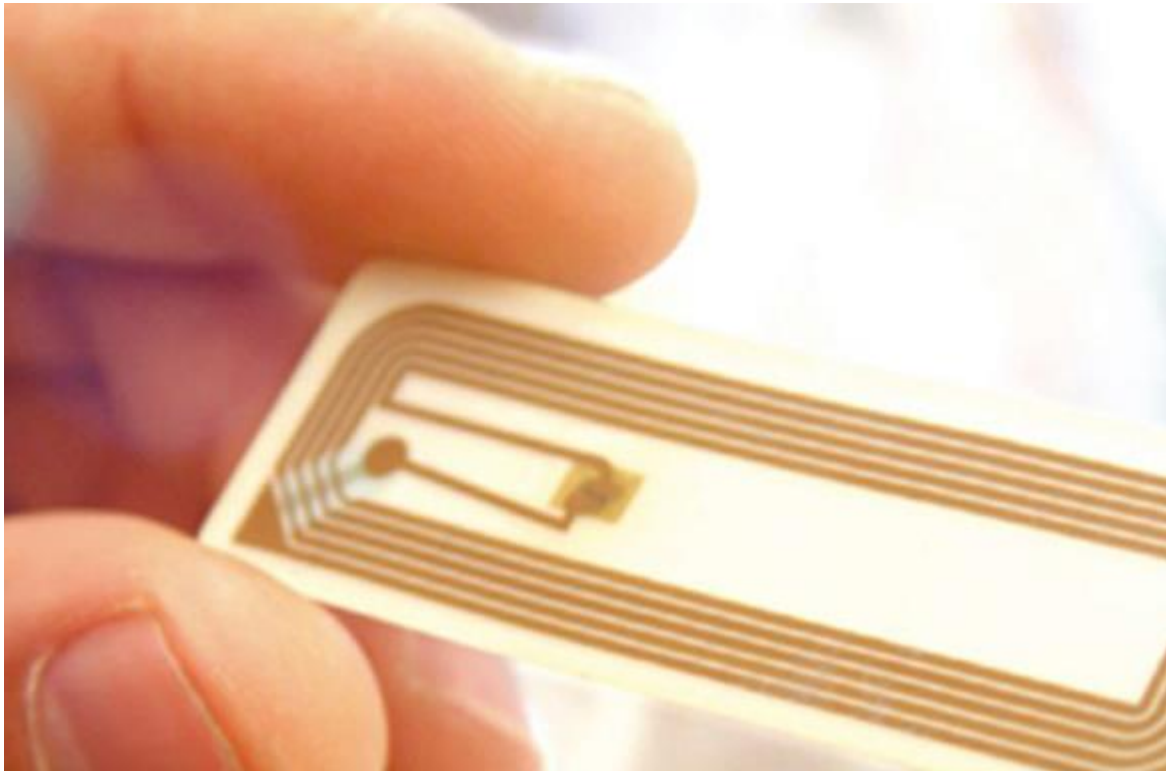


20IS709

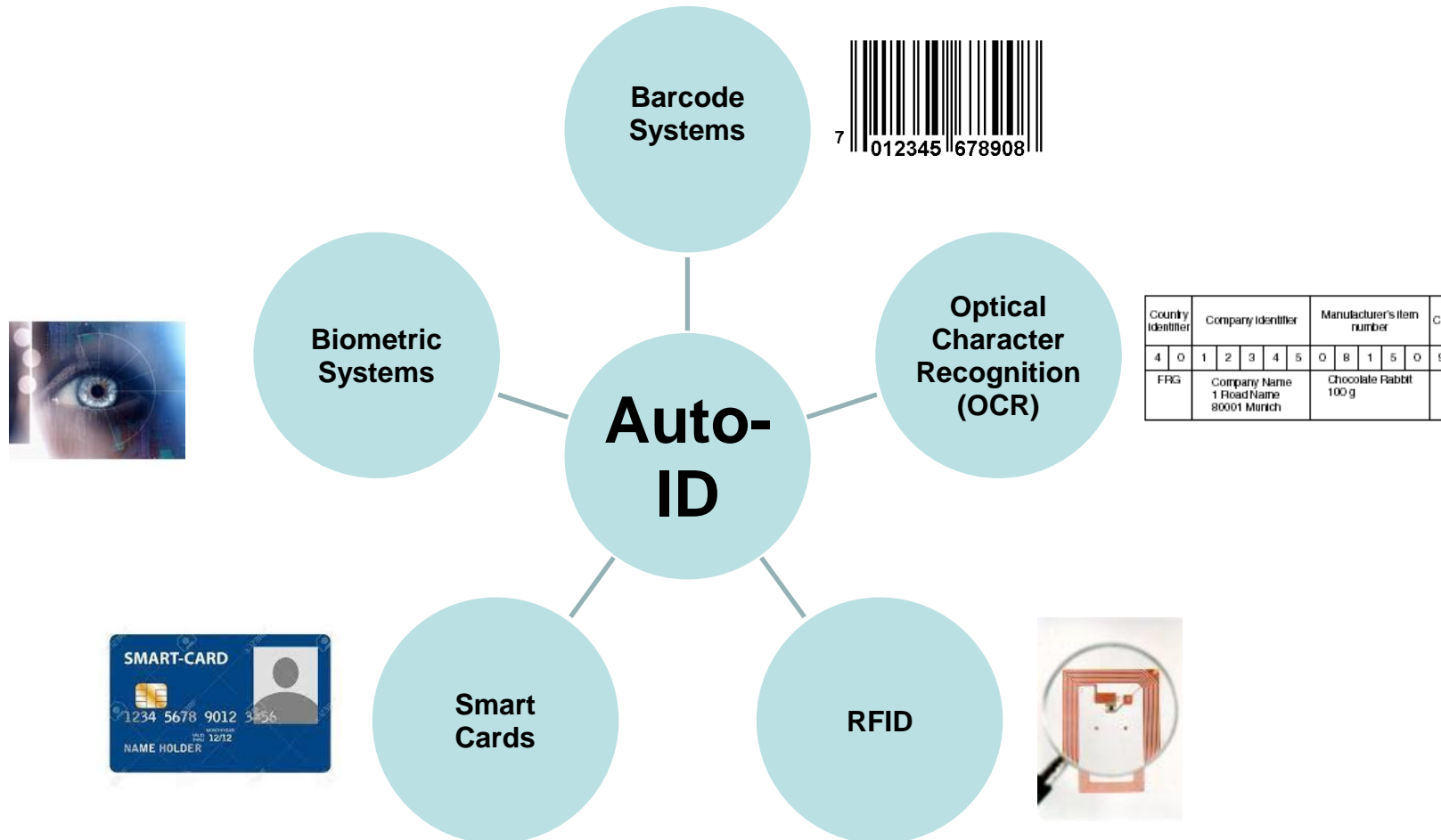
# Communication Systems For Industrial Networking



**Radio Frequency Identification  
(RFID)**

# Automatic Identification System

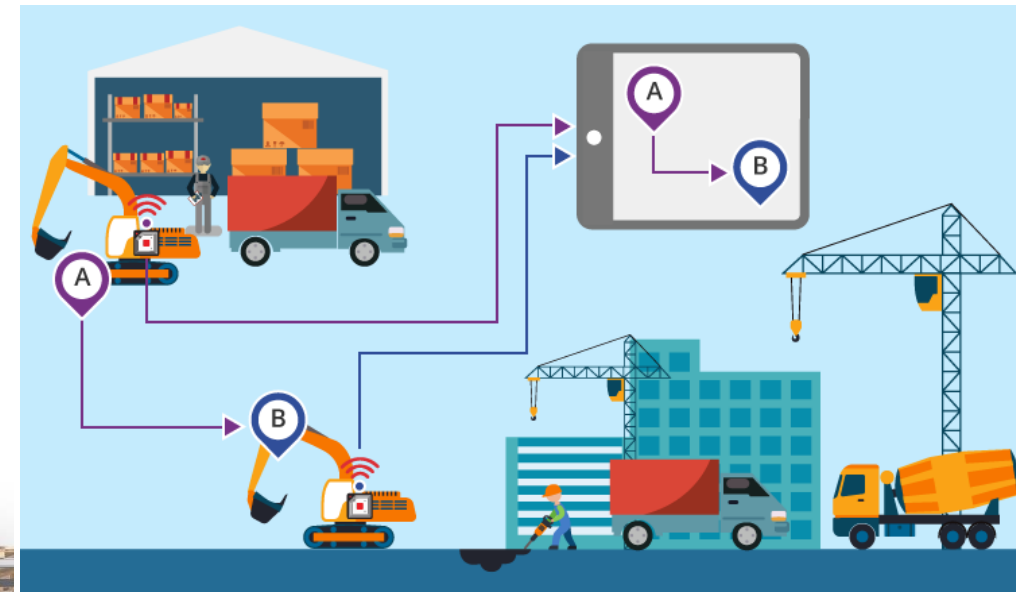
- Auto ID refers to the method of capturing or collecting data via automatic means and storing data in a computer.
- Includes: Bar codes, Magnetic stripe, Radio frequency identification, Smart card.



# Radio Frequency Identification

- Applications

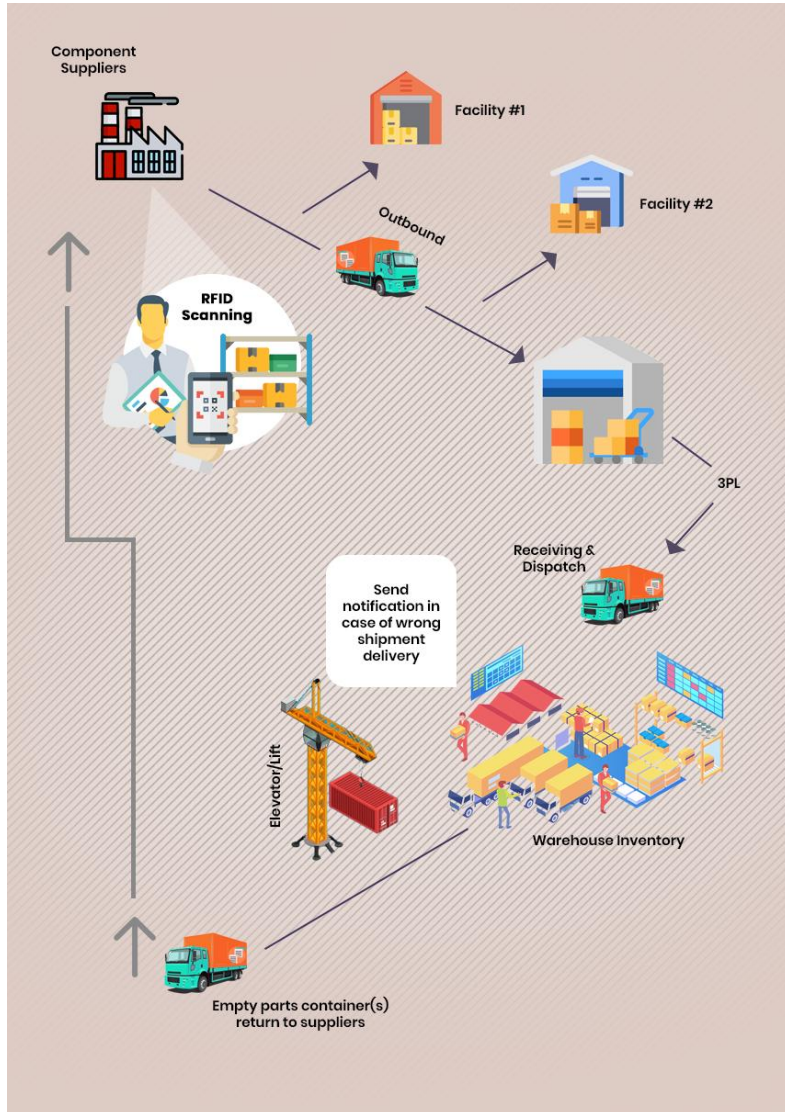
- Automatic Control: classification and assembly line management of automobile, home appliance, electronics industry.
- Material Control: automatic inventory and Control system of material in Factory.



Asset Tracking

# Radio Frequency Identification

- Applications



Supply chain management



Counterfeit prevention

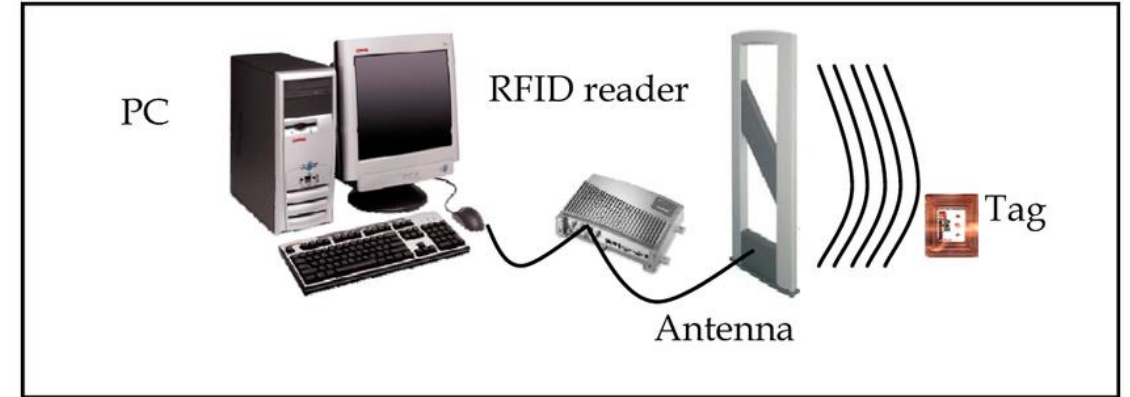
# RFID

- A form of **wireless communication** that incorporates the use of electromagnetic coupling in the **radio frequency portion of the electromagnetic spectrum** to uniquely identify an object, animal or person.
- Used for **automatic data capture** which allows **contact-less identification** of objects via Radio Frequency (RF).
- Also called electronic tag, electronic chip, and non-contact card.
- Can identify high-speed moving objects and identify multiple objects at the same time, which is fast and convenient to operate.
- Short-range and long-range RF products

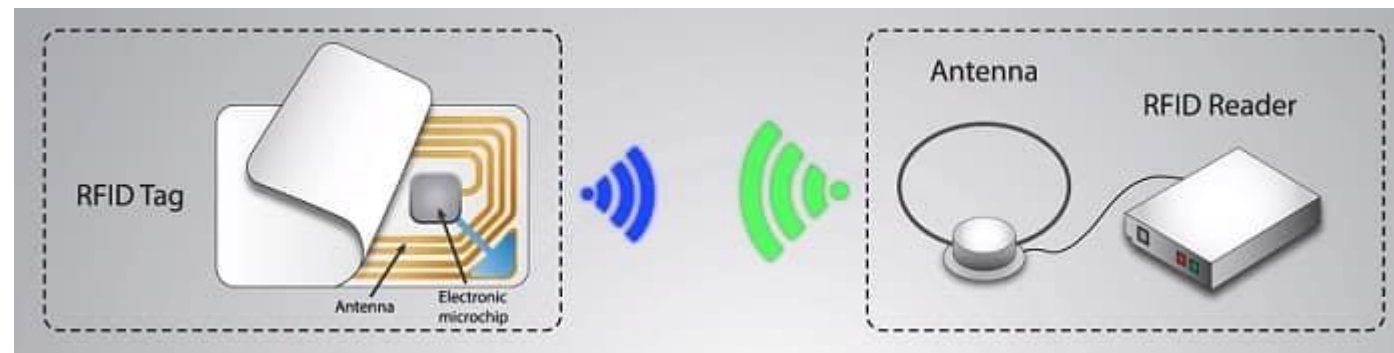


# Components of RFID System

- A basic RFID system consists of three components
  - A **transponder** (RFID tag)
  - Reader or **Interrogator**
  - Host computer

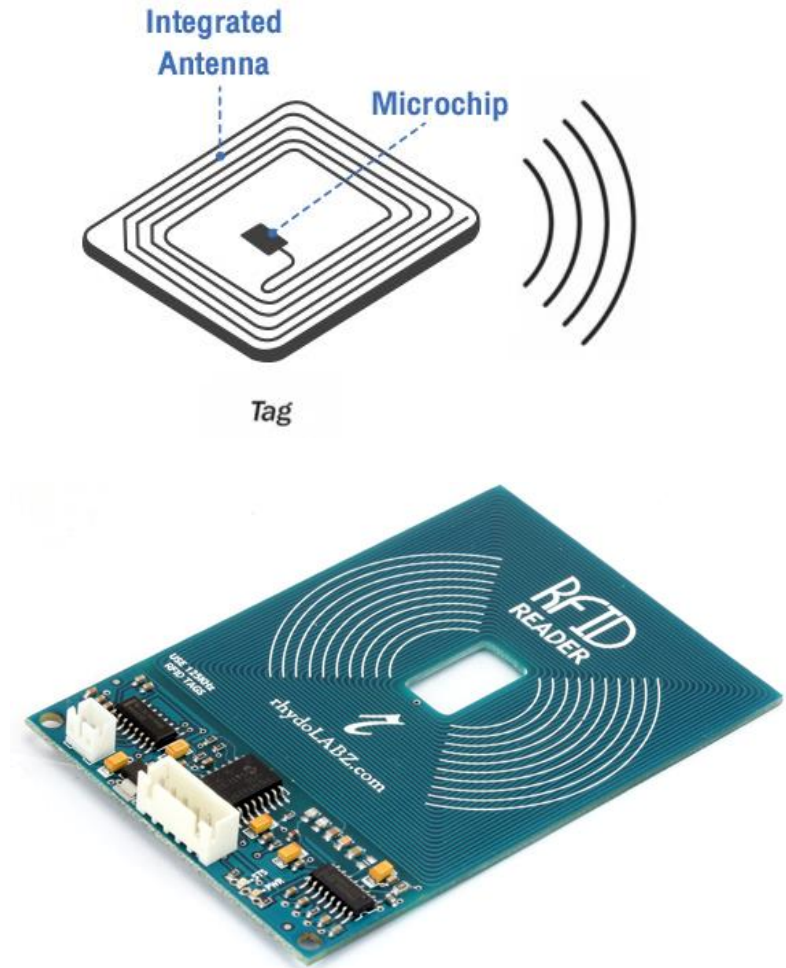
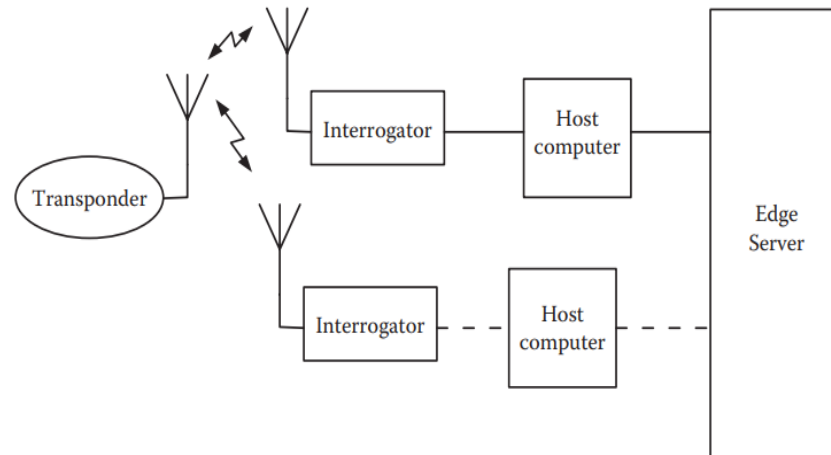


- The scanning antenna and transceiver are combined - referred to as an RFID reader or interrogator.
- RFID reader is a network-connected device - uses radio waves to transmit signals that activate the tag.



# Basic structure of an RFID system

- The devices that store and carry the information are called **transponders** or **tags**.
- Contain Integrated circuit for storing and processing information, modulating and demodulating a RF signal; an antenna for receiving and transmitting the signal.
- The device that is used to capture and transfer information is commonly called a **reader** or **interrogator**,
- Interrogators composed of a RF module, control unit and antenna to interrogate tags via RF communication.
- A host computer connected to the interrogator and acts like the interface between the RFID system and the ultimate application.



# Passive versus Active RFID Systems

## Passive RFID systems

- Passive RFID systems use passive transponders - do not have an internal power source.
- They harvest the energy needed by their internal circuits from the electromagnetic field generated by the interrogator.
- The interrogator transmits a low power radio signal through its antenna to the tag, which in turn receives it through its own antenna to power the integrated circuit.
- Tag chip can contain non-volatile, EEPROM for storing data.
- For this reason, they have a short range, limited to a few inches /feet.
- Simple low cost and small.

## Active RFID systems

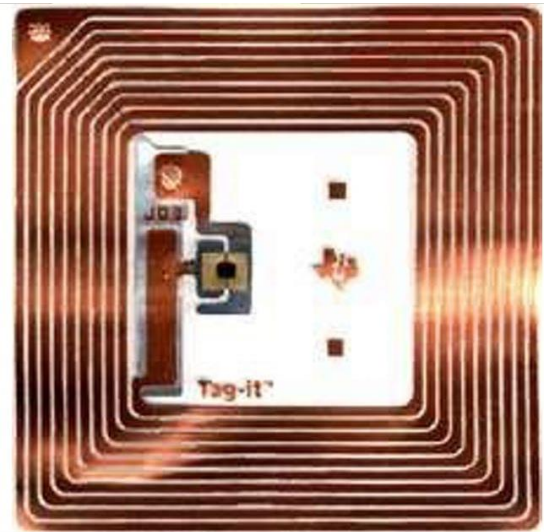
- Active RFID systems use active transponders - have an internal power source, typically a battery that allows broadcasting the signal to the interrogator.
- Because of not being limited to the power harvested by the antenna, they have an extended read range, typically several hundred feet - typically operate in the ultra-high-frequency (UHF) and microwave ranges.
- The inclusion of the power source increases their cost in two ways: the cost of the battery as well as the maintenance costs required to check the status of the internal power source and replace it when it has reached an unacceptably low level.
- The cost is approximately 100 times higher than the cost of a passive transponder.



# Passive versus Active RFID Systems

## Semipassive or battery-assisted transponders

- Include a battery, but contrary to active transponders, the battery is not used to generate the power to transmit the signal to the interrogator.
- The battery is used to support secondary functions like the data logging from different types of sensors.
- These transponders also harvest the energy from the electromagnetic field generated by the interrogator to power its internal circuits other than the sensing and data-logging parts



Passive



Active



Semi passive

# Passive versus Active RFID Systems

	Active RFID	Passive RFID
Tag Power Source	Internal to tag	Energy transferred using RF from reader
Tag Battery	Yes	No
Availability of power	Continuous	Only in field of reader
Required signal strength to read tag	Very Low	Very High
Range	Up to 100 meters	Up to 3-5m, usually less
Multi-tag reading	1000's of tags recognized – speeds up to 100 miles/hour.	Few hundred within 3m of reader
Data Storage	Up to 1Mb of read/write with sophisticated search and access	128 bytes of read/write

# Functional Classification of RFID Transponders

Based on their electronic product code (EPC) class divided into different classes and generations

- **Generation 1, Class 0**: Passive tags with read-only functionality, also called **write one, read many** (WORM) transponders - **programmed at the factory** with their unique identification number and user is not able to change it or include additional information.
- **Generation 1, Class 0+**: WORM transponders - differ from Generation 1, Class 0 transponders in that it is the **user** who **programs** them and no further programming or changing of data is allowed.
- **Generation 1, Class 1**: similar to Generation 1, Class 0 or 0+ transponders, but **could be read by interrogators from other companies**. Gen 1, Class 1 transponders have evolved into the different transponders from Generation 2.

Generation 1 transponders employ **proprietary data structures and can be read only by interrogators manufactured by the same vendor**; Generation 2 transponders are vendor neutral in their specifications - this means the elimination of duplicate reads within the read range.

# Functional Classification of RFID Transponders

Based on their electronic product code (EPC) class divided into different classes and generations

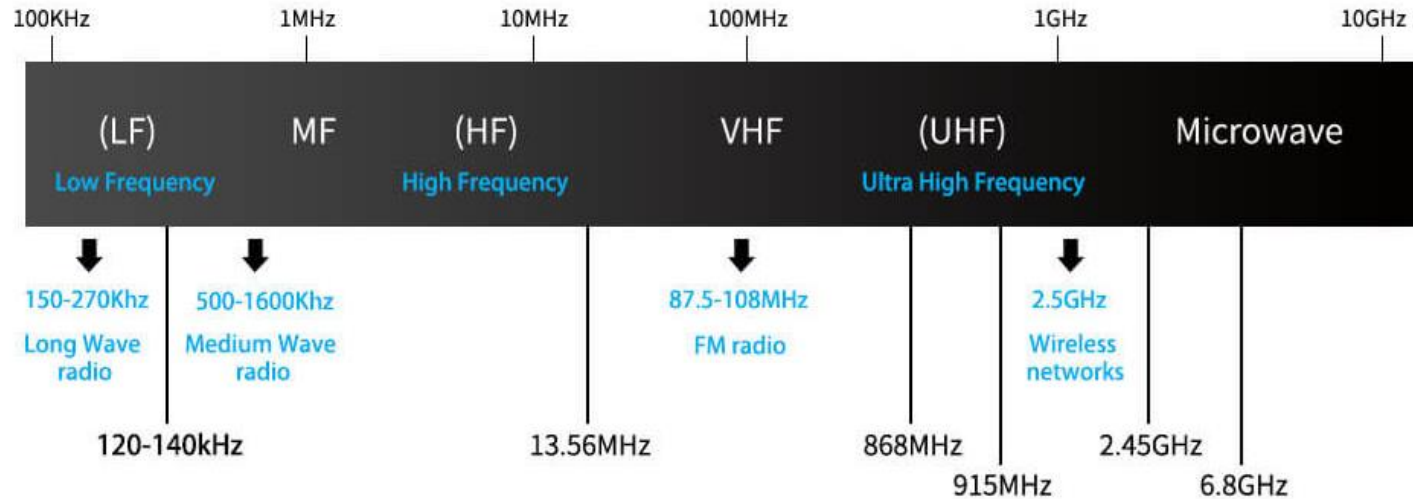
- **Generation 2, Class 1:** WORM transponders - programmed at the factory, but they can be read with equipment from different vendors, support the higher read rates, and have more noise immunity than the Generation 1 transponders.
- **Generation 2, Class 2:** rewritable transponders - can be written several times by the user using equipment different from the vendor's equipment.
- **Generation 2, Class 3:** semipassive or battery-assisted transponders
- **Generation 2, Class 4:** active transponders
- **Generation 2, Class 5:** These transponders are essentially interrogators - able to power other transponders.

# RFID Frequencies

- Selecting the most adequate frequency is a function of two variables: the **technological developments of systems** at the different operating frequencies—directly related to the cost of systems—as well as the **properties of electromagnetic waves** at those different frequencies.

Commonly Used Frequency Band for RFID Systems

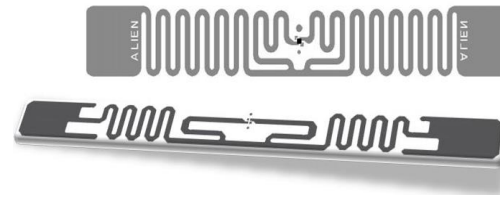
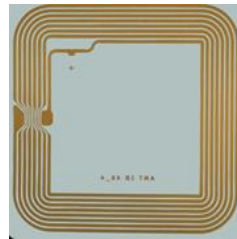
Frequency Band	Frequency Range	Typical Frequencies Used in RFID Systems
Low Frequency (LF)	100 kHz – 500 kHz	125 kHz 134.2 kHz
High Frequency (HF)	10 MHz – 15 MHz	13.56 MHz
Ultra High Frequency (UHF)	400 MHz – 950 MHz	866 MHz Europe 915 MHz United States
Microwaves ( $\mu$ W)	2.4 GHz – 6.8 GHz	2.45 GHz 3.0 GHz



LF





HF



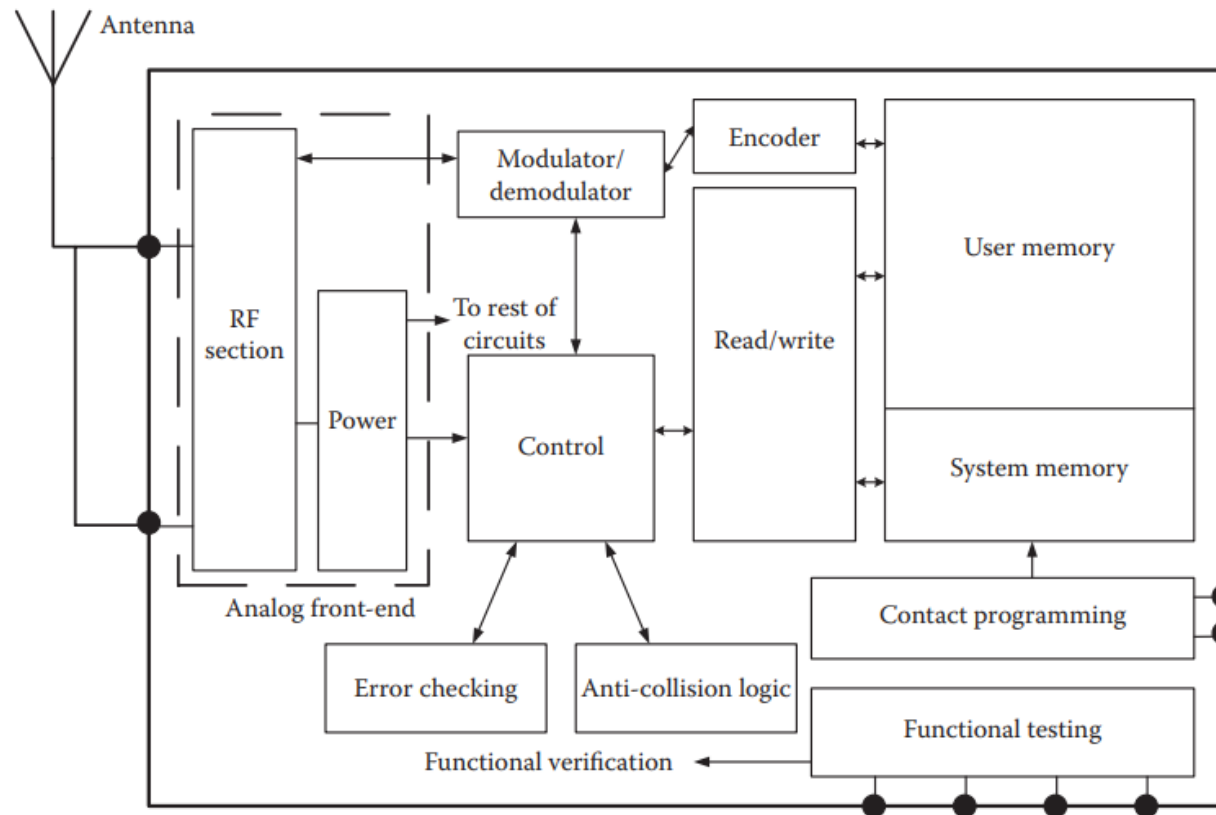
UHF

# RFID Frequencies

Frequency	LF 125 ~ 135 kHz	HF 13.56 MHz	UHF 850 ~ 960 MHz
Read Range	0.5 ~ 2 m	< 1m	> 3m
Cost	Relatively expensive	Less expensive	Least expensive
Penetration of materials	Excellent		
Affected by water?	No	To some extent	Yes
Power source	Passive (Inductive)	Passive (Inductive)	Passive (Propagation)
Data Rate	Slower		
Reading Multiple tags	Poor	Good	Very Good
Applications	Car immobilisers, Animal identification, POS	"Pharma", Libraries Baggage tracking, Tickets Payments, Passports	Pallet/ Case tracking, Tolls Baggage tracking

# Transponders

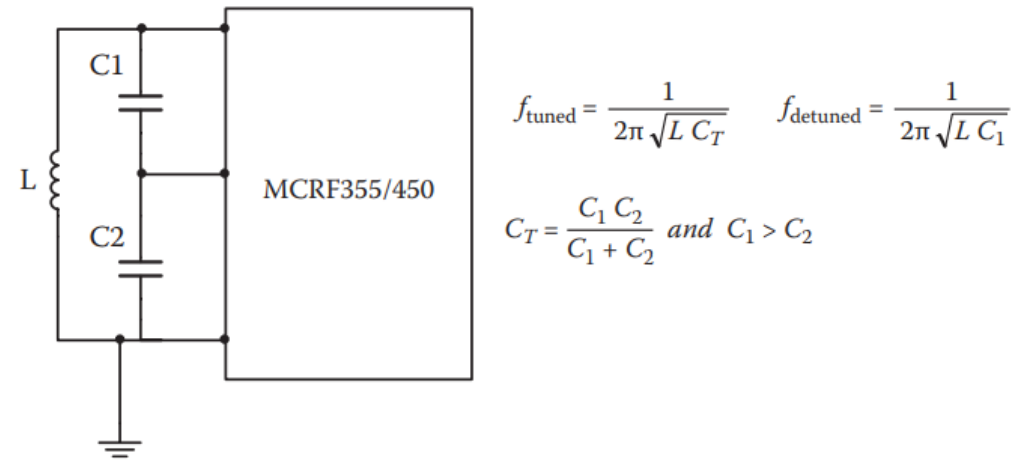
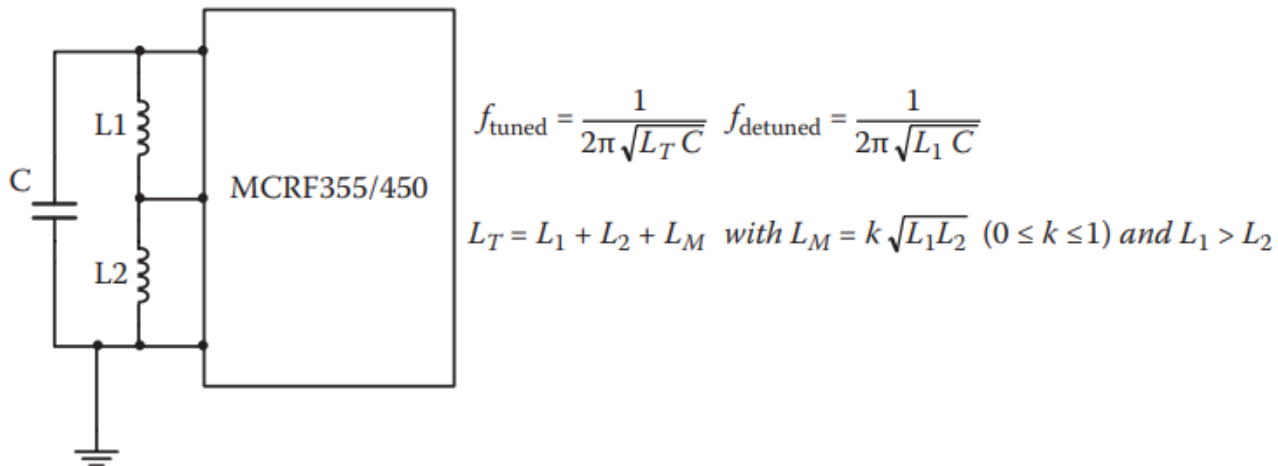
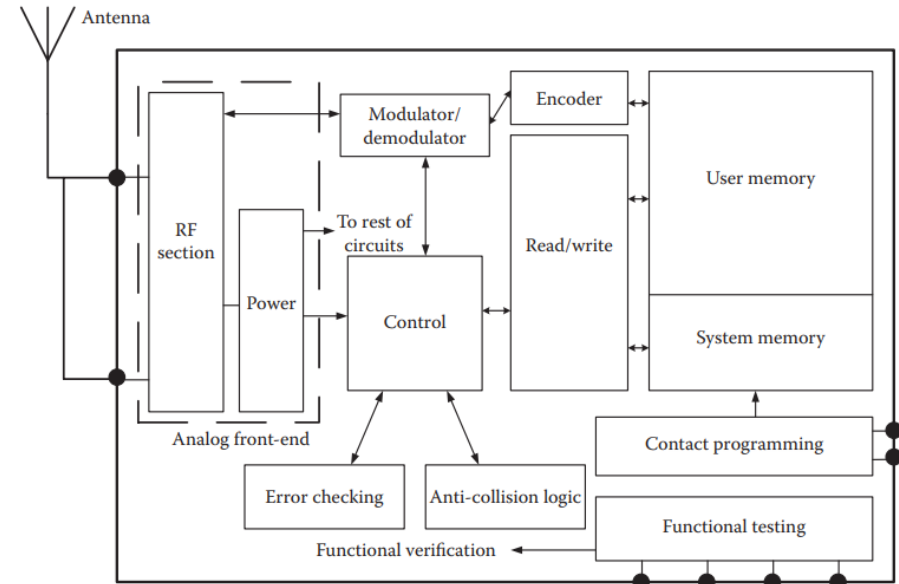
- The two main components are **internal circuits** and **antenna**.
- The antenna is used to **collect energy from the electromagnetic fields** in which the transponder is embedded as well as to transmit the information back to the interrogator.
- The integrated circuit is also known as the chip or device, have the ability to **store information to be transmitted to the interrogator**, execute a series of commands, and, in some cases, store new information sent by a remote station.



# Transponders

## Analog front end

- When the transponder is immersed in an electromagnetic field of the appropriate frequency, a **radiofrequency voltage appears across the antenna terminals**.
- The task of the front-end stage is to **rectify that radiofrequency voltage and convert it into a continuous voltage (DC)** with a value high enough to power the rest of the circuits inside the device.
- The first step in the energy conversion process between the electromagnetic field and the DC voltage is the **resonant circuit tuned to the frequency of the field**.

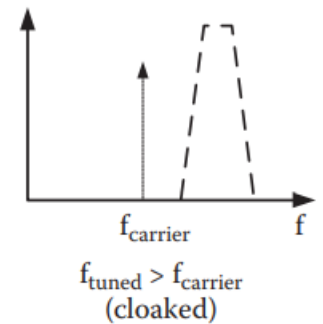
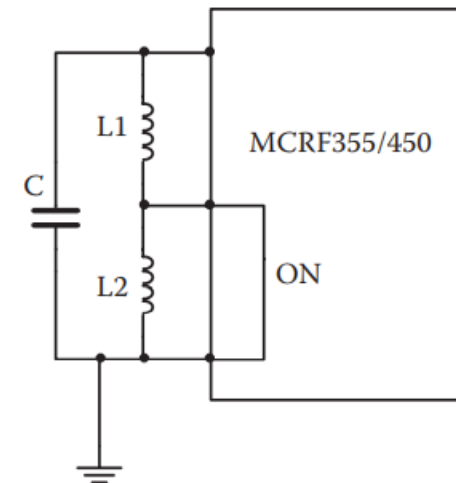
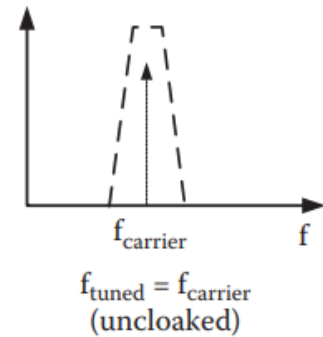
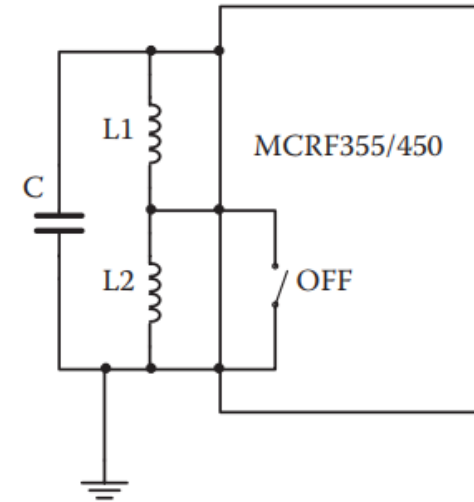




# Transponders

## Analog front end

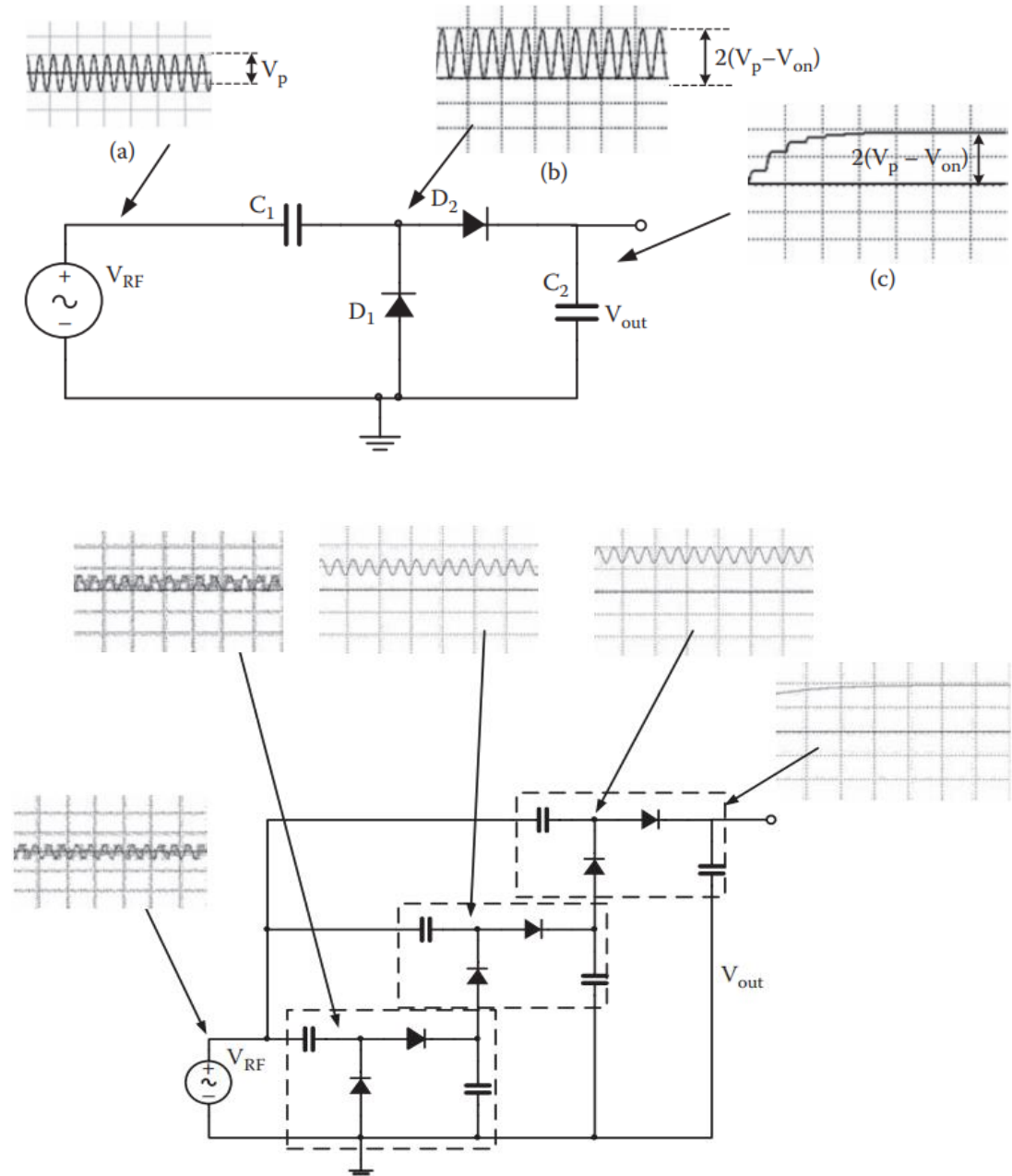
- The resulting resonance frequency when the **modulation transistor is OFF** is chosen to be equal to the frequency of the electromagnetic field emitted by the interrogator.
- Because of the **resonance condition, the energy of the field is transmitted through the front end to the device**, resulting in the radiofrequency voltage at the input of the device being maximal - This situation is called **uncloaking**
- When the **modulation transistor is turned ON**, it shortens one of the inductors, resulting in a resonant frequency for the circuit different from the frequency of the electromagnetic field.
- When it shortens one of the two inductors connected in series, the resulting resonant frequency is higher than the frequency of the field.
- In any case, the **frequency of the circuit and the frequency of the field are different**, and therefore most of the **energy of the electromagnetic field is rejected by the filter**, resulting in the voltage generated at the input of the device being minimal, ideally zero. This situation is called **cloaking**.
- The **cloaking–uncloaking approach** is used by the transponder to transmit data to the interrogator.



# Transponders

## Power Management

- In order to be operative, the transponder needs to convert the radiofrequency voltage detected by the antenna into a DC voltage.
- The voltage required to bias the internal components in the transponder is higher than the voltage detected by the antenna - therefore, the transponder requires the use of voltage multipliers to reach the values necessary by the biasing voltage.
- A voltage multiplier is a circuit that converts a lower AC voltage into a higher DC voltage – voltage doubler.



# Transponders

## Memory

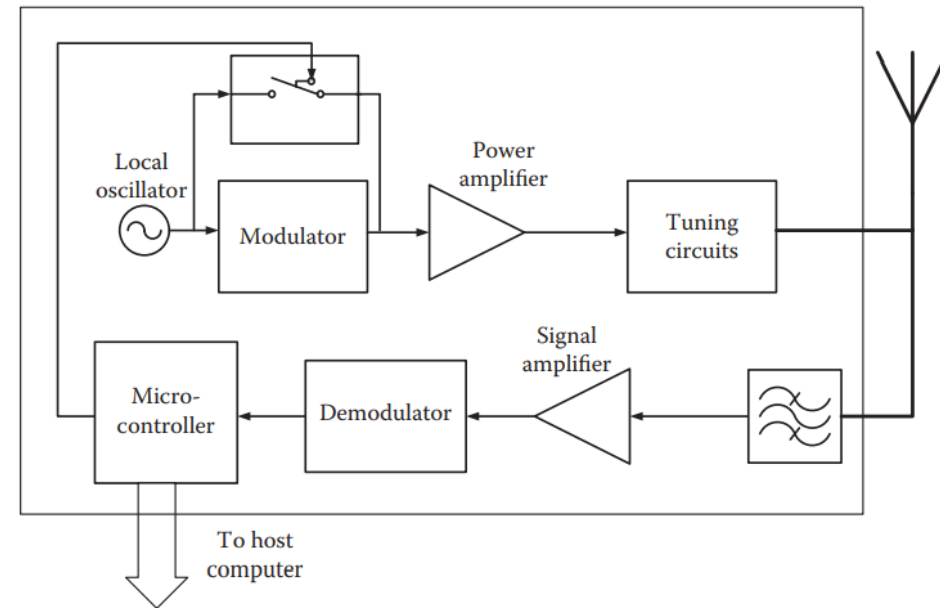
- The memory is divided into **data memory** and **configuration memory**.
- **Data memory** stores the **information** that will be transmitted back to the interrogator.
- Configuration memory stores data regarding the **configuration parameters** for the transponder.
- Memory varies in size, rewriting capabilities, and structure.
- The size of the memory ranges from 1 bit to 64 kbits or even larger.

## Transponder Programming

- Done by the manufacturer at the time of production or by the end user.
- Programming the transponders means to **store a unique identification number** in its memory, as well as to set up the configuration parameters for the communication between the transponder and the interrogator and additional parameters such as password protection.
  - Initial, power-up RF signal (125 kHz for the MCRF200/250 family) lasting between 80  $\mu$ s and 180  $\mu$ s.
  - Absence of RF field lasting between 50  $\mu$ s and 100  $\mu$ s.
  - A continuous FSK signal that serves as a verify signal, lasting 131 ms. The device is blank at the time of programming, the output data are all 1.
  - The symbol 1 is programmed by sending a low-power RF signal with an amplitude similar to the one used for the initial power-up. The symbol 0 is programmed by sending a high-power RF signal with an amplitude approximately equal to 2.2 times the amplitude used for the symbol 1.

# Interrogators

- Two basic functions: to **generate and transmit the RF signal** used to energize the transponders and to **receive and decode the backscattered signal** generated by the transponders.
- Also handles the bidirectional communication with a host computer to process the information from the transponders and to issue commands to the interrogator.
- If the transponder is able to accept commands from the interrogator, the **RF signal generated by the interrogator has to be further modulated** with the specific code; otherwise, the interrogator will only transmit the RF carrier.
- In either case, the RF signal is then **amplified to specific power levels and passed through the tuning circuits** before reaching the antenna. The antenna is also used to detect the backscatter signal generated by the transponder, which, after being filtered, is then amplified and demodulated if necessary.
- The **resulting signal is then sent to a microcontroller** that will transmit it to the host computer using the appropriate communications protocol.



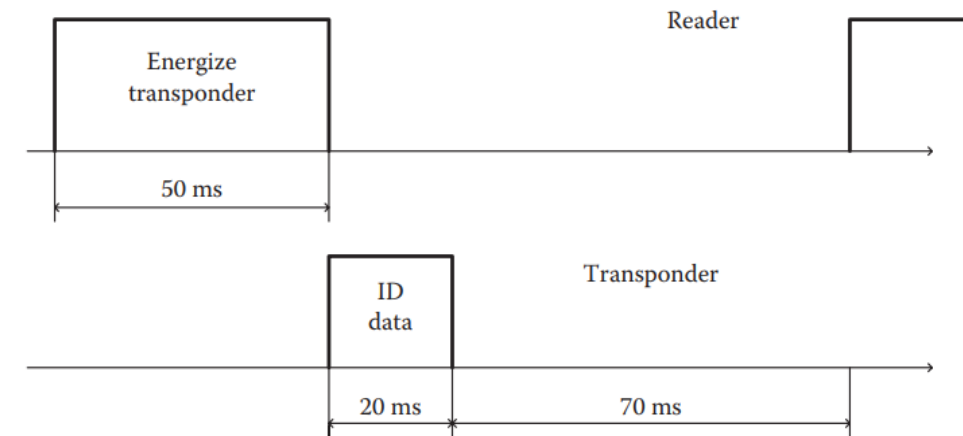
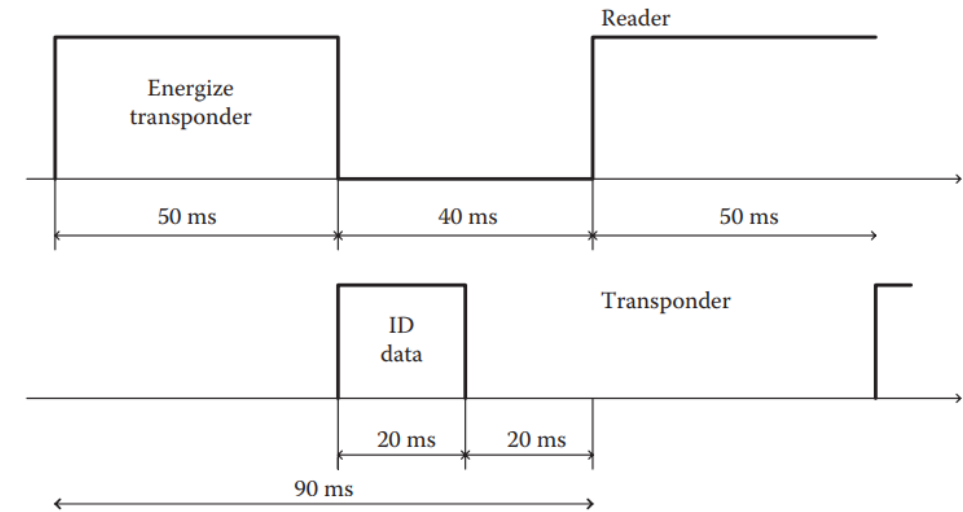
# Interrogators

## Long-Range Considerations

- Increasing the transmitter output power.
- Increasing the transmitter output power.
- Optimizing the sensitivity of the receiver

## Synchronization

- Used to prevent interference between the interrogators in applications that have **multiple interrogators operating in the same area** - by coordinating their transmission and reception windows.
- Synchronization is only required when the different interrogators are **located physically close to each other**.
- The distance between interrogators alone is not sufficient to determine the need for synchronization - electrical path between interrogators is affected by the presence of metallic structures such as buildings, the existence of conveyors, the layout of nearby power or data cables, and even the existence of reinforcing metal bars in concrete floors.
- Maximum distances that require synchronization for interrogators is 18 meters.



# Reference

1. Albert Lozano-Nieto, RFID Design Fundamentals and Applications, CRC Press, 2010.