Overview

Internet of Things

Jorge Finochietto
Horacio Mendoza

NEON
Network of Competence on Internet of Things
Co-funded by the Erasmus+ Programme of the European Union
UNC Universidad Nacional de Córdoba
FCEFyN
FACULTAD DE CIENCIAS EXACTAS, FÍSICAS y NATURALES

What is IoT?

Dictionaries' definitions

"The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data" [Oxford]

"Objects with computing devices in them that are able to connect to each other and exchange data using the Internet" [Cambridge]

"A system of devices with the ability to transfer data over a network without requiring human interaction" [Wikipedia]

"A network of objects that are fitted with microchips and connected to the internet, enabling them to interact with each other and to be controlled remotely" [Collins]

Bankers’ definitions

“The Internet of Things is the next revolution in computing. By connecting billions of everyday things to the Web, the IoT will collect enormous volumes of data that could reshape almost every aspect of our lives.” [Morgan Stanley]

“The Internet of Things (IoT) is emerging as the next technology mega-trend, with repercussions across the business spectrum. By connecting to the Internet billions of everyday devices – ranging from fitness bracelets to industrial equipment – the IoT merges the physical and online worlds, opening up a host of new opportunities and challenges for companies, governments and consumers.” [Goldman Sachs]

Analysts’ definitions

“The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.” [Gartner]

“A network of uniquely identifiable end points (or things) that communicate bi-directionally without human interaction using IP connectivity.” [IDC]

“Sensors and actuators embedded in physical objects linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet.” [McKinsey]

“Connection of devices to the internet using embedded software and sensors to communicate, collect and exchange data with one another” [EY]

Governments’ definitions

“Things such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet.” [Federal Trade Commission (FTC)]

“The Internet of Things (IoT) enables large numbers of previously unconnected devices to communicate and share data with one another.” [Ofcom]

“A distributed network connecting physical objects that are capable of sensing or acting on their environment and able to communicate with each other, other machines or computers. The data can be collected and analysed in order to reveal insights and suggest actions that will produce cost savings, increase efficiency or improve products and services.” [European Parliament]

Professionals’ definitions

“A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.” [ITU]

“A trend where a large number of embedded devices employ communication services offered by the Internet protocols. Many of these devices are not directly operated by humans.” [Internet AB]

“An extension of network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered computers.” [Internet Soc.]

“A network of items - each embedded with sensors - which are connected to the Internet.” [IEEE]

Vendors’ definitions

“The IoT links objects to the Internet, enabling data and insights never available before.” [Cisco]

“Network of physical objects accessed through the internet. These objects contain embedded technology to interact with internal states or the external environment. In other words, when an object can sense and communicate, it changes how and where decisions are made, and who makes them.” [IBM]

“Network of physical objects - “things” - that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.” [Oracle]

¿How would you define IoT?

ⓘ Start presenting to display the poll results on this slide.

Historical Background

Historical Background (World War II)

Radio frequency identification (RFID) can be seen as a crucial technology for IoT.

Back to World War II, radars were used to warn of approaching enemy planes while they were still miles away, but there was no way to identify which planes belonged to the enemy and which were own pilots returning from a mission.

Germans discovered that if pilots *rolled their planes* as they returned to base, it would change the radio signal reflected back to radar systems. This crude alerted the radar crew on the ground that these were German planes. Essentially, this was the first passive RFID system.

British developed the first active “RFID” system. When a British plane received a radar signal, it would broadcast a signal back that identified the aircraft as friendly.

Historical Background (1950 - 1960)

US, Europe and Japan explored how RF can be used to identify objects remotely.

Companies began commercializing *anti-theft systems* that used radio waves to determine whether an item had been paid for or not (object state).

Electronic article surveillance tags, for instance, which are still used in packaging today, have a 1 bit tag, which is either on or off (but does not identify the item)

- If someone pays for the item, the bit is turned off, and he can leave the store.
- But if he doesn't pay and tries to walk out of the store, automated readers at the door detect the tag and sound an alarm.

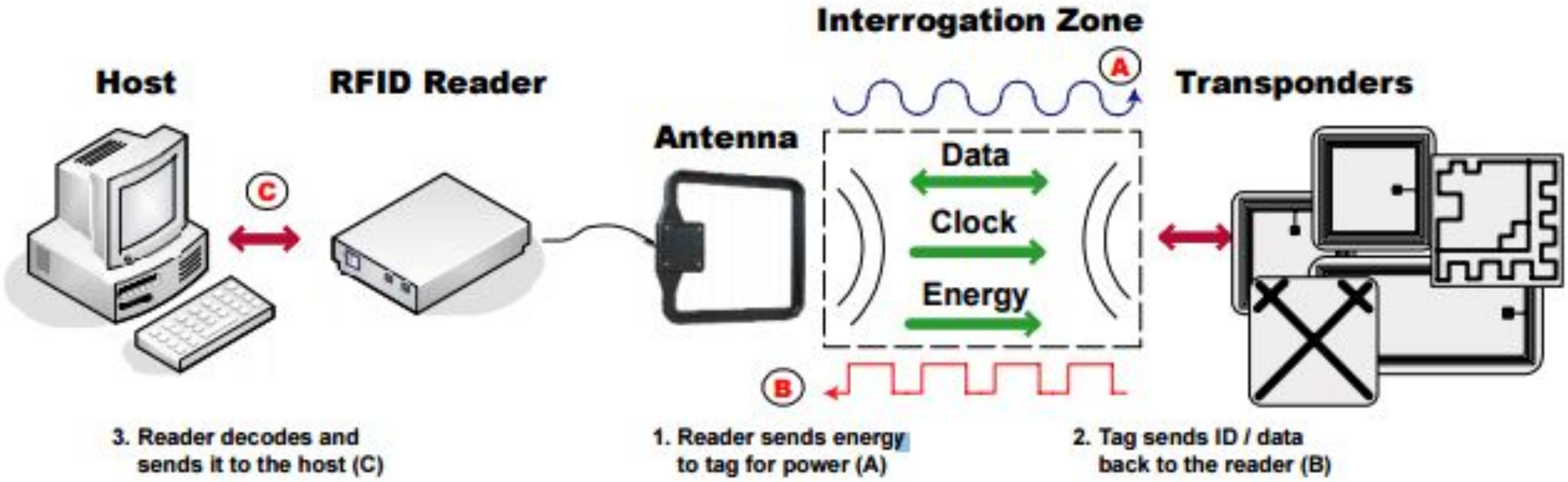
Historical Background (1970 - 1980)

Los Alamos National Laboratory developed a system for tracking nuclear materials.

The concept used an active transponder in a truck and readers (with antennas) at the gates of secure facilities. The gate antenna would *wake up* the transponder in the truck, which would respond with an ID.

This system was later used to develop automated toll payment systems. These systems became widely used on roads, bridges and tunnels around the world.

RFID Working Principle



Historical Background (1970 - 1980)

A passive RFID tag that used UHF (~GHz) was developed to track cows and their doses of hormones and medicines to ensure that each cow wasn't given two doses accidentally.

The device drew energy from the reader and simply reflected back a modulated signal to the reader (backscatter)

Later, a low frequency (125 kHz) system (smaller transponders but shorter distance) was developed, which encapsulated in glass could be injected under a cow’s skin.

Low frequency transponders were also put in cards and used to control access to buildings.

Historical Background (1990 - 2000)

UHF RFID got a boost in late 1990, when Auto-ID Center at MIT was created.

Low-cost RFID tags to track products through the supply chain: a “serial number” on the tag to keep the price down. Simple microchip with little information less expensive to produce than a more complex chip with more memory.

Data associated with this “serial number” on the tag stored in a database accessible over the Internet. Tags were not any more a mobile database carrying information about the product or container as they traveled.

The Auto-ID Center used the term "Internet of Things" in ~2000 and developed the Electronic Product Code scheme designed to identify each item manufactured, as opposed to just the manufacturer and class of products, as bar codes do today.

Electronic Product Code

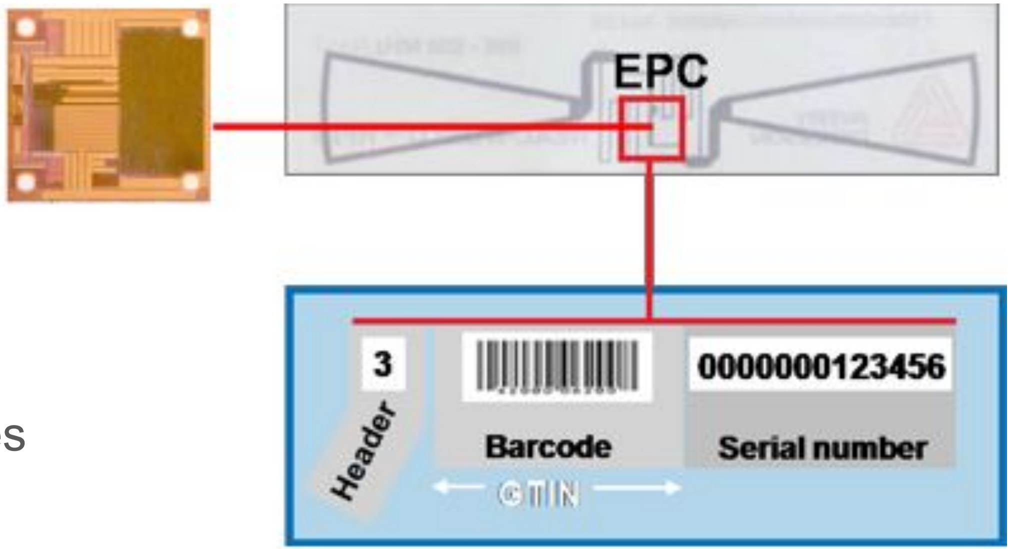
A 96-bit EPC has 4 distinct parts:

Header (8): type of EPC.

Manager (28): 268.435.455 different product manufacturers

Class (24): 16.777.215 different types of object.

Serial Number (36): 68.719.476.735 potential unique identification numbers per object.



Each object has an unique ID

Machine to Machine (M2M)

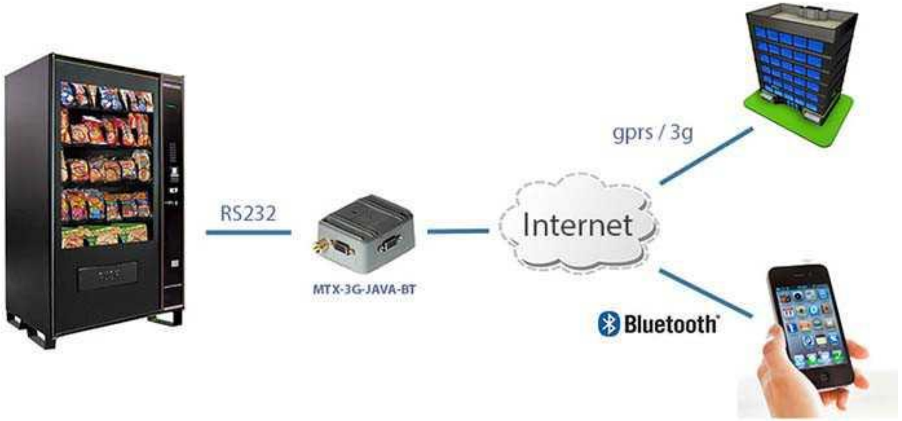
Machine to machine (M2M)

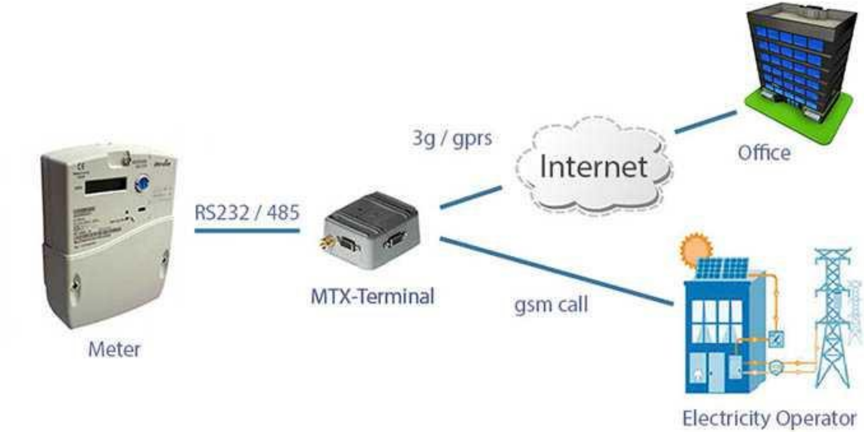
Direct communication (point-to-point connection) between two devices (in general, terminal and client roles) using any communications channel, including wired and wireless, without any human intervention.

Sensor telemetry is one of the original uses of M2M communication. For decades, businesses have used M2M to remotely monitor factors like temperature, energy consumption, moisture, pressure and more through sensors.

ATMs offer another great example of M2M technology: ATM’s internal computer is constantly communicating with a host processor that routes transactions to the appropriate banks and accounts. The banks then send back approval codes through the host processor, allowing transactions to be completed.

M2M Devices & Use Cases





M2M is not IoT

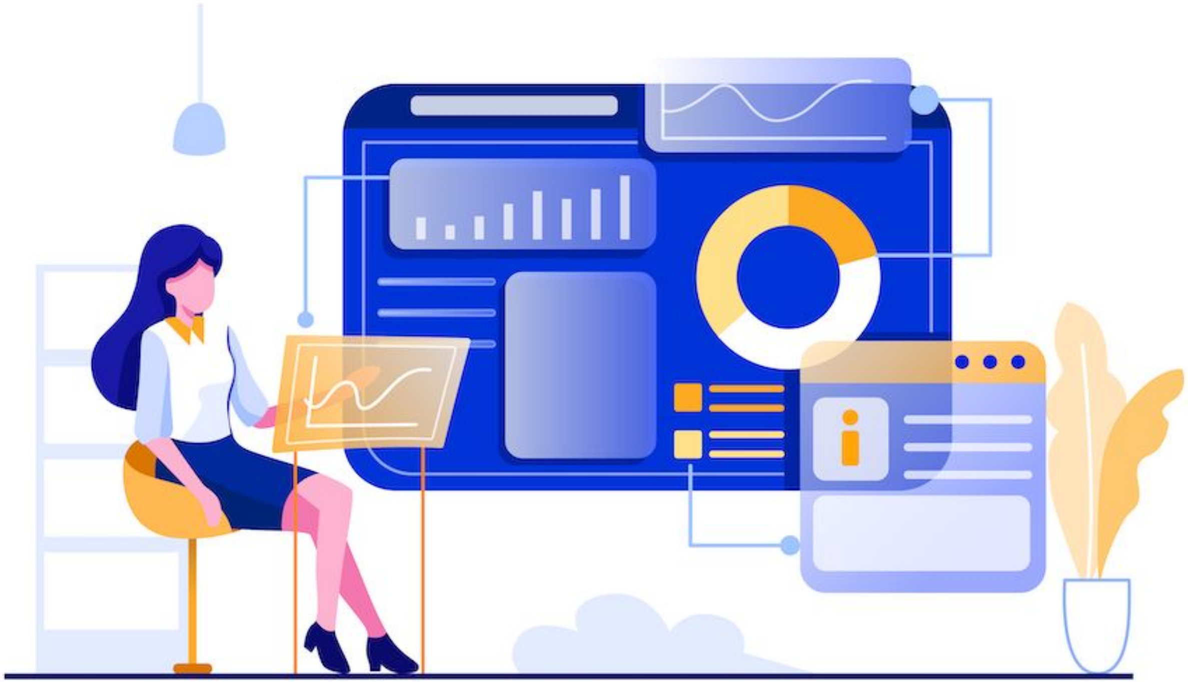
M2M can be considered a forerunner of IoT

M2M communication model is point-to-point, while IoT is network-based (Internet)

M2M data is usually directed towards performing a single task strongly coupled with the device application. Instead, IoT collects data that is used for different applications.

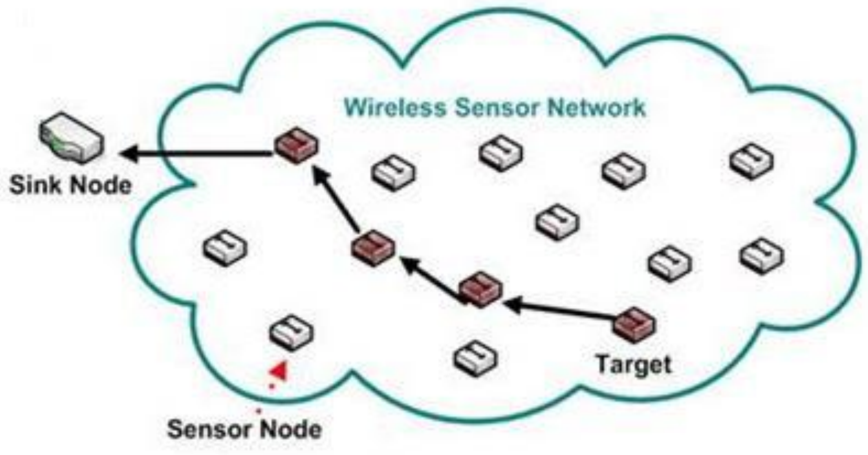
M2M communications are strictly device-based (i.e., between devices). IoT has a broader circle of possible communication subjects. Apart from devices, it can connect humans with machines, a device and a gateway, a gateway and the data system, as well as two data systems.

Wireless Sensor Networks (WSN)



Wireless Sensor Networks (WSN)

Group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind, etc.



WSN is not IoT

WSN is used mainly for coordinated collection of data. IoT goes beyond this, in a way, where smartness can be added to the objects so that they can do the work of actuation to achieve a certain goal without human intervention.

WSN uses only wireless communications. IoT can rely on both wired and wireless.

WSN uses a network-based communication model, but not necessarily compatible with Internet. IoT assumes nodes can be connected to the Internet.

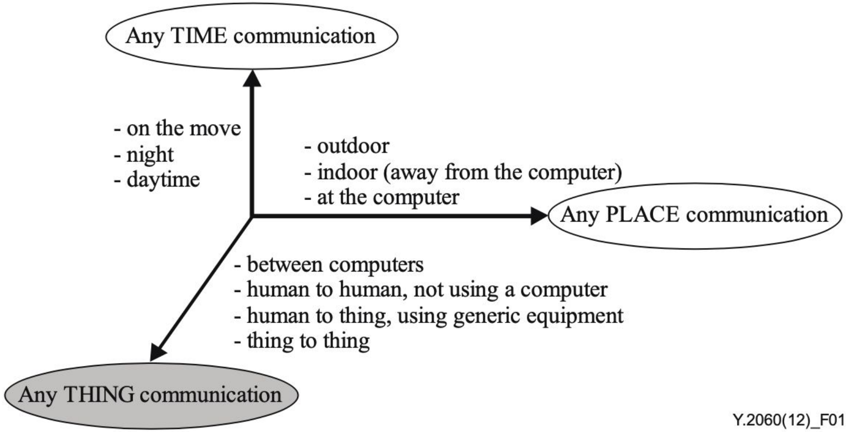
WSN assumes small, low-cost and similar nodes. IoT considers any type of node, from small ones to vehicles, or even bigger.

Back to IoT Definition

An IoT is a network that connects uniquely identifiable “Things” to the Internet.

These “Things” have sensing, actuation and potential programmability capabilities.

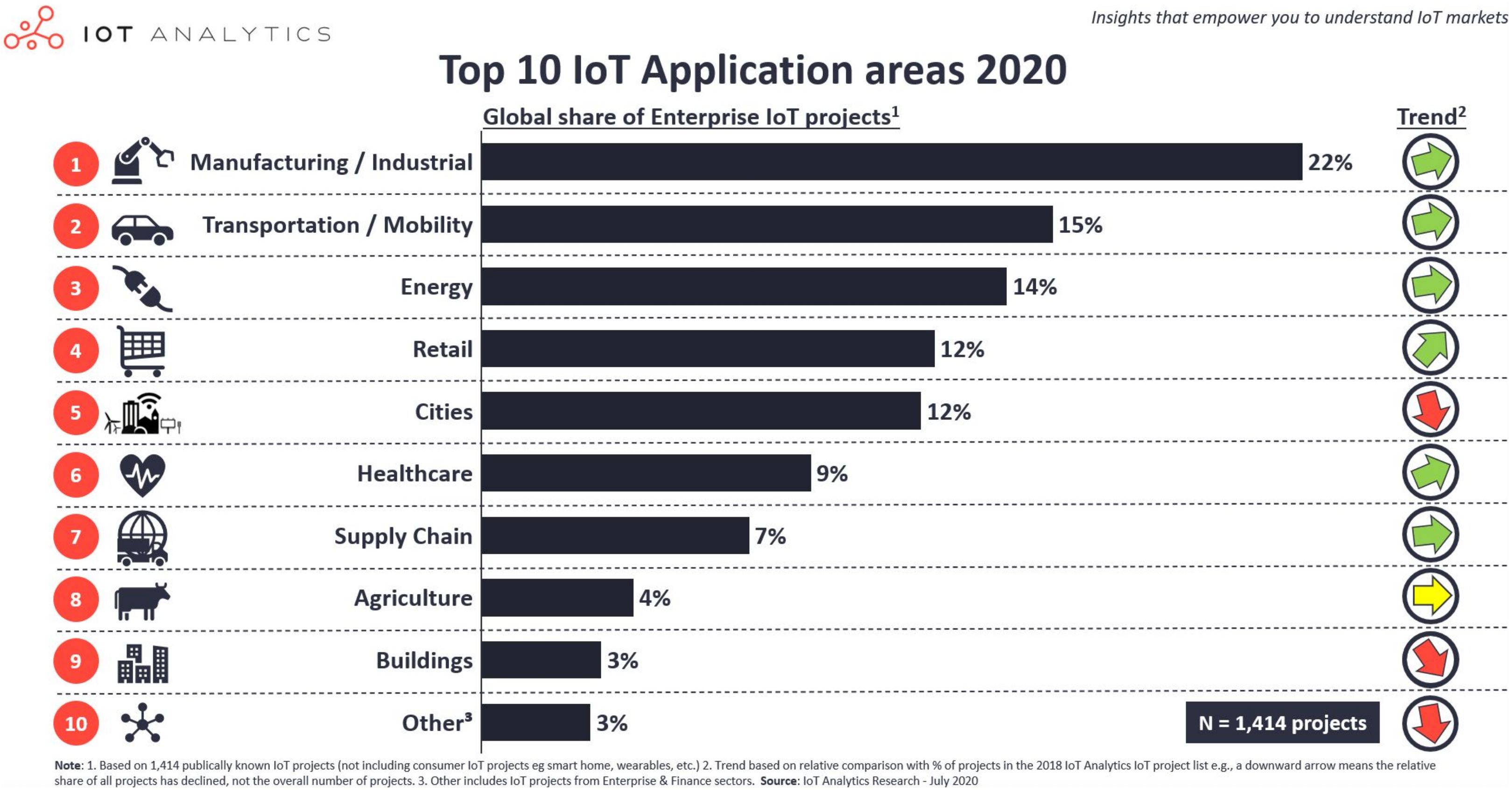
Through the exploitation of unique identification information about the “Thing” can be collected and its state changed from anywhere, anytime, by anything.“



IoT adds the "Any THING communication" dimension to ICT, which already provide "any TIME" and "any PLACE" communication.

Where is IoT?

IoT Top Applications



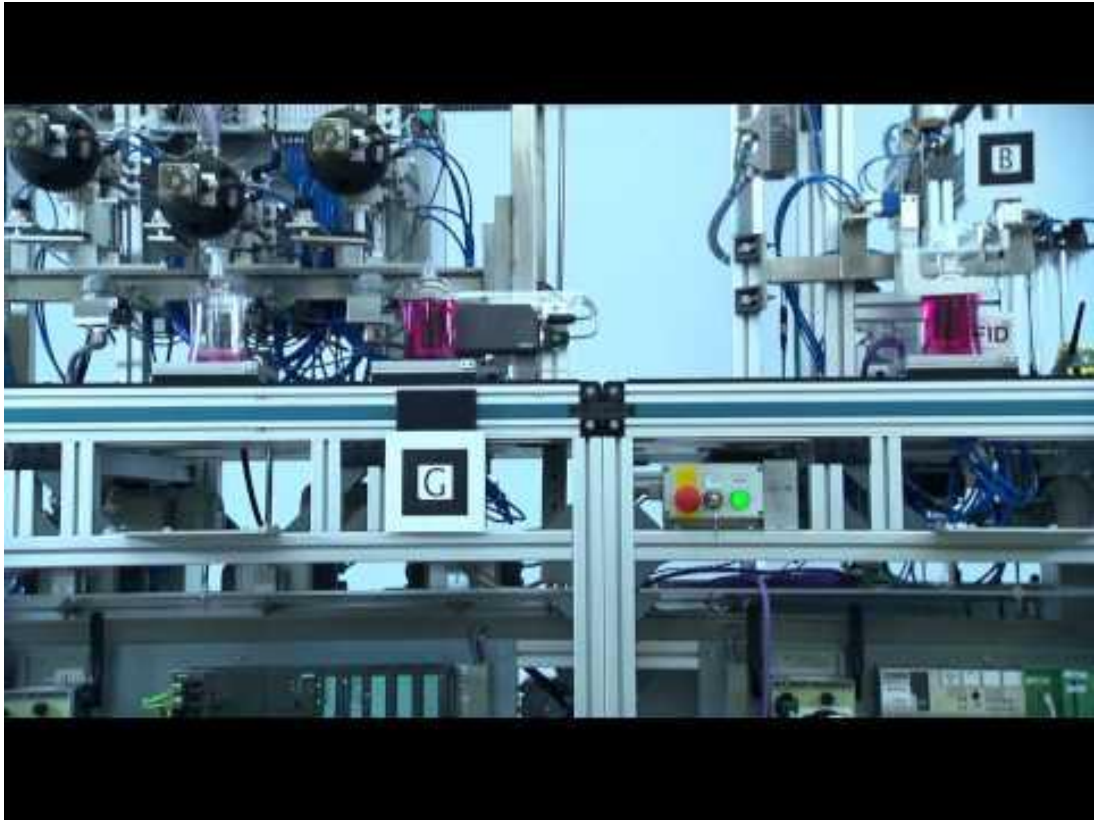
(1) IoT @ Manufacturing / Industrial

Industrial IoT application area covers a wide range of connected “things” projects both inside and outside the factory.

Inside: many IoT-based factory automation and control projects include holistic smart factory solutions with numerous elements such as production floor monitoring, wearables and Augmented Reality on the shop-floor, remote PLC control, or automated quality control systems.

Outside: include remote control of connected machinery, equipment monitoring, or management and control of entire remote industrial operations such as oil rigs. Many of the case studies mention “reducing operational downtime and cost saving” as the key drivers for OEMs to introduce industrial IoT solutions.

Example: Siemens Intelligent Factories



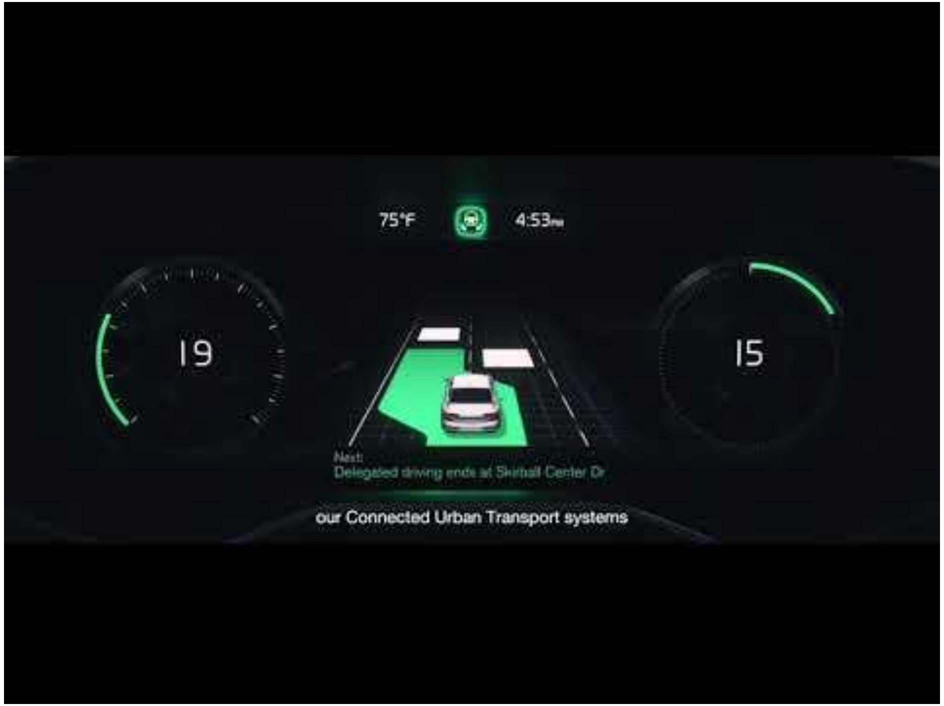
Example: Howden Mixed Reality solutions

Howden, a Scottish manufacturer of air and gas handling solutions, developed a scalable mixed reality solutions that overlay real-time IoT data from connected products with 3D Augmented Reality experiences to provide step-by-step instructions on how to solve problems with the equipment.

[More details]

(2) IoT @ Transportation / Mobility

Typical applications include telematics and fleet management solutions that connect with the local operating system within the car for vehicle diagnostic/monitoring such as battery monitoring, tire pressure monitoring, driver monitoring or simply vehicle tracking.



Example: Volvo Transport of the Future

Example: Accident Prevention

(3) IoT @ Energy

IoT is revolutionizing nearly every part of the energy industry from generation to transmission to distribution and changing how energy companies and customers interact. Both solution providers and energy companies themselves understand the need for and value of connected IoT solutions in the sector.

IoT projects focus on energy distribution, grid optimization, remote asset monitoring and management, predictive maintenance and creating more transparency for better informed customers.

Example: Enel’s grid reliability solution

To improve grid reliability and reduce the occurrence of faults, Enel, an Italian multinational energy company, deployed the C3.ai Predictive Maintenance application for 5 control centers.

The application uses AI to analyze real-time network sensor data, smart meter data, asset maintenance records, and weather data to predict feeder failure.

More details.

Example: Telefónica Smart Energy

(4) IoT @ Retail

Retailers recognize that they can improve their cost-efficiency and in-store customer-experience through innovative IoT use cases.

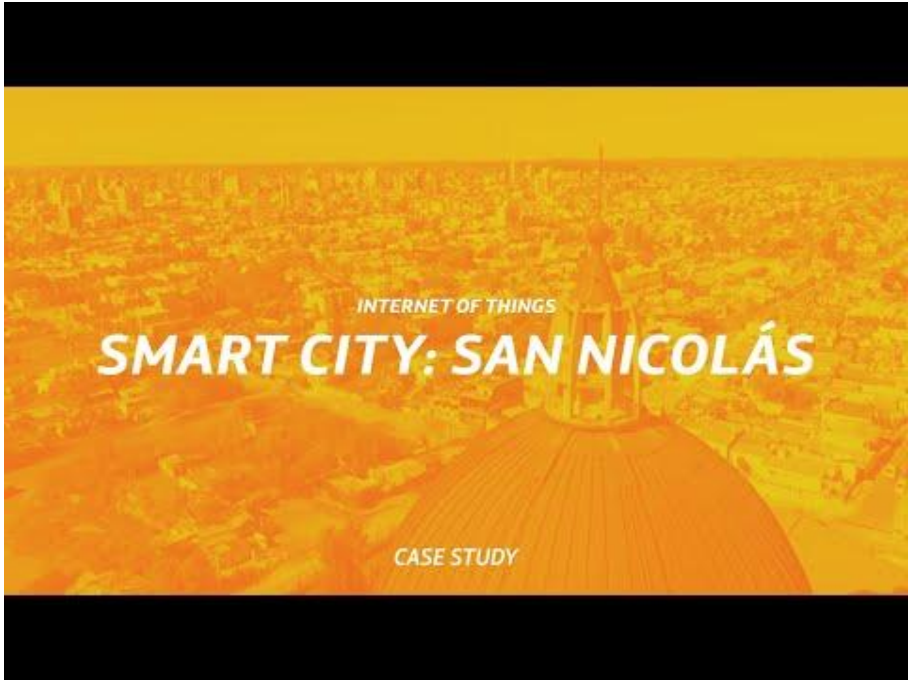
Typical IoT in retail solutions include in-store digital signage, customer tracking and engagement, goods monitoring and inventory management and smart vending machines among others.

Example: Telefónica Smart Retail

(5) IoT @ Cities

Smart cities are growing and blossoming in all parts of the world.

Typical IoT projects in Smart Cities include connected traffic (smart parking, traffic management), utilities (smart waste, lighting), public safety (video surveillance) and environmental monitoring (air pollution).



(6) IoT @ Healthcare

Slowly proliferated itself in healthcare, but changing in light of the center of COVID-19 pandemic. Early data suggests that digital health solutions that relate to COVID-19 are surging.

Demand for specific IoT health applications such as telehealth consultations, digital diagnostics, remote monitoring, and robot assistance is increasing.

Example: Medisanté remote patient monitoring.

Simple remote patient monitoring with continuous monitoring of assets connected to healthcare applications, including battery life and general health of devices, which allows personalized patient care anytime, anywhere and equips care teams with a near real-time view of the patient's health and activities.

More details.

(7) IoT @ Supply Chain

As supply chains extend more and more to the end customers, resulting in more intricate flows of goods that are more complex to deliver, logistics providers are increasingly integrating connected digital solutions to tackle the complexity

Typical supply chain IoT projects include asset tracking, condition monitoring (e.g., cold chain, medical goods), inventory and storage management, automated guided vehicles, connected workers, among others.

Example: Smart Label

Example: DHL SmartSensor

Example: Telefónica Home Delivery

(8) IoT @ Agriculture

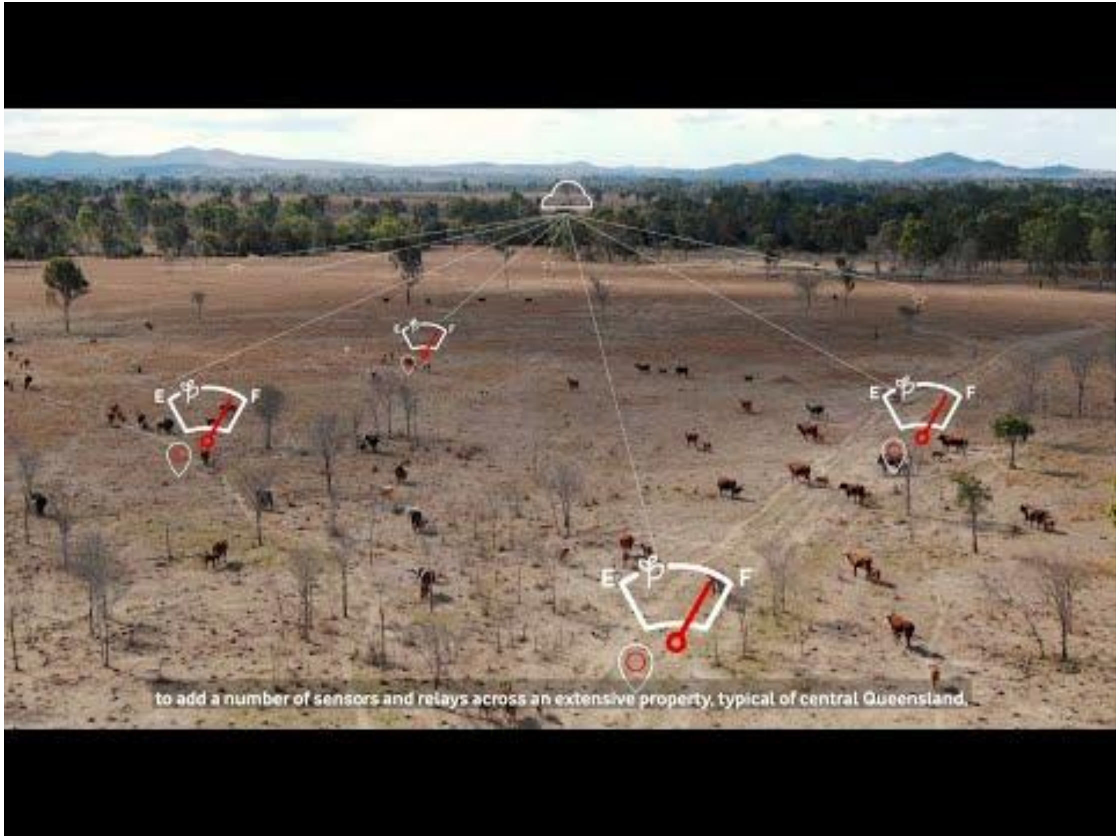
In 2050, it is estimated that a population of almost 10 billion people will need up to 70 percent more food than we do today. One way to address this challenge is through smart agriculture.

IoT sensors can help farmers make more informed decisions to achieve higher crop yield, better quality produce, and save costs by reducing the use of fertilizers and pesticides.

Example: Plantae

Example: Winery of the Future

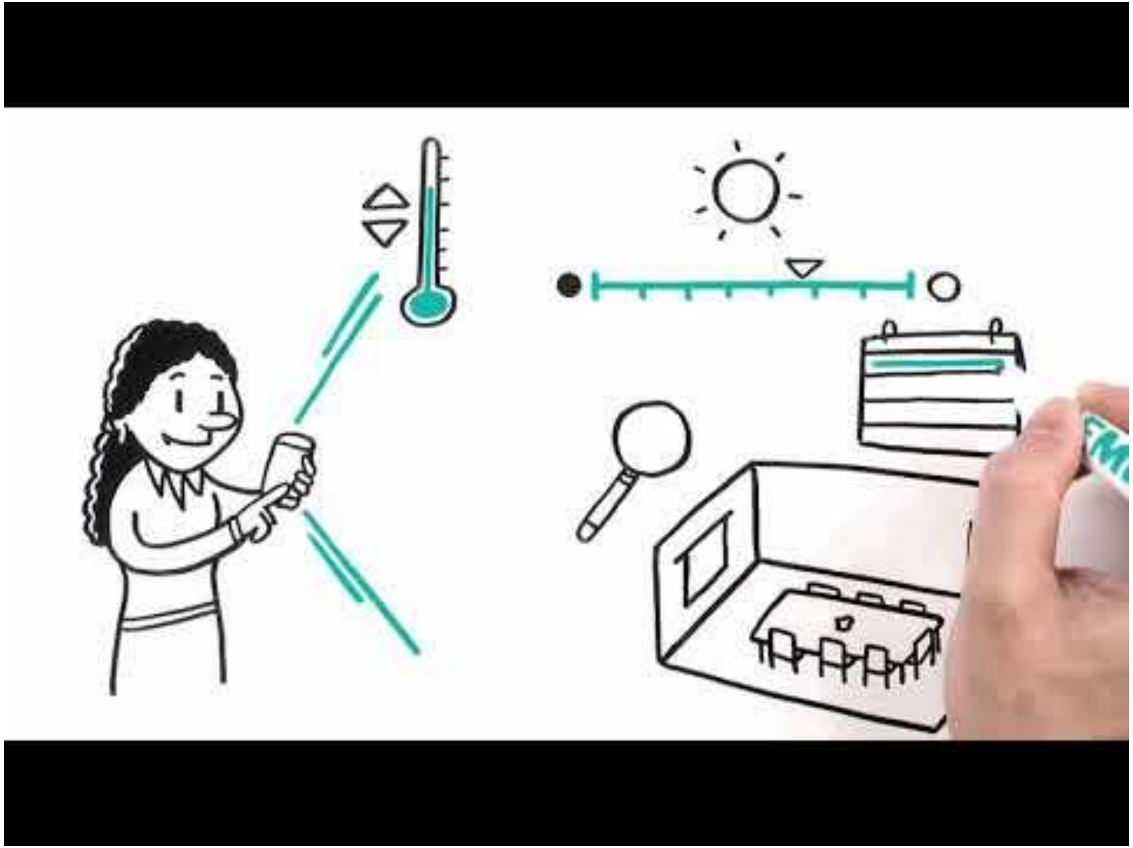
Example: Smart Farm



(9) IoT @ Buildings

Typical connected building projects involve facility-automation and monitoring for building systems (HVAC, lighting, elevators, smoke alarms, fire extinguishers), building utilization and security (room use, access, surveillance).

Example: Siemens Smart Building



Example: Microsoft IoT for Buildings