Data Communication for Smart Factory

Agenda

- Introduction
- The nature of connectivity
- The Principles and Characteristics of Digital Communication Systems
- Modularization of digital communication: the ISO OSI model
- The logic signal encoding
- Ethernet
- Field buses
- RFId and WSN
- LP WAN
- Conclusions

Introduction

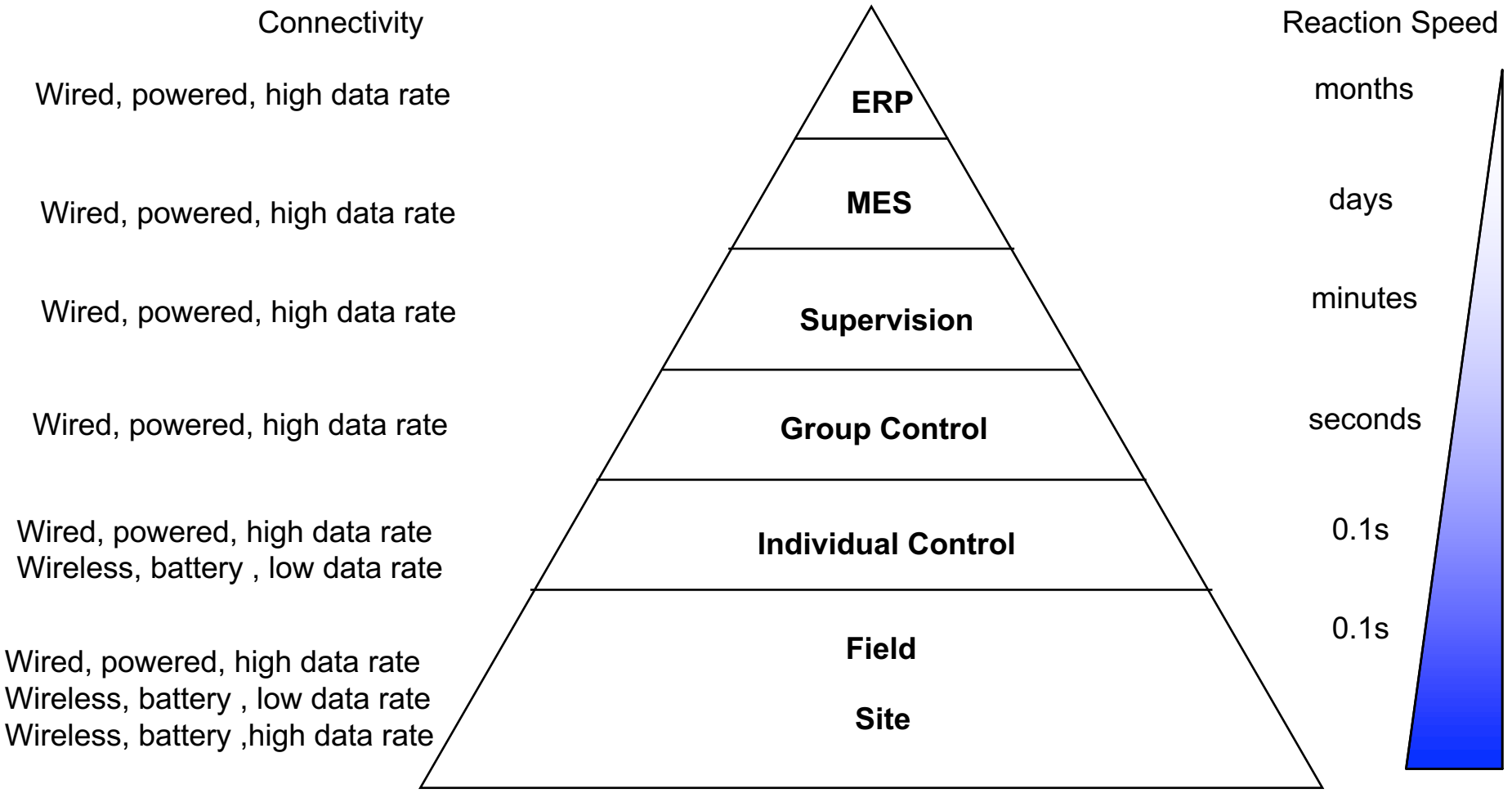
- The different systems, systems, sensors that are part of the Digital Factory must of course communicate with each other in order to physically exchange information
- The first idea that can arise from common sense is the following: no problem we can all connect to the Internet
- But this idea is a bit naïve because the Internet is undoubtedly an extremely powerful and widespread communication system but it is not said to have all the necessary features of a communication that requires an industrial environment: reliability, response times
- On the other hand, if we look at the landscape of industrial communication systems, we can find many different systems between them both for wired, wireless connection and communication rules (protocols ..)
- This lesson will provide a framework of control architectures, communication networks to understand what to use and why.

- Introduction
- The nature of connectivity
- The Principles and Characteristics of Digital Communication Systems
- Modularization of digital communication: the ISO OSI model
- The logic signal encoding
- Ethernet
- Field buses
- RFId and WSN
- LP WAN
- Conclusions

The nature of connectivity

- Connecting devices between them requires understanding the features and constraints of communication and equipment.
- First of all, we can have communications that use physical connections such as wired or wireless (wireless) connections,
- Secondly, it is important to know whether the power supplying the communication systems is virtually unlimited (connected to an electrical network) or limited (batteries).
- Third, it is necessary to know what kind of data and how much it is exchanged: transmitting a movie requires high communication capacity (high data rate) compared to when we send a single low data rate,
- But the response time of the communication system can be completely different: immediate (real time) for transmitting an alarm, distributed over a long time when a new version of an operating system is unloaded
- Last but not least, the geographic dimension of communication is important, or the distance between the objects connected, especially in the case of wireless systems.

Connectivity and CIM level



The types of management communication systems

- We can analyze different existing communication systems according to their characteristics.
- First of all, we can have communication systems that use physical connections such as wired or electromagnetic (wireless) connections with the ability to transfer large amounts of data (high data rates)
- Typically, we have to subdivide them further according to the type of application: management systems or operating systems such as production machines.
- Management systems use wired fixed or wireless telephony networks in the Internet network based on TCP IP protocols.
- These networks do not have geographic or network size limits and allow you to identify connection points with unique IP codes across the network
- The factory connection systems use networks that are called field buses and also allow processes that require quick and repetitive response times

Types of communication systems of sensors or IP nodes

- We can analyze different existing communication systems according to their characteristics.
- First, most of the communication systems with sensors are increasingly wireless.
- Typically, we still have to divide them according to the size of the geographic network.
- When the network is limited we can use Wireless Sensor Network
- But when the network begins to be extended we have to use LP Wan (Low Power Wide Area Network))
- In either case, the optimization of energy use is the critical element of both solutions, as batteries that are eventually rechargeable from the environment are often used
- So the communication apparatus, the protocols must be optimized to minimize energy consumption

The types of communication using load modulation

- Finally, we can use communication systems between an active device and a passive device from an energy point of view
- Typically, communications are between an active RFId reader and a passive RFId tag
- Passive RFId tags are used in industry to identify the objects to which they are associated and have a very low cost of 5-10 cents per euro
- But they are very simple objects that do not have battery but are powered by the reader itself and then communicate in a single mode: load modulation
- Load modulation literally means modulation of the load or better than the impedance seen from the generator that is the reader
- When the passive tag has to respond to the reader it only limits its impedance to the field generated by the reader.
- In this way, the reader can detect the variation of the absorbed current and then detect the associated communication

The differences between different types of communication

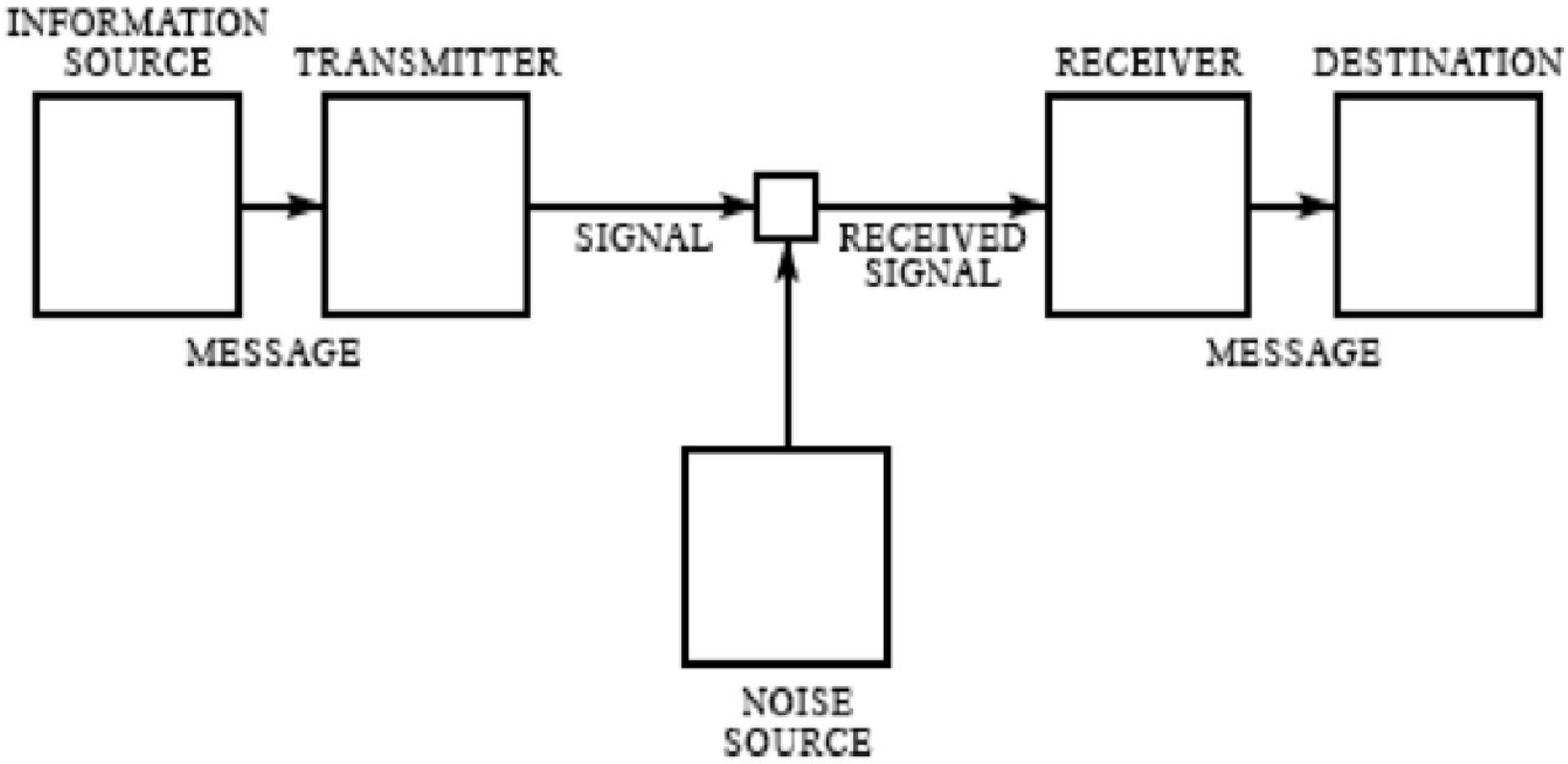
- The communication systems presented are almost always different from each other both from the point of view of the physical interfaces and the logical interfaces.
- Different physical interfaces means that physical communication principles are used that are not compatible each other.
- For example, a wireless connection uses antennas and the electromagnetic field to communicate information
- Instead a wired connection based on electromagnetism, it uses connectors, cables and current or voltage to communicate
- Conversely, a light-based radio connection uses fiber optic connectors, and light to communicate
- For this reason, when we have to connect a communication system to another we have to use suitable converters that adapt the signals and physical quantities.
- If the signals and physical quantities are compatible there may be different communication (protocol) management mode and protocol converters can be used

- Introduction
- The nature of connectivity
- The Principles and Characteristics of Digital Communication Systems
- Modularization of digital communication: the ISO OSI model
- The logic signal encoding
- Ethernet
- Field buses
- RFId and WSN
- LP WAN
- Conclusions

Digital communication networks

- First of all we are dealing with digital communication networks because we transmit digital and non-analogic information.
- Even analogic information like human voice, we prefer to treat them digitally and then convert from analogic to digital, then all transmission and management are digital: only the received digital message is converted from digital to analogue to allow the ear human being to hear
- We prefer digital communication instead of analogic because it is more noise immune
- Digital communication does not eliminate biases, but it can reduce and / or eliminate its effects or lack of information or distorted information

Digital communication networks: the Shannon model



Digital communication networks

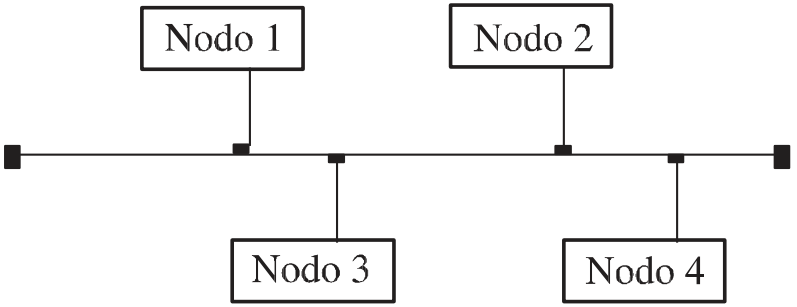
- Digital communication networks can be modeled by components and architectures
- For this reason we must begin to define the components of digital networks and network architectures
- Fortunately, communication systems can be defined within a universally accepted standard architecture: the 7 lvels of ISO / OSI model
- All networks can be represented on the basis of this fundamental model that allows modularizing the hardware and software elements of communication

What is a Computer Network?

- A network of computers is a computer system consisting of one or more computers connected by a communication system.
- We can define various topologies (ie physical components of the components) of the network, among which the most important are three (wired or wireless) :

- Point to point

- Multidrop



- Daisy Chain

The Protocol allows the communication

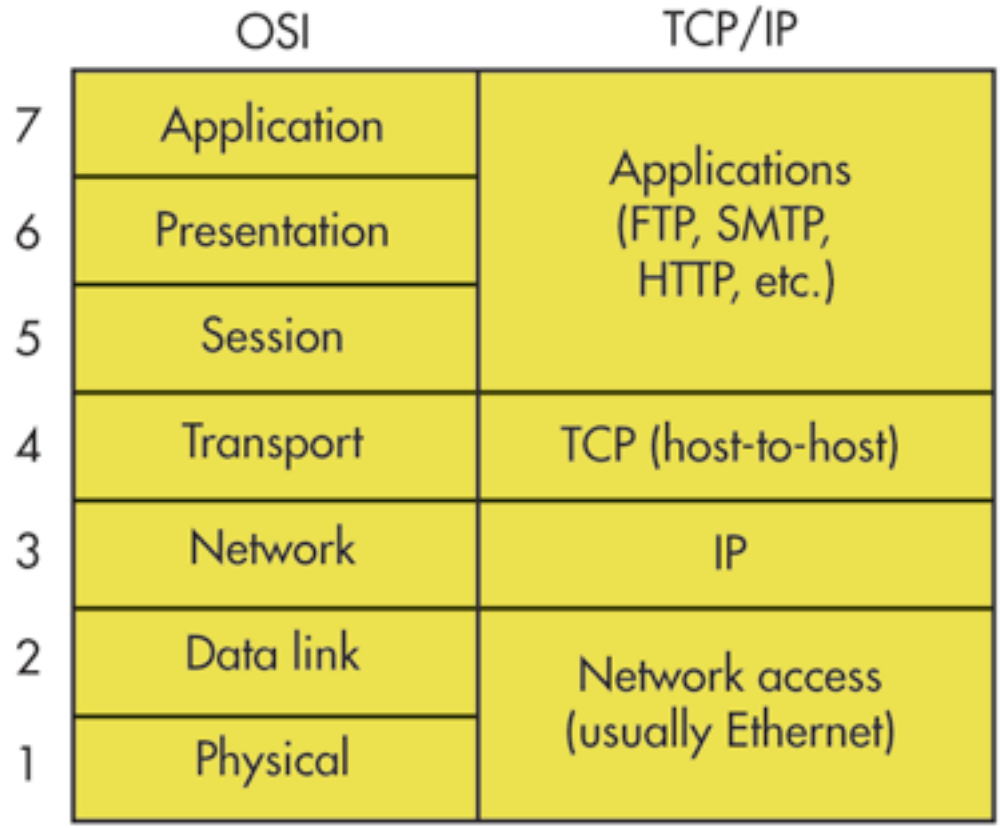
- The communication protocol is the set of rules that two or more network nodes must follow in order to communicate with each other and understand what is communicated.
- But communication is made of different features like physical communication (tension ...), he definition of the way to communicate, the content of communication
- For this reason, protocols used by computers are organized according to a hierarchy.
- Each protocol relies on the lowest-level protocols to provide the service (for example, an error correction protocol can be built on a transport protocol)
- Obviously, it is not necessary for all levels of communication to be present to ensure communication

- Introduction
- The nature of connectivity
- The Principles and Characteristics of Digital Communication Systems
- Modularization of digital communication: the ISO OSI model
- The logic signal encoding
- Ethernet
- Field buses
- RFId and WSN
- LP WAN
- Conclusions

The ISO / OSI Model allows to modularize communication

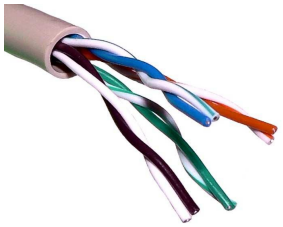
OSI Model			
Layer		Protocol data unit (PDU)	Function[3]
Host layers	7. Application	Data	High-level APIs, including resource sharing, remote file access
	6. Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
	5. Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4. Transport	Segment (TCP) / Datagram (UDP)	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Media layers	3. Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2. Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
	1. Physical	Bit	Transmission and reception of raw bit streams over a physical medium

ISO/OSI and Internet

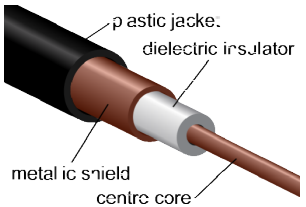


Transmission media can physically be very different

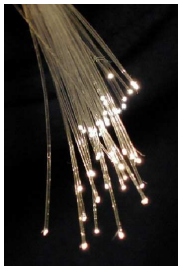
- **Twisted pair**
  - Made up of a pair of copper wires wrapped in a sheath and twisted
  - It can be with or without shield
  - Typically used in telephony, it allows medium to high-speed communication (100 Mbps on local area network, less on telephone network) with ADSL



- **Coax**
  - Copper header covered with copper shield that allows for good immunity to the disturbances
  - Allows medium to high speeds (100 Mbps)



- **Optical Fiber**
  - Glass fiber capable of carrying light signals
  - It gives minimum noise effect it has a high cost



- **Wireless**
  - Extremely flexible
  - Potentially critical energy management

Why should we choose a specific transmission medium?

Because the data communication systems can be very different depending on the needs and the environmental characteristics

- Quantity of data to be transmitted
  - The opening state of an electrical cabinet door
  - Images of a product
- The level of noise
  - Electric Foundry
  - Warehouse for metal shelves
- The level of security required
  - Electric Grid
  - Quality circle blog
- Connection costs
  - Sensors distributed in a large area
  - Production lines

Examples of communication systems

- Smart phone and tablet
- Field Bus
- Wireless sensor network
- Tag RFId
- Real Time Localization Systems (LTLS)
- Global Positioning Systems (GPS)

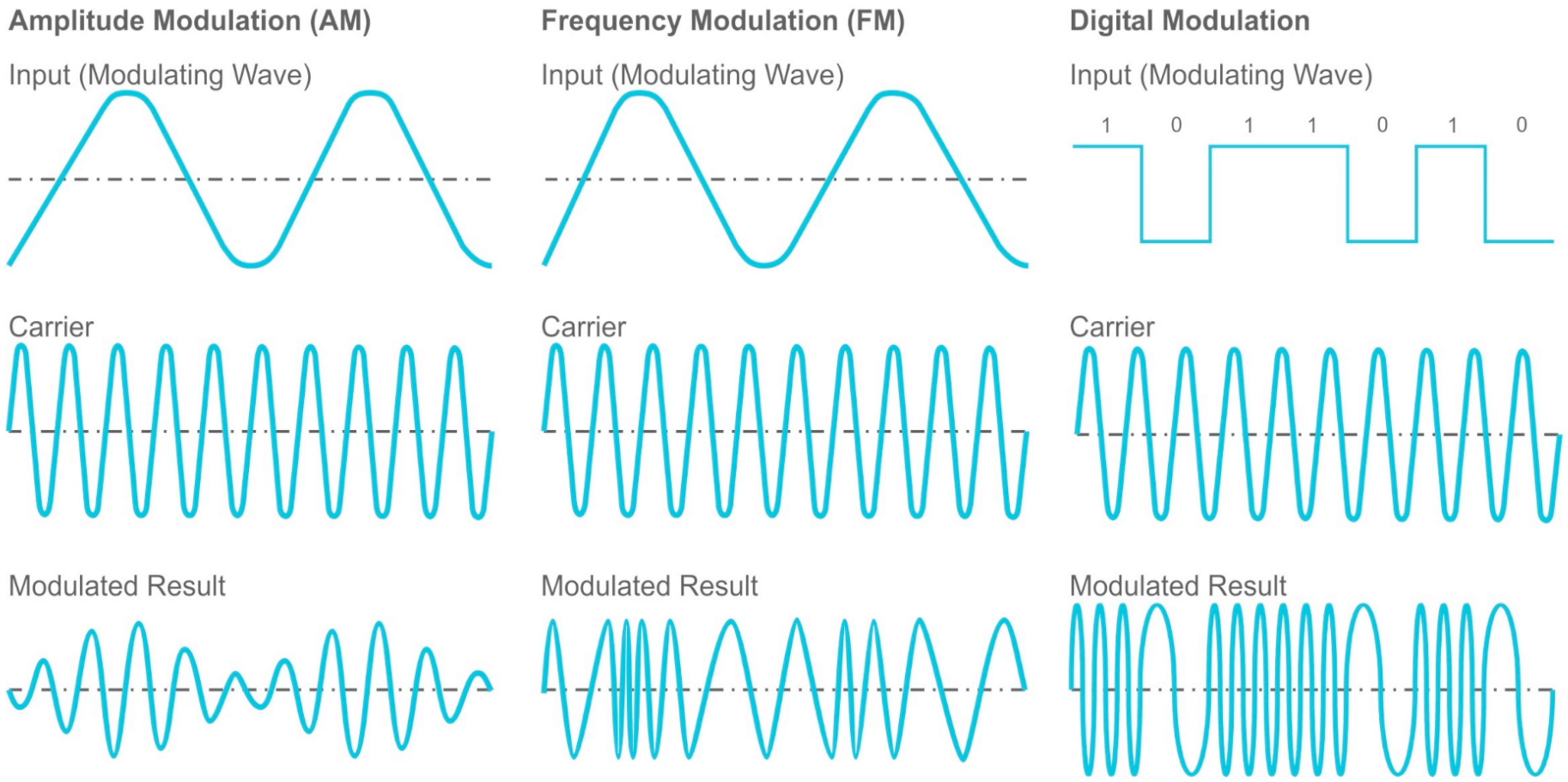
- Introduction
- The nature of connectivity
- The Principles and Characteristics of Digital Communication Systems
- Modularization of digital communication: the ISO OSI model
- The logic signal encoding
- Ethernet
- Field buses
- RFId and WSN
- LP WAN
- Conclusions

Logic Signal coding

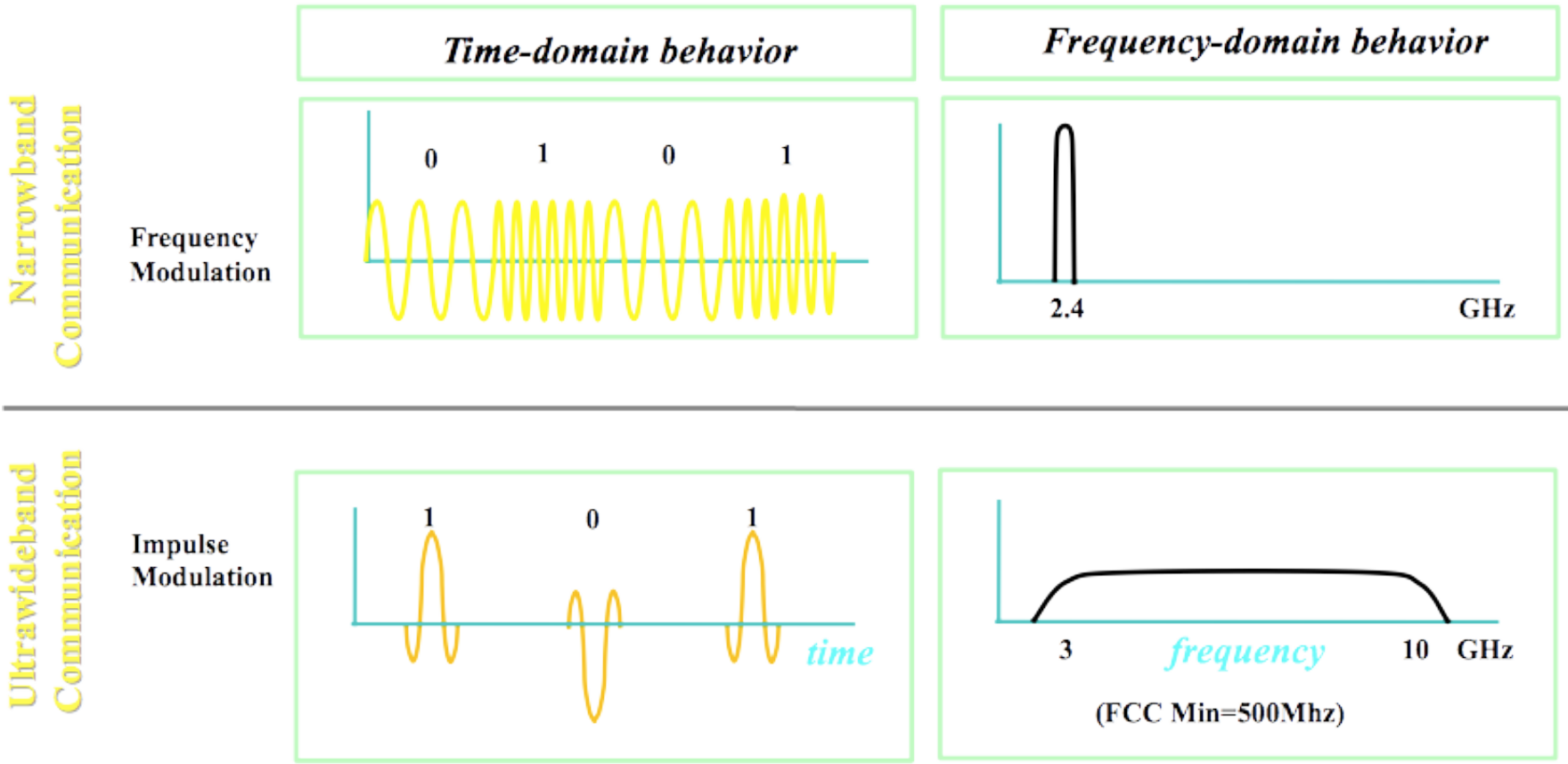
Binary data exchanged between two computers can be transmitted directly in three modes

- Modulation of the carrier in frequency or amplitude (both sender and receiver both active), frequencies up to 2.4 GH and analogic transmission
- Ultra wide band (sender and receiver both active), frequencies beyond 4GH and digital broadcasting
- RFId (the tag is passive and the reader is active), UHF frequencies and load modulation or backscattering)

Carrier Modulation



What is UltraWideBand?



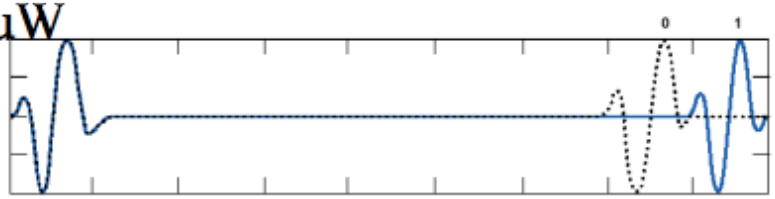
- Communication that occupies more than 500 MHz of spectrum
- Communication with fractional bandwidth of more than 0.2
- More possibilities than pulses

Basic Impulse Information Modulation

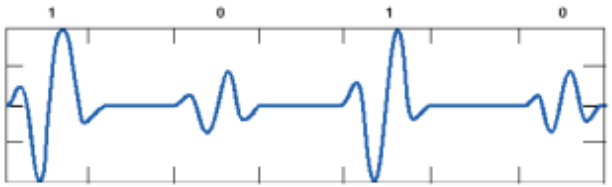
Pulse length ~ 200ps; Energy concentrated in 2-6GHz band;

Voltage swing ~100mV; Power ~ 10uW

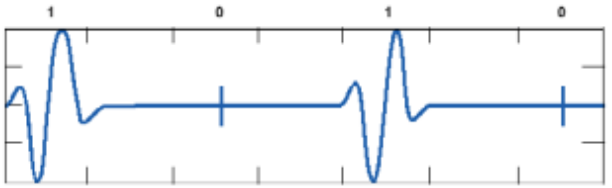
- **Pulse Position Modulation (PPM)**



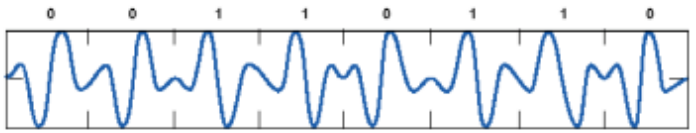
- **Pulse Amplitude Modulation (PAM)**



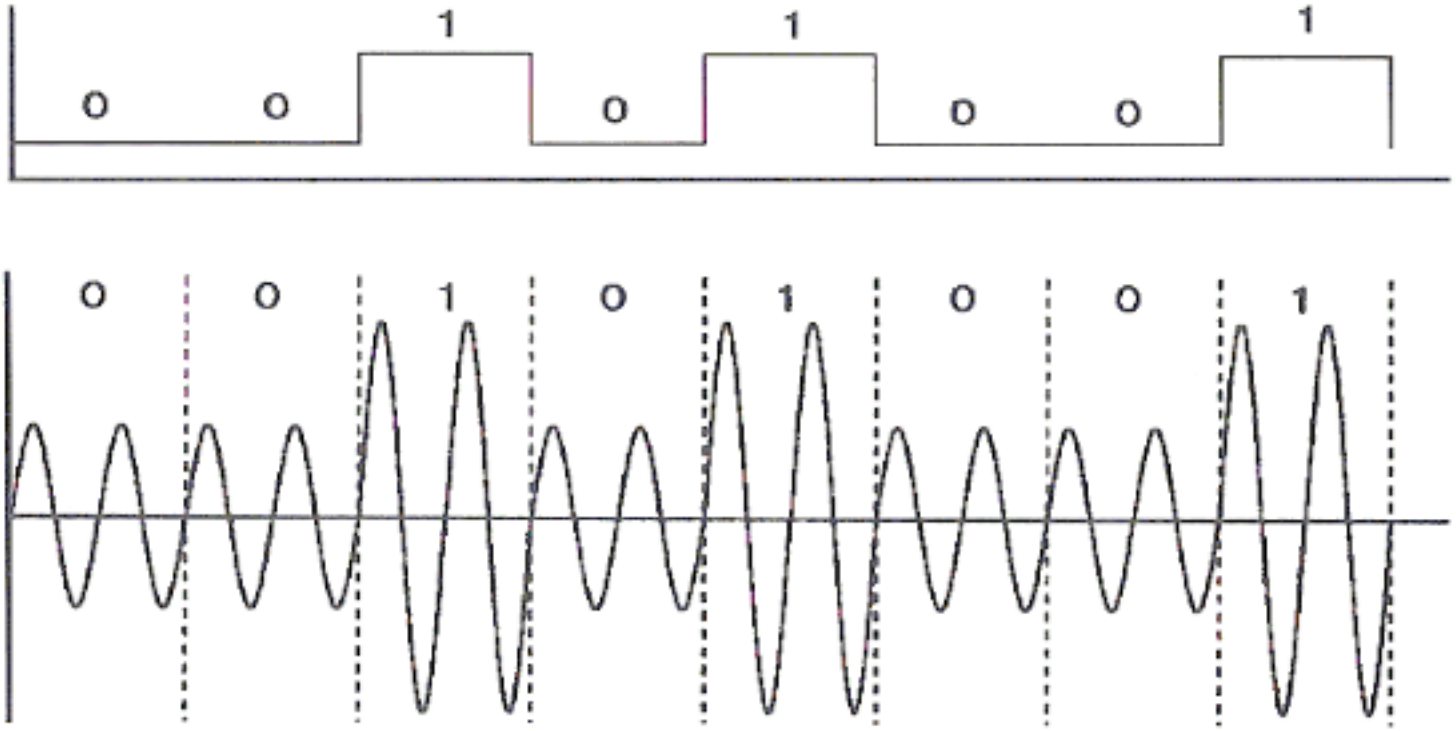
- **On-Off Keying (OOK)**



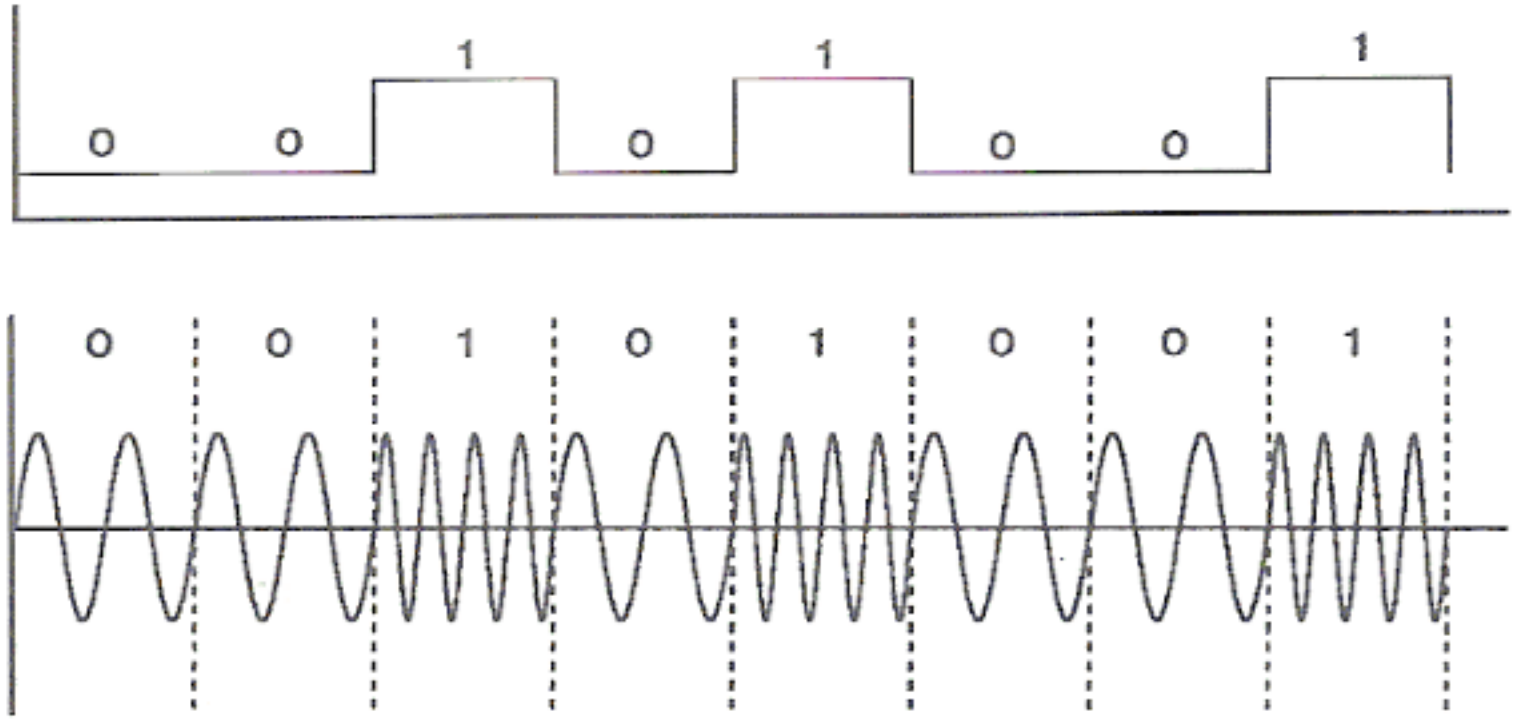
- **Bi-Phase Modulation (BPSK)**



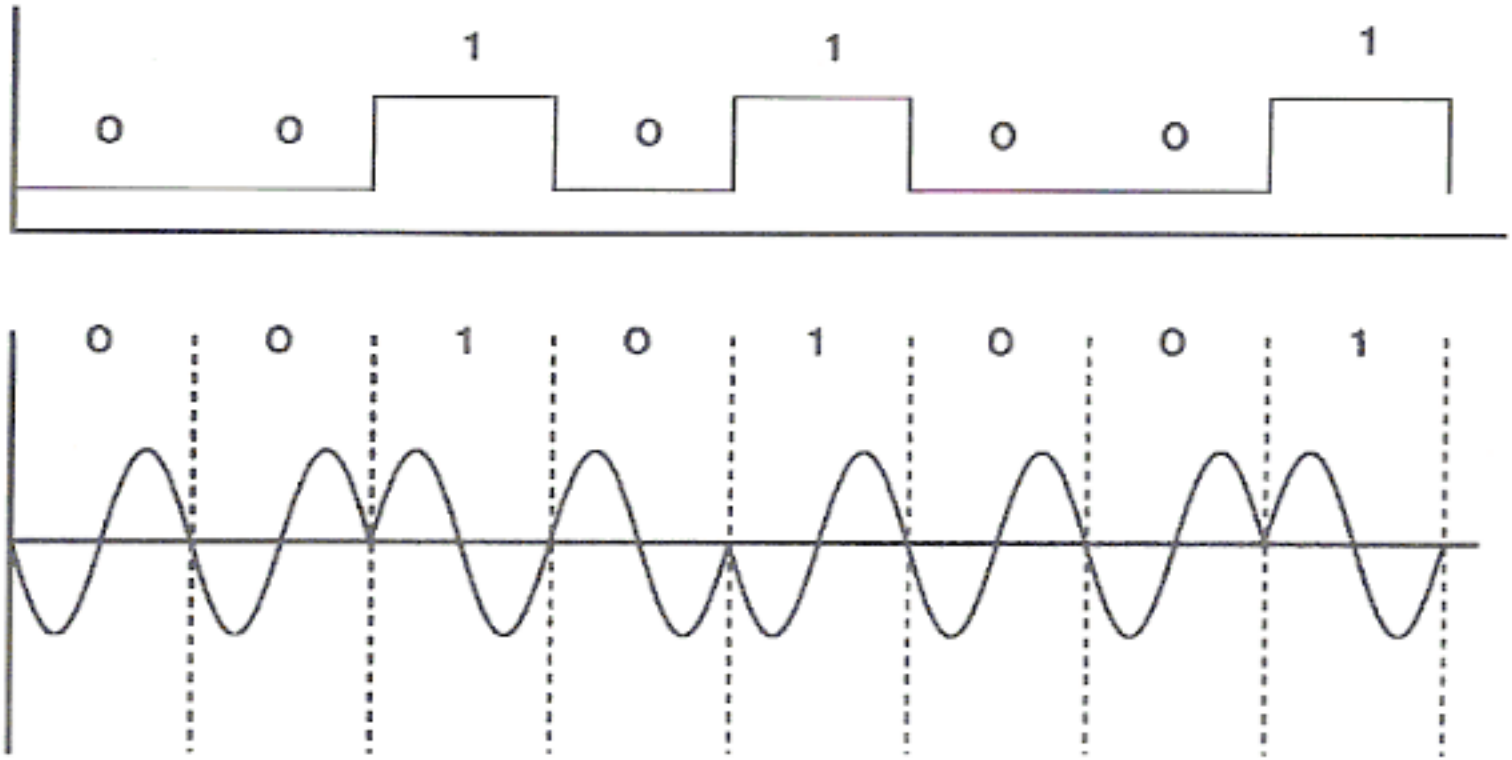
Signal Coding using amplitude modulation



Signal Coding using frequency modulation



Signal Coding using phase modulation



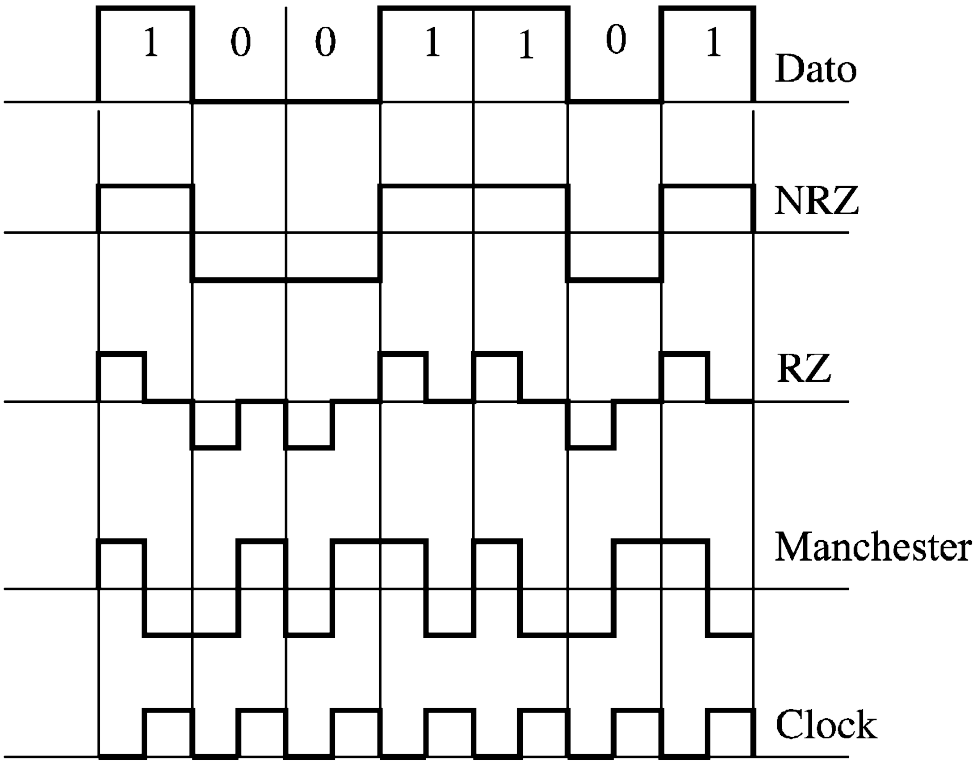
Logic signal coding is more insensitive to noise

Binary data exchanged between two computers can be transmitted directly to the channel (baseband communication)

- Coding Non Return to Zero: Does not force the transition to a reference level (zero)

  Return to Zero coding: requires the transition to zero

  Coding Manchester: codes values with transitions signs (in practice, it transmits the clock or inverted clock)



In particular, Manchester coding

- Manchester coding provides a simple way to code arbitrary binary sequences without ever having long periods of time without clock transitions

- This allows you to prevent loss of clock synchronization or bit errors caused by low frequency drifts on unequal analog connections.

- Transmitted as AC signal ensures that the DC component of the coded signal is zero, preventing repeat signal base levels, and making it easy to regenerate.

- One of the best known uses of the Manchester coding is in local Ethernet networks

Electrical and Mechanical Standards

Some standards:

- EIA RS-232C
  - one of the oldest standards, but still in use
  - maximum distance: 15 m, maximum speed: 20 kbit / s
  - uses 3 wires: GND (common return), TXD (transmission), RXD (reception)
- EIA RS-422
  - maximum speed: 115 kbit / s for distances up to 1200 m, 10 Mbit / s up to 12 m
  - uses differential instead of single-ended connections more suitable for industrial use
  - Up to 10 receivers can be connected
- EIA RS-485
  - much used in the industrial field
  - speeds and distances such as RS-422
  - Up to 32 transmitters and 32 receivers can be connected
  - the transmitters may be in the high impedance state (and disconnect)

Transmission Direction

The transmission can take place with the following direction modes:

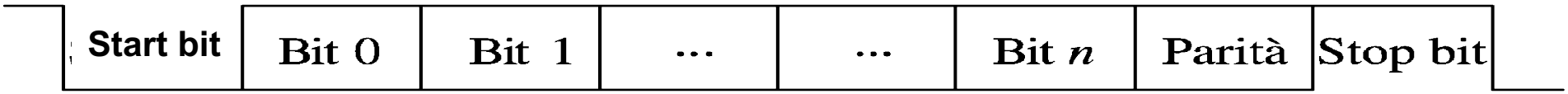
- Simplex (the drive's sense is unique)
- Half duplex (transmission is possible, alternatively, in both directions)
- Full duplex (transmission is possible simultaneously in both directions)

Almost all current equipment is, physically, ready for full duplex transmission.

However, protocols may limit the transmission to half duplex mode.

Asynchronous transmission

- In the asynchronous transmission, the transmitter takes the initiative to send the data
- Transmission is by character (5 to 8 bits of information)
- The format of the broadcast is as follows:



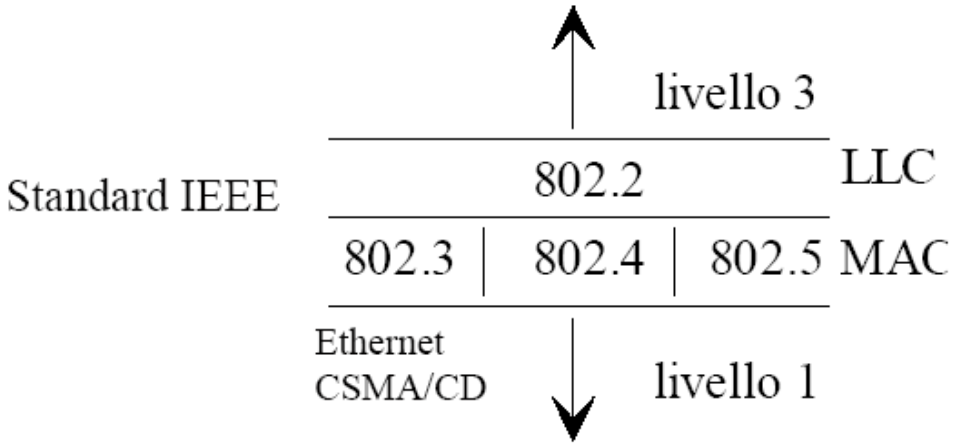
Synchronous transmission

- In synchronous transmission, transmitter and receiver synchronization (via clock or Manchester signal)
- The information is transmitted as a preceding data block and followed by synchronization and control bit sequences.
- The set is called frame:

- The transmission efficiency is higher than the asynchronous transmission
- Synchronous line management is, however, more burdensome
- The Universal Synchronous Asynchronous Receiver Transmitters (USARTs) manage the transmission / reception modes (both synchronous and asynchronous), downloading the computer from these tasks

Data link

- It works to make error-free connections between network pairs of nodes.
- It divides the data it receives from the network layer and organizes them into frames, introducing control information, such as sender and recipient address, and additional bits.
- Transmits the frames and verifies the correct reception on the basis of the acknowledge signals of the recipient, repeating, if necessary, the transmission.



- LLC Logical Link Control
- MAC Medium Access Control

Stochastic control of access to the physical medium

The following alternative standards have been defined for the MAC:

- CSMA/CD (IEEE 802.3)
- Token-Bus (IEEE 802.4)
- Token-Ring (IEEE 802.5)

CSMA/CD (Carrier Sensing Multiple Access / Collision Detection)

- Spontaneous Protocol: Each node may decide to transmit at any time. Contemporary transmissions are operated by a collision detection mechanism that provides a logic of "retentive".

- It is not able to guarantee a certain upper bound on the response delay: it is therefore not considered suitable for applications where this needs to be guaranteed (eg real-time applications)

- It is used in Ethernet (whose speed is very high, so the problem is not critical)

Deterministic control of access to the physical means

Token-Bus / Token-Ring

- At any moment, it has the right to transmit only one node, the one that owns the token (that is, a particular code).
- The nodes pass in the "round" sequence (round-robin) the token
- The token entitles you to transmit for a set maximum time (THT: Token Holding Time), after which it is left.
- There may be active (master) and passive (slave) stations: slaves can transmit only if they are interrogated by a master.
- The response delay of each unit has a higher limit (worst-case)
- There is, however, a useless wait time

Access by arbitrator

- In field networks, physical allocation is often accomplished by means of a master bus.
- It is a device connected to the bus with the function of deciding its allocation between the different nodes of the network.

- Introduction
- The nature of connectivity
- The Principles and Characteristics of Digital Communication Systems
- Modularization of digital communication: the ISO OSI model
- The logic signal encoding
- Ethernet
- Field buses
- RFId and WSN
- LP WAN
- Conclusions

Ethernet

- Developed by Xerox in 1976, it is the most used protocol for office applications and is also widely used for industrial applications.
- Ethernet protocol covers layers 1 and 2 of the OSI stack
- The physical medium has undergone various evolutions:
  - thick coaxial cable (Thick Ethernet): 10 Mbit / s up to 500 m
  - thin coaxial cable (Thin Ethernet): 10 Mbit / s up to 200 m
  - Twisted Pair Ethernet, for hub networks: 10 Mbit / s up to 100 m or 500 m
  - twisted pair (Fast Ethernet), for nets with concentrator (hubs): 100 Mbit / s up to 100 m
  - optical fiber: 10 Mbit / s up to 2 km
  - Gigabit Ethernet: 1Gbit / s
- The signaling is in base band with Manchester encoding
- The link topology varies (linear bus, star with hub, ...)

Ethernet: link level

- Sublevel MAC: protocol CSMA/CD
- Sublevel LLC: frame Ethernet II (802.2)

Preamble	Receiver Address	Sender Address	Tipo	Data	Frame check CRC
7 byte + SFD SFD = 01010111	6 byte	6 byte	2 byte	46-1500 byte	4 byte

- Preamble (7 bytes): allows synchronization
- SFD (Start Frame Delimiter): sequence 10101011, indicates the beginning of the useful part
- Address fixed in the hardware (interface card) from the manufacturer (if you change the board it changes the address)
- Type: Specifies the protocol encapsulated in the frame
- Data: 46 to 1500 bytes
- Frame check CRC: Verification of transmission correctness

Ethernet: link level

- The address of the Ethernet card is called MAC address
- It consists of 48 bits: the first 24 identify the Organization Unique Identifiers (OUI), the other 24 are assigned by the organization with the unique constraint of unity
- Computers connected to Ethernet can send useful data using high-level protocols (such as the TCP / IP protocol used on the Internet).
- The Ethernet interface ignores packets with addresses other than their own (does not charge the CPU with this test)

- Introduction
- The nature of connectivity
- The Principles and Characteristics of Digital Communication Systems
- Modularization of digital communication: the ISO OSI model
- The logic signal encoding
- Ethernet
- Field buses
- RFId and WSN
- LP WAN
- Conclusions

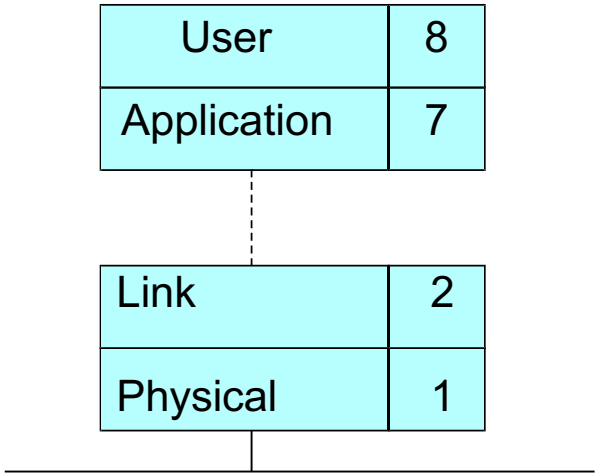
Fieldbus

- A fieldbus is a digital network conceived to connect field devices (sensors, actuators, controllers) to each other and possibly to computers or other network companies by eliminating analogic connections (4 ÷ 20 mA or ± 10 V lines)
- The idea of "fieldbus" is that all components of a control system, from the PC to the operator interface to the sensor or the actuator, are thought to be network devices.
- This way, conceptually, only one "cable" (or bus) runs through the entire system and connects all the devices.
- There are consequently benefits in terms of cost savings in wiring and transmission quality (digital rather than analog)
- In general, field buses allow the optimum transmission of small data volumes, with time criticality.

Fieldbus and OSI Model

Field buses do not achieve all levels of the OSI stack.

- Levels 1 (physical), 2 (connection) and 7 (application) are implemented.
- Levels 3 to 6 are not realized (network, transport, session, presentation).
- Additionally, a layer 8 (user level) is added that provides many important functions, such as functional blocks, device description services, and network management.



Fieldbus and standardization

- For a long time, various manufacturers and component users try to define a standard protocol for device networks (which defines hardware, software, type and format information

- Such a standard would ensure interchangeability and interoperability of field devices of different manufacturers

- However, it has not yet been possible to define this universal standard

- An important standardization initiative is FOUNDATION Fieldbus is a network created to replace analogue lines 4 ÷ 20 mA in the H1 version
  - it has a speed of 31.25 kbit / s
  - is used mainly in the process industry's
  - web: http://www.fieldbus.org

IEC Standards

IEC 61158 (1999):

- Type 1: Foundation Fieldbus H1
- Type 2: ControlNet
- Type 3: PROFIBUS
- Type 4: P-Net
- Type 5: FOUNDATION fieldbus HSE (High Speed Ethernet)
- Type 6: SwiftNet (protocol developed by Boeing, today retired)
- Type 7: WorldFIP
- Type 8: Interbus

The market in process control is dominated by:
FOUNDATION Fieldbus
PROFIBUS PA

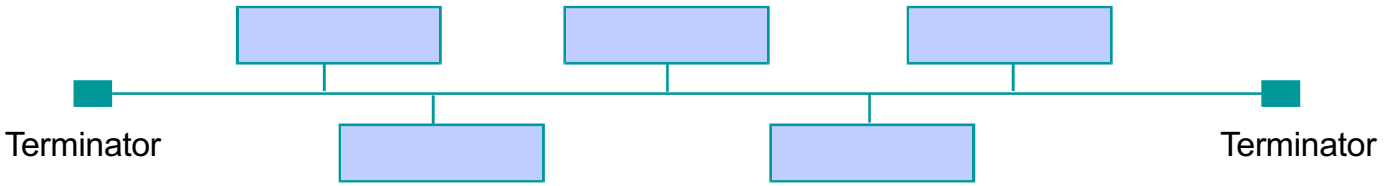
The two technologies use the same physical layer (bifilar links, Manchester encoding, current modulation, 31.25 kbit / s speeds) but are not interchangeable.

Fieldbus for smart factory

- Generally, in field automation, there are the following standards:
- **PROFIBUS DP**
  industrial standard and worldwide supported
- **CAN**
  conceived several years ago, but still of great importance,
  especially in the car industry
- **Industrial Ethernet**
  in rapid evolution and diffusion

PROFIBUS

- PROFIBUS (Process Field Bus) is the most diffused field bus
- Different version but the two most diffused are:
  - PROFIBUS PA (Process Automation), used in process industry
  - PROFIBUS DP (Decentralized Peripherals), used in factory automation
- Bus with terminators
- 32 stations on single link
- Web : http://www.profibus.com



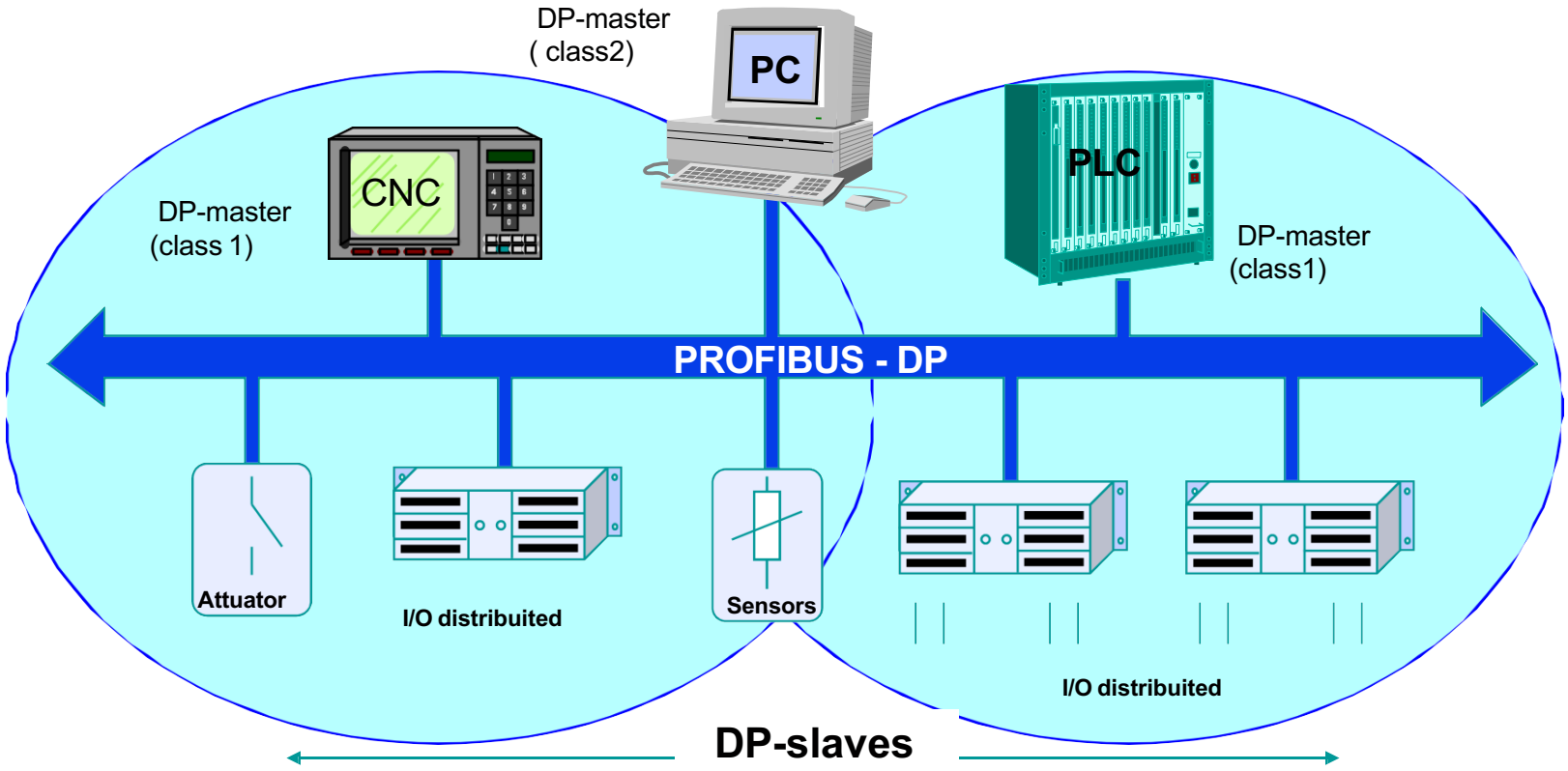
PROFIBUS-DP

- Factory automation standard
- Level OSI 1 e 2 (physical and link)
- Level 1 of OSI stack with two technologies:
  - RS 485 (speeds from 9.6 Kbit/s to 12 Mbit/s)
  - Optical fiber
- Above these levels defines profiles (user level) typical of industrial automation. Profiles are specific defined by end-users or end-users that concern properties, features, and behavior of connected devices.
- Several products: PLC, PC, I/O, Drives, Valves, Encoder,…

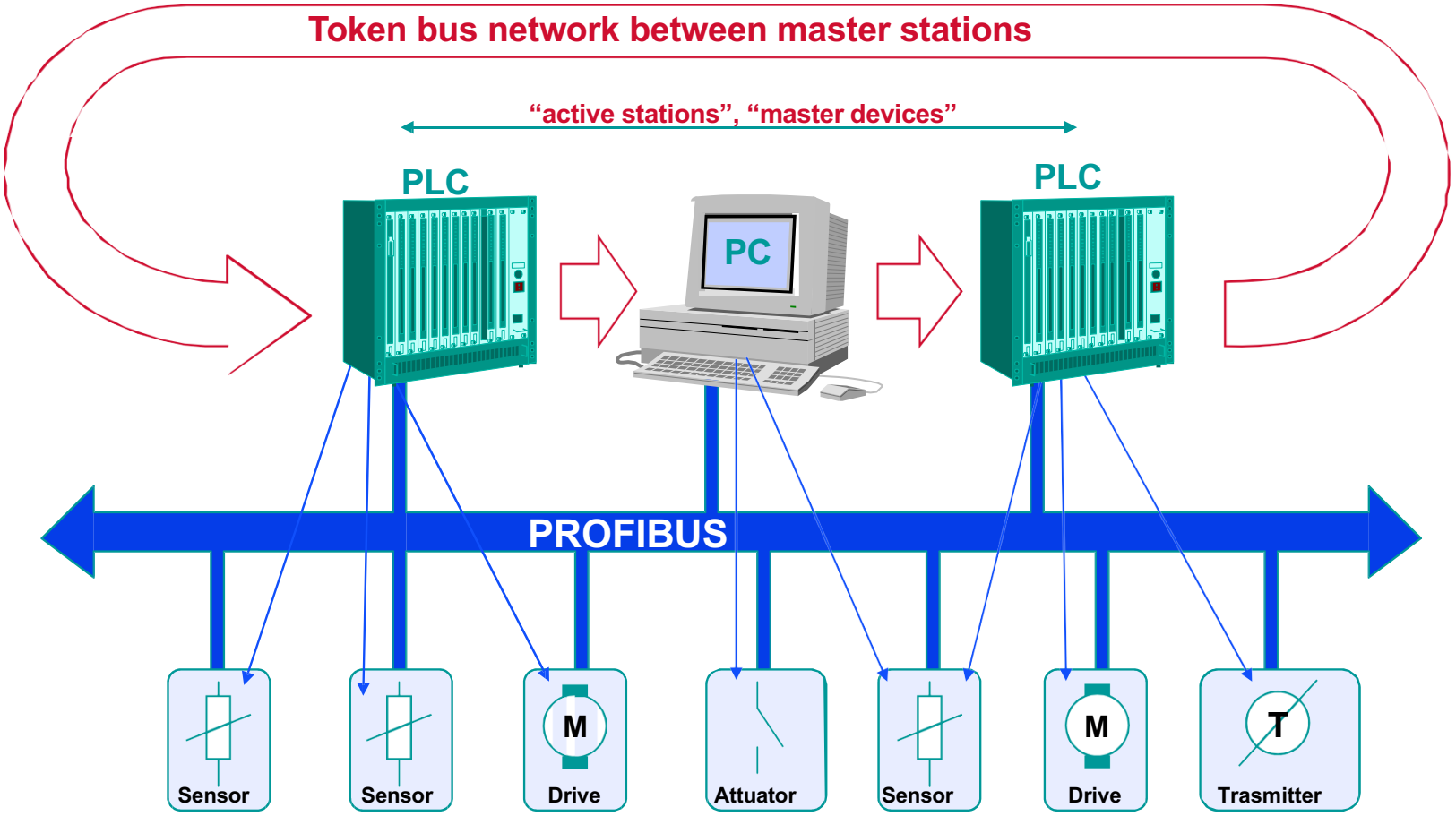
PROFIBUS-DP: multi-master system

Master-slave communication system:

- Master class 1: always connected
- Master class 2: not always connected



PROFIBUS-DP: token management



CAN (Controller Area Network)

- CAN is a serial communication bus, designed for real-time applications and born in a vehicle, although today it is used in different applications.

- The original CAN bus was introduced by Bosch in 1986

- The CAN bus allows communication between controllers, sensors and actuators with speeds up to 1Mbit / sec, and has several strengths:
  - low design and implementation costs
  - operation in critical conditions (eg vehicles, but also industrial ones, such as rooms with strong vibrations and electromagnetic disturbances)
  - ease of configuration and modification (especially its evolutions)
  - automatic error detection and self-diagnosis

- In industrial automation it is mainly used in two versions :
  - CANOPEN (**`http://www.can-cia.org`**)
  - DeviceNet (**`http://www.odva.org`**)

CAN – physical layer

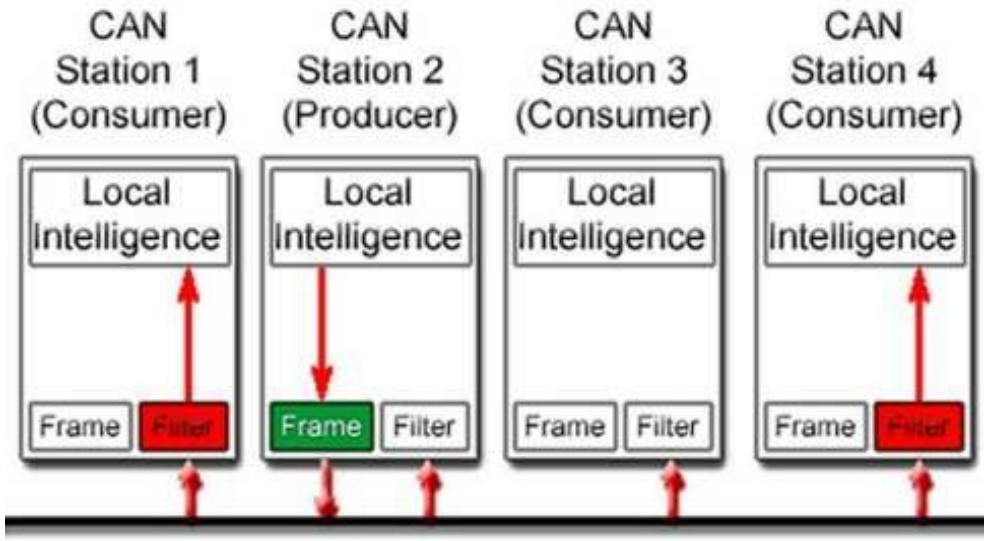
- A differential pair is used whose two conductors are called CAN L (Can Low) and CAN H (Can High).

- There are two possible types of transmission:
  - Low Speed: 125 kb / s, max 40 m, 2 to 20 knots
  - High Speed: 125 kb / s at 1 Mb / s, max 40 m, 2 to 30 knots.

- For error correction, each message is retransmitted until all receivers (and therefore the bus) report any errors.

CAN – link layer

- Communication is always broadcast.
- Packages do not contain addresses but an identifier, which also defines the priority of the message.
- Each node "listens" all the traffic and filters, elaborating, only the messages of its interest.



CAN – bus access

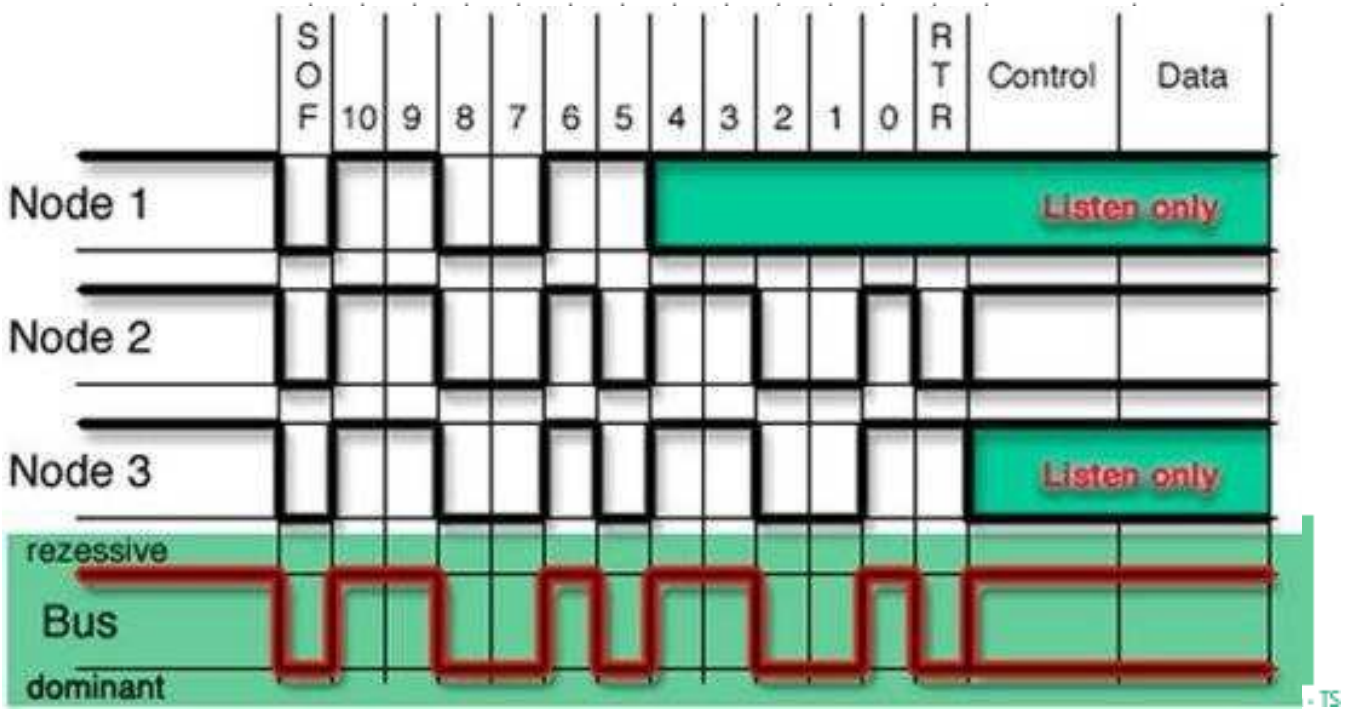
- The approach used by CAN generates conflicts for bus access. These are solved by means of a bit-wise arbitrage system based on the fact that the two possible values of bits placed on the bus from the devices are interpreted as ”dominant" and "recessive".

- When a recessive bit is sent on the bus and some other node puts the dominant bit, the node that issued the recessive bit must retreat. Nodes that do not win arbitrage automatically become receiving stations and do not retry transmissions until the bus is again free.

- This type of arbitrage is called CSMA / CA (Carrier Sens Multiple Access / Collision Avoidance), and is of the type used by Ethernet.

CAN – bus access

Example of access arbitration:



Industrial Ethernet

- An important trend in use is the use of Industrial Ethernet, that is to say, Ethernet in industrial environment (automation and process control).
- The huge spread of Ethernet cards reduces network implementation costs and promotes interoperability
- There are several protocols where Ethernet is suited for use in a field network (which requires real-time performance):
  - EtherCAT (http://www.ethercat.org/)
  - EtherNet/IP (www.odva.org/default.aspx?tabid=67)
  - Powerlink (http://www.ethernet-powerlink.org/)
  - PROFINET (http://www.profibus.com/index.php?id=9)
  - SERCOS III (http://www.sercos.com/)

Integration with information systems

- Control systems are increasingly seen as part of the factory / plant information system (hardware / software).
- The control system in the strict sense must increasingly integrate with plant monitoring production management supply management logistics
- A reference model for representing all the functions of the company, from marketing to production and distribution, is a CER (Computer Integrated Manufacturing)

- Introduction
- The nature of connectivity
- The Principles and Characteristics of Digital Communication Systems
- Modularization of digital communication: the ISO OSI model
- The logic signal encoding
- Ethernet
- Field buses
- RFId and WSN
- LP WAN
- Conclusions

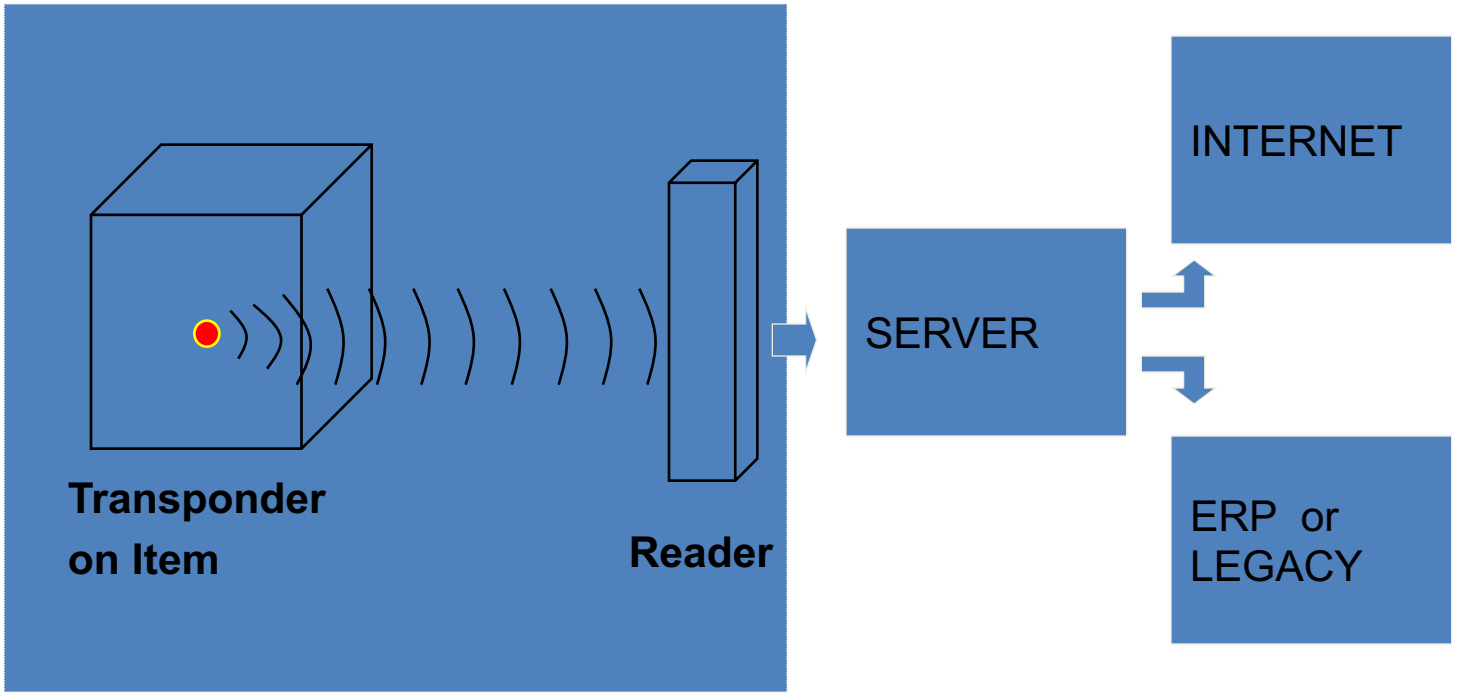
RFId Key words

- Individual Identification
- Automatic Identification
- Passive transponder
- Physical constraints
- Stardardization

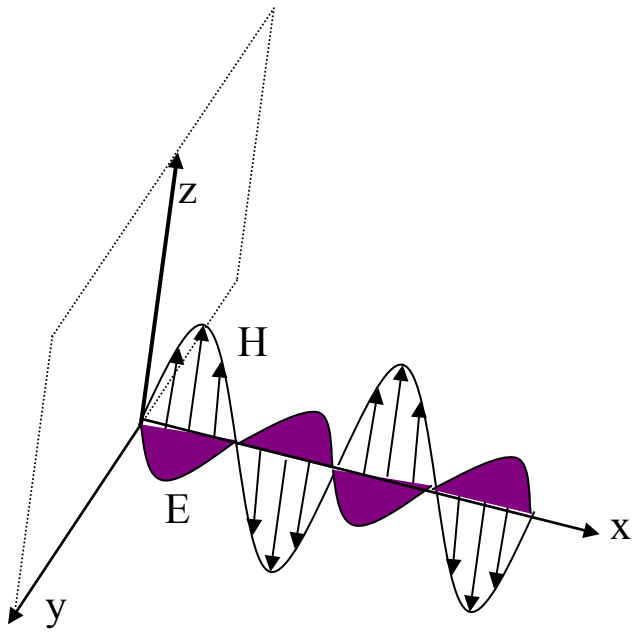
So RFID is not an “electronic bar code” but an intelligent label and …..

- Identify individual items
- Line of sight not required
- Stable in variety of conditions
- Read through most non-metals
- Transponder Cost 5 cents to 50 euro
- RFID readers: 2 euro a 3.000 euro

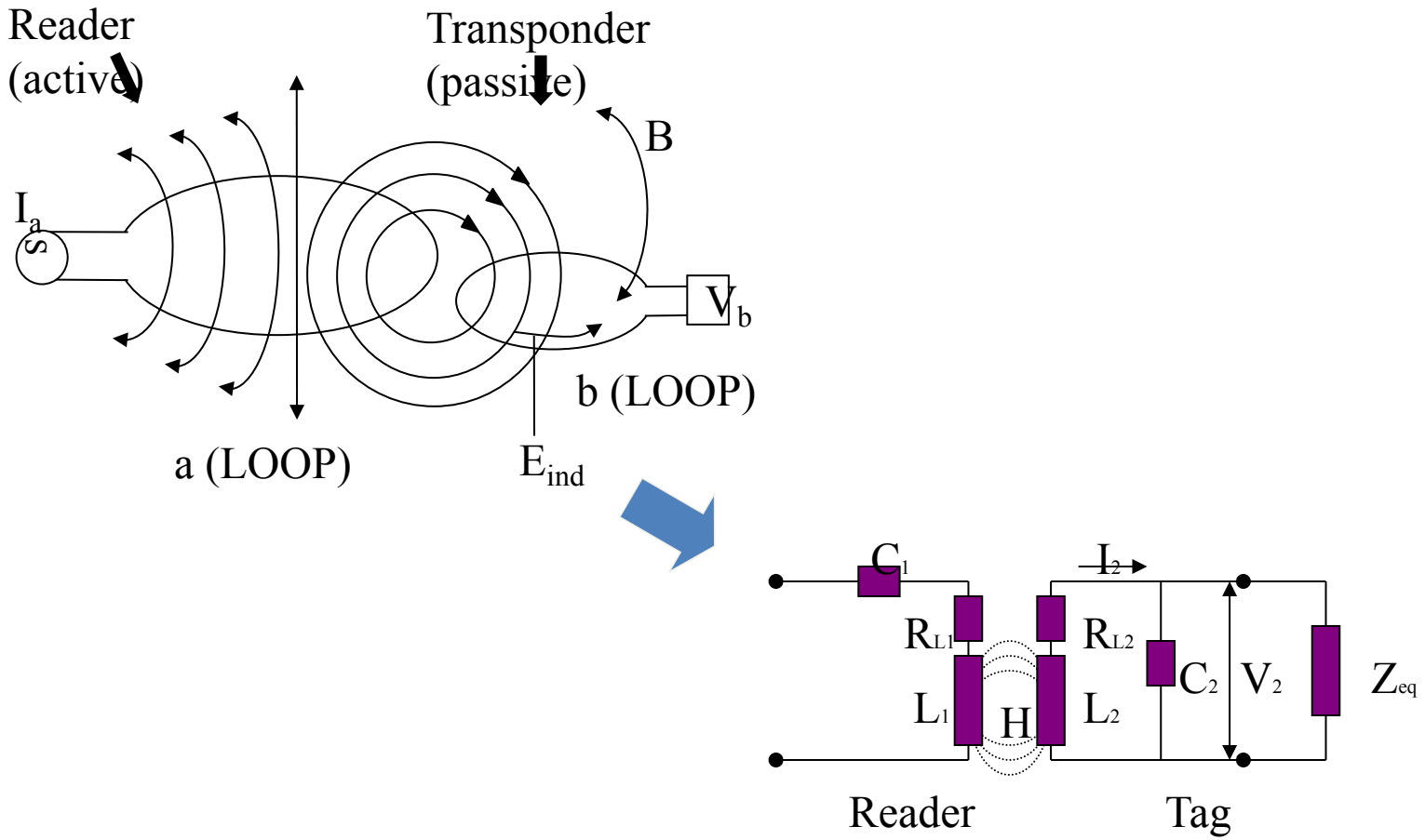
The Structure of RFID System is easy to link to existing Systems



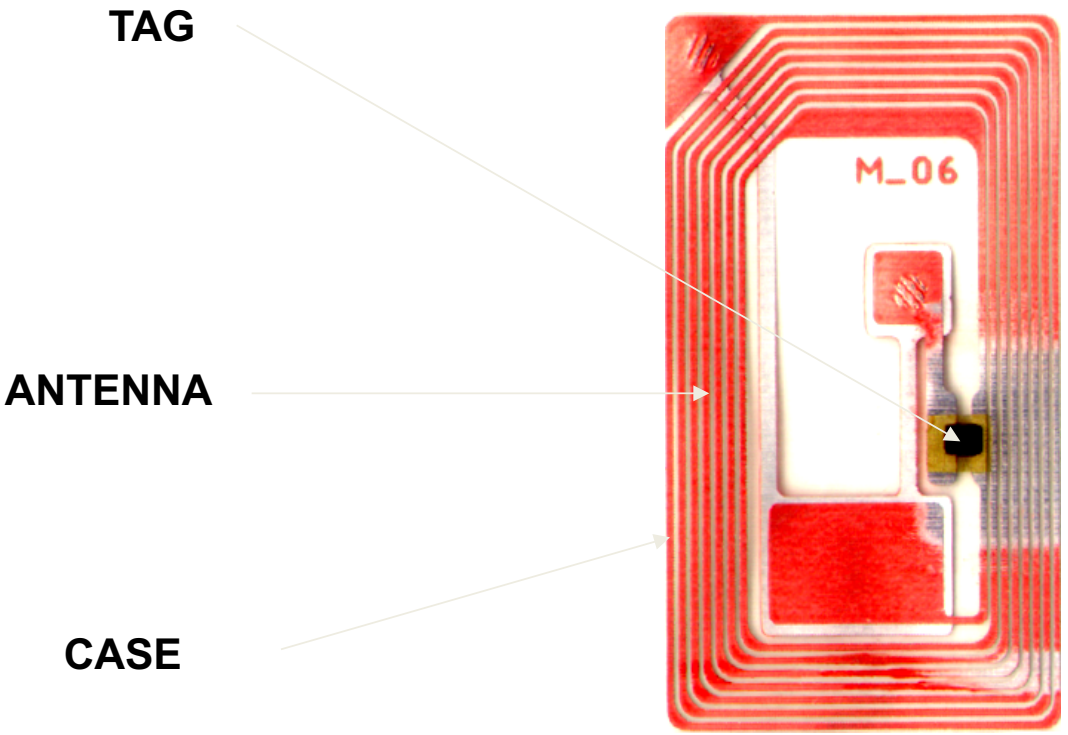
The Electromagnetic fields have two components: E and H



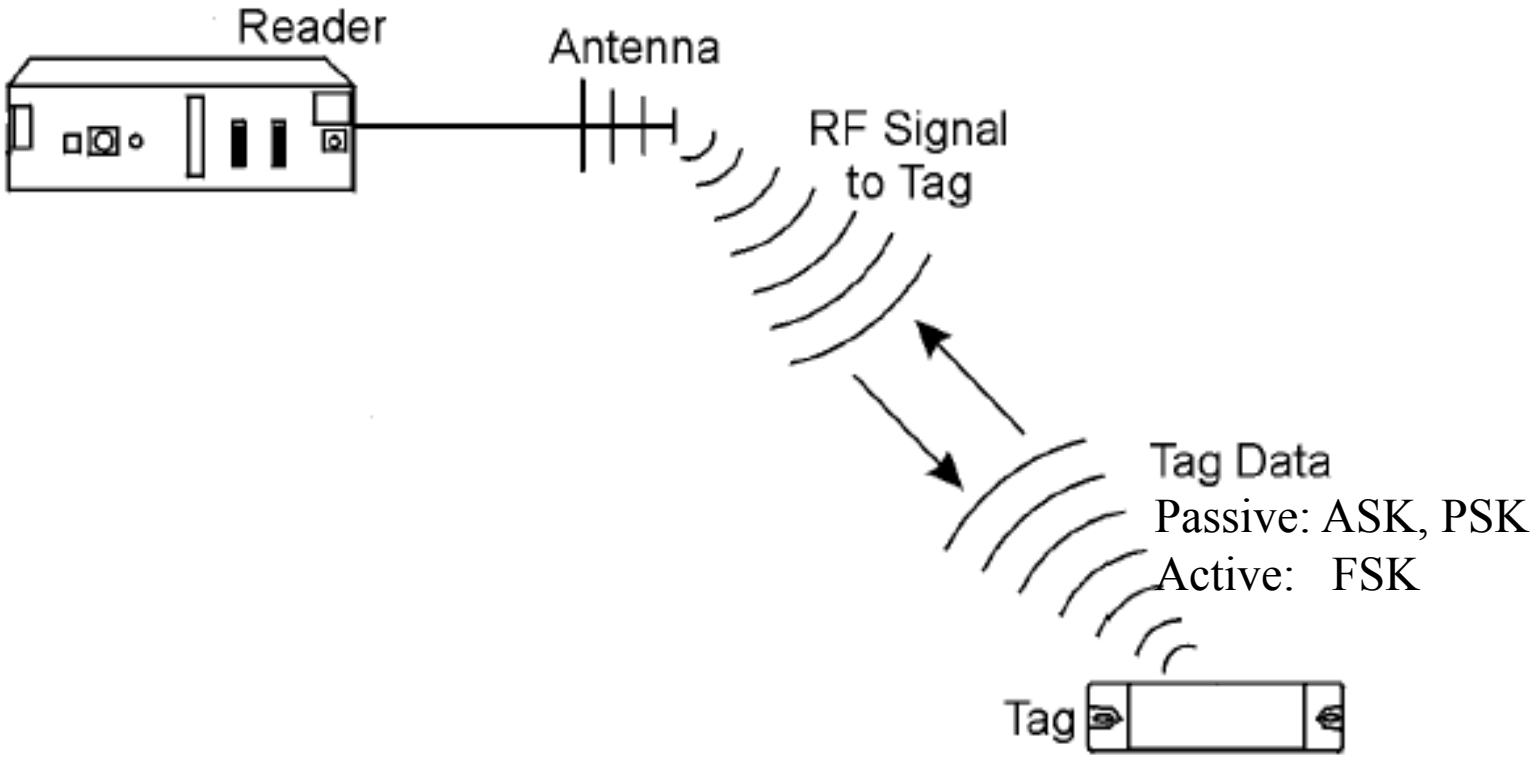
The magnetic alternating field H links reader to transponder as an electric transformer



Magnetic Coupling Passive Transponder with a coil antenna



The electric alternating field E links reader to transponder as a radio system…

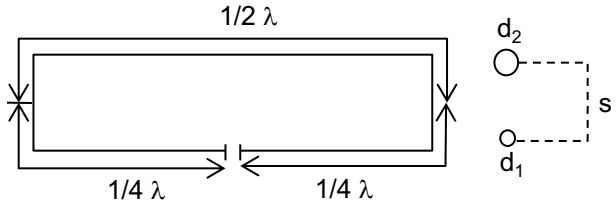


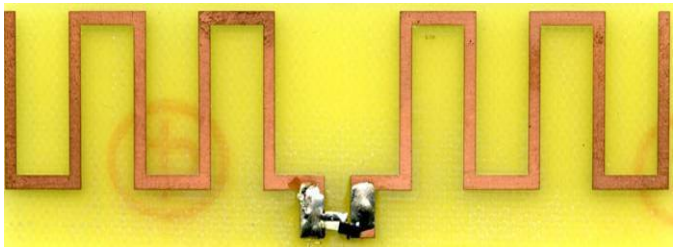
0.5-1.0 m (far field) 4W
Active: 15-20 meters

….with different types of antennas

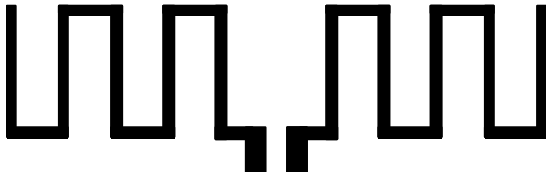
Dipole antenna is the simplest form of radio antenna for transponders

- **Dipole antenna** consists solely of a straight piece of line: e.g. a copper wire
- A simple extended half wave dipole consists of a piece of line of length 0,5λ

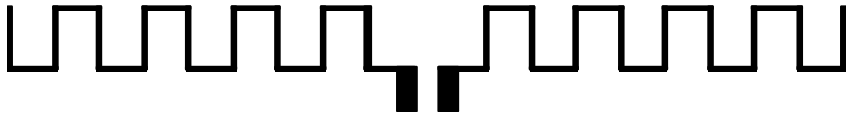




Other Dipole antennas for electric coupling

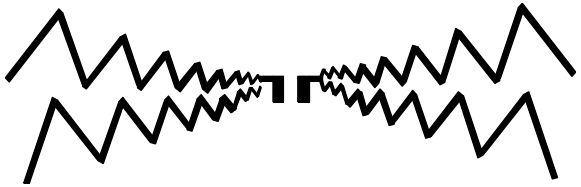


Meander Dipole:SDip1

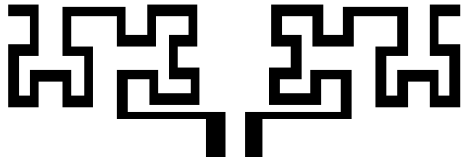


Meander Dipole:SDip5

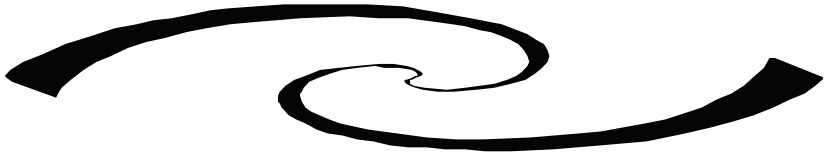
LogPeriodic Dipole:LP1



LogPeriodic Dipole:LP5

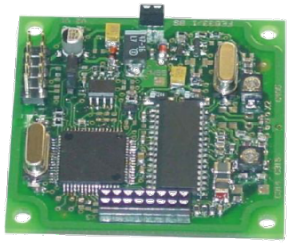


HilbertFractal Dipole:HilbD2



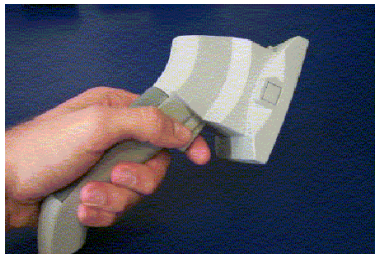
Fermat Dipole:SpirLamb1_9

Different type of readers and antennas*



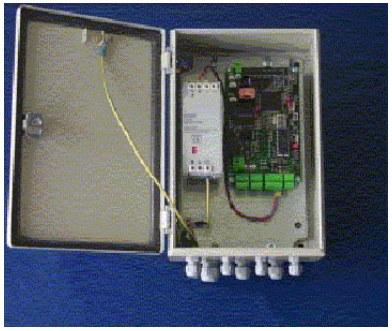
Reader card

Proximity Reader



Portable Reader

Mid Range Reader



Long Range Reader

Mid and Long Range Antennas

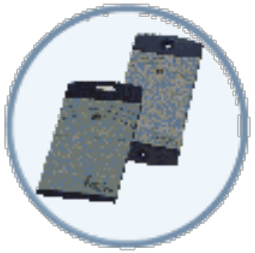
Gates

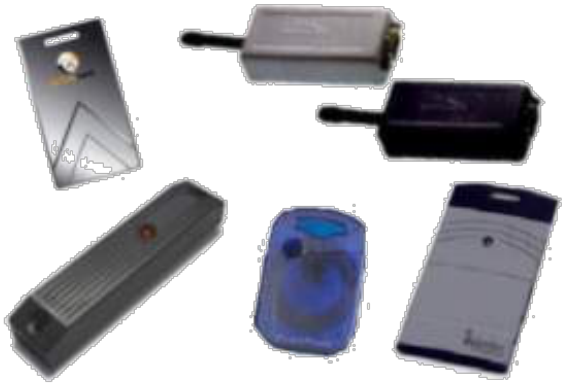
*Source SOFTWORK

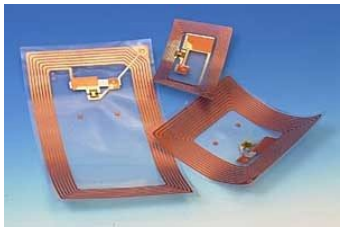
The major Physical Constraints of RFID Systems

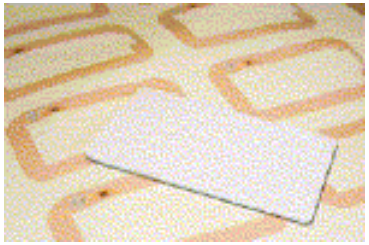
- Circuit Resonance
- Power Supply to transponder
- Data Transfer transponder-reader
- Magnetic materials
- Material absorption
- Water, alcohols etc

Transponder can have different shapes









*Source SOFTWORK

Frequency range and coupling are dependents

- **Close coupling systems**: distance reader transponder **up to 1 cm**
  - Electric and magnetic coupling: usually magnetic
  - Frequency between DC and 30 MHz: usually 125 kHz-13,56 MHz
  - ID-1 format contactless smart card (ISO 10536)

- **Remote coupling systems**: distance reader transponder **up to 1m**
  - magnetic (inductive) coupling
  - Frequency 125 kHz-27,125 MHz
  - Proximity coupling (ISO 14443 contactless smart card)
  - Vicinity coupling (ISO 15693 smart label)

- **Long range systems: distance reader transponder above 1m**
  - Electric fields: UHF and microwave
  - Frequency between 400 MHz to 5,8 GHz

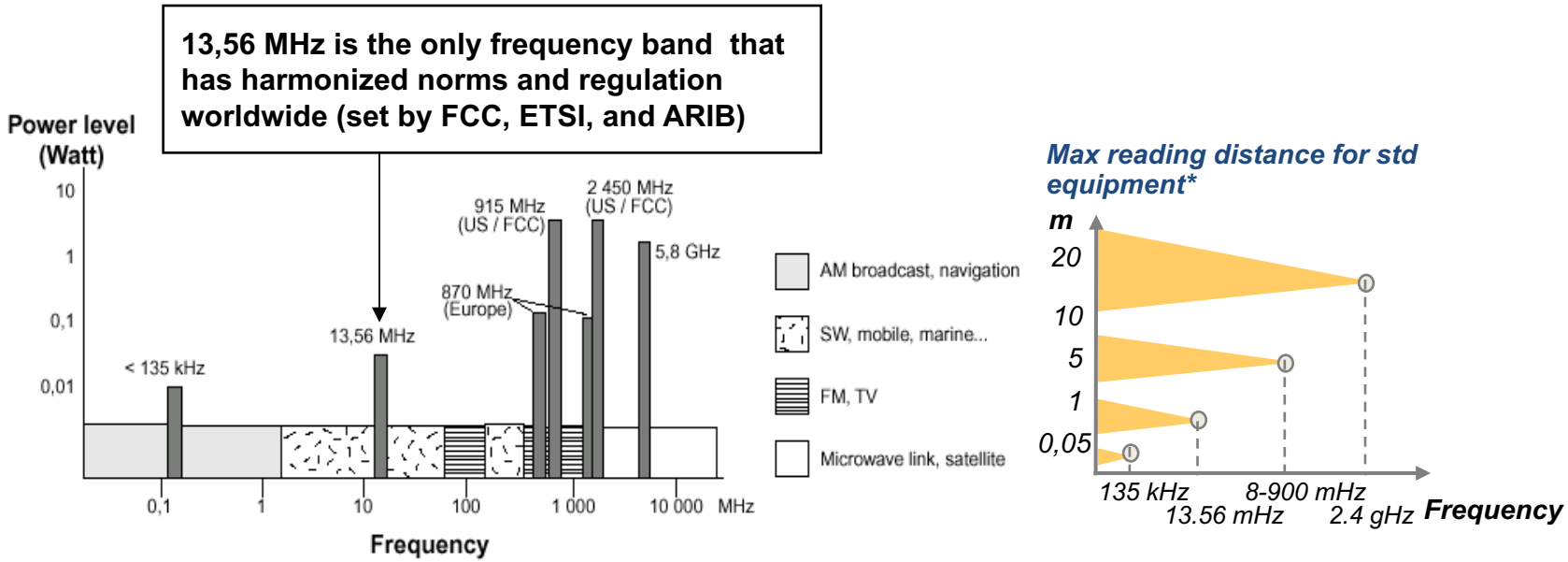
Three Regions of Normalization Worldwide

We have different organizations on standardization of RFID frequency bands

- International Organization
  - **ISO** (International Standard Organization)

- Regional or National Organizations
  - **CEPT**: European Licensing Organization on short range devices
  - **ETSI**: European licensing Organization for inductive radio systems
  - **FCC**: USA Licensing Organization for RFID Systems

So we have several Frequency bands but only one standard worldwide: 13,56 MHz



- The frequencies dedicated to RFID are included in ranges already in use for other applications (e.g. TV, radio,…)
- It is hard to envision possible product alterations or interference with electronic equipments
- As frequency increases, usually:
  - *tag cost*, *power level*, *reading distance*, *reading rate* increase
  - *tag size*, *penetration through different materials (e.g. water)* decrease

** Max reading distance depends also on other tag characteristics – e.g. dimensions, with/without battery, ... – and environment – e.g. metals, water,...*

Wireless Sensor Networks: more than RFID

• A **wireless sensor network** (WSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants.

•The development of wireless sensor networks was motivated by military applications such as battlefield surveillance.

•They are now used in many industrial and civilian application areas,
•including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control.

•In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery.

WSN features

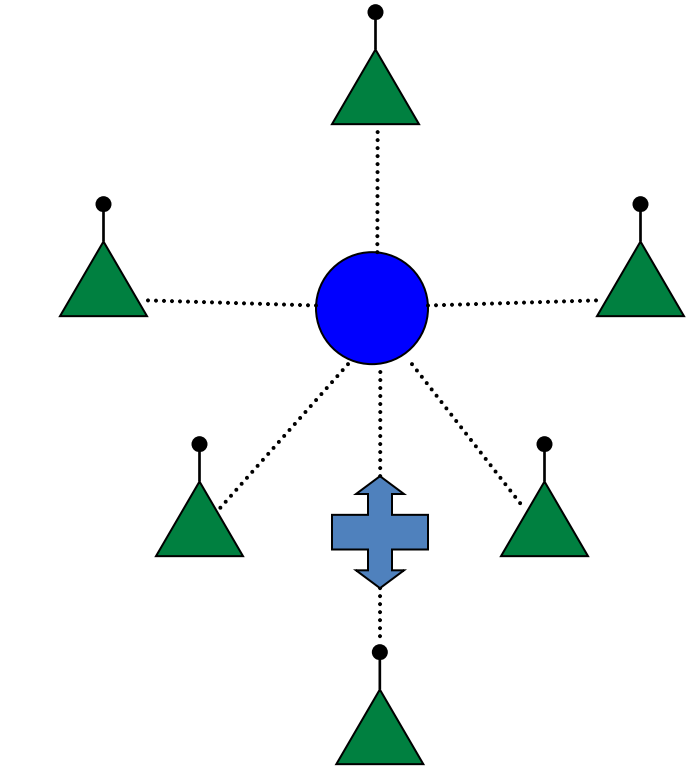
•A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created.

•The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few pennies, depending on the size of the sensor network and the complexity required of individual sensor nodes.

•Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth.

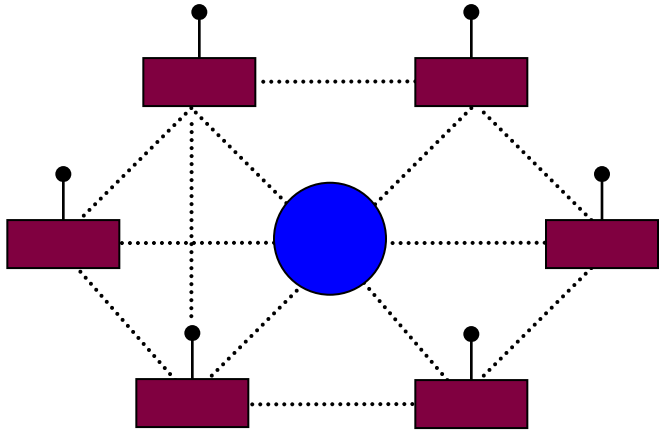
•A sensor network normally constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm (several nodes may forward data packets to the base station

Star Network Key Attributes



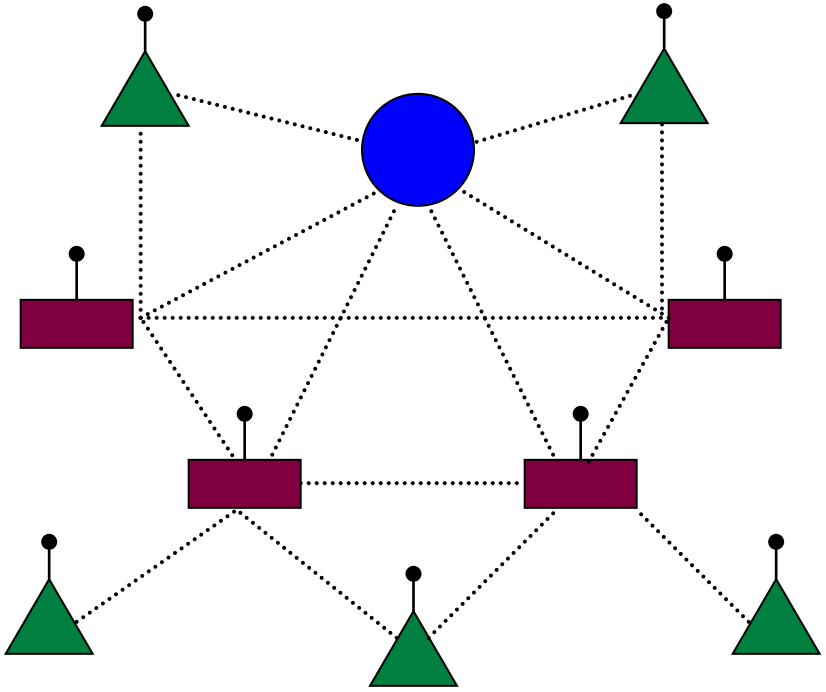
- **Simplicity**
- **Low Cost**
- **Long Battery Life**
- **Single Point of Failure**

Mesh Network Key Attributes



- **Reliability**
- **Extended Range**
- **No Battery Life**
- **Routing Complexity**

Hybrid Network Key Attributes



- **Flexibility**
- **Reliability/Range of Mesh**
- **Battery Life of Star**
- **Design Complexity**

ZigBee: an interesting technology for process controlling

•**ZigBee** is a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4-2003 standard for wireless personal area networks(WPANs), such as wireless headphones connecting with cell phones via short-range radio.

•The technology defined by the ZigBee specification is intended to be simpler and less expensive than other WPANs, such as Bluetooth. ZigBee is targeted at radio-frequency(RF) applications that require a low data rate, long battery life, and secure networking.

•The ZigBee Alliance is a group of companies that maintain and publish the ZigBee standard

Examples of Wireless Networking Standards

Market Name Standard	GPRS/GSM 1xRTT/CDMA	Wi-Fi™ 802.11b	Bluetooth™ 802.15.1	ZigBee™ 802.15.4
Application Focus	Wide Area Voice & Data	Web, Email, Video	Cable Replacement	Monitoring & Control
System Resources	16MB+	1MB+	250KB+	4KB - 32KB
Battery Life (days)	1-7	.5 - 5	1 - 7	100 - 1,000+
Network Size	1	32	7	255 / 65,000
Bandwidth (KB/s)	64 - 128+	11,000+	720	20 - 250
Transmission Range (meters)	1,000+	1 - 100	1 - 10+	1 - 100+
Success Metrics	Reach, Quality	Speed, Flexibility	Cost, Convenience	Reliability, Power, Cost

6lowpan, may be the future internet of thinks

•**6lowpan** is an acronym of *IPv6 over Low power Wireless Personal Area Networks*, or (as the "personal" qualification is no longer relevant), *IPv6 over LoW Power wireless Area Networks*.

•6lowpan is the name of a working group in the internet area of the IETF. The 6lowpan group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received from over IEEE 802.15.4 based networks.

•IPv4 and IPv6 are the work horses for data delivery for local-area networks, metropolitan area networks, and wide-area networks such as the Internet. Likewise, IEEE 802.15.4 devices provide sensing
communication-ability in the wireless domain.

•The inherent natures of the two networks though, is different. The base specification developed by the 6lowpan IETF group is RFC 4944.

DASH

•**DASH7** is an ultra-low power (coin cell batteries) wireless sensor networking technology originally created for military use and now being repurposed for commercial applications. DASH7's has a range of more than 2 kilometers, 10 year battery life, "mesh" capabilities, and penetrates concrete and water.

•Also known as ISO 18000-7, DASH7 is an open standard operating in the unlicensed 433 MHz spectrum with support for sensors, encryption, and other features.

•433 MHz is available for use worldwide and can be used to monitor temperature of flu vaccines, monitoring the exact pressure in automobile tires, monitoring electrical usage in a building, or monitoring CO2 emissions from a vehicle.

DASH

•According to Michael Liard, an analyst with ABI Research: The primary competition for 433 MHz solutions comes from 2.45 GHz Wi-Fi and UWB-based active RFID systems; however, many of these systems are proprietary.

•In comparison, 433 MHz offerings are backed by ISO 18000-7, an open international standard. Active 433 MHz devices also boast better power efficiency, lower power drain, no 802.11n (2.45 GHz) interference, better tag-to-tag communication, military-grade reliability, and lower cost than their primary alternatives.

•In January 2009, the U.S. Department of Defense announced the largest RFID award in history, a $429 million contract for DASH7 devices, to four vendors: Savi Technology, SPEC, Northrop Grumman, and Unisys.[1] In March 2009, more than 30 organizations announced their participation in the DASH7 Alliance, a non-profit industry consortium to promote interoperability among DASH7-compliant devices

- Introduction
- The nature of connectivity
- The Principles and Characteristics of Digital Communication Systems
- Modularization of digital communication: the ISO OSI model
- The logic signal encoding
- Ethernet
- Field buses
- RFId and WSN
- LP WAN
- Conclusions

LR-WPAN device types

Two different device types can participate in an LR-WPAN network:

- Full-function devices (FFD) can operate in three modes serving as a personal area network (PAN) coordinator, a coordinator, or a device.
- Reduced-function devices (RFD) are intended for applications that are extremely simple.

An FFD can talk to RFDs or other FFDs, while an RFD can talk only to an FFD.

Network topologies (1)

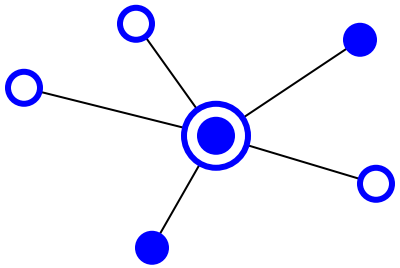
Two or more devices communicating on the same physical channel constitute a WPAN. The WPAN network must include at least one FFD that operates as the PAN coordinator.

The PAN coordinator initiates, terminates, or routes communication around the network. The PAN coordinator is the primary controller of the PAN.

The WPAN may operate in either of two topologies: the star topology or the peer-to-peer topology.

Network topologies (2)

Star topology



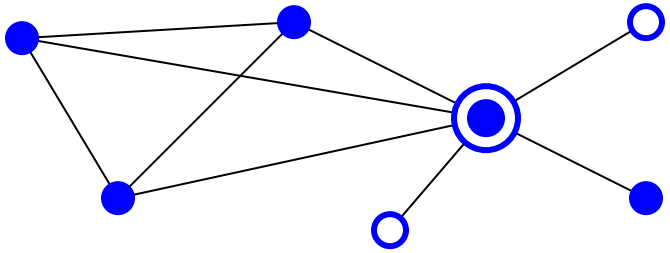
In a star network, after an FFD is activated for the first time, it may establish its own network and become the PAN coordinator.

The PAN coordinator can allow other devices to join its network.

Network topologies (3)

In a peer-to-peer network, each FFD is capable of communicating with any other FFD within its radio sphere of influence. One FFD will be nominated as the PAN coordinator.

Peer-to-peer topology



A peer-to-peer network can be ad hoc, self-organizing and self-healing, and can combine devices using a mesh networking topology.

ZigBee PHY and MAC parameters

Topology	Ad hoc (central PAN coordinator)
RF band	2.4 GHz ISM frequency band
RF channels	16 channels with 5 MHz spacing
Spreading	DSSS (32 chips / 4 bits)
Chip rate	2 Mchip/s
Modulation	Offset QPSK

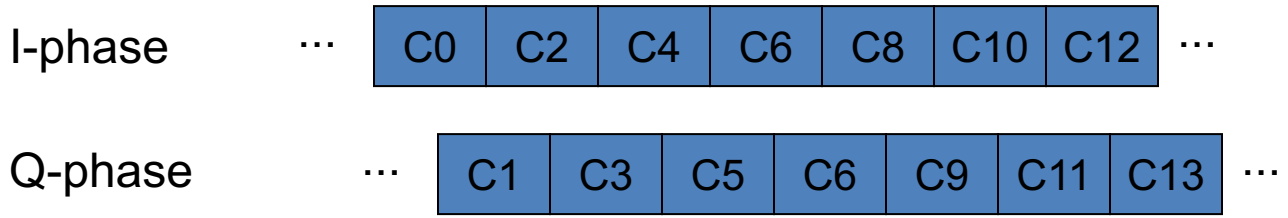
Access method	CSMA/CA (or slotted CSMA/CA)

Spreading and modulation

Four consecutive bits are mapped into a data symbol.

Each symbol is mapped into a 32-chip pseudorandom sequence.

The even-indexed and odd-indexed chips of the chip sequence representing each data symbol are modulated onto the carrier using Offset-QPSK in the following way:



Beacon frames

- The LR-WPAN standard allows the optional use of a superframe structure.
- The format of the superframe is defined by the coordinator.
- The superframe is bounded by network beacons, sent by the coordinator, and is divided into 16 equally sized slots.
- The beacon frame is transmitted in the first slot of each superframe. If a coordinator does not wish to use a superframe structure, it may turn off the beacon transmissions.
- The beacons are used to synchronize the attached devices, to identify the PAN, and to describe the superframe structure.

CSMA/CA operation (1)

- Non beacon-enabled networks use an un slotted CSMA-CA channel access mechanism.
- Each time a device wishes to transmit data frames or MAC commands, it shall wait for a random period.
- If the channel is found to be idle, following the random backoff, the device shall transmit its data.
- If the channel is found to be busy, following the random backoff, the device shall wait for another random period before trying to access the channel again.
- Acknowledgment frames shall be sent without using a CSMA-CA mechanism.

CSMA/CA operation (2)

- Beacon-enabled networks use a slotted CSMA-CA channel access mechanism, where the backoff slots are aligned with the start of the beacon transmission.
- Each time a device wishes to transmit data frames, it shall wait for a random number of backoff slots.
- If the channel is busy, following this random backoff, the device shall wait for another random number of backoff slots before trying to access the channel again.
- If the channel is idle, the device can begin transmitting on the next available backoff slot boundary.

LPWAN Characteristics

Constrained and challenged network (as defined RFC 7228)

License-exempt or Licensed bands

Property industrial deployments, huge potential

Battery powered devices with limited communications

Deep Coverage

LPWAN Technologies

Asymmetric Lines

Small message size

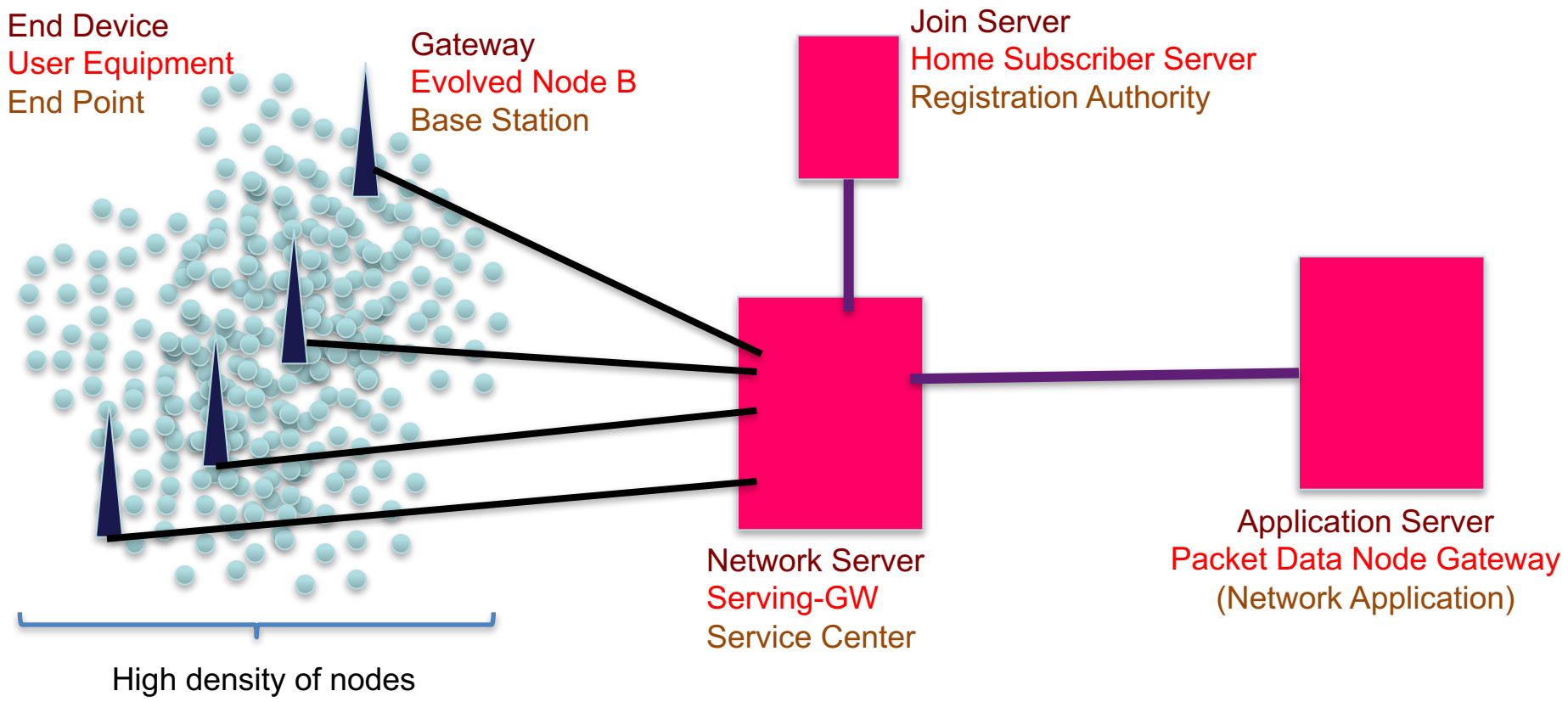
Limit number of messages per device and per day

Complex Device and Network management

Acknowledgement management

NO
IP CAPABILITIES

Similar architecture: : Lora Wan, NB-IoT, SIGFOX



Radio characteristics

- LoRaWAN – Sigfox : Mostly in unlicenced spectrum
  - 868 MHz (EU), 915 MHz (US), 433 MHz (Asia),
  - 868 MHz (EU), 902 MHz (US)
  - Duty cycle : 1% (up), 10% (down)

- NB-IoT – licenced bands
  - LTE/GSM spectrum
  - No duty cycle

Frame characteristics: Maximum payload

- LoRaWan:
  - Differs with the modulation and management information
    - 59-230 bytes (EU)
    - 19-250 bytes (US)
- NB-IOT:
  - 1600 Bytes
- Sigfox:
  - 12 bytes down stream (* 140/day)
  - 8 bytes upstream (* 4/day)

Frame Characteristics: Security

- LoRAWAN:
  - AES-128 AppKey =>
    - 128 NwkSkey for Frame integrity
    - 128 appSkey for payload encryption
- NB-IOT:
  - TS 33.203 v13.1.0
- SIGFOX:
  - Pre provisioned security key to authentication and integrity
  - Application can encrypt payload

Control plane

- LoRaWAN
  - A node must join the network
  - Network can pilot a node (frequency, Spreading factor)
- NB-IOT:
  - control the radio access bearers and the connection between the UE and the network. It is responsible for authentication, security control, mobility management and bearer management.
- SIGFOX:
  - No

LPWAN Family characteristics

- Thousand of nodes per gateway
- Star Topology
- Very small frame payload (8 – 250bytes)
  - Practical limitation : < 50 Bytes
- Limit number of frames per day (10)
  - Duty cycle limits the transmission is unlicenced bands
- Low bandwidth offering throughput between 50 bit/s to 250kbit/s
- High packet loss (caused by collisions or bad transmission conditions)
- MTU variable (changing with modulation)
- Highly asymmetric (up/down) links or unidirectional links only
- Sleepy nodes (not as DTN)
- No Fragmentation in L2 (not all)

LPWAN at IETF

- IP communication
  - Global connectivity (reachability)
  - Independence from L2
  - Use or adapt actual protocols
  - Use existing addressing spaces and naming schemes
- Strong Security
  - Adapted to the LP-WAN applications as: health, personal usages (water, gas, bus timing, etc.)
- Scalability
- High Reliability
- Interoperability
- Header Compression to reduce overhead

IPv6 => LPWAN

Impossible to send directly IPv6 packet, even with a fragmentation layer:

- The overhead of IPv6 is not compatible with LPWAN
- The variable MTU gives a variable fragmentation solution
- Need to adapt NDP (Neighbor Discovery) to LPWAN

6Lowpan, 6lo => LPWAN

- 6LoWPAN reduce header overhead for reliable L2 protocols
- 6LoWPAN traditionally used for constrained node networks
  - The LPWAN technologies are even more constrained than typical 6LoWPAN
- Challenge for 6LoWPAN mechanisms is that LPWAN does not send ACK at L2
- 6Lo adapts 6LoWPAN for other technologies
  - In LP-WAN the network is also constrained
  - In LP-WAN devices are challenged
- Best IPv6/UDP header compression: 6 Bytes (10% of a LoRaWAN frame) and 37 bytes with global @.

Configuration

- Neighbor Discovery
  - Decentralized configuration
  - 6LoWPAN ND uses unicast messages

- Messages size: [**draft-gomez-lpwan-ipv6-analysis-00]**
  - -- Size of RS with SLLAO = 14 bytes
  - -- Size of RA with SLLAO, PIO and 6CO = 62 bytes
  - -- Size of NS with ARO and SLLAO = 46 bytes
  - -- Size of NA + ARO = 40 bytes

RoHC

- Define originally for IP/UDP/RTP streams
  - LPWAN traffic is not a stream => long convergence time
  - Bandwidth is extremely short to support IR packets (larger than a full header)
- Allows unidirectional and bidirectional links
- Extented to any protocol with RoHCv2
- Send full header, followed by field deltas
  - Impossible to send full headers in LPWAN
- Manage by a Master SN
- No Routable
- Complex: Profiles, Operation Modes, Level of Compression, Compression Parameters, Header Formats, & Patents?

- Introduction
- The nature of connectivity
- The Principles and Characteristics of Digital Communication Systems
- Modularization of digital communication: the ISO OSI model
- The logic signal encoding
- Ethernet
- Field buses
- RFId and WSN
- LP WAN
- Conclusions

Conclusions

- In this lesson we have understood the dimensions of connectivity
- the principles, characteristics and standards of digital communication systems
- the different wired, wireless, and low power communications architectures and application domains as a function of processes