SNS COLLEGE OF ENGINEERING

An Autonomous Institution

Coimbatore-107

19IT503-INTERNET OF THINGS

UNIT-2

FUNDAMENTAL MECHANISMS & KEY TECHNOLOGIES

TOPIC: Key IoT Technologies

Key IoT Technologies

- List of Technologies are:
  - Device Intelligence
  - Communication Capabilities
  - Mobility Support
  - Device Power
  - Sensor Technology
  - RFID Technology
  - Satellite Technology

Key IoT Technologies

Device Intelligence

- Device Intelligence
  - In order for the IoT to become a reality,
- Objects should be able to intelligently sense and interact with the environment
- Possibly store some passive or acquired data
- Communicate with the world around them
  - Object-to-gateway device communication or even direct object-to-object communication is desirable

Key IoT Technologies

Device Intelligence

- These intelligent capabilities are necessary to support ubiquitous networking to provide seamlessly interconnection between humans and objects
  - Some have called this mode of communication *Any Services, Any Time, Any Where, Any Devices, and Any Networks* (also known as “5-Any”)

Key IoT Technologies

Communication Capabilities

- It is highly desirable for objects to support ubiquitous end-to-end communications
- To achieve ubiquitous connectivity for human-to-object & object-to-object communications, networking capabilities will need to be implemented in the objects (“things”)
- IP is considered to be key capability for IoT objects
- Self-configuring capabilities, especially how an IoT device can establish its connectivity automatically without human intervention, are also of interest
- IPv6 auto-configuration & multihoming features are useful, particularly scope-based IPv6 addressing features

Key IoT Technologies

Mobility Support

- Another consideration related to tracking and mobility support of mobile object
- Mobility-enabled architectures & protocols are required
- Some objects move independently, while others will move as one of group
- Therefore, according to the moving feature, different tracking methods are required.
- It is important to provide ubiquitous and seamless communication among objects while tracking the location of objects.
- Mobile IPv6 (MIPv6) offers several capabilities that can address this requirement.

Key IoT Technologies

Device Power

- Related to the powering of the “thing”
- Especially for mobile devices or devices that do not have intrinsic power
- M2M/IoT applications are always constrained by following factors:
  - Devices have ultra-low-power capabilities
  - Devices must be of low cost
  - Devices must have small physical size & light in weight

Key IoT Technologies

Device Power

- The following factors that must be considered in selecting the most suitable battery for a particular application :
- Operating voltage level
- Load current and profile
- Duty cycle—continuous or intermittent
- Service life
- Physical requirement
  - Size
  - Shape
  - Weight
- Environmental conditions
  - Temperature
  - Pressure
  - Humidity
  - Vibration
  - Shock
  - Pressure
- Safety and reliability
- Shelf life
- Maintenance and replacement
- Environmental impact and recycling capability
- Cost

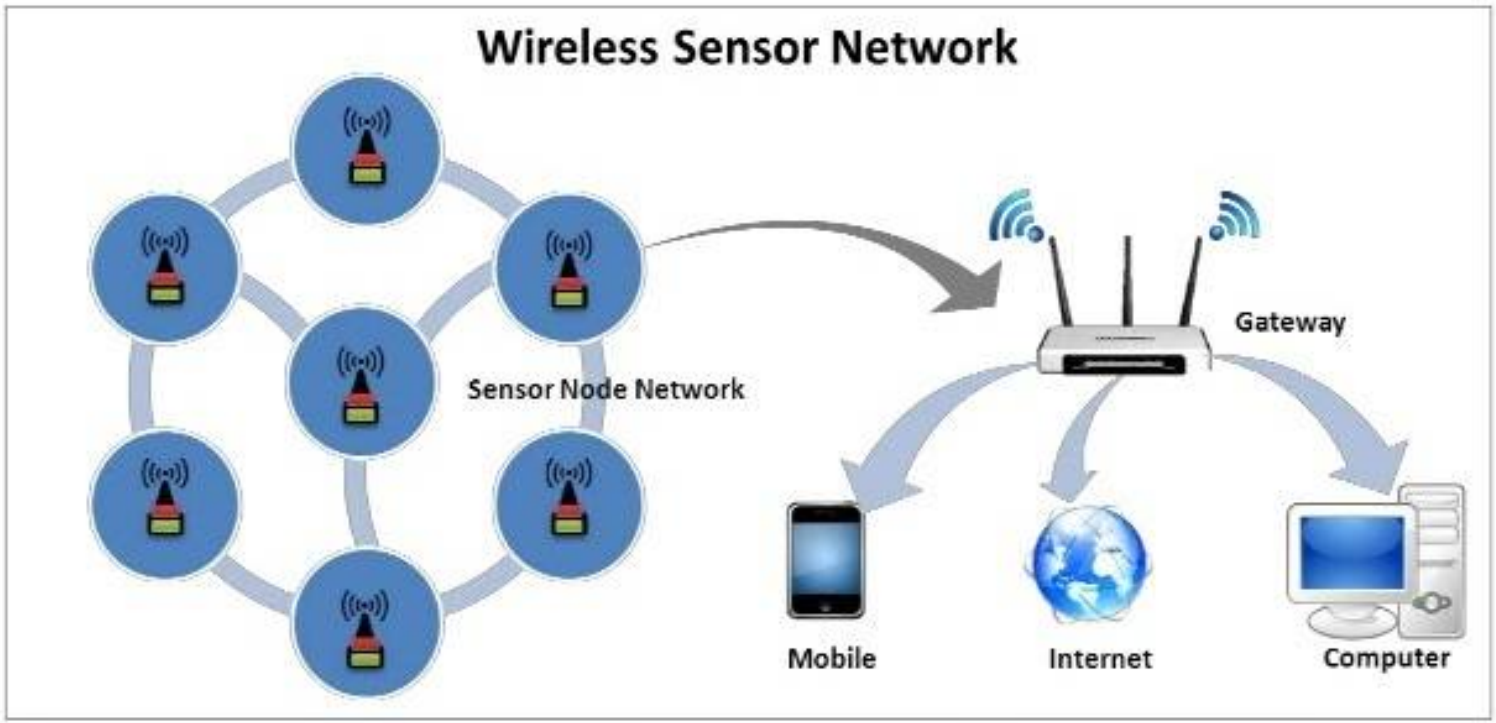
Key IoT Technologies

Sensor Technology

- A sensor network is an infrastructure comprising sensing (measuring), computing, communication, data collection, monitoring, surveillance, and medical telemetry.
- Sensor network technology, specifically, with embedded networked sensing, ships, aircrafts, and buildings can "self-detect" structural faults (e.g., fatigue-induced cracks).
- Earthquake-oriented sensors in buildings can locate potential survivors and can help assess structural damage; tsunami-alerting sensors can certainly prove useful for nations with extensive coastlines.
- Sensors also find extensive applicability in battlefield for reconnaissance and surveillance

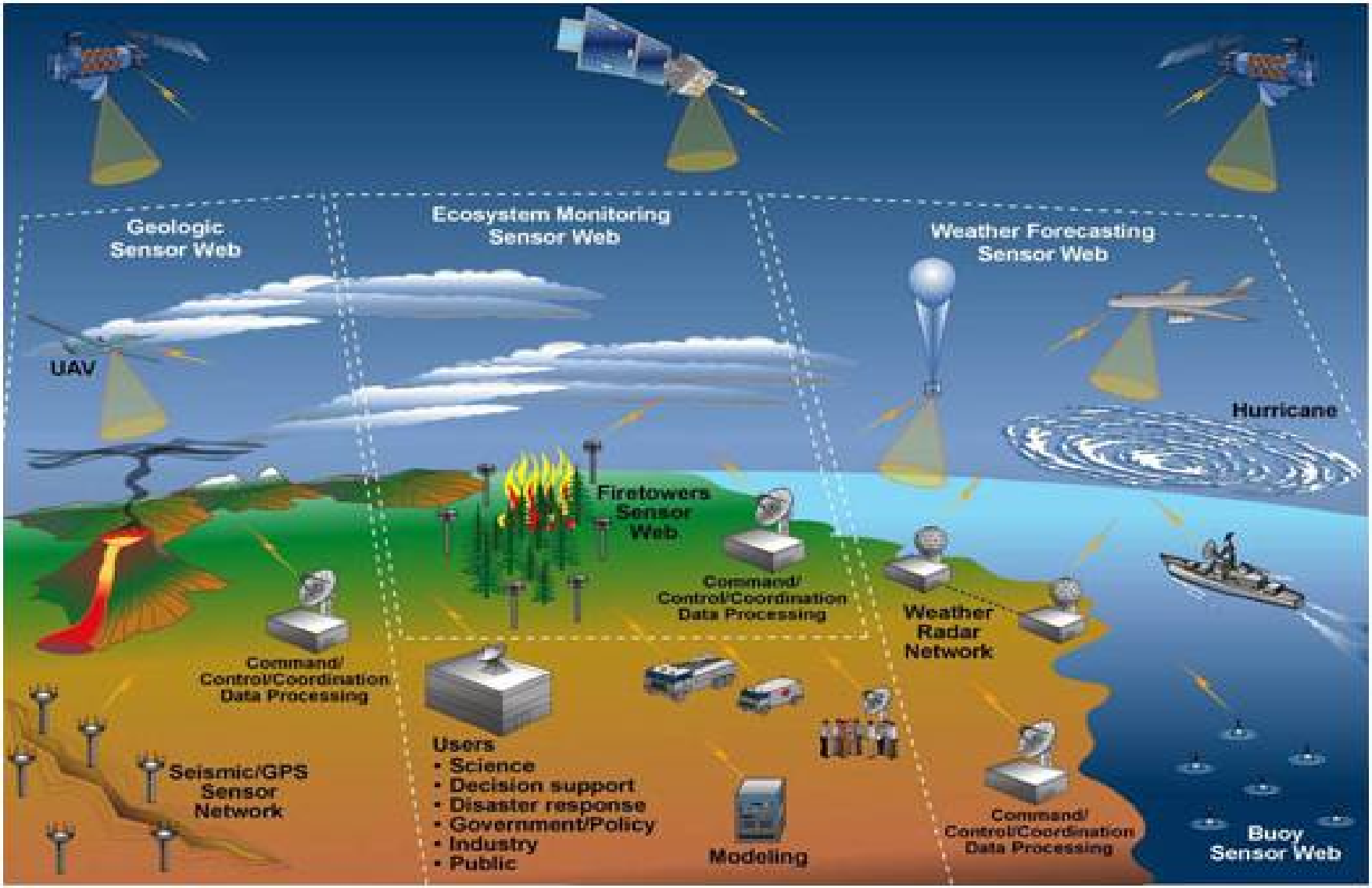
Key IoT Technologies

Sensor Technology



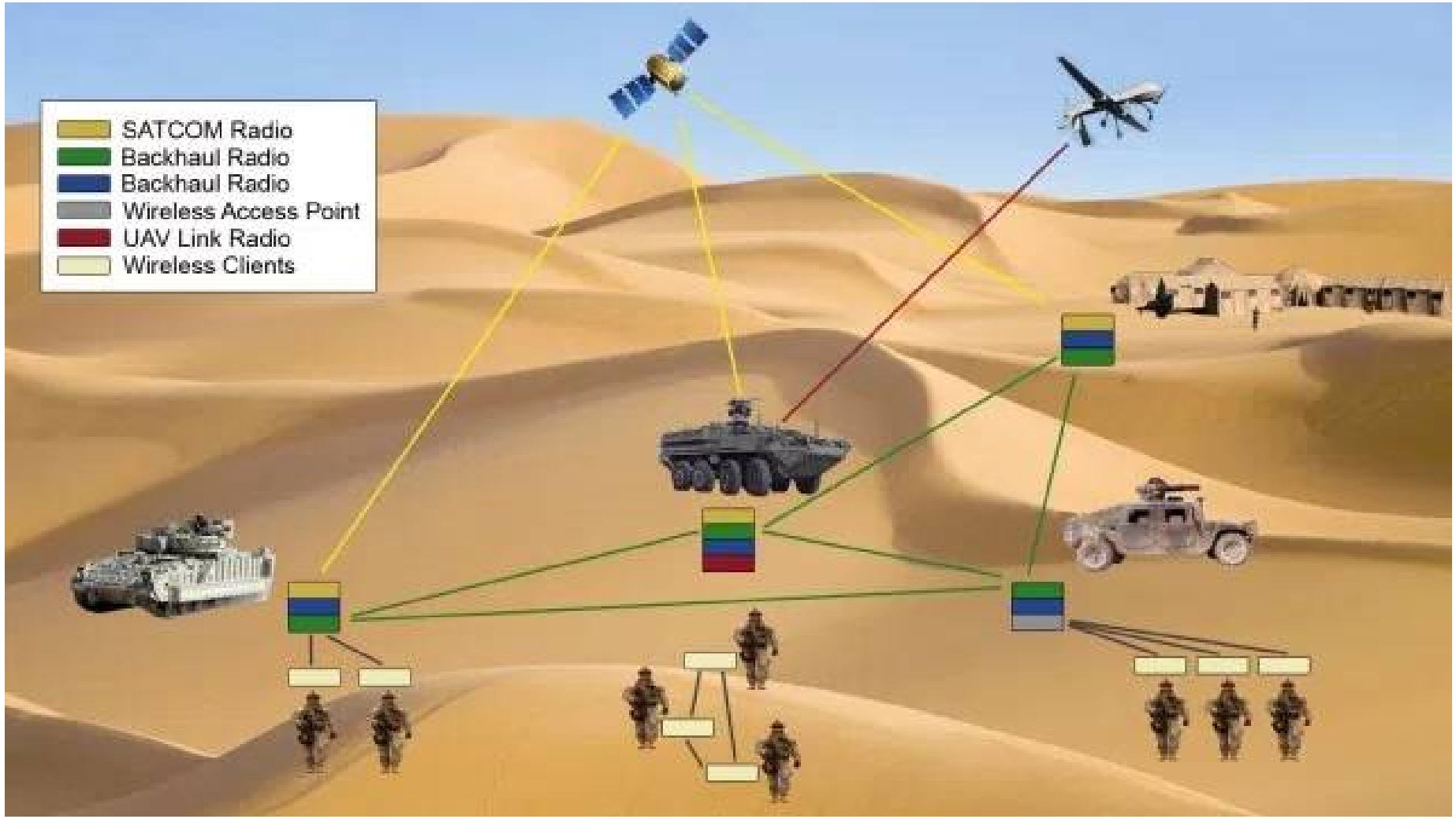
Key IoT Technologies

Sensor Technology



Key IoT Technologies

Sensor Technology



Key IoT Technologies

Sensor Technology

- There are four basic components in a sensor network:
  - (i) an assembly of distributed or localized sensors
  - (ii) an interconnecting network (usually, but not always, wirelessbased)
  - (iii) a central point of information clustering
  - (iv) a set of computing resources at the central point (or beyond) to handle data correlation, event-trending, querying, and data mining.
- Because the interconnecting network is generally wireless, these systems are known as wireless sensor networks (WSNs).
- WSN have the potentially large quantity of data collected, algorithmic methods for data management play an important role in sensor networks.
- In-network processing is desirable in sensor networks; furthermore, node power (and/or battery life) is a key design consideration.

Key IoT Technologies

Sensor Technology

- Sensors can be described as “smart” inexpensive devices equipped with multiple on-board sensing elements:
  - they are low cost, low power, untethered multifunctional nodes that are logically homed to a central sink node.
- Sensor utilize the Internet or some other network for long-haul delivery of information to a point (or points) of final data aggregation and analysis.
- Sensors are typically internetworked via a series of multihop short-distance low power wireless links called “sensor field”.
- Sensors are typically deployed in a high density manner and in large quantities:
  - a WSN consists of densely distributed nodes that support sensing,
  - signal processing, embedded computing, and connectivity;
  - sensors are logically linked by self-organizing means (sensors that are deployed in short-hop point-to-point master-slave pair arrangements are also of interest).

Key IoT Technologies

Sensor Technology

- New wireless design methodologies are needed across a set of disciplines, information transport, network and operational management, confidentiality, integrity, availability, and in-network/local processing, low battery status, other wireless sensor malfunction and lightweight protocol stack.
- Physical size can range from nanoscopic-scale devices to mesoscopic-scale devices at one end; from microscopic-scale devices to macroscopic-scale devices at the other end.
  - Nanoscopic (nanoscale) in the order of 1–100 nm in diameter;
  - Mesoscopic scale refers to objects between 100 and 10,000 nm in diameter
  - The microscopic scale ranges from 10 to 1000 microns
  - The macroscopic scale is at the millimeter-to-meter range.
- Biological sensors, small passive microsensors (such as “smart dust”), and “lab-on-a-chip” assemblies
- The miniaturized ones that are directly embedded in some physical infrastructure, as “microsensors.”

Key IoT Technologies

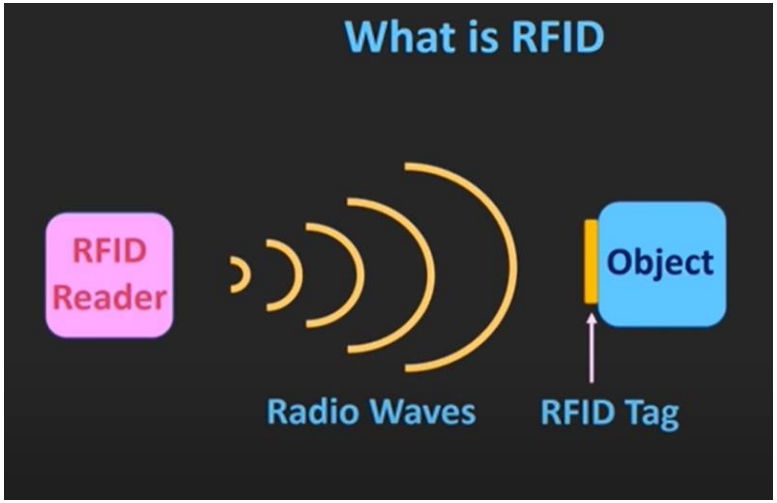
Sensor Technology

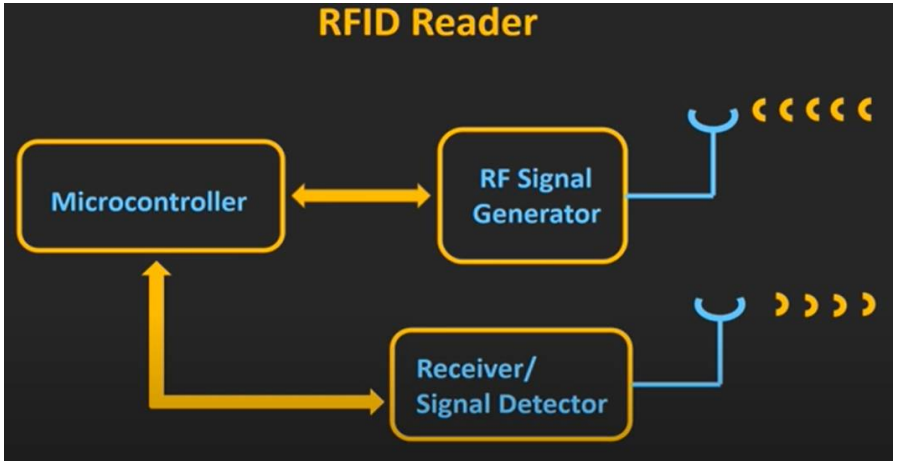
- Sensors may be passive and/or be self-powered; further along in the power consumption chain, some sensors may require relatively low power from a battery or high power.
- Low power consumption for transmission over low bandwidth channels and low power-consumption logic to pre-process and/or compress data.
- Power efficiency in WSNs is generally accomplished in three ways:
  - (i) Low duty cycle operation
  - (ii) Local/in-network processing to reduce data volume (and, hence, transmission time)
  - (iii) Multihop networking (this reduces the requirement for long-range transmission since signal path loss is an inverse power with range/distance) each node in the sensor network can act as a repeater, thereby reducing the link range coverage required, and, in turn, the transmission power

Key IoT Technologies

RFID Technology

- RFIDs are electronic devices associated with objects (“things”) that transmit their identity (usually a serial number) via radio links.
- RFID tags are devices that typically have a read-only chip that stores a unique number but has no processing capability.
- RFID and barcode facilitate the global supply chain and impact all subsystems within that overall process, including material requirement planning (MRP), just in time (JIT), electronic data interchange (EDI), and electronic commerce (EC).





Key IoT Technologies

RFID Technology

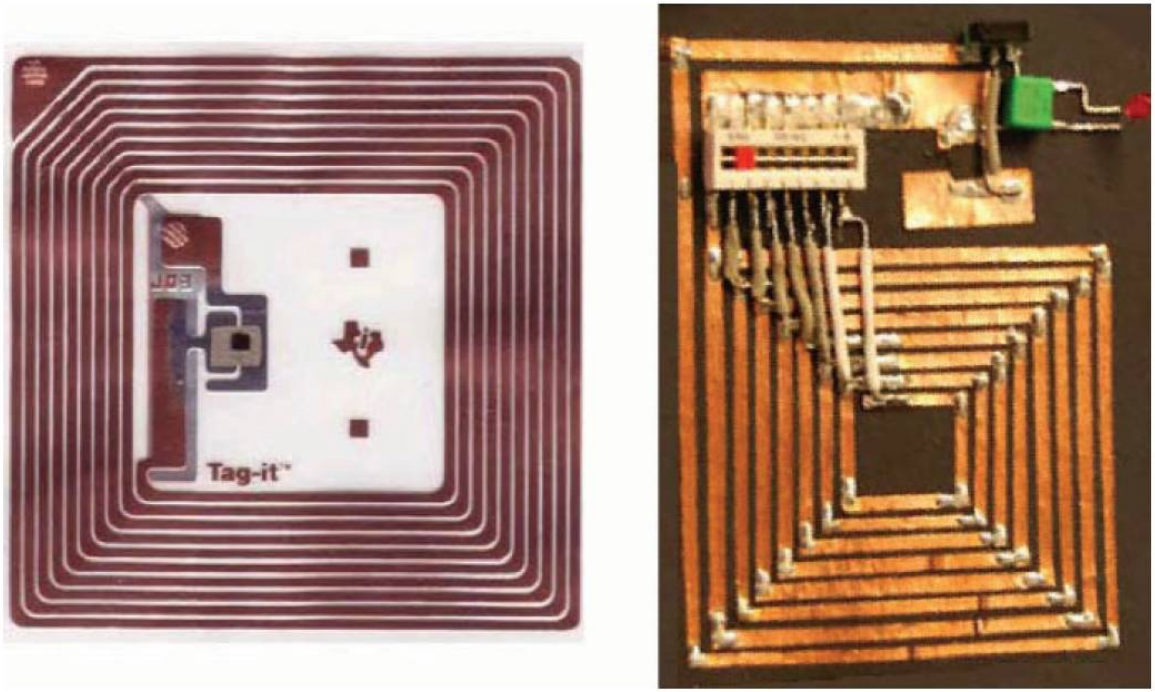
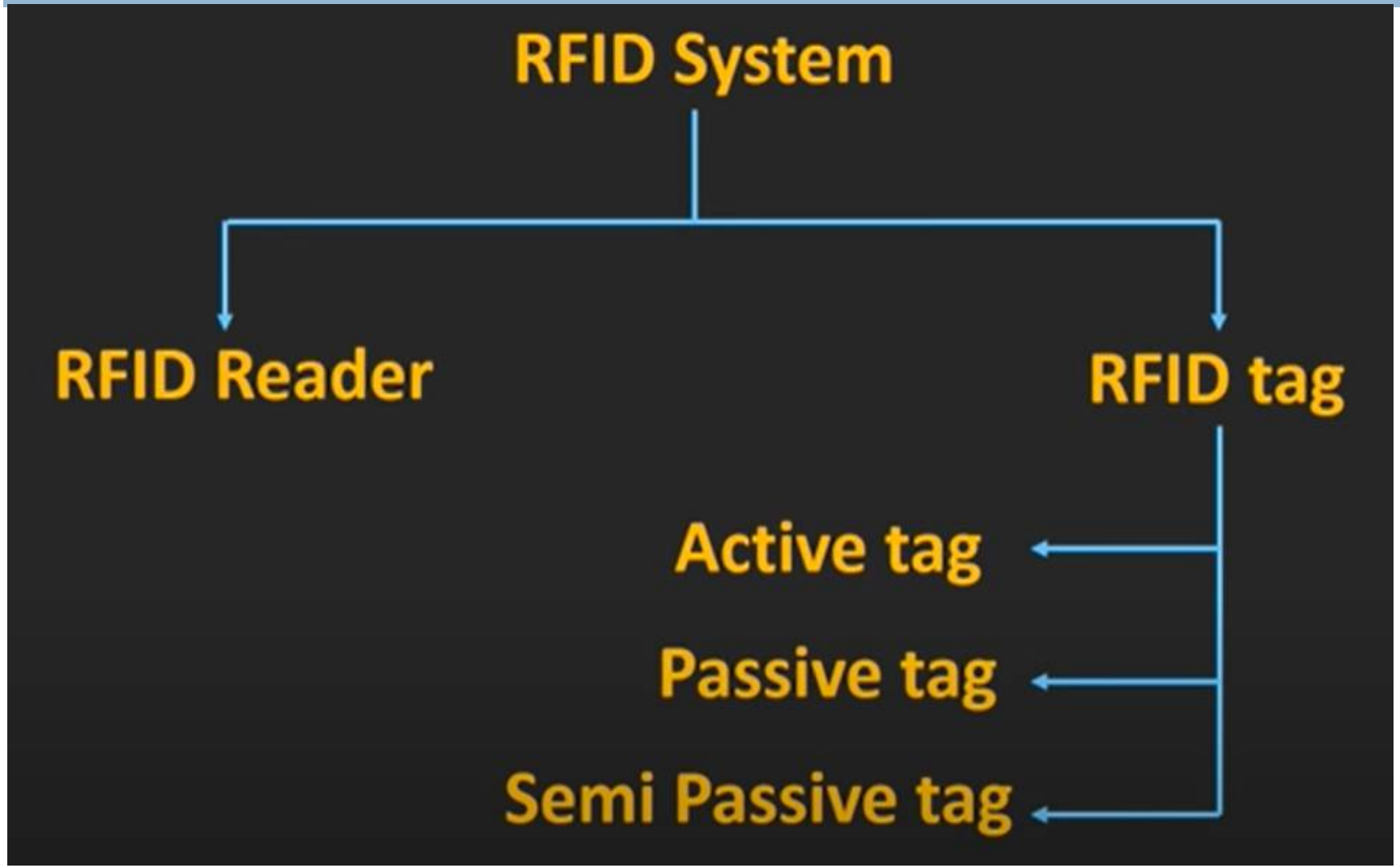
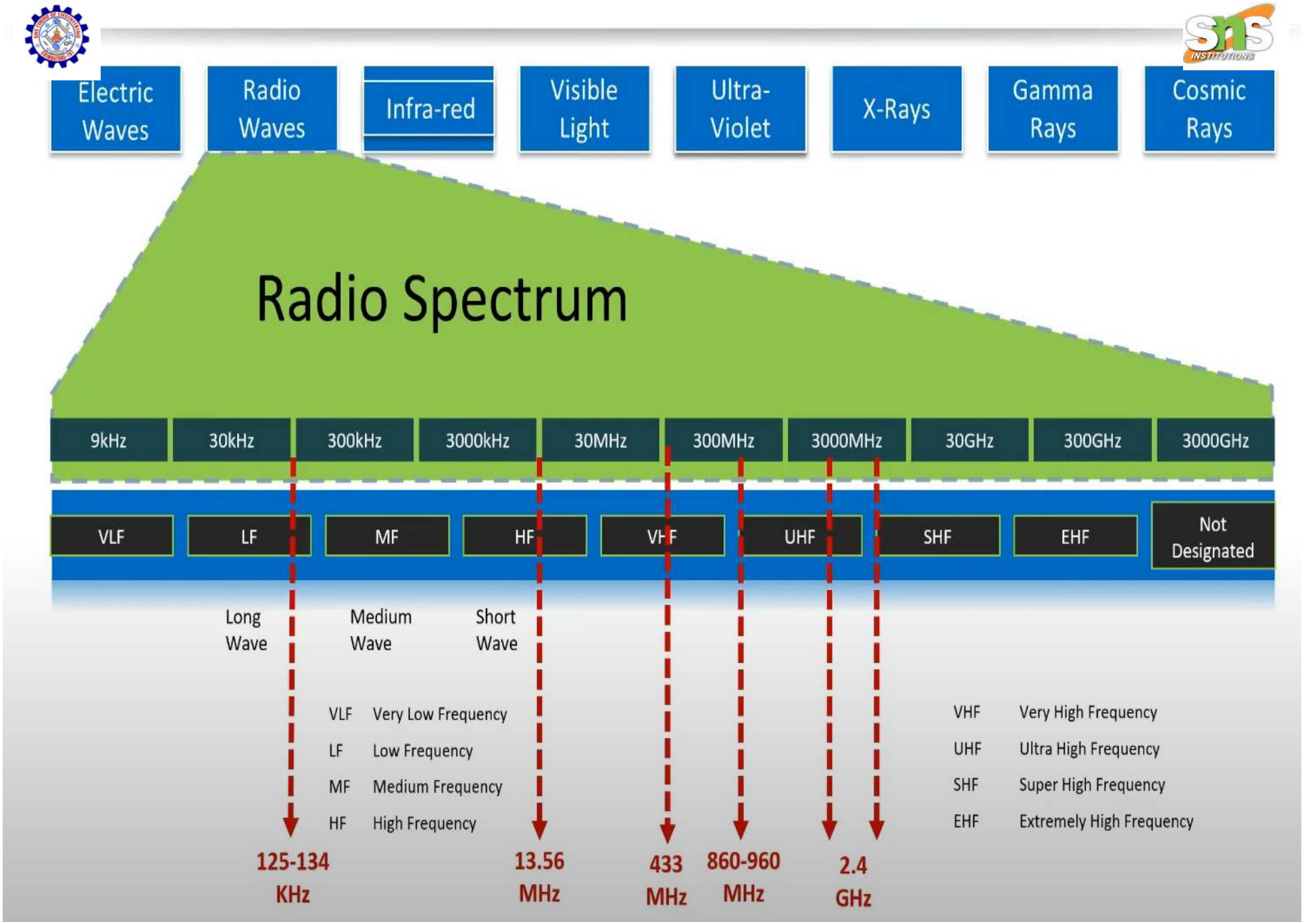


FIGURE 4.1 Illustrative examples of RFIDs.

RFID System


RFID System
RFID Reader
RFID tag
Active tag
Passive tag
Semi Passive tag


Electric Waves
Radio Waves
Infra-red
Visible Light
Ultra-Violet
X-Rays
Gamma Rays
Cosmic Rays
Radio Spectrum
9kHz
30kHz
300kHz
3000kHz
30MHz
300MHz
3000MHz
30GHz
300GHz
3000GHz
VLF
LF
MF
HF
VHF
UHF
SHF
EHF
Not Designated
Long Wave
Medium Wave
Short Wave
VLF Very Low Frequency
LF Low Frequency
MF Medium Frequency
HF High Frequency
VHF Very High Frequency
UHF Ultra High Frequency
SHF Super High Frequency
EHF Extremely High Frequency
125-134 KHz
13.56 MHz
433 MHz
860-960 MHz
2.4 GHz

Key IoT Technologies

RFID Technology

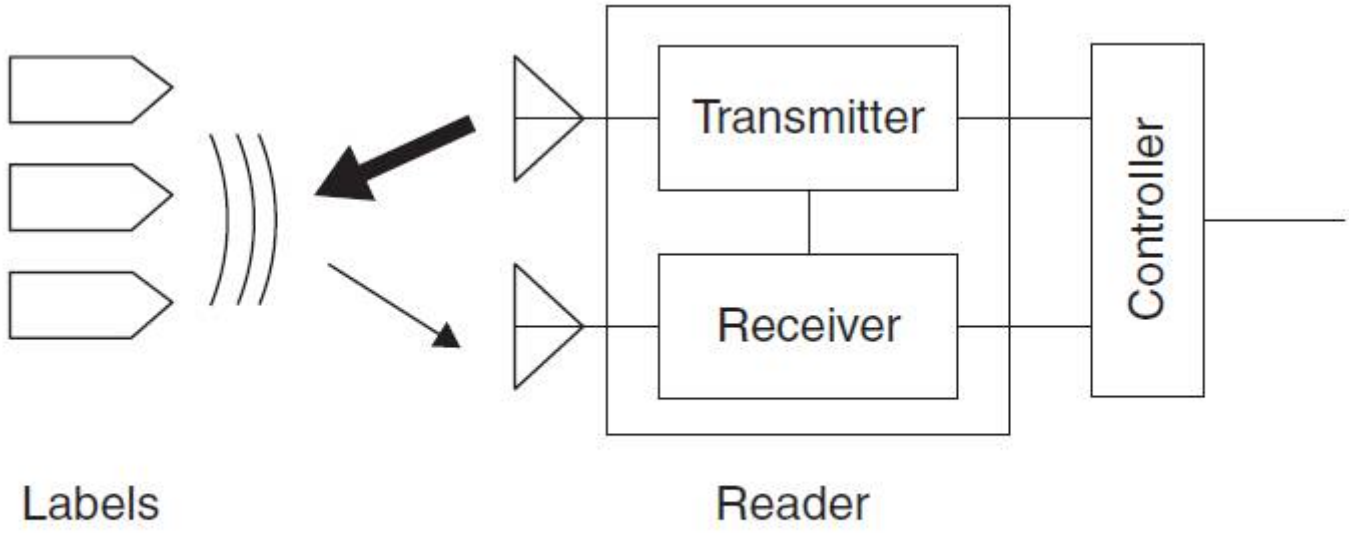


FIGURE 4.2 RFID reader operation.

Key IoT Technologies

RFID Technology- Basic Concept

TABLE 4.2 Basic RFID Concepts

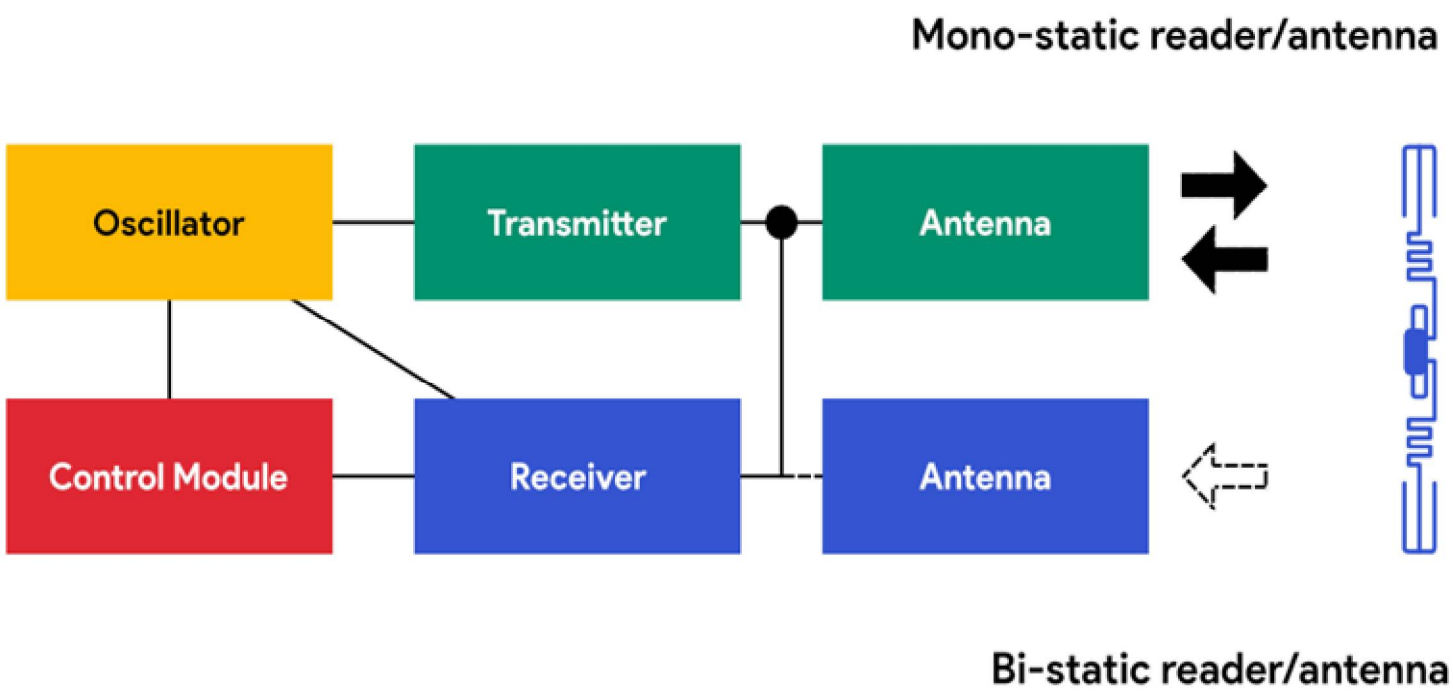
Concept	Definition
Air interface	The complete communication link between an interrogator and a tag including the physical layer, collision arbitration algorithm, command and response structure, and data-coding methodology
Continuous wave (CW)	Typically a sinusoid at a given frequency, but more generally any interrogator waveform suitable for powering a passive tag without amplitude and/or phase modulation of sufficient magnitude to be interpreted by a tag as transmitted data
Cover-coding	A method by which an interrogator obscures information that it is transmitting to a tag. To cover-code data or a password, an interrogator first requests a random number from the tag. The interrogator then performs a bit-wise EXOR of the data or password with this random number and transmits the cover-coded (also called ciphertext) string to the tag. The tag uncovers the data or password by performing a bit-wise EXOR of the received cover-coded string with the original random number
EPC	A unique identifier for a physical object, unit load, location, or other identifiable entity playing a role in business operations. EPCs are assigned following rules designed to ensure uniqueness despite decentralized administration of code space, and to accommodate legacy coding schemes in common use. EPCs have multiple representations, including binary forms suitable for use on RFID tags, and text forms suitable for data exchange among enterprise information systems
EPCglobal architecture framework	A collection of interrelated standards ("EPCglobal Standards"), together with services operated by EPCglobal, its delegates, and others ("EPC Network Services"), all in service of a common goal of enhancing business flows and computer applications through the use of EPCs

Key IoT Technologies

RFID Technology - Basic Concept

Interrogator	A device that modulates/transmits and receives/demodulates a sufficient set of the electrical signals defined in the signaling layer to communicate with conformant tags, while conforming to all local radio regulations. A typical interrogator is a passive-backscatter, interrogator-talks-first (ITF), RFID system operating in the 860–960 MHz frequency range. An interrogator transmits information to a Tag by modulating an RF signal in the 860 MHz–960 MHz frequency range. The tag receives both information and operating energy from this RF signal. Tags are passive, meaning that they receive all of their operating energy from the interrogator's RF waveform. An interrogator receives information from a tag by transmitting a continuous-wave (CW) RF signal to the tag; the Tag responds by modulating the reflection coefficient of its antenna, thereby backscattering an information signal to the interrogator. The system is ITF, meaning that a tag modulates its antenna reflection coefficient with an information signal only after being directed to do so by an interrogator. Interrogators and tags are not required to talk simultaneously; rather, communications are half-duplex, meaning that interrogators talk and tags listen, or vice versa

RFID-Interrogator



Key IoT Technologies

RFID Technology - Basic Concept

TABLE 4.2 (*Continued*)

Concept	Definition
Operating environment	A region within which an interrogator's RF transmissions are attenuated by less than 90dB. In free space, the operating environment is a sphere whose radius is approximately 1000 m, with the interrogator located at the center. In a building or other enclosure, the size and shape of the operating environment depends on factors such as the material properties and shape of the building and may be less than 1000 m in certain directions and greater than 1000 m in other directions
Operating procedure	Collectively, the set of functions and commands used by an interrogator to identify and modify tags (also known as the *tag-identification layer*)
Passive tag (or passive label)	A tag (or label) whose transceiver is powered by the RF field
Physical layer	The data coding and modulation waveforms used in interrogator-to-tag and tag-to-interrogator signaling
Singulation	Identifying an individual tag in a multiple-tag environment
Slotted random anticollision	An anticollision algorithm where tags load a random (or pseudo-random) number into a slot counter, decrement this slot counter based on interrogator commands, and reply to the interrogator when their slot counter reaches zero
Tag air interface	As defined in ISO 19762–3, a conductor-free medium, usually air, between a transponder and a reader/interrogator through which data communication is achieved by means of a modulated inductive or propagated electromagnetic field
Tag-identification layer	Collectively, the set of functions and commands used by an interrogator to identify and modify tags (also known as the *operating procedure*)

Key IoT Technologies

RFID Technology

- Contactless smart cards (SCs) are more sophisticated than RFID tags
- RFID tags are typically less expensive than SCs.
  - When an RFID tag or contactless SC passes within a defined range, a reader generates electromagnetic waves; the tag's integrated antenna receives the signal and activates the chip in the tag/SC, and a wireless communications channel is set up between the reader and the tag enabling the transfer of pertinent data.

Overview: what happens in RF (radio frequency) communication

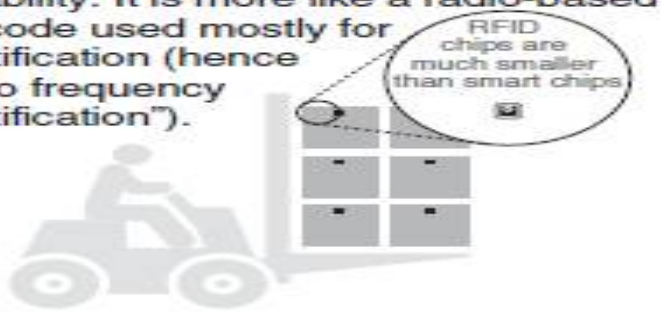
1. When a contactless smart card or an RFID tag passes within range, a reader sends out radio frequency electromagnetic waves.
2. The antenna, tuned to receive these waves, wakes up the chip in the smart card or tag.
3. A wireless communications channel is set up between the reader and the smart card or tag.

The contactless smart card contains a microprocessor, a small but real computer that makes calculations, communicates both ways, remembers new information, and actively uses these capabilities for security and many other applications.

Characteristics of a contactless card

- Strong security capacities:
  - mutual authentication before providing access to information
  - access can be further protected via PIN or biometric
  - encryption to protect data on card during exchange
  - hardware and software protection to combat attacks or counterfeiting
- Hundreds of security features mean an individual's personal ID, financial details, payment transactions, transit fares or physical access privileges can be safely stored, managed, and exchanged
- Read and write memory capacity of 512 bytes and up, with very large memory storage possible
- Short-distance data exchange, typically two inches

RFID tags are devices that typically have a read-only chip that stores a unique number but has no processing capability. It is more like a radio-based bar code used mostly for identification (hence "radio frequency identification").



Characteristics of an RFID tag

- Minimal security:
  - one-way authentication; card cannot protect itself
  - insufficient storage for biometrics
  - no on-chip calculations of new information
  - relies on static keys
- Single function; used to help machines identify objects to increase efficiency. Example: inventory control
- Small memory (92 bytes); often read-only
- Larger distance data exchange, typically several yards

Because of their more restricted capabilities, RFID tags are generally cheaper.

FIGURE 4.3 Comparison between contactless SCs and RFID tags. *Source:* Gemalto (used with Permission).

Key IoT Technologies

RFID Technology

- There are a number of standards for RFIDs. Some of the key ones include the following:
  - The ISO 14443
    - operating frequency of 13.56 MHz that embed a CPU; power consumption is about 10mW; data throughput is about 100 Kbps and the maximum working distance (from the reader) is around 10 cm.
  - The ISO 15693
    - operating at 13.56 MHz frequency, but it enables working distances as high as 1 m, with a data throughput of a few Kbps.
  - The ISO 18000
    - with frequency such as 135 KHz, 13.56 MHz, 2.45 GHz, 5.8 GHz, 860–960 MHz, and 433 MHz.
    - The ISO 18000–6 standard uses the 860–960MHz range and is the basis for the Class-1 Generation-2 UHF RFID, introduced by the EPCglobal Consortium.

Key IoT Technologies

RFID Technology

- Typically, EPC codes used for active RFIDs or IP addresses are transmitted in clear form
  - Provide strong privacy for the IoT.
  - The host identity protocol (HIP) with this protocol, active RFIDs do not expose their identity in clear text, but protect the identity value (e.g., an EPC) using cryptographic procedures.

Key IoT Technologies

RFID Technology

- An RFID system is logically comprising several layers, as follows:
  - the tag layer,
  - the air interface (also called media interface) layer,
  - the reader layer;
- Tag (device) layer:
  - Architecture and EPCglobal Gen2 tag finite state machine
- Media interface layer:
  - Frequency bands, antennas, read range, modulation, encoding, data rates
- Reader layer:
  - Architecture, antenna configurations, Gen2 sessions, Gen2

Key IoT Technologies

RFID Technology- standards in the EPCglobal environment

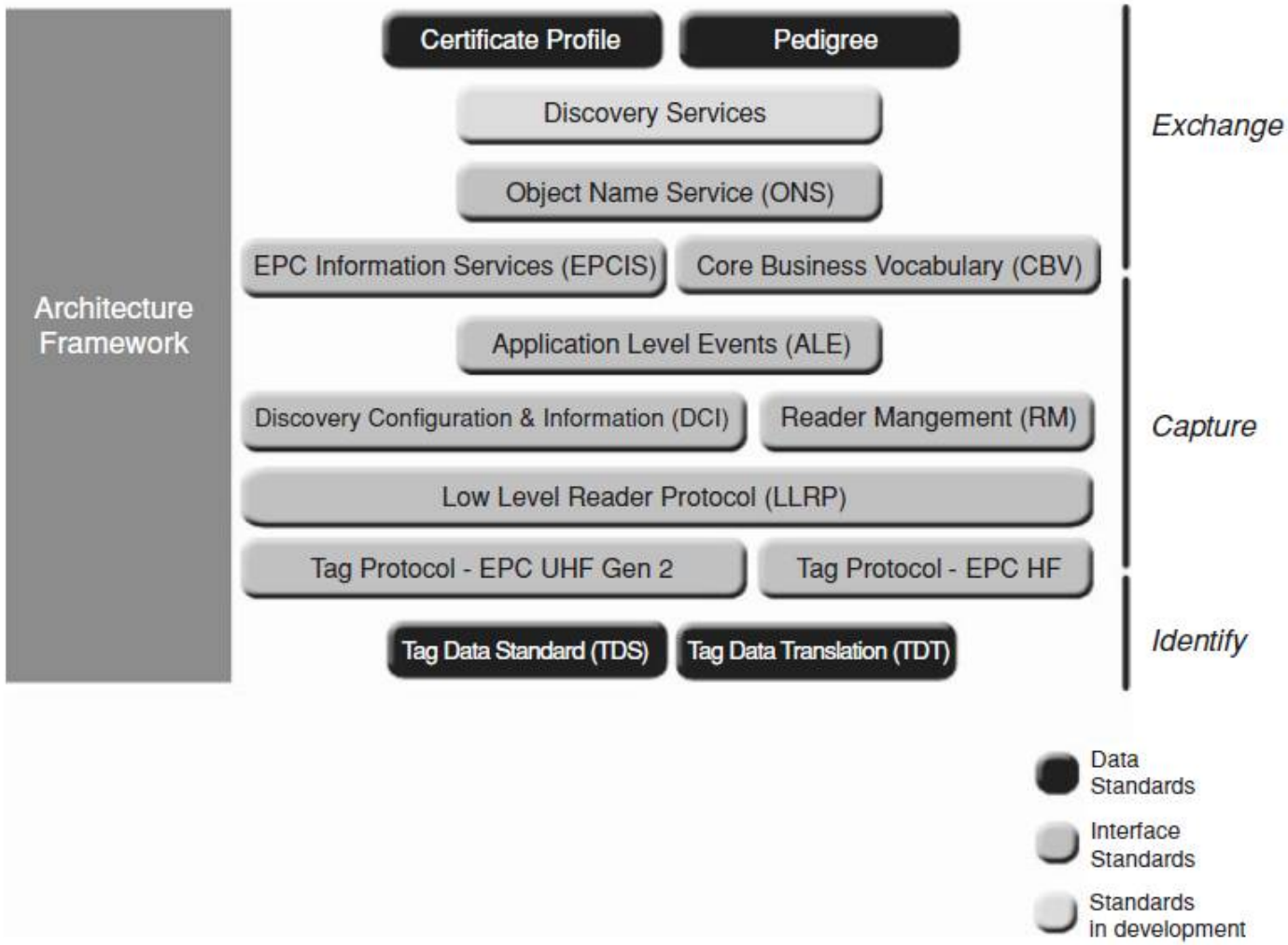


FIGURE 4.4 Standards that comprise the EPCglobal environment.

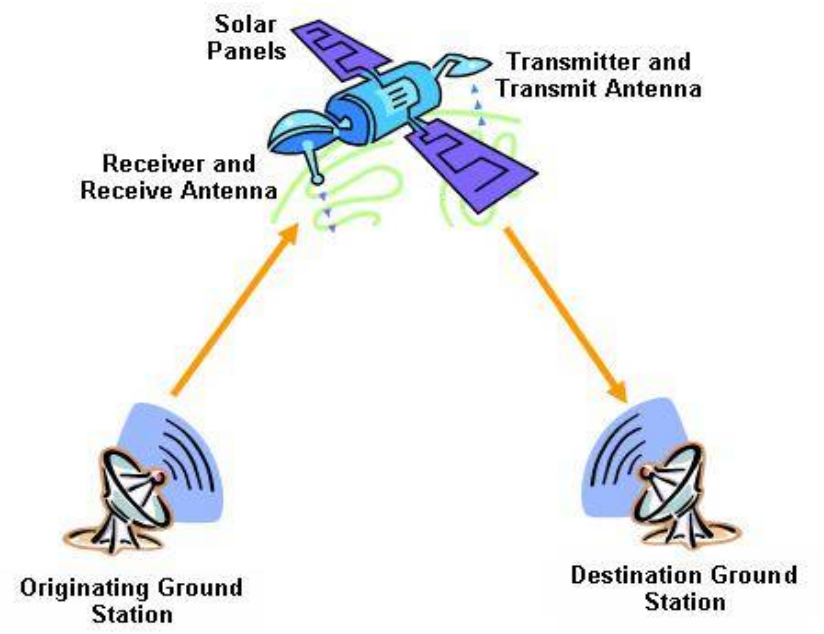
Key IoT Technologies

RFID Technology- standards in the EPCglobal environment

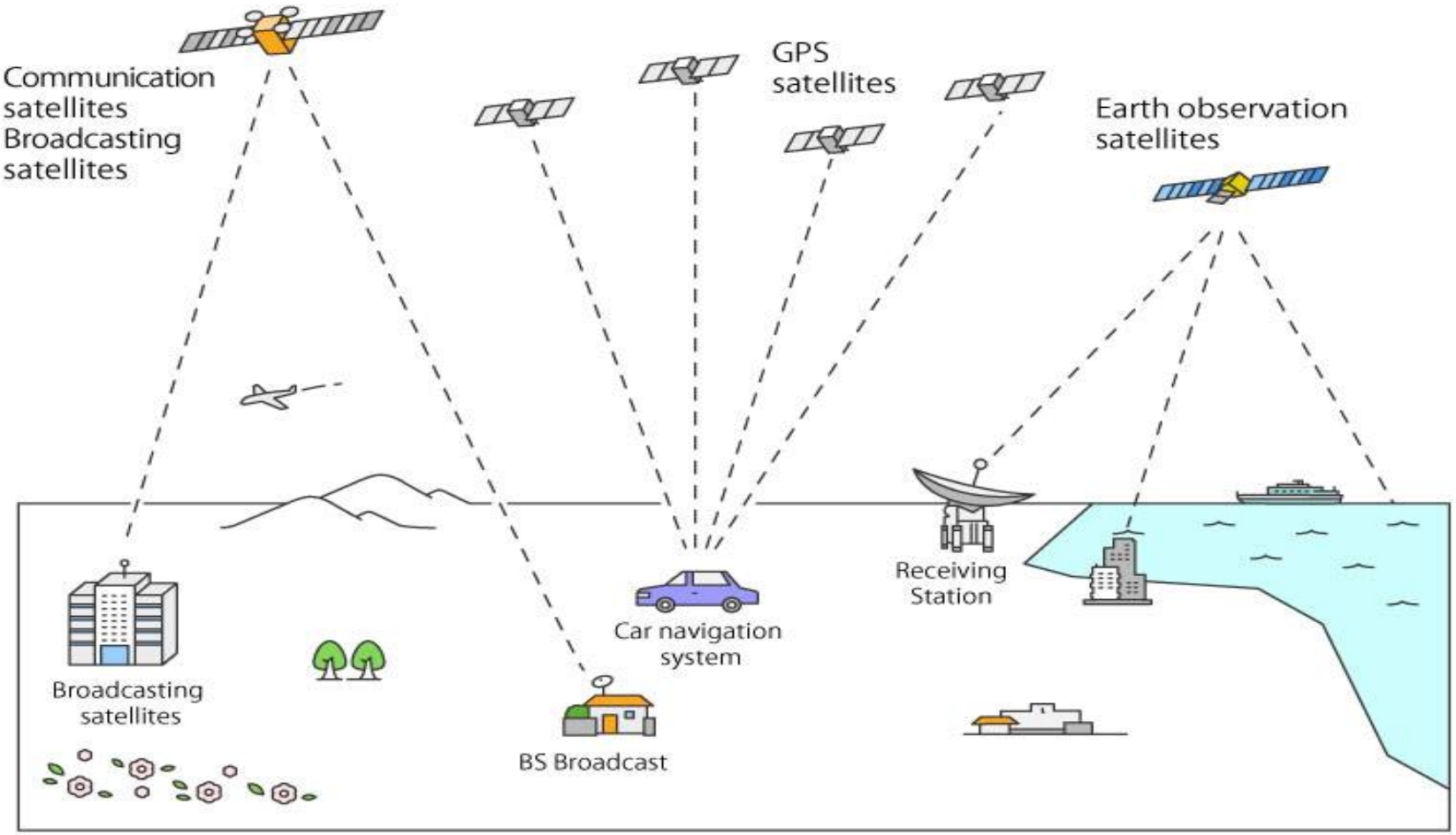
- An interface is the UHF Class-1 Gen-2 tag air interface, which specifies a radio-frequency communications protocol by which an RFID tag and an RFID reader device may interact.
- A component is an RFID tag that is the product of a specific tag manufacturer.
- An EPC Network Service is the ONS, which provides a logically centralized registry through which an EPC may be associated with information services.

Key IoT Technologies
Satellite Technology

- Ability to support mobility in all geographical environments (including Antarctica)
- Global reach
- Offers interesting commercial possibilities



Examples


Communication satellites
Broadcasting satellites
GPS satellites
Earth observation satellites
Receiving Station
Car navigation system
Broadcasting satellites
BS Broadcast

Thank you