System
3. Military Surveillance system
4. manufacturing process control in large industries.
5. Smart Building System to control indoor climate.

3.8.4) SCADA:-
- SCADA is supervisory control & Data Acquisition.
- SCADA is S/W used to control the H/W. for example PLC, drives, servers, sensors & also obtain the data which is stored on the personal comp. or human m/c interface.

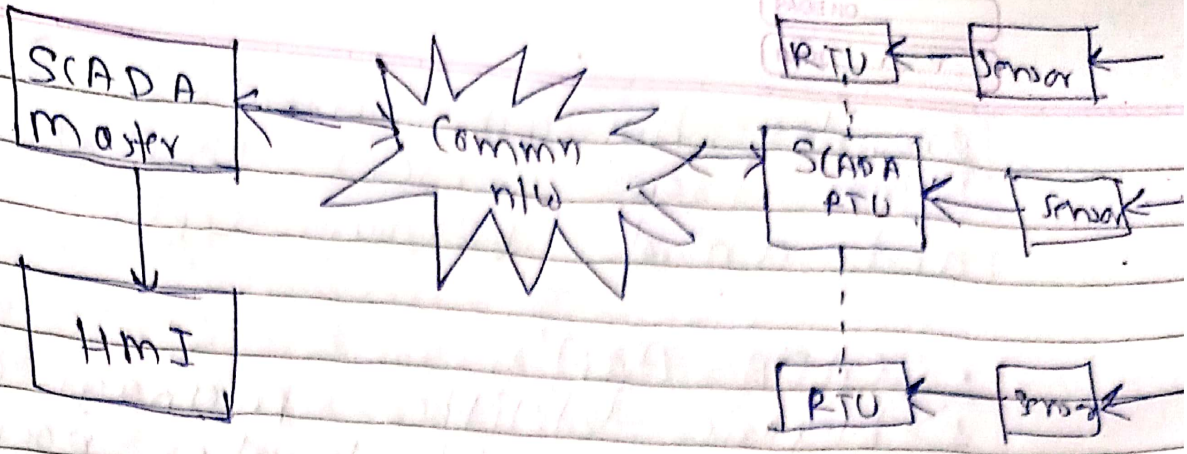

Fig. SCADA Arch.

- SCADA uses BACNet, CanBus & Wired Field Buses.

1) Sensors:- There are two types of sensors analog & digital. Different sensors are use like temp. humidity, current, motion, and water appl^{n}s.

2) RTU - Remote Terminal Unit: RTU connects to sensor in the process as well as SCADA master using comm^n network.

3) HMI - Human Machine Interface:- HMI is interactn on human operators & m/cs. HMI is tools that presents process data to a human operator.

4) SCADA master:- SCADA master consist of programmable controls, multiprotocol support &

provides human interface. It tak. i/ps from sensors through RTUs and controls various appln's.

- SCADA Appln's: -

1) Electric Utilities - manage (unte voltage, circuit breaker, power grid.
2) Water & Sewage:- monitor & control water level, water flow, water pipe pressure.
3) Building:- control heating, ventilatn, air conditioning, violet, lighting & building access systems.
4) Mass transit - Requestn of electricity, trace & locate buses, trains.
5) Railways / Roadways:- control traffic signal lights.