

---

## Introduction

---

This first part recaps fundamental and classic concepts of theories... but first, in order to clarify our approach, let us look at a little vocabulary and examine a few definitions of the “Who is Who” in the “IoX”.

### **1.1. Definition of communicating- or connected Things**

#### **1.1.1. *Connected Things – Communicating Things***

What a marvellous term “Connected Thing” is, which conveys absolutely anything... and its opposite! How many people will delight in that name!

“Thing” is easy: it is easy to imagine that the term covers everything from an extremely miniature Thing to an enormous ocean liner!

“Connected” to what? How? Why? ... etc. In this aspect, we are often still left searching for meaning!

Over the ages, connections have been established in different ways: in smoke signals, ..., over wired connections, but today, all of this now seems somewhat retro to some people. The uni-directional or bi-directional, “wireless” or “contactless”, connection is much more in fashion.

That said, let us keep things simple and open our eyes. Radio-frequency identification (RFID) has been in use for a number of years (decades, even); so too

have contactless chip cards, NFC, Zigbee, Bluetooth BT & BLE, Wi-Fi, etc. and, much like Mr Jourdain in Molière’s *The Bourgeois Gentleman* speaking prose all his life without even knowing it, we have been making “wireless” “Connected Things” –secure ones, even, and even highly secure!

An example from the public “automobile” market:

For 15 years, an electronic valve for cars has been a “Connected Thing” (using UHF), connected to the electronics of the car, but this is not an example of the IoT!

Thus, this current fashion is not truly groundbreaking, except for a certain faction of the press and avid “followers” of new words... even if those new words express the same things as the old ones!

### 1.1.2. Definition of the IoT

What exactly does the IoT consist of, and what is the IoE (i.e. the Internet of Everything)?

It is a physical network of Things (or “devices/objects”) incorporating sensors, electronics, software and connectivity, enabling these Things to exchange data with an operator, a manufacturer, a service provider or other connected devices. Thus, it is based on a number of different things.

#### 1.1.2.1. Infrastructure of the IoT

The IoT works under the auspices of the “ITU – the International Telecommunications Union – Global Standards Initiative (IoT-GSI)”. For information, IoT-GSI covers connected devices and Things (e.g. personal computerized devices, portable or office computers, tablets and smartphones, etc.) via multiples communication protocols connecting the elements to one another, such as Bluetooth, ZigBee, Long-Range Wide-Area Networks such as LoRa, SIGFOX, etc.

#### 1.1.2.2. IoT devices (or nodes or elements or Things)

IoT devices (elements) or indeed what we define generally as Things, often function without a human interface, generally using the energy supplied by a battery,

and are usually devoted to a single task. They are generally described as “smart objects”, or as “connected devices”. As it is, there is a whole host of such devices! For example:

- electrodomestic networks which can be remotely monitored or controlled;
- sensors, industrial equipment and other integrated elements which are connected in networks;
- “Smart home” elements such as lighting, heating or ventilation units with remote management/control, access, etc.
- “wearables”, fashion accessories or connected clothing, etc.
- etc.

This typically means that an IoT device falls into one or several of the following functional domains:

- Surveillance: teledetection and notification of operating conditions and use of other external environmental factors;
- Control: means that certain functions of the Thing can be remotely managed or customized;
- Automation: devices which can operate independently, capable of adapting to environmental or operation factors with minimal human interaction;
- Optimization: monitoring- and control functions meaning that the manufacturers of the Things can optimize their performances and effectiveness in real time, based on the history and/or instantaneous operational data;
- Preventative maintenance or diagnostics: these can also be carried out remotely.

### **1.1.3. Internet of x**

Having barely had the time to gain familiarity with the Internet of Things, suddenly we are talking about the Internet of Everything – IoE. What is the difference between these two concepts? We shall answer this excellent question shortly, but first, let us take something of a purist stance, and call a spade a spade. To begin with, in order for there to be an “Internet of x”, the “Internet” (and its structure) must be involved in the story – otherwise there could not be an IoT and certainly not an IoE; however, there are many, many Connected Things which

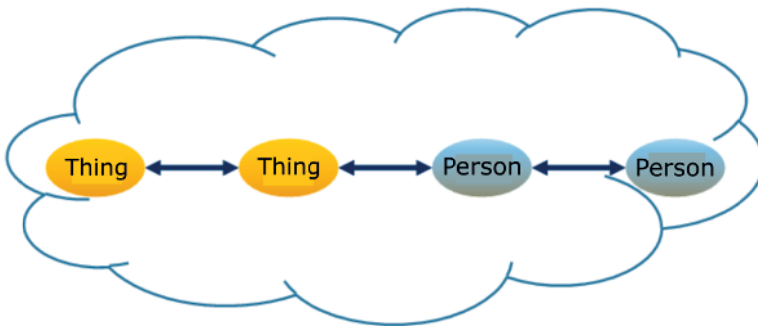
operate with links other than the Internet... thus, it is important not to confuse cabbages and carrots\*!!!

IoT, as the name indicates, implies that sooner or later we must use an Internet connection... but that is not always the case!

NOTE.– *We shall refrain from defining what cabbages and carrots respectively are in this story!*

### 1.1.3.1. *Internet of Things - IoT*

The “Internet of Things” is often defined as being the network of physical Things containing “embedded” technology (integrated, onboard), so as to communicate, detect or interact with their internal states and/or the external environment. Figure 1.1 shows a non-exhaustive example of the functional chain of such a structure.



**Figure 1.1.** *Functional chain of IoT*

Often, by default, in the eyes of many, the Internet of Things is all so-called connected products, monitored by mobile applications: watches, weighing scales, bracelets, toothbrushes, refrigerators, etc., which often do not use the Internet at all, instead using other means of communication such as NFC, BLE or Wi-Fi, for example.

### 1.1.3.2. *Internet of Everything - IoE*

The Internet of Everything – IoE, for short – goes far beyond “Things” (Connected Things). In fact, this is an expression invented in 2015 and promulgated by Cisco – one of the world leaders in network infrastructure. There is every chance

that in tomorrow's world, the Internet of Everything will become a reality, encapsulating not only the world of the Internet of Things, but also that of data, processes... and people (through their smartphones and social networks)! More broadly still, the Internet of Everything is based on the harvesting of the information that we share individually and collectively – that is, it operates at a much higher level than with simple Things in the Internet of Things. That data mining will be organized by private companies capable of processing enormous streams of data – known as “Big Data” (via the Internet) – and charged with turning those data to profit, selling them on either to advertising agencies or marketing networks, or to public-sector organizations wishing to optimize their services and territories, or indeed to public-interest private companies (transport operators, energy providers, works contractors, waste-management companies, etc.), and so on. In other words, the raw material used by this new industry will be our personal information, freely given, without us having any control over the use made of it... Of course, we must not neglect to mention the flip side of the coin: the danger of the servers hosting all these data being hacked!

The admirable goal of the Internet of Everything is to support numerous developments and improvements, such as smart homes, optimized control of energy consumption and natural-resource consumption, smart parking, more appropriate road tolls, etc. and also help improve administrative performances by enhancing agents' productivity and reducing operating expenditure. That, at least, is the dream...

### *Examples*

The Internet of Everything makes it possible for cities to ultimately become “Smart Cities”, and for public administrations to hinge their efforts on the following three axes:

– budget savings:

EXAMPLE.– sensors built into trash cans send a message to indicate that they need to be emptied. Such a system in Finland has already delivered a 40% saving on the waste collection budget.

– new revenues:

EXAMPLE.– in New York, urban screens operating 24/7 are used for surveillance in the city, dissemination of information, offering means of communication (e.g. Wi-Fi), but also generating revenue through advertising.

– advantages for citizens:

EXAMPLE.– “smart parking” employs an intelligent system to inform drivers of the number of free spaces left in the different parking lots in the city.

In Nice, this system has reduced traffic jams by 30%, increased parking revenue and reduced CO<sub>2</sub> emissions.

Having come to the end of these few introductory remarks about our near future, let us now turn our attention to the enormous world of IoT.