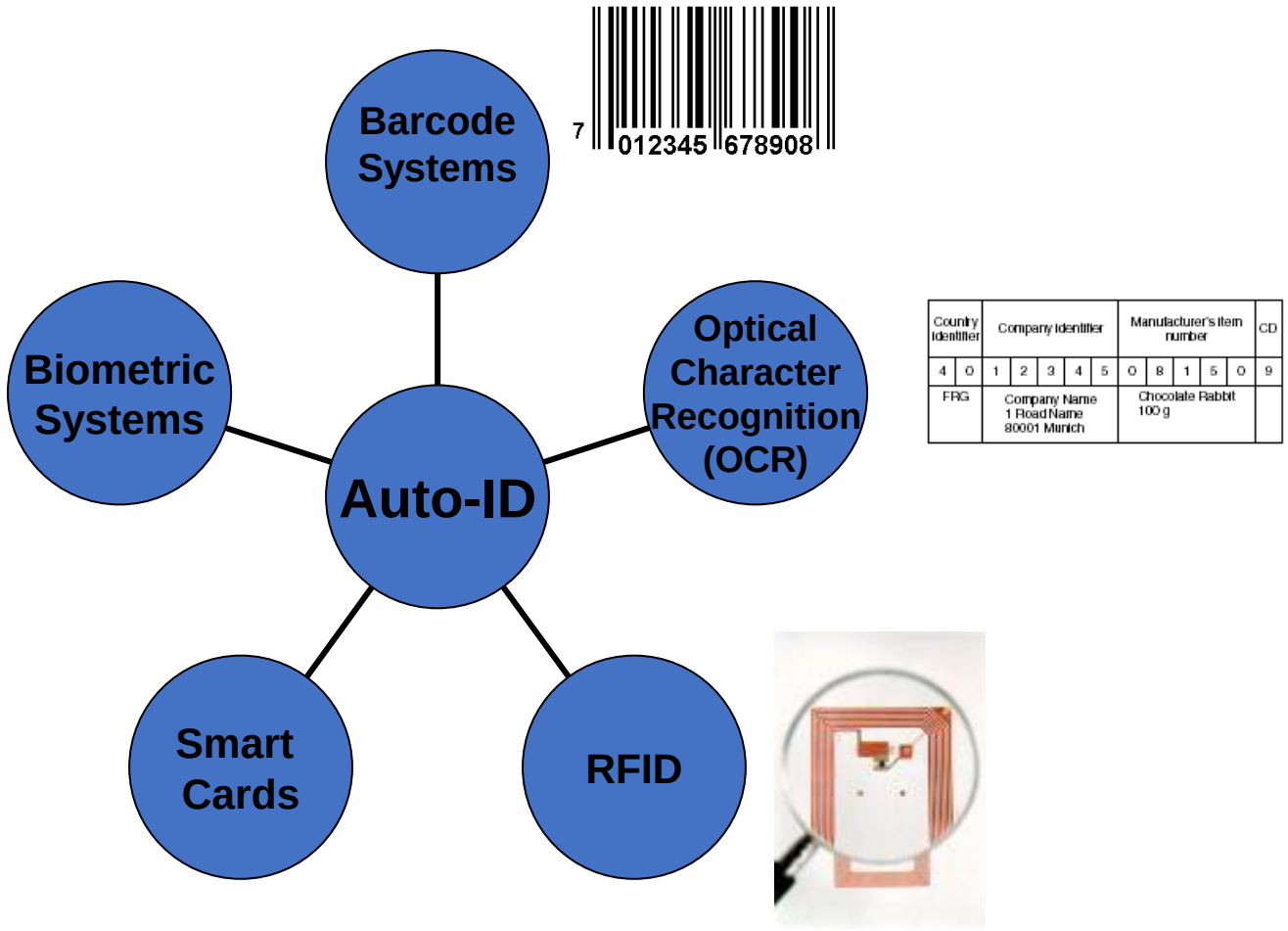
Module 3

Technologies Behind IoT

Four pillars of IoT - RFID,WSN,SCADA and M2M

- RFID = Radio Frequency IDentification
- An ADC (Automated Data Collection) technology that:
  - Uses radio-frequency waves to transfer data between a reader and a movable item to identify, categorize, track
  - Is fast and does not require physical sight or contact between reader/scanner and the tagged item
  - Performs the operation using low cost components
  - Attempts to provide unique identification and backend integration that allows for wide range of applications
- Other ADC technologies: Bar codes, OCR

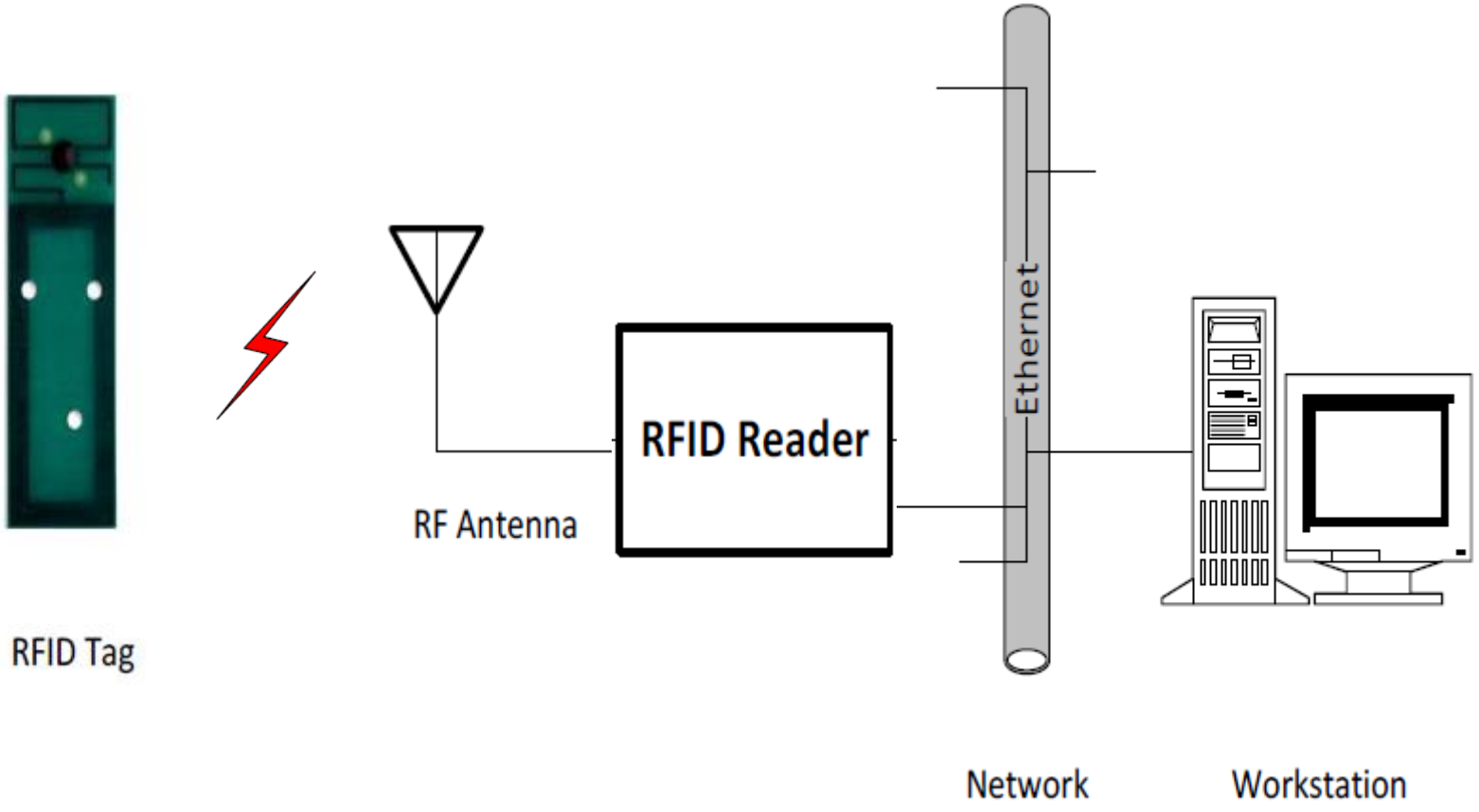
Auto-ID Technologies



- Consider the scenario

- An alternative,
  - just pick up things from the mall, place your bag on the scanner and just pay the bill and leave

RFID System Components

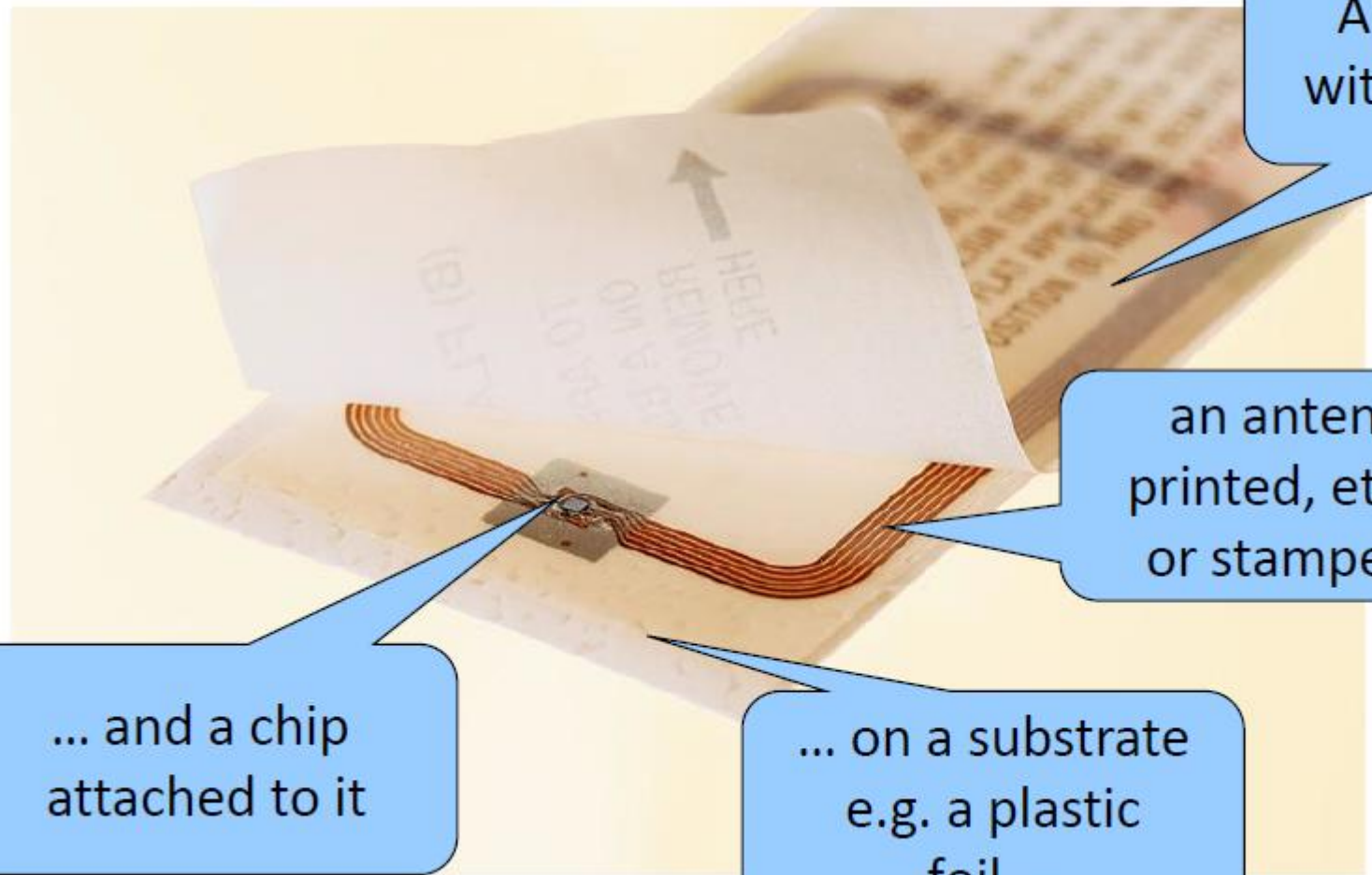


RFID tags

- An **RFID tag** (also referred to as a **transponder**) is an electronic device that communicates with RFID readers.
- An RFID tag can function as a beacon or it can be used to convey information such as an identifier.
- RFID consists of
  - a small integrated circuit chip
  - attached to a miniature antennae (transmitting a unique serial number)
  - a mobile or stationary reader in response to a query
  - database where information about tagged objects is stored.

- Every RFID tag has a unique identification number.
- The identification number includes not only the traditional information contained in a printed barcode (indicating manufacturer and product type)
- a unique serial number for that tag, meaning that each product or item will be uniquely identified.

RFID Tags: Smart Labels



A paper label with RFID inside

an antenna, printed, etched or stamped ...

... and a chip attached to it

... on a substrate e.g. a plastic foil ...

Types of RFID tags

- There are three types of RFID tags.
- **Passive**
  - Most RFID tags are passive.
  - They do not contain a power source and obtain the power needed to operate from the query signal itself.
  - An RFID reader must first query a passive tag, sending electromagnetic waves that form a magnetic field when they “couple” with the antenna on the RFID tag.
  - Consistent with any applicable authorization, authentication, and encryption, the tag will then respond to the reader, sending via radio waves the data stored on it

- **Active**
  - Active tags can initiate communication and typically have onboard power.
  - They can communicate the longest distances — 100 or more feet. Currently, active tags typically cost $20 or more.
  - A familiar application of active tags is for automatic toll payment systems that allow cars bearing active tags to use express lanes that do not require drivers to stop and pay.

- **Semi-passive**
  - A semi-passive tag, like a passive tag, does not initiate communication with readers, but they do have batteries.
  - This onboard power is used to operate the circuitry on the chip, storing information such as ambient temperature.
  - Semi-passive tags can be combined, for example, with sensors to create “smart dust” — tiny wireless sensors that can monitor environmental factors.

RFID Tag Memory

- Read-only tags
  - Tag ID is assigned at the factory during manufacturing
    - Can never be changed
    - No additional data can be assigned to the tag
- Write once, read many (WORM) tags
  - Data written once, e.g., during packing or manufacturing
    - Tag is locked once data is written
    - Similar to a compact disc or DVD
- Read/Write
  - Tag data can be changed over time
    - Part or all of the data section can be locked

Localization

- When a reader receives an ID message from a tag, the reader not only identifies the tag but also obtains the received signal strength (RSS) information from the tag.
- RSS information is a measure of power represented in dBm.
- By placing a number of readers in known locations, different readers receive their own
- RSS readings from the same tag.
- Combining all RSS information from all the tags, the target location can be estimated.
- The major advantage of using RSS information from readers for localization is that it is readily available without additional cost.

Example - An RFID Based Attendance System

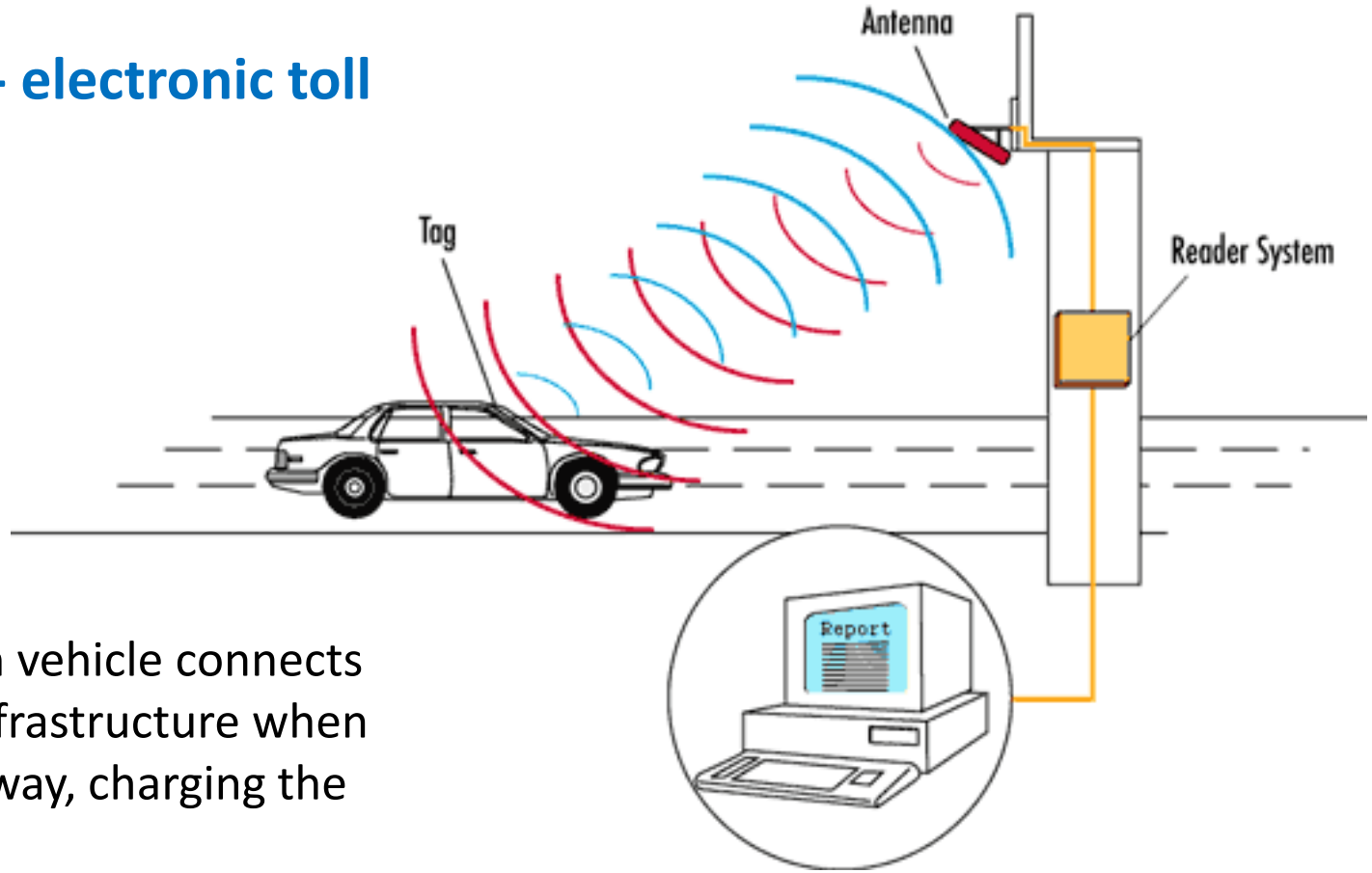
- Basic idea
  - involves each person of the institution having an id card and when this card is swiped against the reader, the person's info is matched with the existing system in the database and the his/her attendance is marked.
  - Which RFID tag can be used?

    Passive tag

Other application

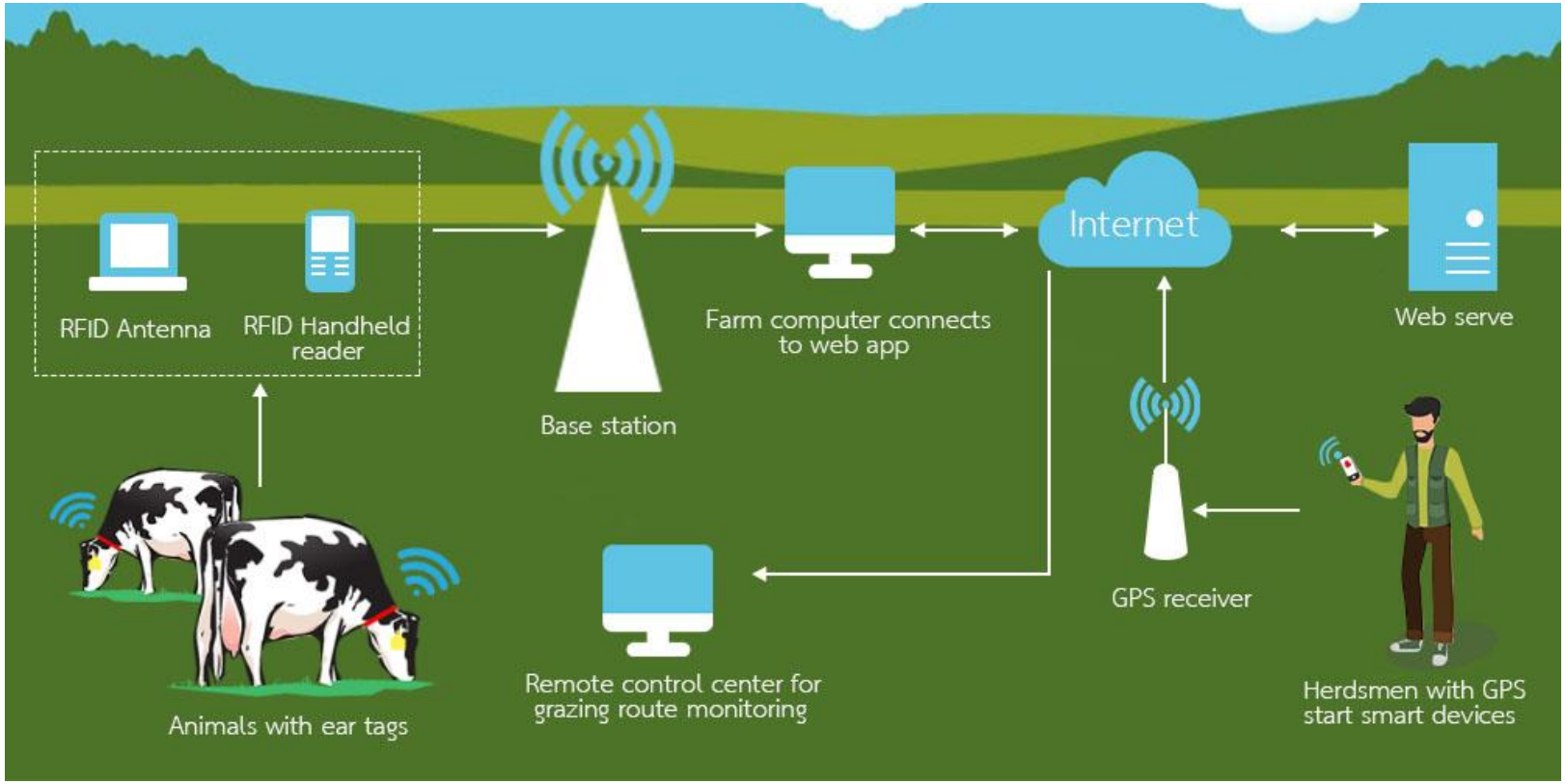
- In an assembly line-based production system, a part can be easily identified.
- Even position can be identified through triangulation technique.
- Location detection can be a very important aspect of a plant operating with hazardous material from the safety point of view.
- In case of an emergency or an emergency evacuation, people can be located and identified.

RFID in transport applications - electronic toll collection.

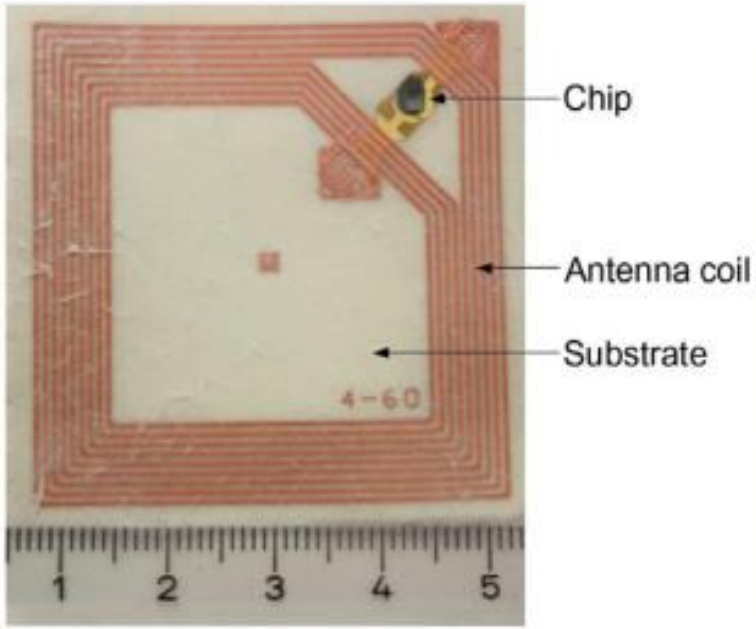


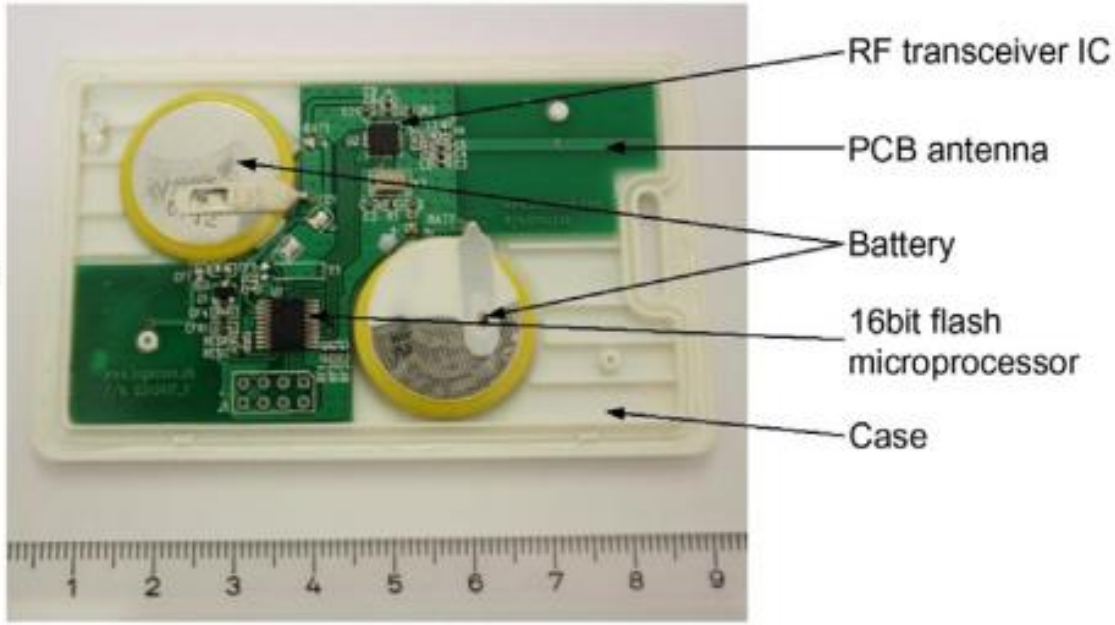
In this case, a RFID tag installed in each vehicle connects and exchanges information with the infrastructure when the car enters onto the ramp of a highway, charging the costs of this access automatically.

- Animal identification
- Goods tracking
- Car key for vehicles
- Tracking of trucks and



Challenges

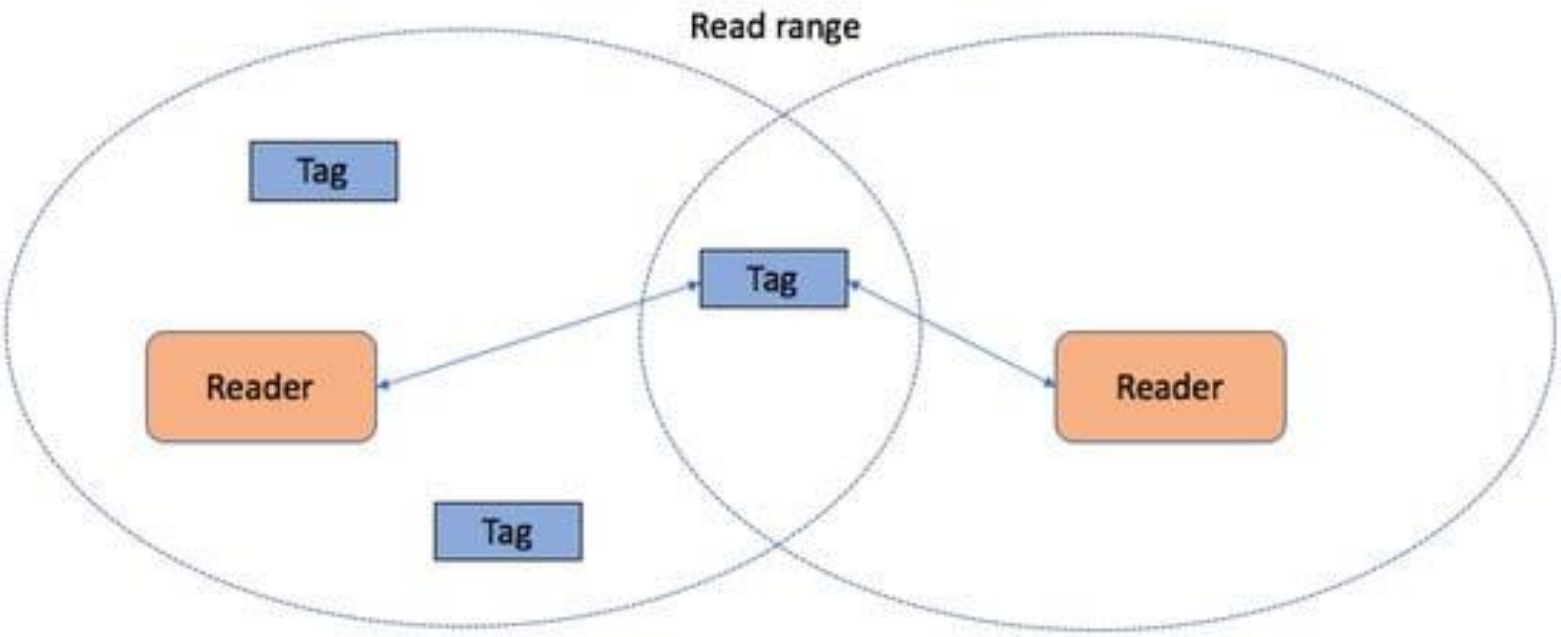




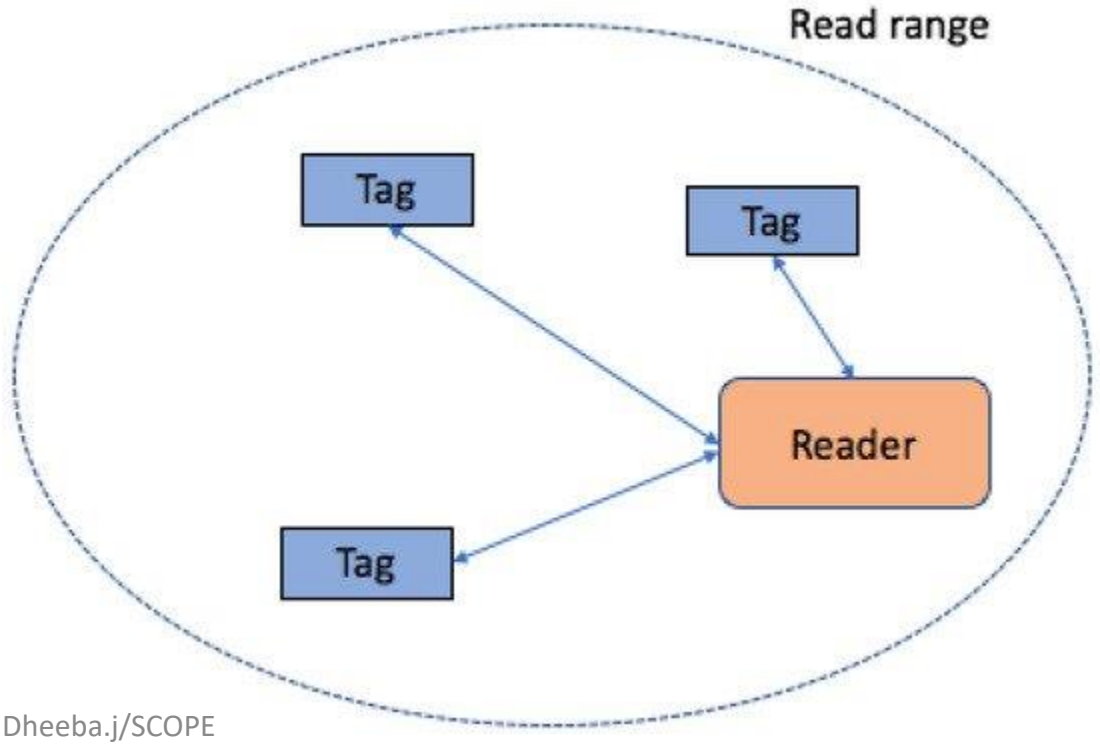
Battery power for active RFIDs

- Tag-to-tag interferences (collision), when multiple tags are simultaneously energized by the reader and reflect the respective signals back. Because of the scattered waves, then the reader cannot differentiate the individual IDs of the tags.
- Reader-to-tag interferences, where a tag is located at the intersection of two or more reader interrogation ranges and the readers attempt to communicate with the tag simultaneously.
- Reader-to-reader interference is induced when a signal from one reader reaches other readers

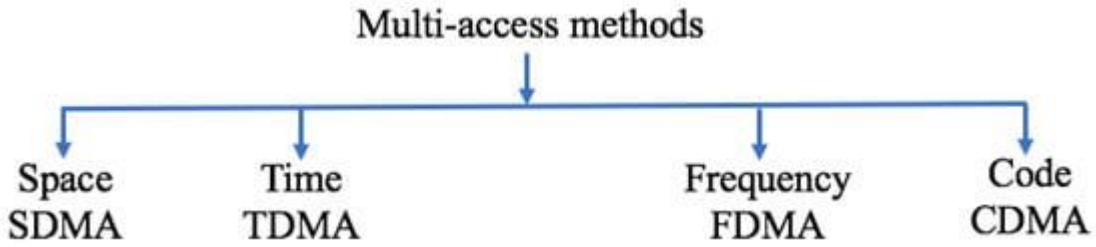
- Signal interference occurs when the fields of two or more readers overlap and interfere.
- This problem can be solved by programming all readers to read at fractionally different times.

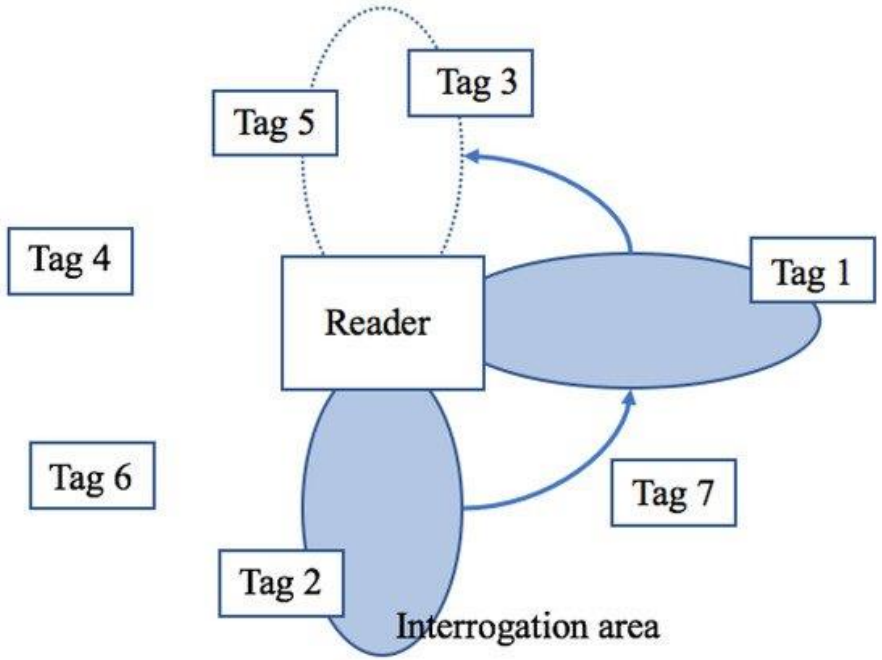


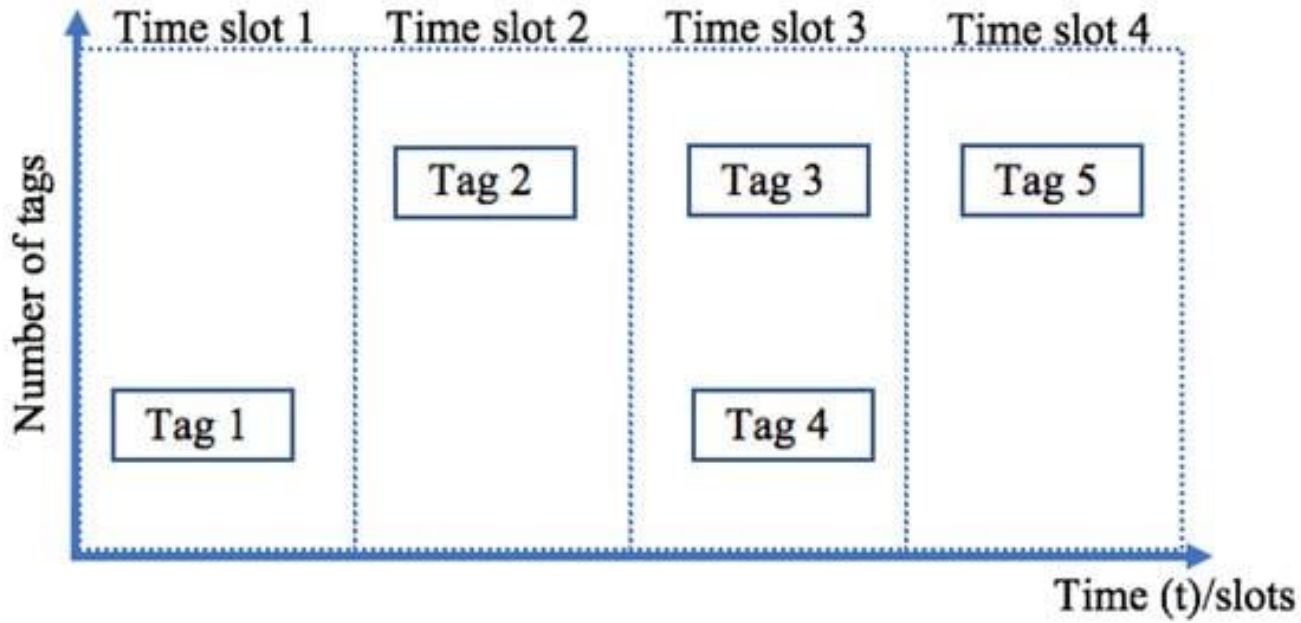
- A tag collision occurs when more than one tag attempts to transmit its ID at the same time: the reader will receive a mixture of the tags' signals and cannot understand it.



- Anti-collision protocol uses certain multi-access methods for identification in order to physically separate the transmitters' signals.

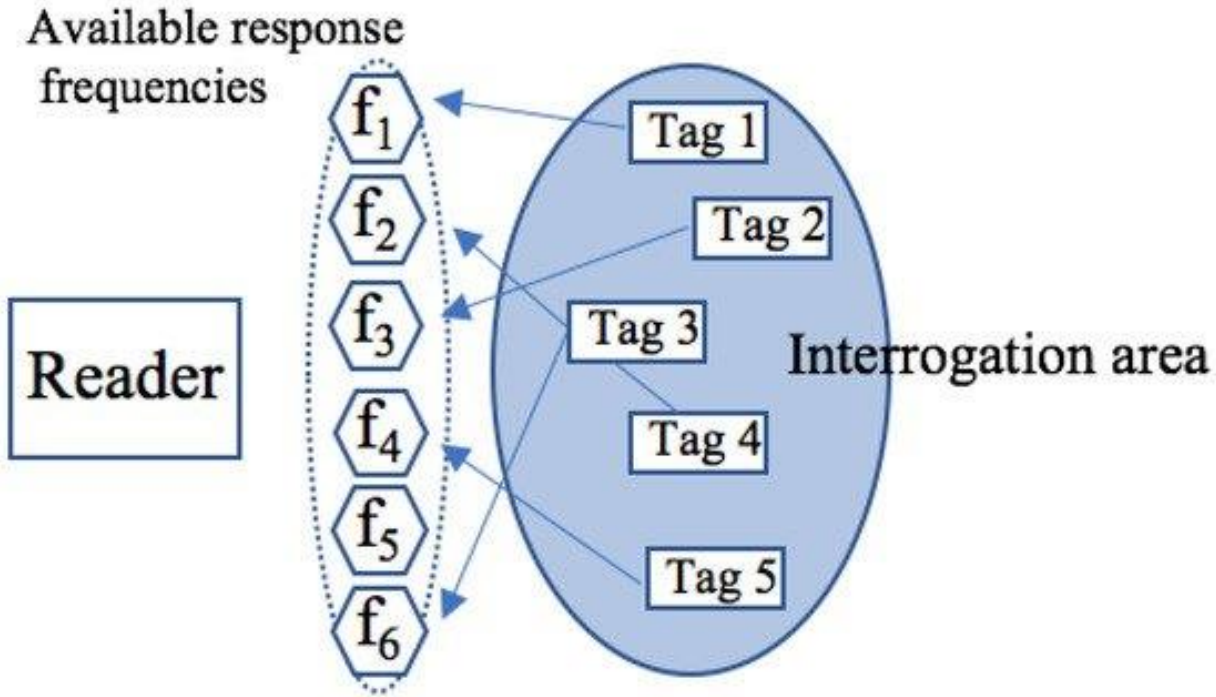


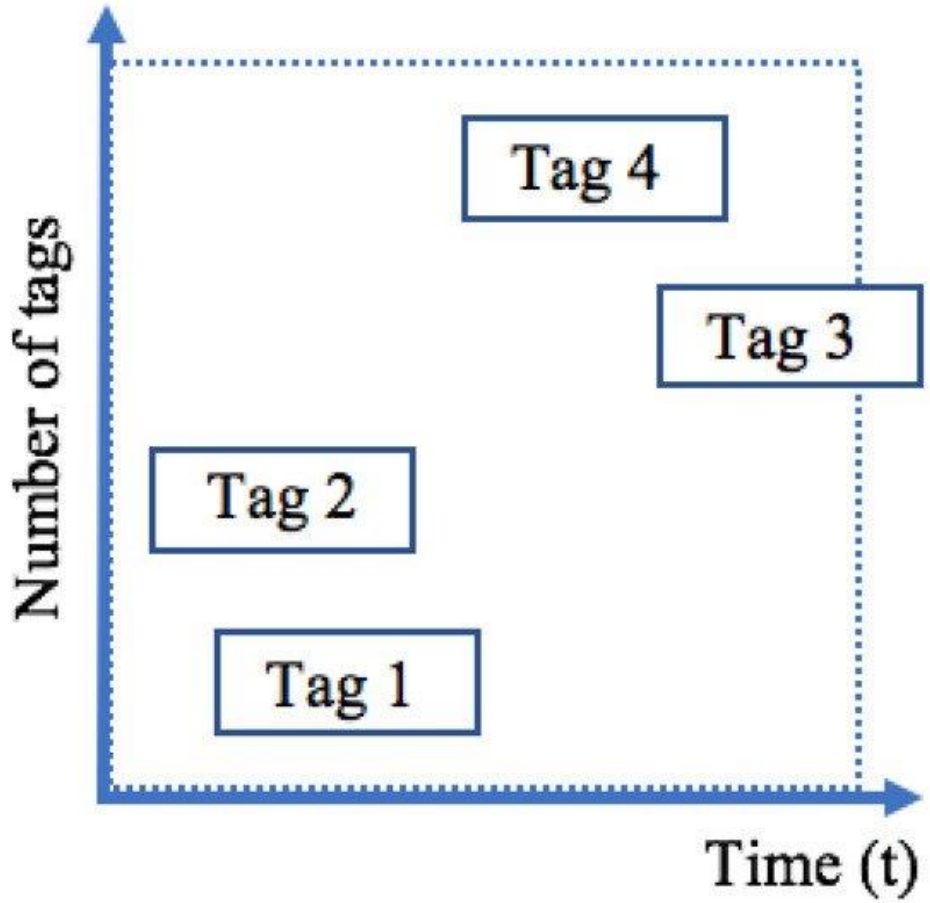




Space Division Multiple Access (SDMA) procedure.

Time Division Multiple Access (TDMA) procedure.

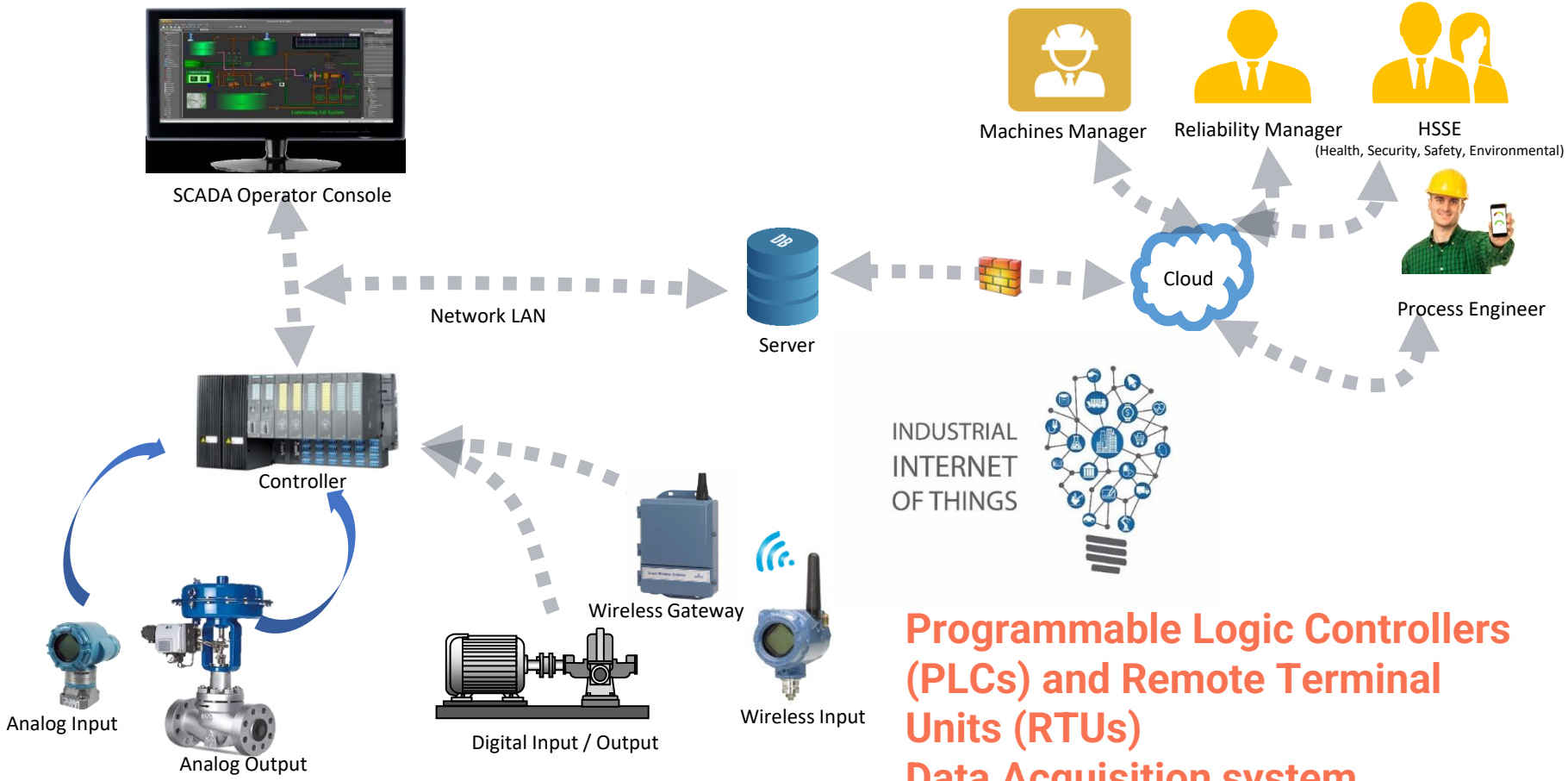

Available response frequencies
f1
f2
f3
f4
f5
f6
Reader
Tag 1
Tag 2
Tag 3
Tag 4
Tag 5
Interrogation area


Number of tags
Tag 4
Tag 3
Tag 2
Tag 1
Time (t)

SCADA

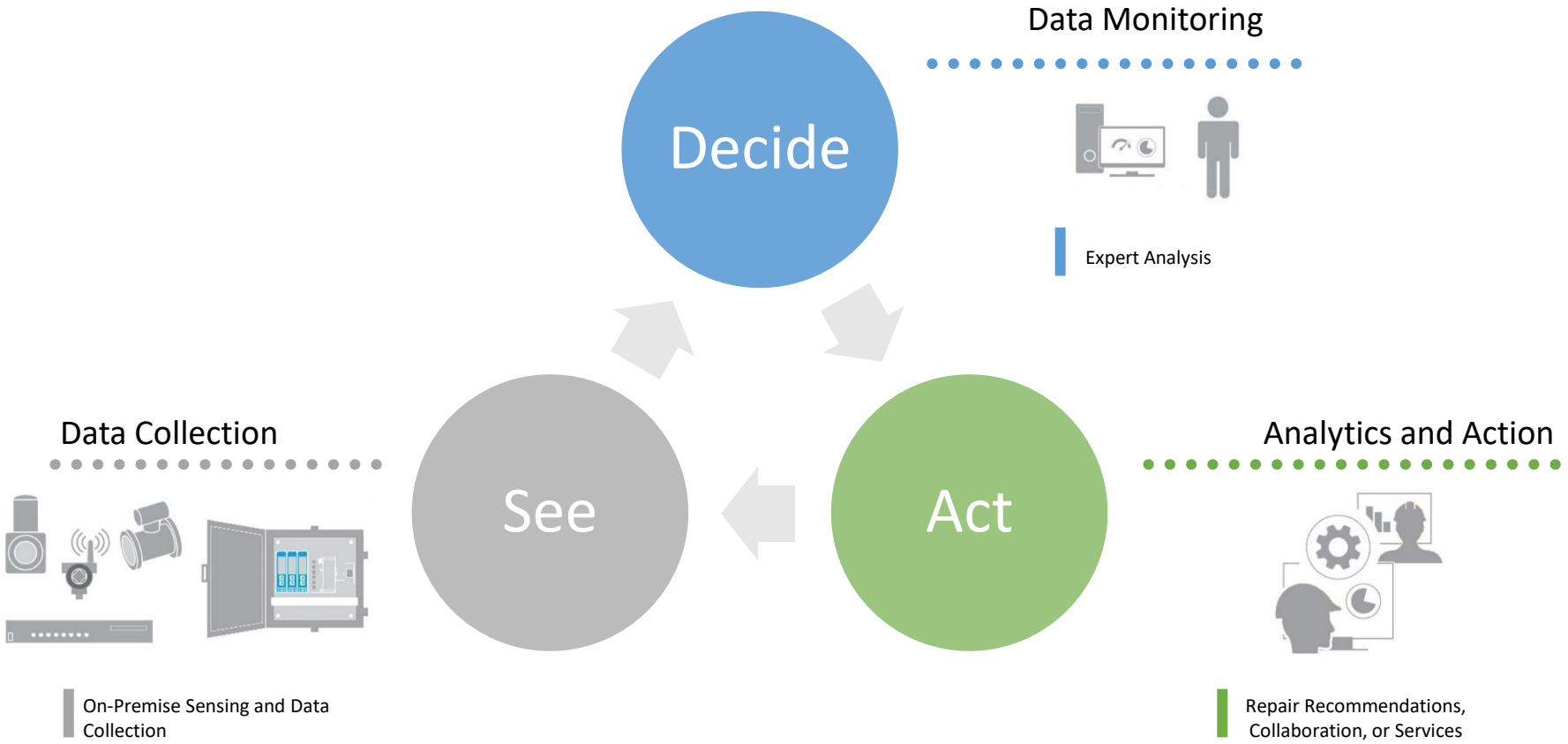
- The **internet of things** is also a natural extension of SCADA (supervisory control and data acquisition), a category of software application program **for process control**, the gathering of data in real time from remote locations to control equipment and conditions.
- The hardware gathers and feeds data into a computer that has SCADA software installed, where it is then processed and presented it in a timely manner.

SCADA – An Overview



Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs)
Data Acquisition system
Supervisory system

Connected Services are based on See, Decide, Act



Wireless Implementation in Tank Farm

Challenge:

- Tight schedule for green field specialty chemical project
- Space constraints with variety of product manufacturing in the same location
- Diversified Manufacturing processes
- Elevated process units with multiple recipe production

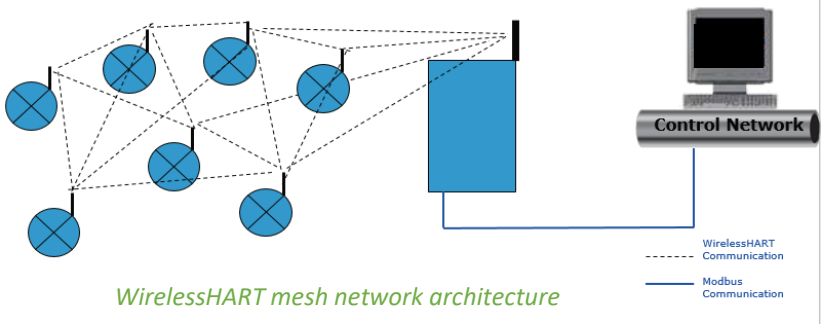
Applications:

- Process measurements Utilities and Tank Farm area
- Remote Data measurement in the Hazardous Chemical storage area

Solution:

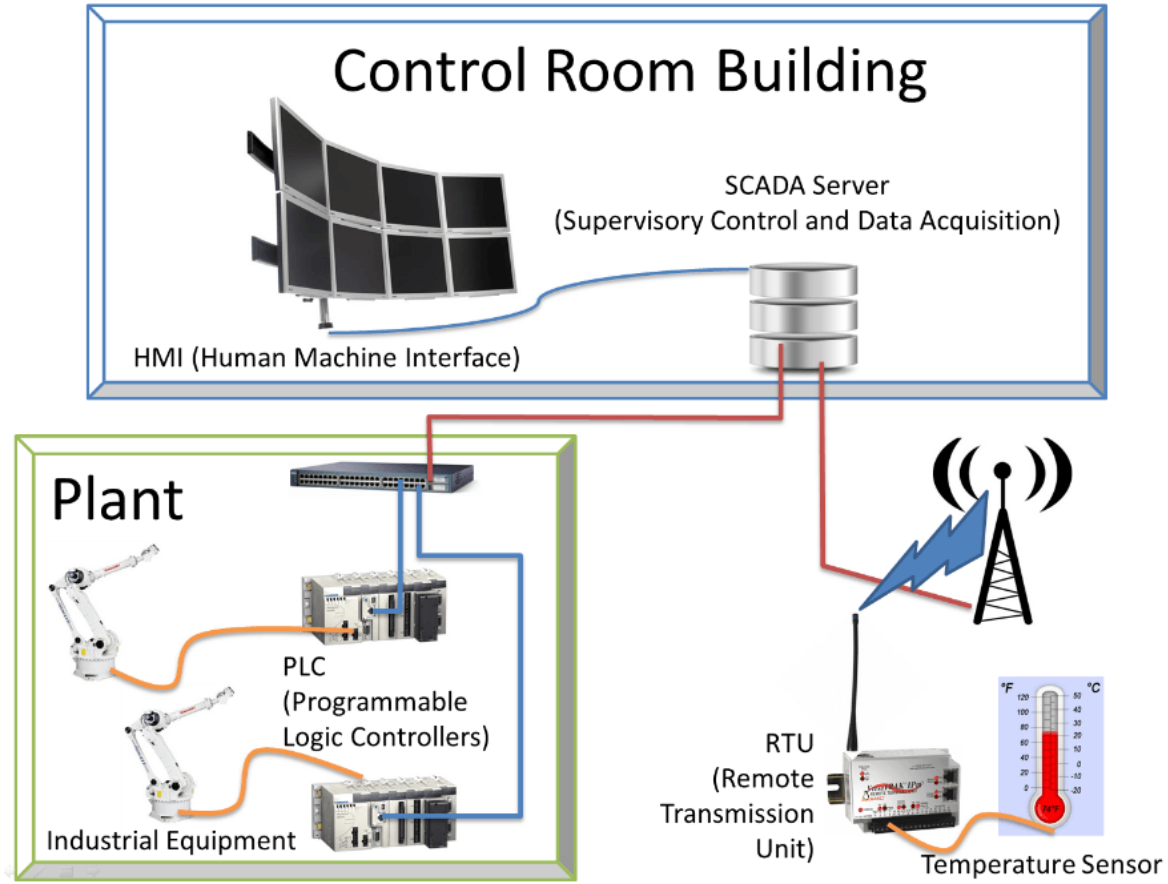
- Wireless networks were deployed for Pressure, Level , Temp and Remote measurements in process plant

Installation in Utilities & remote monitoring area



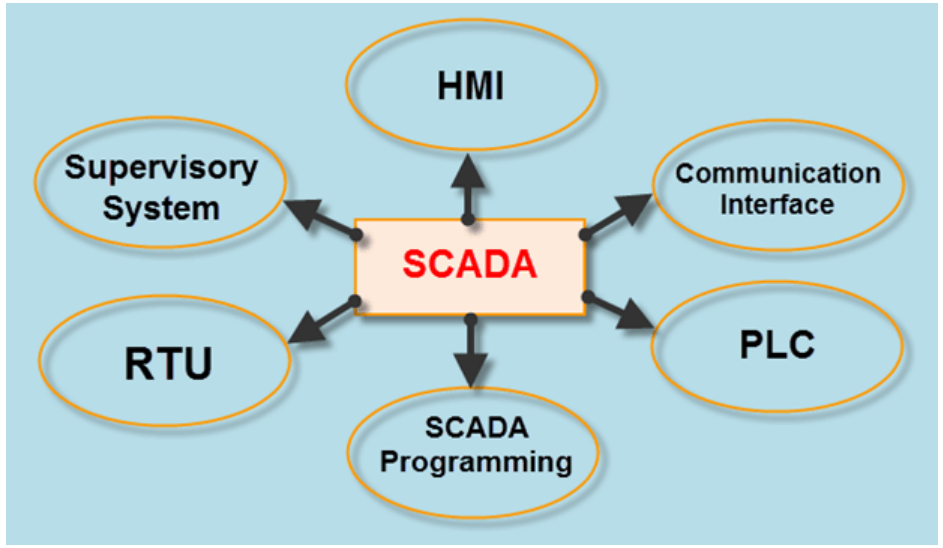
WirelessHART mesh network architecture

- SCADA stands for Supervisory Control and Data Acquisition; it is an industrial computer-based control system employed to gather and analyze the real-time data to keep track, monitor and control industrial equipment in different types of industries.
- Consider the application of SCADA in power systems for operation and control.
- SCADA in power system can be defined as the power distribution application which is typically based on the software package.
- The electrical distribution system consists of several substations; these substations will have multiple numbers of controllers, sensors and operator-interface points.


Control Room Building
SCADA Server
(Supervisory Control and Data Acquisition)
HMI (Human Machine Interface)
Plant
PLC
(Programmable
Logic Controllers)
Industrial Equipment
RTU
(Remote
Transmission
Unit)
Temperature Sensor

- In general, for controlling and monitoring a substation in real time (PLCs) Programmable Logic Controllers, Circuit breakers and Power monitors are used.
- Data is transmitted from the PLCs and other devices to a computer-based-SCADA node located at each substation. One or more computers are located at different centralized control and monitoring points.

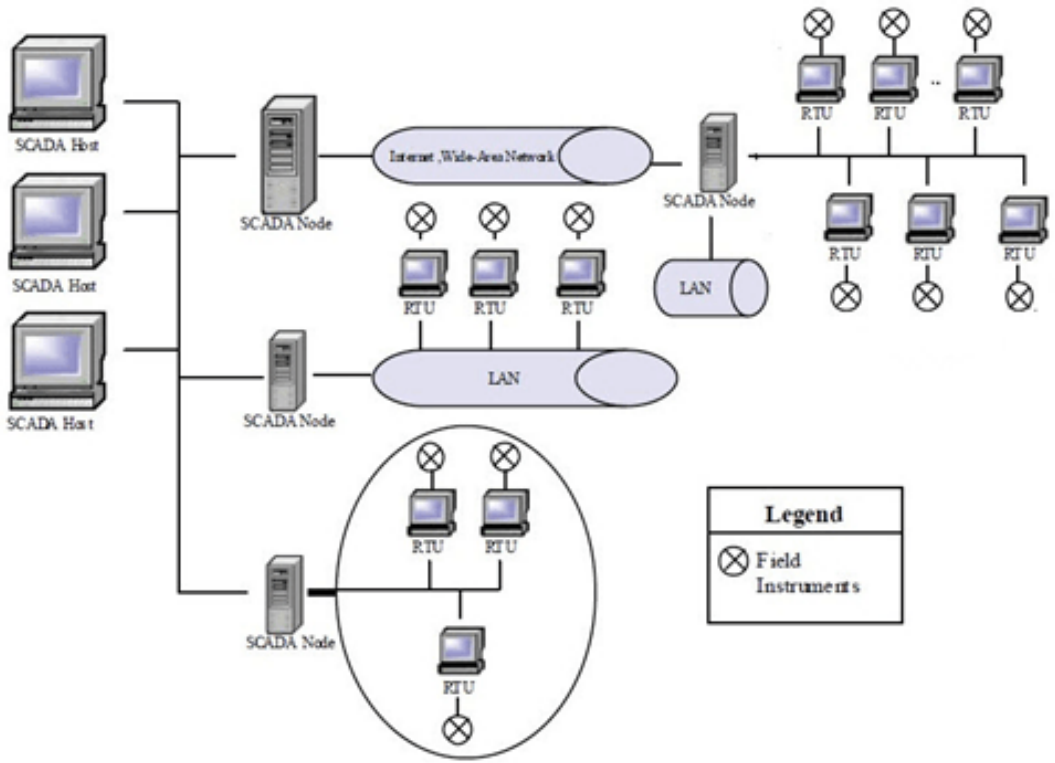
SCADA - Basics



- Human-machine Interface (HMI)
  - It is an input-output device that presents the process data to be controlled by a human operator. It is used by linking to the SCADA system's software programs and databases for providing the management information, including the scheduled maintenance procedures, detailed schematics, logistic information, trending and diagnostic data for a specific sensor or machine. HMI systems facilitate the operating personnel to see the information graphically.
- Supervisory System
  - Supervisory system is used as server for communicating between the equipment of the SCADA system such as RTUs, PLCs and sensors, etc., and the HMI software used in the control room workstations.
  - Master station or supervisory station comprises a single PC in smaller SCADA systems and, in case of larger SCADA systems, supervisory system comprises distributed software applications, disaster recovery sites and multiple servers.
  - These multiple servers are configured in a hot-standby formation or dual-redundant, which continuously controls and monitors in case of a server failure for increasing the integrity of the system.

- Remote Terminal Units
  - Physical objects in the SCADA systems are interfaced with the microprocessor controlled electronic devices called as Remote Terminal Units (RTUs).
  - These units are used to transmit telemetry data to the supervisory system and receive the messages from the master system for controlling the connected objects. Hence, these are also called as Remote Telemetry Units.
- Programmable Logic Controllers
  - In SCADA systems, PLCs are connected to the sensors for collecting the sensor output signals in order to convert the sensor signals into digital data.
  - PLCs are used instead of RTUs because of the advantages of PLCs like flexibility, configuration, versatile and affordability compared to RTUs.
- Communication Infrastructure
  - Generally the combination of radio and direct wired connections is used for SCADA systems, but in case of large systems like power stations and railways SONET/SDH are frequently used.
  - Among the very compact SCADA protocols used in SCADA systems – a few communication protocols, which are standardized and recognized by SCADA vendors – send information only when the supervisory station polls the RTUs.

- SCADA Programming
  - SCADA programming in a master or HMI is used for creating maps and diagrams which will give an important situational information in case of an event failure or process failure.
  - Standard interfaces are used for programming most commercial SCADA systems.
  - SCADA programming can be done using derived programming language or C language

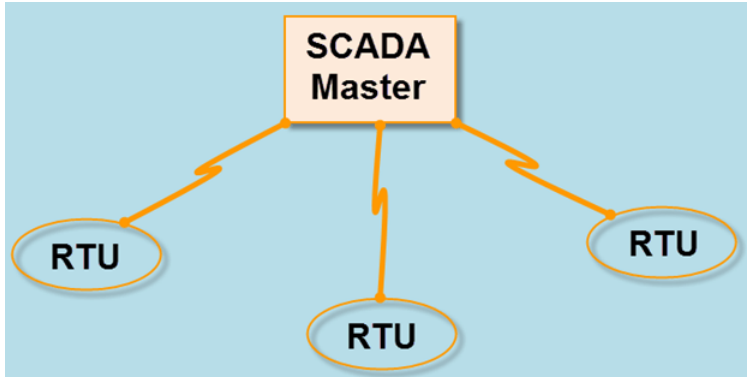

SCADA Host
SCADA Host
SCADA Host
SCADA Node
Internet ,Wide-Area Network
SCADA Node
RTU
RTU
RTU
RTU
RTU
RTU
RTU
RTU
RTU
LAN
SCADA Node
LAN
SCADA Node
RTU
RTU
RTU
Legend
Field Instruments

Types of SCADA

- First Generation: Monolithic or Early SCADA systems,
- Second Generation: Distributed SCADA systems,
- Third Generation: Networked SCADA systems and
- Fourth Generation: Internet of things technology, SCADA systems

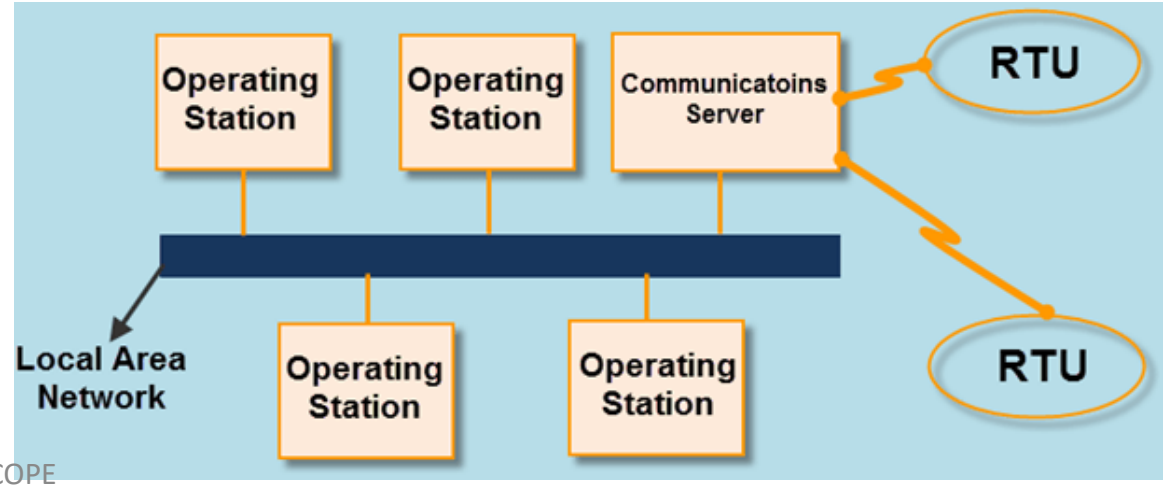
Monolithic or Early SCADA systems

- SCADA systems were developed wherein the common network services were not available. Hence, these are independent systems without having any connectivity to other systems.
- All the remote terminal unit sites would connect to a back-up mainframe system for achieving the first generation SCADA system redundancy, which was used in case of failure of the primary mainframe system.



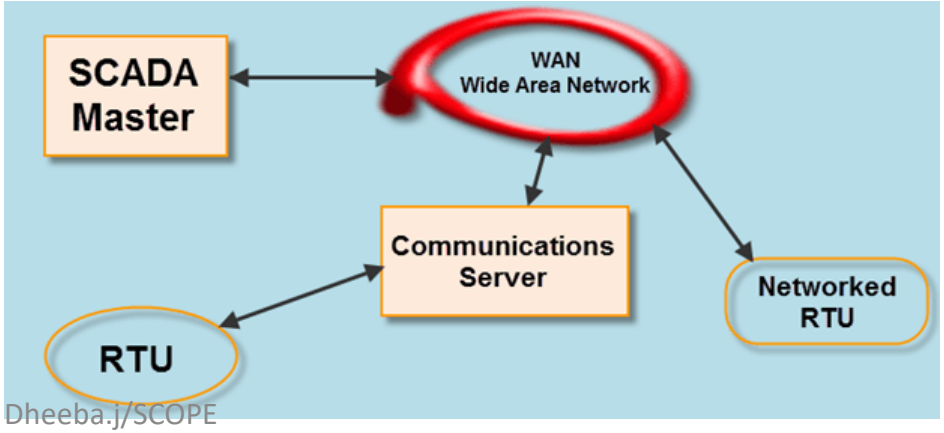
Distributed SCADA Systems

- In the second generation, the sharing of control functions is distributed across the multiple systems connected to each other using Local Area Network (LAN). Hence, these were termed as distributed SCADA systems. These individual stations were used to share real-time information and command processing for performing control tasks to trip the alarm levels of possible problems.

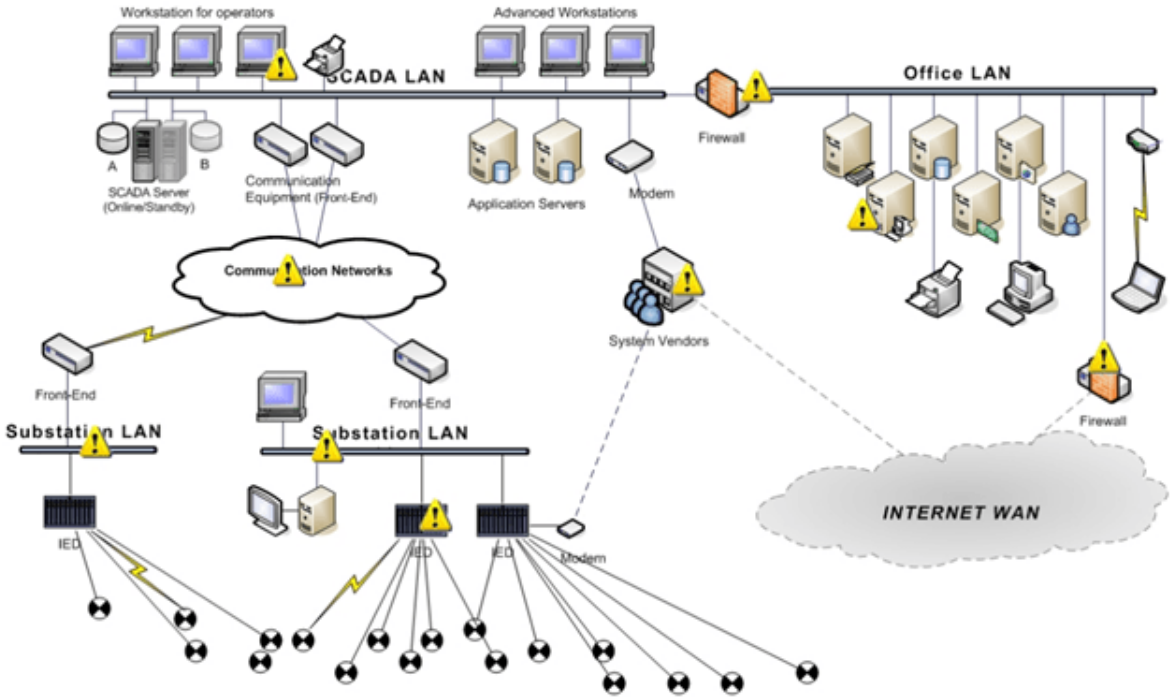


Networked SCADA systems

- The current SCADA systems are generally networked and communicate using Wide Area Network (WAN) Systems over data lines or phone. These systems use Ethernet or Fiber Optic Connections for transmitting data between the nodes frequently. These third generation SCADA systems use Programmable Logic Controllers (PLC) for monitoring and adjusting the routine flagging operators only in case of major decisions requirement.



Internet of things technology, SCADA systems



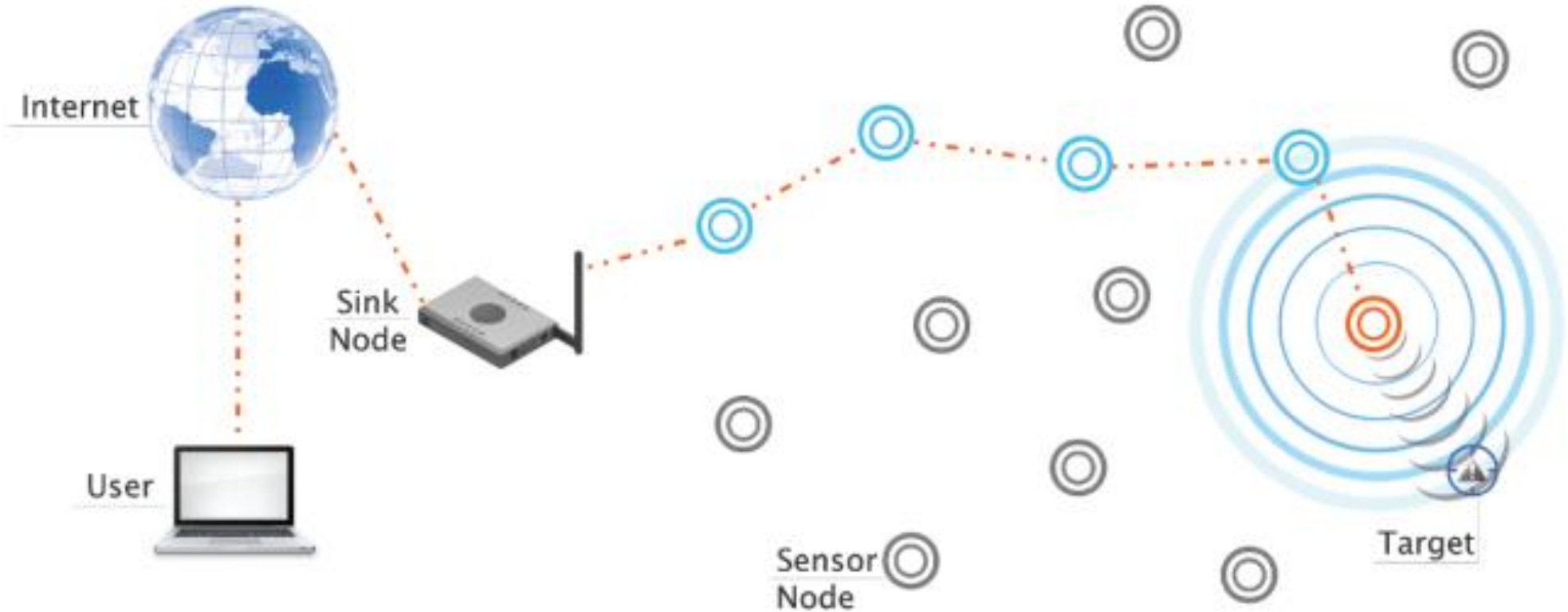
Applications of SCADA

- There are numerous applications of SCADA systems, but a few most frequently used SCADA applications include:
  - Manufacturing Industries
  - Waste Water Treatment and Distribution Plants
  - SCADA in Power System

Wireless sensor Network

- **Sensor nodes**
  - A sensor is a device that responds to physical quantities such as heat, and converts them into electricity to enable automatic interpretation and processing.
  - A sensor node (generally referred to as sensor or mote) is an autonomous, compact device that not only integrates sensors but also includes other units to process and deliver sensory data.
  - A typical sensor node comprises the following units: sensor, communication, microcontroller, memory and power.
  - Depending on the application requirements, other units could be included such as: GPS, locomotory, energy harvesting, etc.

- A WSN consists of spatially distributed sensors, and one or more sink nodes (also called base stations).
- Sensors monitor, in real-time, physical conditions, such as temperature, vibration, or motion, and produce sensory data.
- A sensor node could behave both as data originator and data router.
- A sink, on the other hand, collects data from sensors.
- For example, in an event monitoring application, sensors are required to send data to the sink(s) when they detect the occurrence of events of interest.
- The sink may communicate with the end-user via direct connections, the Internet, satellite, or any type of wireless links.


Internet
Sink
Node
User
Sensor
Node
Target

Structure of a node

- a sensor
- a unit for analog (processing the sensor's output, analog/digital conversion and radiofrequency levels) and digital processing (filtering, memorizing, clock and modulation) signals
- a wireless transmission device
- an energy source (a necessity given that the node is isolated from any cable network).
- a wireless reception device
- an actuator
- a specialized positioning unit (like GPS, which makes it possible to retrieve a temporal reference).

- Special cases of WSNs
  - Wireless multimedia sensor networks (WMSNs)
  - Underwater wireless sensor networks (UWSNs)
  - Wireless underground sensor networks (WUSNs)
  - Wireless body sensor networks (WBSNs)

WSN models and architectures

- small, medium, large and very large-scale WSNs
  - the size of the WSN varies depending on several factors such as the sensors' characteristics, the Region of Interest, and the user's requirements.
- homogeneous versus heterogeneous WSNs
  - A WSN is homogeneous if all sensors of the network have the same capabilities (sensing, processing, communication, etc).
  - A heterogeneous WSN consists of sensors endowed with different capacities, which may serve for different applications
- stationary, mobile, and hybrid WSNs
  - A stationary WSN is a network consisting of stationary sensor nodes that cannot move once deployed.
  - With the advances in mobile devices, some of the sensors are able to move on their own; this is generally achieved by embedding the sensors on mobile platforms.
  - A mobile WSN comprises only mobile sensors, while a hybrid WSN consists of both stationary and mobile sensors

- flat versus hierarchical WSNs:
  - in flat WSNs, all the sensor nodes are assumed to be homogeneous and play the same role.
  - However, in hierarchical WSNs, a sensor node can be dedicated to a particular special function.
  - For instance, a sensor could be designated as a cluster-head, in charge of communicating with adjacent clusters
- single-hop versus multi-hop WSNs:
  - in a single-hop WSN, sensor nodes transmit their data directly to the sink.
  - In a multi-hop WSN, multiple relaying sensor nodes exist between sensors and sinks.

Challenges

- Hardware Constraints
  - A sensor may need to fit into a tight module on the order of 2 x 5 x 1 cm or even as small as a 1 x 1 x 1 cm.
  - The key components include a power unit (batteries and/or solar cells), a sensing unit (sensors and analog-to-digital converters), a processing unit (along with storage), and a transceiver unit (connects the node to the network).
  - The optional components include a location-finding system, a power generator, a control actuator, and other application-dependent elements
  - Sensor nodes may also have to be disposable, autonomous, and adaptive to the environment.

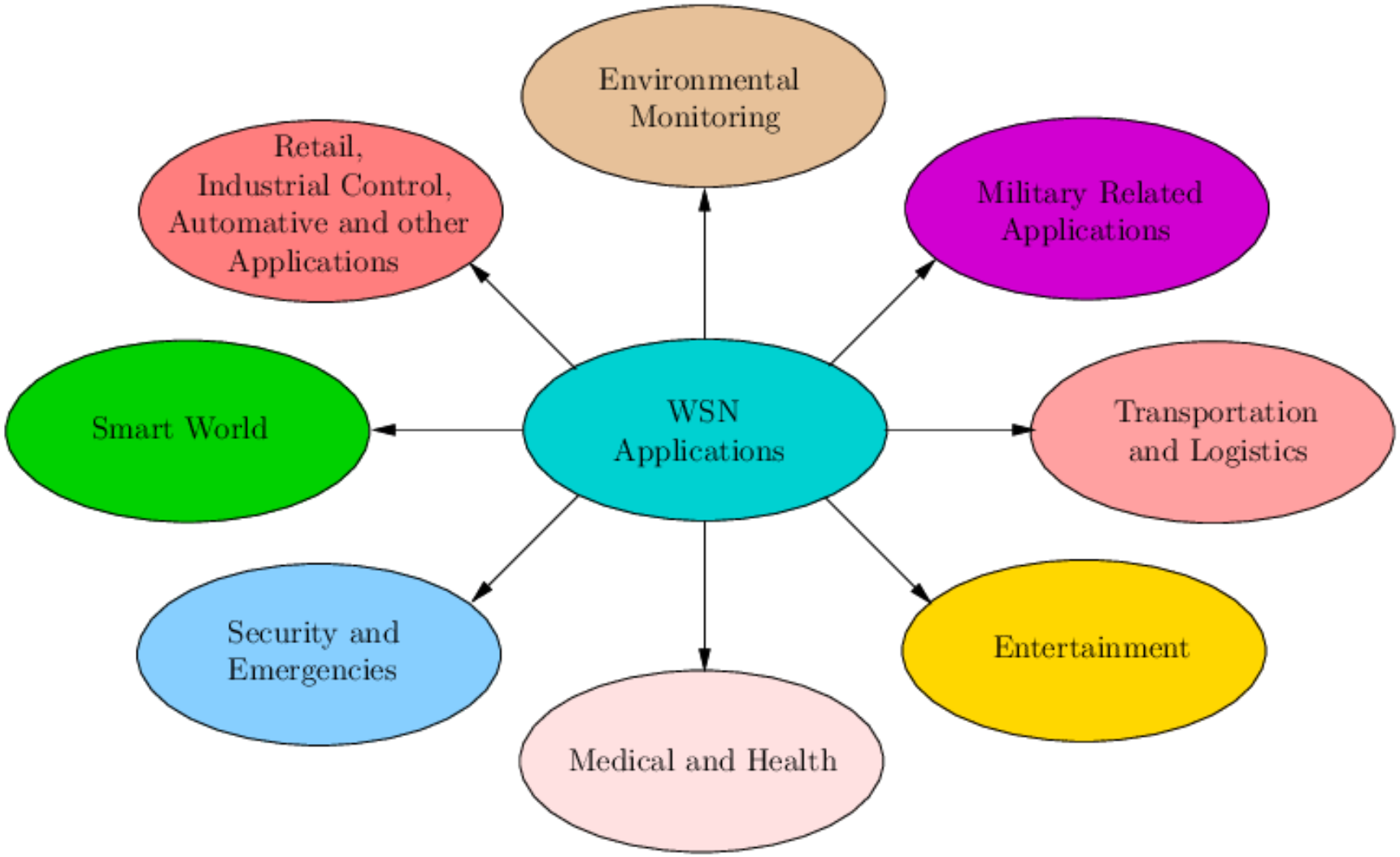
- Power Consumption
  - The sensor node lifetime typically exhibits a strong dependency on battery life.
  - In many cases, the wireless sensor node has a limited power source.
  - Power consumption can therefore be allocated to three functional domains: sensing, communication, and data processing, each of which requires optimization.
  - In the context of communications, in a multihop sensor network a node may play the dual role of data collection and processing and of being a data relay point.
  - As can easily be understood, (excessive) rerouting and/or retransmission will require additional power.

- Node Unit Costs
  - Current sensor systems based on Bluetooth technology cost about $10; however, Bluetooth is limited as a transmission technology in terms of both bandwidth and distance.
  - However, the cost of a sensor node is generally targeted to be less than $1
- Environment
  - Sensor networks often are expected to operate in an unattended fashion in dispersed and/or remote geographic locations.
  - Nodes may be deployed in harsh, hostile, or widely scattered environments.
  - Such environments give rise to challenging management mechanisms.

- Connectivity and Topology
  - Deploying and managing a high number of nodes in a relatively bounded environment requires special techniques.
  - Hundreds to thousands of sensors in close proximity (feet) may be deployed in a sensor field. The density of sensors may be as high as 27 nodes/m^3.
  - Nodes could be deployed in mass or be injected in the sensor field individually (e.g., they could be deployed by dropping them from an helicopter, scattered by an artillery shell or rocket, or deployed individually by a human or a robot).
  - Any time after deployment, topology changes may ensue, due to changes in sensor node position; power availability, dropouts, or brownouts; malfunctioning; reachability impairments; jamming; and so on

WSN applications

- Categorized as,
  - Mesh-based systems with multihop radio connectivity among or between WNs, utilizing dynamic routing in both the wireless and wireline portions of the network.
  - Point-to-point or multipoint-to-point (star based) systems generally with single-hop radio connectivity to WNs, utilizing static routing over the wireless network; typically, there will be only one route from the WNs to the companion terrestrial/wireline forwarding node


Environmental Monitoring
Retail, Industrial Control, Automative and other Applications
Military Related Applications
Smart World
WSN Applications
Transportation and Logistics
Security and Emergencies
Entertainment
Medical and Health

Machine to Machine (M2M)

- Machine-to-machine (M2M) communications is an emerging technology that envisions the interconnection of machines without the need of human intervention.
- The main concept lies in seamlessly connecting an autonomous and self-organizing network of M2M-capable devices to a remote client, through heterogeneous wired or wireless communication networks.
- ETSI has been actively engaged in the development of a standard for M2M systems, with the objective of ensuring interoperability between the diverse M2M components and the already existing technologies

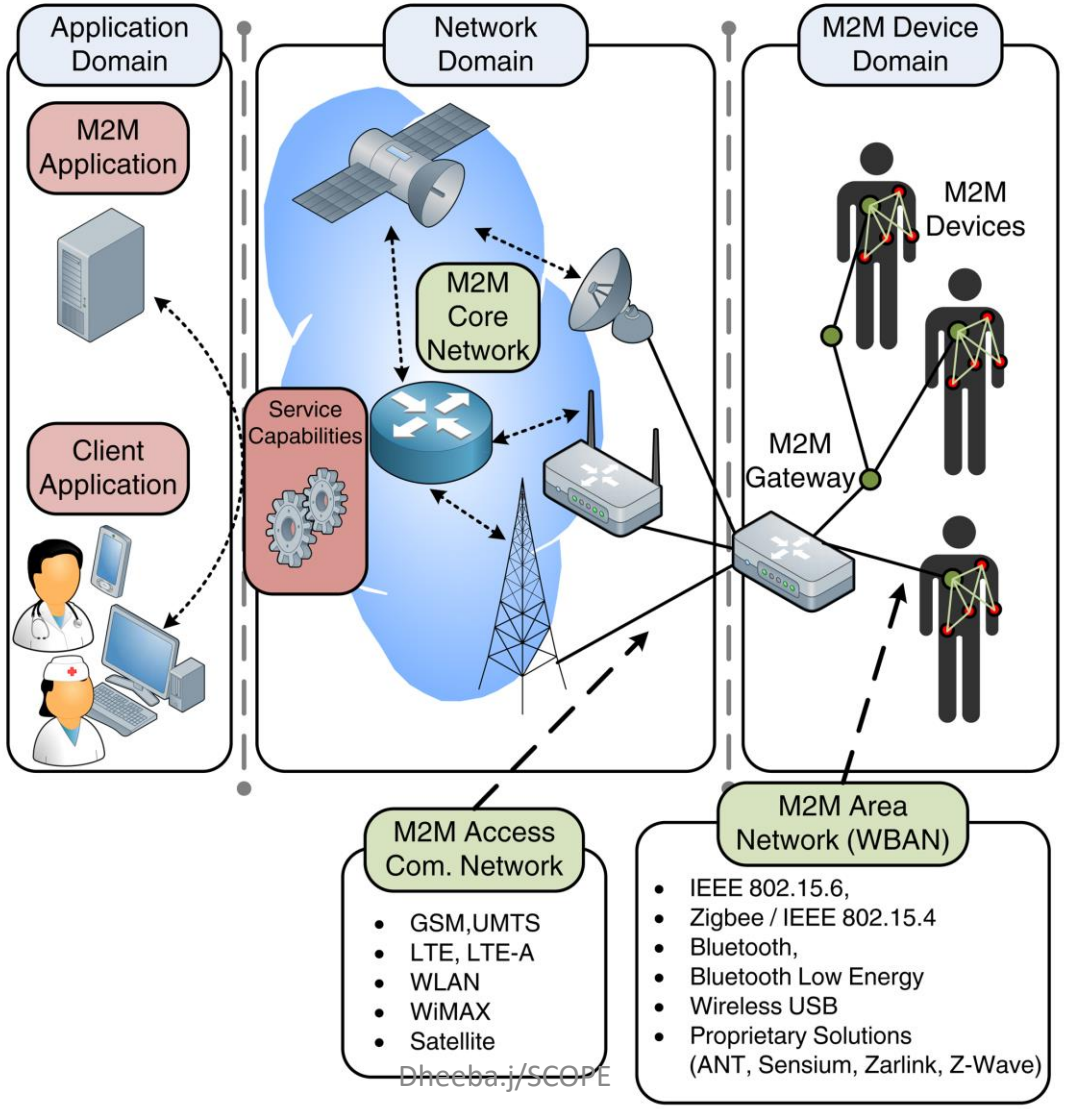
- Provides a High-level horizontal architecture, dividing the system into three domains
  - The device and gateway domain, where the M2M devices communicate with a gateway through short-range area networks.
  - The network domain that connects the gateway to the applications through long-range access and core communication networks
  - The application domain, where various application services are defined depending on the use case

Five key elements

- The M2M devices - which are devices capable of transmitting data autonomously or after receiving a data request.
  - In the context of healthcare applications, the M2M devices are principally low-power medical sensor or actuator devices with embedded wireless communication modules.
- The M2M area network, also known as the capillary network, which is a short-range network that provides connectivity between the M2M devices and the gateway.
  - In medical application, the area network will also be referred to as WBAN, given that the M2M devices are deployed near or within the human body.
- The M2M gateway, which acts as a proxy between the M2M devices (interconnected through the WBAN) and the network domain. Practically, the gateway must be a portable device with advanced processing capabilities and multiple radio interfaces, able to operate in technologies employed by both the WBAN and the communication network

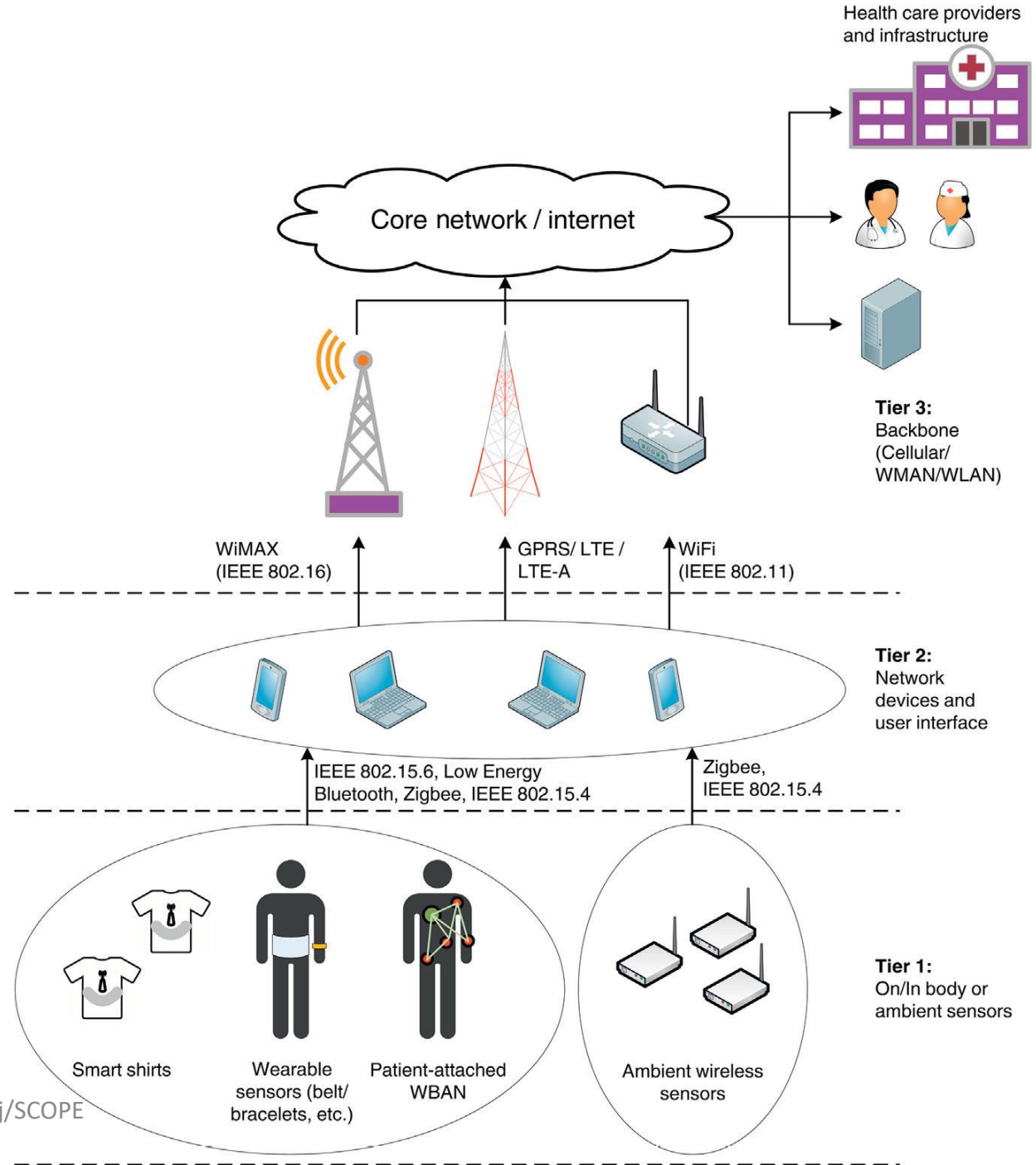
- The M2M access communication network, which connects the M2M gateway to the M2M application server via the Internet.
- The M2M application server, which is the middleware layer that provides data to the specific business applications.

M2M architecture for wireless connectivity in healthcare application scenarios



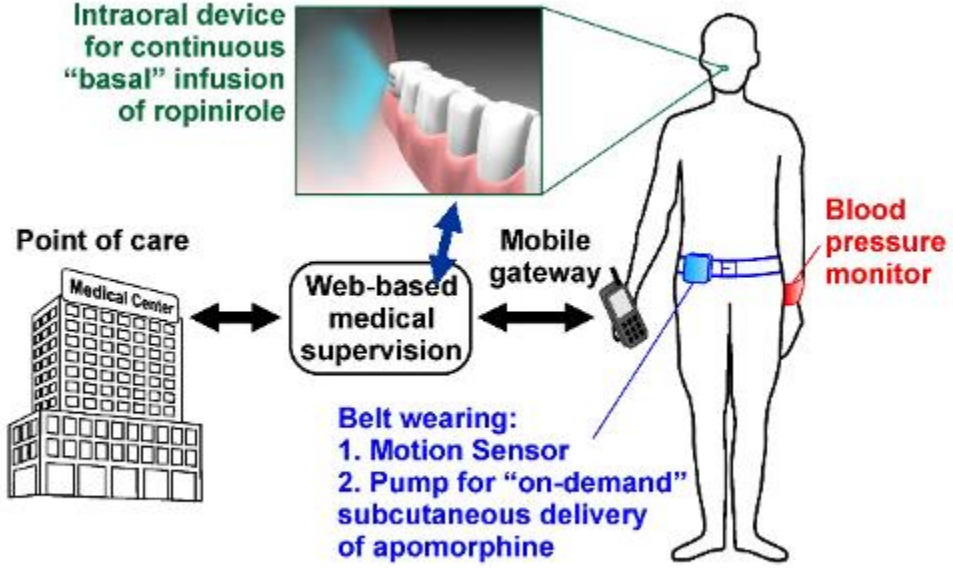
End-to-end solutions for M2M communication: connectivity

- Goal of an e-health application is to provide a bridge between the patient and the medical personnel.
- Hence, the M2M system must provide end-to-end connectivity, connecting the medical sensor devices via the M2M gateway to the Internet and ultimately to the application server



Examples

- HEALTH@HOME (Health at Home) –
- (www.aal-europe.eu/projects/healthhome)
  - provide an end-to-end solution for the remote monitoring of cardiovascular and respiratory patient parameters
- HELP: Home-based Empowered living for Parkinson Disease Patients
- (www.aaleurope.eu/projects/help)
  - targets at designing a health monitoring system able to control disease progression and to mitigate Parkinson disease (PD) symptoms, thus improving the quality of life of affected elderly people



- Examples of M2M in use - https://topconnect.com/m2m-iot-connectivity/5-examples-of-m2m-in-use/

- Thank You