

Master di I livello

INDUSTRY 4.0 DESIGN

Enterprise Digitalization
and 4.0 Technologies

Modulo 2.1

Internet of Things

Materiale didattico realizzato sulla base della lezione di:

Ignazio Infantino, *Sensori, attuatori, elaborazione intelligente dei dati sensoriali*

Luigi Cerfeda, *Strumenti e tecnologie per lo sviluppo di soluzioni IoT: introduzione a Zerynth*

Stefano Giordano, *Introduzione all'IoT e 5G*

A cura di:
F. Loi

Sommario

Sintesi.....	1
Internet of Things.....	3
Introduzione all'IoT: gli elementi di base.....	3
Una premessa: sicurezza e privacy	3
Definizioni e tipologie	5
I modelli di elaborazione del dato.....	10
Intelligenza artificiale nell'IoT	12
Piattaforme di elaborazione dei dati sensoriali	15
Le reti di telecomunicazione	16
La nascita di Internet.....	16
Le reti sviluppate dall'uomo.....	17
Le differenze tra le reti e la convergenza futura delle tecnologie	19
La Commutazione	20
Le reti e l'Internet of Things	22
Le reti mobili cellulari.....	24
Applicazioni reali dell'IoT	28
Appendice: Introduzione a Zerynth	30
Storia e presentazione azienda	30
L'IoT in Zerynth	30
Caso d'uso	32

Nota: le definizioni riportate nelle note a piè pagina sono tratte da Wikipedia.

Sintesi

Introduzione all'IoT

Con **Internet of Things** si intende l'estensione del concetto di Internet al mondo degli oggetti e luoghi concreti.

Gli **oggetti (smart)**:

1. si rendono riconoscibili (identificazione);
2. comunicano dati su loro stessi (connessione);
3. accedono a dati o informazioni aggregate di altri (capacità di elaborare dati).

In particolare, risulta rilevante la problematica della **sicurezza e privacy**: qualsiasi tipo di *device*, essendo connesso ad una rete, diventa un punto di attacco potenziale. Le regole base per prevenirlo sono **password** e **cifratura**.

Per poterlo comprendere il mondo dell'IoT, è necessario conoscere alcuni elementi:

- ☐ **sensori**, dispositivi input di rilevamento che raccolgono informazioni dall'ambiente fisico;
- ☐ **attuatori**, dispositivi output per controllare un processo, seguire un'azione o influenzare le condizioni dell'ambiente esterno;
- ☐ **microcontrollori**, dispositivi elettronici integrati su singolo circuito elettronico che contengono RAM, CPU e tutto ciò che serve a svolgere le funzionalità tipiche di un microprocessore per pc, ma in sistemi *embedded* (per applicazioni specifiche di controllo digitale);
- ☐ **gateway**, un nodo centrale che raccoglie i dati e permette di utilizzare al minimo le risorse per la comunicazione;
- ☐ **carrier**, il tipo di rete che permette la connessione ad internet e trasferimento di dati (vedi Wi-Fi, 5G, etc.) ad un *server* di *storage* che, a sua volta, organizza i dati e li fornisce agli output.

Il paradigma che sta dietro l'IoT è quello di avere **Agenti Intelligenti**. Essi possono seguire diversi modelli di calcolo:

- ☐ **Edge computing**. Si tratta di un modello distribuito dove l'elaborazione dei dati avviene più vicino possibile a dove i dati vengono richiesti (in prossimità del sensore). È largamente **adottato nell'ambito dell'IOT**;
- ☐ **Cloud computing**. Si tratta di un paradigma di erogazione di servizi offerti su richiesta da un fornitore a un cliente finale attraverso la rete internet (come l'archiviazione, l'elaborazione o la trasmissione dati). È usato per i **dati meno 'time-sensitive'**.

Reti di telecomunicazioni

Internet of Things è da considerarsi come una rete di telecomunicazioni. Ma cosa sappiamo di queste ultime?

Partendo dalle origini di **Internet** (rete di dati), nato dall'elitario Arpanet (con il protocollo IP), ed arrivando all'attuale *www*, ovvero protocollo *http* per la connessione, in questa dispensa si racconta l'evoluzione della **rete di dati** e, in parallelo, di quella **telefonica**. La rete telefonica presenta come requisito fondante l'interattività e come caratteristica principale (relativa alla variante digitale) un bit rate variabile che ha comportato, negli anni, una

spasmodica ricerca di alternative al collegamento classico (**commutazione di circuito**), in quanto poco efficiente.

La soluzione trovata è la **commutazione a pacchetto** (adatta sia alla rete di dati che alla rete telefonica grazie al *Voice over IP*), che può però comportare congestione dei buffer di dati, motivo per cui risulta necessario il controllo di congestione (*Congestion Control*). Questo aspetto rischia di inficiare l'interattività: infatti, per lungo tempo, la soluzione è stata utilizzata solo per la rete di dati tra calcolatori (internet) e non per i telefoni, dove tale requisito è fondamentale.

In questo contesto, è dunque necessario specificare che l'IoT *M2M Communication*, ma di una **rete**, un'**infrastruttura globale che abilita nuovi servizi avanzati grazie all'interconnessione di oggetti fisici e virtuali**.

Si giunge a parlare delle **reti mobili**, in particolare della tanto discussa **rete 5G**, ultima evoluzione: è una rete fortemente densificata, con banda larga ad 1 Gbit, ritardo di trasmissione ridotto a 1 millisecondo e permetterà il *massive IoT* (1 milione di dispositivi per ogni metro). Tutti questi progressi sono resi possibili dai **due nuovi paradigmi delle telecomunicazioni**: *software define networking* (separazione software e hardware) e *network function virtualization* (macchine virtuali che girano su data centre).

Infine, nella presente dispensa vediamo anche alcune applicazioni di IoT:

- *Intelligent transportation service* (geometrie variabili e applicazioni di fluidodinamica al mondo dell'automotive);
- *Precise Agricultural Production* e in particolare LoRaWAN, soluzione dell'azienda Natech.

Introduzione a Zerynth

Zerynth, startup innovativa che offre una **piattaforma IoT** basata su programmazione dei microcontrollori con linguaggio python, mostra il proprio punto di vista sull'argomento, ponendo l'accento sulla distinzione importante tra linguaggio di programmazione di basso livello (C++, Assembly, etc) e di alto livello (Java, python, Java Script), il quale è più vicino al linguaggio naturale (commentato e ordinato).

La piattaforma Zerynth presenta la funzione di **ponte** tra hardware (ad esempio il suo *4zerobox*) e cloud (*zdm*), abilitando anche una serie di servizi resi da terze parti (quali il servizio di creazione di dashboard dai dati raccolti, fornito da Ubidots).

Nella parte *hands-on* della lezione, sono stati fatti vari esercizi step-by-step (con device fisico per chi era in aula e virtuale per chi era online).

Internet of Things

Introduzione all'IoT: gli elementi di base

Il termine “*Internet of Things*” (**IoT**) è nato da un ricercatore, Kevin Ashton, nel 1999: inizialmente, consisteva nel dare una maggiore capacità ai computer in modo che potessero, in qualche modo, vedere e sentire il mondo. Nel corso del tempo la definizione è stata **raffinata** e sono stati definiti i **principi** alla base: esistono degli oggetti che devono essere riconoscibili (**identificazione**), devono avere la capacità di comunicare dati su loro stessi (**connessione**) e devono poter accedere a dati aggregati di altri dispositivi (**capacità di elaborare i dati**).

Questi sono perciò i presupposti per considerare gli oggetti come **smart object** (dispositivi, apparecchiature, impianti e sistemi, materiali e prodotti tangibili, opere e beni, macchine e attrezzature).

Tali oggetti possono essere applicati in diversi contesti: Smart Home/Building, Smart Factory, Smart City, Smart Car, etc. Inoltre, le possibilità di connessione degli smart objects sono diverse:

- ☐ A corto raggio
- ☐ A lungo raggio (ad esempio utilizzando il 4G e il 5G)

Il settore IoT, attualmente, possiede una grande rilevanza: il suo mercato risulta in costante espansione (in Italia si stimava già dal 2019 che valesse 6,2 Miliardi di euro).

Una premessa: sicurezza e privacy

Un tema importante riguardante l'IoT è relativo alla **sicurezza e privacy**: è sicuramente necessario avere consapevolezza su quali sono i vantaggi nell'introdurre nuove tecnologie, ma anche sapere come trattare aspetti legati alla privacy nel momento di introduzione dei dispositivi IoT. Infatti, si ricevono in continuazione notizie relative ad attacchi informatici nei confronti di numerose aziende attraverso dispositivi IoT in quanto questi ultimi sono fonti di ingenti moli di dati.

“...negli ultimi tre anni qualcosa come un'azienda su 5 ha subito almeno un attacco ai propri ambienti Internet of Things” (società di ricerca Gartner nello studio “Worldwide IoT security spending forecast 2018-2021 per segment”).

Qualsiasi tipo di **device**, essendo connesso ad una rete, diventa un **punto di attacco potenziale**.

Da tale aspetto conseguono, perciò, alcune **regole base** per prevenirlo:

- ☐ Password e metodi di autenticazioni robuste;
- ☐ Cifratura (encryption).

Bisogna, in sintesi, avere consapevolezza dei limiti e possibilità di protezione dall'esterno, tenendosi sempre aggiornati su quelli che possono essere nuovi rischi poiché è un mondo molto dinamico.

Bisogna quindi fare in modo che tutte le componenti hardware abbiano sempre le componenti software aggiornate al fine di assicurare la massima protezione e il massimo livello di privacy.

Inoltre, anche i **dispositivi di storage** devono essere protetti da accessi indesiderati, non solo i **device per acquisire i dati**.

Perciò, con l'aiuto di esperti, dopo *attacchi a dispositivi IoT*, bisogna analizzare questi ultimi per implementare accorgimenti, in modo da evitarlo nel futuro.

I **dispositivi IoT** spesso sono **sottovalutati**, si pensa che siano dispositivi sensoriali passivi: rappresentano, invece, dei prolungamenti di capacità percettiva delle persone!

In questo senso possono essere visti come strumenti che possono portare ad avere un **occhio all'interno di un ambiente** in cui fisicamente non si può essere. Costando poco, possono sembrare davvero semplici oggetti, ma son sempre **punti di ingresso**.

Esistono, perciò, numerose strategie: ad esempio, nel caso di una rete aziendale molto ampia con tanti dispositivi connessi tra di loro, si potrebbero creare delle **sottoreti**, in modo tale che, se avviene un attacco, si limita ad una certa porzione di rete. Da tale soluzione deriva, però, il rovescio della medaglia: a volte non si tiene a mente che l'attacco ad una parte della rete poco importante rischia di compromettere tutto il resto perché si sottovaluta l'attacco, ritenendolo poco significativo.

Nell'ambito industriale, come vedremo nei paragrafi successivi, l'IoT riporta diverse **applicazioni (l-IoT)**:

- ❑ **Smart Factory**: permette il controllo della produzione in maniera avanzata, di implementare procedure di sicurezza sul lavoro con prezzi bassi e con grande pervasività, di gestire le merci e i rifiuti;
- ❑ **Smart Logistics**: risulta utile per la tracciabilità e monitoraggio della filiera tramite tag RFID (Radio-Frequency Identification) e sensoristica, monitoraggio della catena del freddo, gestione della sicurezza in poli logistici complessi, gestione delle flotte (ad esempio tramite GPS / GPRS)
- ❑ **Smart Lifecycle**: consente il miglioramento del processo di sviluppo di nuovi prodotti (ad esempio tramite dati provenienti da versioni precedenti dei prodotti connessi), end-of-life management e la gestione fornitori nella fase di sviluppo nuovi prodotti.

I dati che vengono acquisiti devono essere spesso rielaborati per **estrarne altre informazioni**.

Esempio: *Google Maps* è una raccolta dati in un certo istante utile ad avere informazioni geografiche e sul traffico, ma anche ad avere *trend* di evoluzione del traffico. I sensori in questo caso sono i tanti cellulari a cui accede Google che inviano informazioni sulla loro posizione e, in base alla velocità di spostamento, vengono ricavati dei modelli di traffico.

Esempio: esistono vasetti di medicine con sensori posti sulla chiusura o su un blister per verificare se viene aperto al fine di prelevare la pillola, così da permettere che l'operatore medico abbia consapevolezza se quella medicina è stata assunta dal paziente e, eventualmente, intraprendere operazioni per ricordare o chiedere al paziente di seguire le prescrizioni mediche.

A seguire si riportano le **caratteristiche (capacità chiave)** degli **oggetti smart**:

1. Poter rielaborare le informazioni
2. Comunicare in modalità bidirezionale
3. Essere riconfigurabili
4. Intraprendere azioni conseguenti ad eventi
5. Trasmettere dati in *real-time*, ovvero in tempo reale

Esistono una serie di **casi attuali** e **attuati** di intelligenza aggiunta a vari contesti, di cui riportiamo alcuni esempi conosciuti:

- ❑ Il monumento che comunica al turista informazioni sulla sua storia, abilitando ricostruzioni virtuali;

- ☐ L'autovettura che, comunicando i suoi dati sul tipo di guida, permette di fornire informazioni non solo per il monitoraggio del traffico, ma anche dati utili alle assicurazioni per capire la dinamica di un incidente;
- ☐ Contatori di tipo digitale in casa che, evitando la lettura fisica, forniscono l'entità dei consumi, dalla quale si possono ricavare le abitudini dell'utente.

In tutti questi casi ci sono diverse **problematiche**:

- ☐ Costi ingenti;
- ☐ Problemi di privacy e sicurezza;
- ☐ Implicazioni derivanti da un utilizzo non efficiente dei dispositivi.

Definizioni e tipologie

Vediamo in questo sotto-paragrafo alcune definizioni cardine del mondo IoT.

I **sensori** sono dispositivi di rilevamento che raccolgono informazioni dall'ambiente fisico in cui si trovano.

Gli **attuatori** sono dispositivi per controllare un processo, eseguire un'azione o influenzare le condizioni dell'ambiente esterno in cui si trovano.

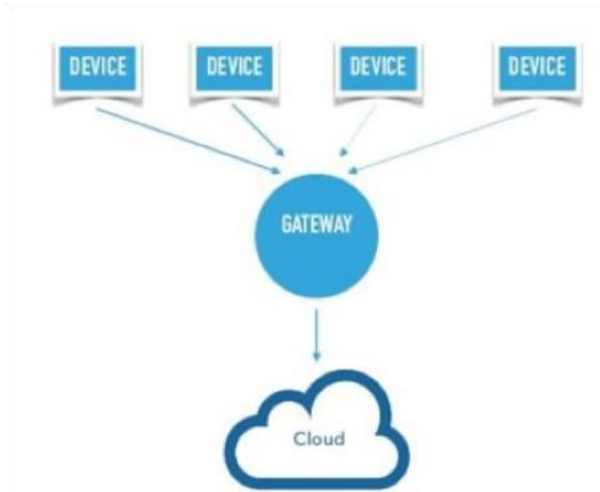
In alcuni casi i dispositivi periferici rivestono il **duplice ruolo** di **dispositivi di rilevamento** e di **azionamento** per raccogliere dati dell'ambiente fisico ed effettuare il controllo.

Sensori SMART

Le **caratteristiche** chiave sono le seguenti:

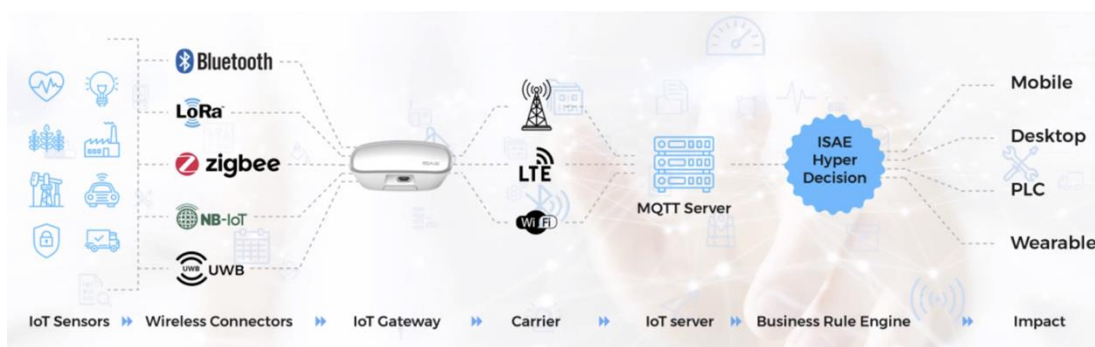
- ☐ Tecnologia di sensing: determina il tipo di dato o dati rilevabili e le prestazioni ottenibili;
- ☐ Alimentazione: fattore principale che determina l'autonomia e la durata di funzionamento del dispositivo, la sua collocazione e alloggiamento nell'ambiente;
- ☐ Elaborazione e memoria: dipendono dall'intelligenza richiesta per determinare i dati desiderati in uscita e le capacità di mantenere una collezione di misure e informazioni (anche esterne) nel tempo. Si può fare una rilevazione a intervalli diversi, perciò il meccanismo di memoria potrebbe permettere di vedere, ad esempio, un intero pacchetto o gli ultimi dati.
- ☐ Comunicazione: deve essere possibile stabilire una comunicazione affidabile, sicura e protetta per mezzo della rete.

Immaginiamo ora di dislocare nell'ambiente diversi **dispositivi a basso costo** (che possono misurare informazioni e parametri variegati).



Tali *device* sono collegati fra loro attraverso un nodo centrale che raccoglie i dati locali (**Gateway**): esso permette di utilizzare al minimo le risorse per la comunicazione, raccogliendo i dati con la frequenza richiesta dai device stessi (che nel mentre potrebbero essere in sospensione per risparmiare batteria e accendersi solo all'occorrenza).

La freccia in figura indica il *flusso dei dati*, ma si può immaginare anche nel verso opposto: dal *Cloud* (esterno) si può dirigere verso il Gateway, che a sua volta manda i dati ai device per supportare alcune operazioni.



Approfondendo ulteriormente, è importante specificare che nel mercato sono presenti numerosi **ambienti con sensori IoT** (in figura, a sinistra), una serie di **connessioni wireless a breve distanza** che li connettono al **gateway** e poi vari **provider** che offrono **connessione a maggiore distanza**. Spesso i provider possiedono anche un **server** che si occupa dell'immagazzinamento dei dati, permettendo di avere il dato trasformato e condiviso a diversi **device** (PLC, desktop, mobile, etc).

Sensori classici

Per completezza, ripassiamo alcune **caratteristiche** fondamentali dei sensori classici, indipendenti da applicazioni nel **mondo IoT**:

- **Sensibilità.** Essa viene definita come la pendenza della curva caratteristica di uscita, oppure, più in generale, l'ingresso minimo del parametro fisico che creerà una variazione rilevabile dell'uscita, ovvero la divergenza dalla pendenza ideale della curva caratteristica.
- **Gamma.** Si tratta del massimo e minimo valore misurabile del parametro applicato, e la gamma dinamica, cioè la gamma totale del sensore, dal valore minimo a quello massimo.
- **Precisione.** Si tratta del grado di ripetibilità di una misurazione.
- **Risoluzione.** È la più piccola variazione incrementale del parametro di ingresso rilevabile nel segnale di uscita.
- **Accuratezza.** Si tratta della differenza massima tra il valore effettivo e il valore indicato in uscita al sensore.
- **Offset.** È l'uscita che si verifica rispetto all'uscita zero che dovrebbe verificarsi, oppure la differenza tra il valore di uscita effettivo e quello specificato in condizioni particolari.

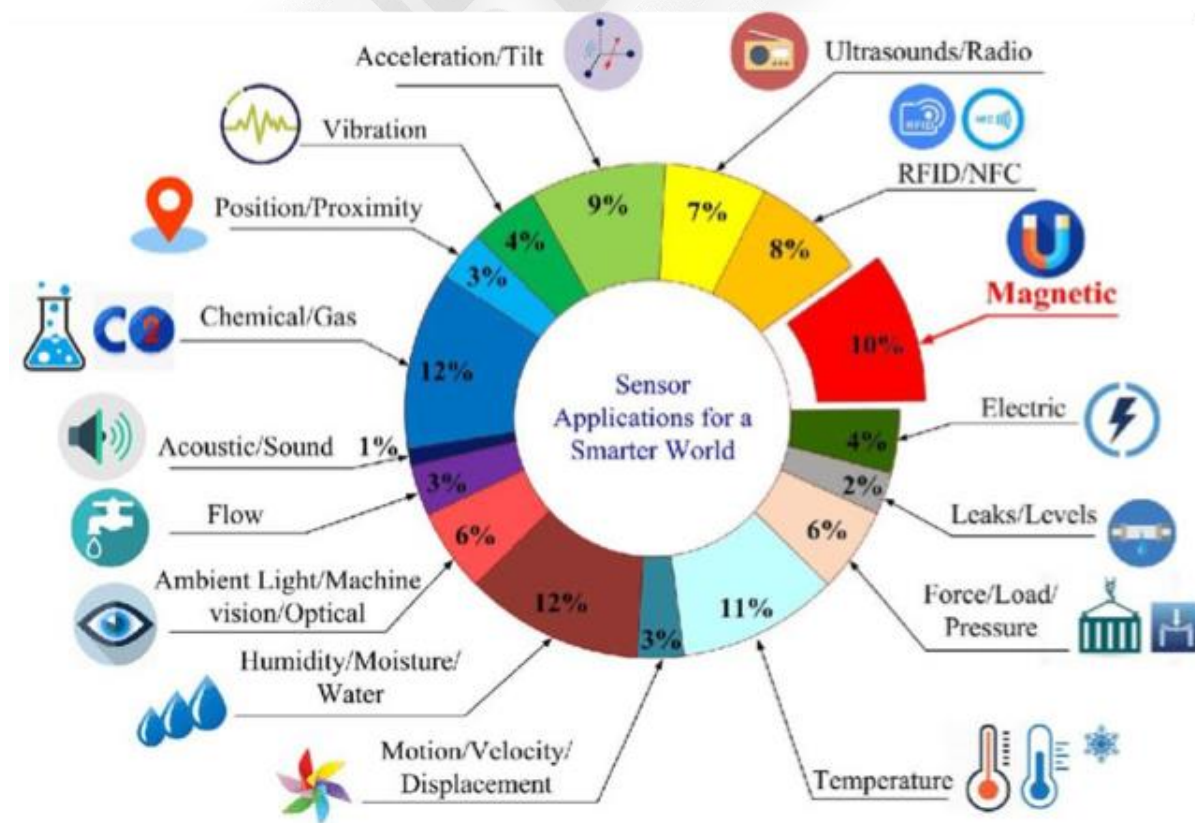
- ❑ **Linearità.** Essa è la misura in cui la curva effettiva di un sensore devia dalla curva ideale: ad esempio, siamo sicuri che un cambio di temperatura dello stesso intervallo comporti lo stesso spostamento di mercurio?
- ❑ **Isteresi.** Si intende l'efficacia con cui un trasduttore è capace di seguire le variazioni del parametro di ingresso indipendentemente dalla direzione da cui avviene la variazione.
- ❑ **Tempi di risposta.** Esso è il tempo richiesto per la variazione dell'uscita del sensore dalla condizione precedente fino a un valore finale stabilito entro una fascia di tolleranza del nuovo valore corretto.
- ❑ **Linearità dinamica.** Si tratta della misura della capacità di un sensore di seguire variazioni rapide nel parametro di ingresso: come varia l'uscita della misura al variare dell'input (che subisce variazioni rapide)?

I **fattori chiave nella scelta** dei sensori sono:

- ❑ Costo
- ❑ Facilità con cui l'uscita del sensore si interfaccia con l'elettronica di misurazione e controllo (generalmente un microcontrollore).

Interfacciare dei comuni sensori per le applicazioni IoT è relativamente semplice, in quanto esistono solo **tre tipi di uscita**: analogica, modulata (che utilizza una tecnica come la modulazione della larghezza d'impulso) o digitale (che utilizza interfacce standard di comunicazione seriali come SPI o I2C).

A seguire una figura che rende conto della vastità di sensori attualmente utilizzabili nel mondo: da un'indicazione del mercato.



MEMS

“La rivoluzione della nanotecnologia”

I **MEMS** (Micro Electro-Mechanical Systems) sono dispositivi a basso costo: con una tecnologia complessa è possibile realizzare micro-prodotti con costo unitario basso grazie alla **miniaturizzazione**. Essi sono:

- **dispositivi di varia natura** (meccanici, elettrici ed elettronici) integrati in forma altamente miniaturizzata su uno stesso substrato di materiale semiconduttore, ad esempio silicio;
- coniugano le **proprietà elettriche** degli integrati a semiconduttore con proprietà **opto-meccaniche**¹;
- **sistemi "intelligenti"** che abbinano funzioni elettroniche, di gestione dei fluidi, ottiche, biologiche, chimiche e meccaniche in uno spazio ridottissimo, integrando la tecnologia dei sensori e degli attuatori e le più diverse funzioni di gestione dei processi.

Il funzionamento di tali dispositivi si basa sui seguenti elementi:

- Il **circuito integrato** è il "cervello" del sistema che rende possibile il monitoraggio dell'ambiente circostante tramite gli altri dispositivi sensoriali presenti sullo stesso chip;
- Il **sistema raccoglie le informazioni** misurando fenomeni meccanici, termici, biologici, ottici e magnetici;
- **l'elettronica processa** le informazioni derivate dai sensori e reagisce **abilitando gli attuatori** a rispondere tramite movimenti, posizionamenti, filtrazioni, pompaggi o anche ri-verificando, tramite gli stessi sensori, le variazioni avvenute nell'intervallo di tempo nell'ambiente circostante.

Il sistema, dunque, è in grado di captare informazioni dall'ambiente traducendo le grandezze fisiche in impulsi elettrici, di elaborare tali informazioni facendo uso di opportune logiche ed, infine, di rispondere con alcune azioni.

I sensori possono misurare **fenomeni di varia natura**: meccanica (ad esempio suoni, accelerazioni e pressioni), termica (temperatura e flusso di calore), biologica (potenziale cellulare), chimica (pH), ottica (intensità della radiazione luminosa, spettroscopia), magnetica (intensità del flusso).

Vantaggi

A seguire si riportano alcuni vantaggi di questa tecnologia:

- Le tecnologie MEMS promettono di **rivoluzionare intere categorie di prodotti** proprio per il fatto di integrare in uno stesso dispositivo le funzioni più diverse: il minuscolo chip di silicio diventa un sensore di pressione, un accelerometro, un giroscopio, etc;
- I MEMS sono in grado di eseguire le **stesse funzioni** di rilevazione, elaborazione e attuazione di **oggetti molto più ingombranti e costosi**.

Curiosità: Esiste un'ulteriore evoluzione nei sistemi nano-elettromeccanici o **NEMS** (miniaturizzazione alla nano-scala).

¹ L'opto-meccanica il sottocampo della fisica che coinvolge lo studio dell'interazione della radiazione elettromagnetica (fotoni) con i sistemi meccanici tramite pressione di radiazione o la fabbricazione e la manutenzione di parti e dispositivi ottici.

Curiosità: Esistono anche i **Bio-MEMS**, sistemi micro-elettromeccanici biomedici/biologici, evoluzione dei LOC² (Lab-On-Chip), che permettono di eseguire analisi in maniera veloce, efficiente e complessa in spazi ridotti.

Applicazioni

A seguire si riportano alcuni esempi di applicazione:

- ☐ Microscopici specchi o lenti oscillanti in versione singola o *array* che vengono usati per realizzare complessi **apparati opto-elettronici**³, quali per esempio: commutatori per segnali laser, sensori per telescopi, lenti deformanti e proiettori e display avanzati;
- ☐ Nella chimica e bioingegneria vengono utilizzati per realizzare **micromotori elettrici** del diametro di due millimetri e della lunghezza di dieci, ingranaggi epicicloidali inclusi.
- ☐ Nell'elettronica delle microonde sono usati per realizzare **sfasatori**, reti di adattamento, filtri risonanti, reti di alimentazioni per antenne array ed in genere sistemi riconfigurabili.

Sensori indossabili

Stanno assumendo sempre più importanza i **sensori indossabili**, ovvero direttamente posti sull'uomo, allo **scopo** di:

- ☐ monitorare parametri relativi al benessere fisico;
- ☐ rilevare movimenti ed attività;
- ☐ aumentare le capacità percettive dell'utente (*smart glasses* che proiettano sull'asset informazioni che non sono presenti nell'ambiente reale, tali da far percepire l'ambiente in maniera differente);
- ☐ monitorare i parametri ambientali in prossimità dell'utente, quindi indicatori esterni ma relativi alla posizione dell'uomo.

In futuro saranno sempre **meno invasivi e sempre più miniaturizzati**, addirittura posti direttamente sulla pelle oltre che integrati nei capi di abbigliamento e in accessori.

Ad esempio, attualmente sono presenti sul mercato consumer: *smart watches*, *fitness tracker* e *smart glasses*.

ATT! Un esempio di sensore invasivo è invece la cuffia che rileva i segnali del nostro cervello, usati soprattutto in casi di difficoltà di capacità cognitive.

Sensori ambientali nelle smart city

Nel caso di sensori ambientali installati in **ambito urbano** (spesso sulla pubblica illuminazione):

- sono distribuiti capillarmente sul territorio;
- riescono ad accedere ad una sorgente elettrica facilmente;
- sono una garanzia sull'avere un certo spazio non coperto da ostacoli;

² *Lab-on-a-chip* (LOC) è un termine per un dispositivo che integra funzioni multiple che si possono svolgere in laboratorio in un singolo chip che va da pochi millimetri a qualche centimetro quadrato di grandezza ed è capace di trattare volumi di fluidi estremamente piccoli, sotto i microlitri.

³ L'optoelettronica è la branca dell'elettronica che studia i dispositivi elettronici che interagiscono con la luce e le loro applicazioni, facendo da interfaccia tra il dominio elettrico e quello ottico e viceversa; in questa definizione il termine luce va inteso in senso lato includendo radiazioni elettromagnetiche non percepibili all'occhio umano come raggi gamma, raggi X, radiazione ultravioletta e radiazione infrarossa. In genere l'optoelettronica è considerata una branca della fotonica.

- sono usati per il rilevamento di gas inorganici e composti organici volatili (per gestire situazioni di smog troppo intenso, agendo con decisioni della PA) o particolato con dispositivi ottici;
- sono utilizzati per rilevare l'inquinamento acustico.

Sensori per ambienti industriali

L'ambiente industriale è un ambiente operativo, spesso difficile, in cui i sensori devono svolgere la loro funzione in modo affidabile e a lungo termine, se possibile senza troppi interventi di manutenzione.

Sono quindi **versioni robuste** adatte alle linee di produzione industriale e agli impianti industriali.

Si utilizzano metodi di misurazione idonei alle condizioni ambientali (per esempio, non deve essere influenzato dall'accumulo di polvere e di sporcizia, olio o umidità):

- ☐ Per la produzione in **campo alimentare o farmaceutico** devono essere in grado di resistere alle normali procedure di pulizia ad alta pressione;
- ☐ Per il funzionamento in **ambienti potenzialmente esplosivi**, sono necessari sensori certificati ATEX⁴.

Si intende quindi costi e applicazioni specifici.

Sensori nell'Industria 4.0

Considerando le **3 dimensioni** della digitalizzazione del manifatturiero (lo *smart product*, lo *smart manufacturing* e i *cambiamenti nei business model delle aziende*), l'introduzione di **sensori intelligenti e comunicanti** fornisce il supporto necessario per:

- ☐ l'introduzione di **sistema autonomi, intercomunicanti e intelligenti** che sfruttano tutti i dati sensoriali a disposizione nell'ambiente, così da raggiungere livelli di automazione elevati e in grado di adattarsi e introdurre la robotica collaborativa (interagiscono con gli uomini);
- ☐ realizzare un **Digital Twin**: rappresentazione dell'impianto che permette analisi, predizione, simulazione della filiera senza interruzione del ciclo produttivo poiché tutto simulato.

I modelli di elaborazione del dato

Il luogo dove risiede l'elaborazione determina il **modello**:

- ☐ *Edge computing* è un modello di calcolo distribuito nel quale l'elaborazione dei dati avviene più vicino possibile a dove i dati vengono richiesti (in prossimità del sensore);
- ☐ *Cloud computing* è un paradigma di erogazione di servizi offerti su richiesta da un fornitore ad un cliente finale attraverso la rete internet (come l'archiviazione, l'elaborazione o la

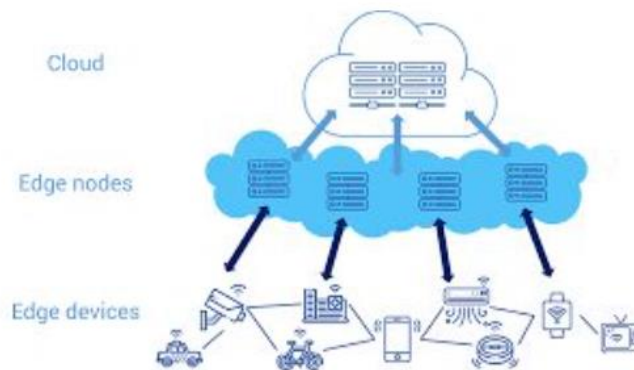
⁴ **ATEX** è il nome convenzionale che raggruppa due direttive dell'Unione europea:

- la *2014/34/UE* per la regolamentazione di apparecchiature destinate all'impiego in zone a rischio di esplosione; la direttiva si rivolge ai costruttori di attrezzature destinate all'impiego in aree con atmosfere potenzialmente esplosive e si manifesta con l'obbligo di certificazione di questi prodotti; la direttiva *94/9/CE* risulta da questa abrogata con effetto decorrente dal 20 aprile 2016;
- la *99/92/CE* per la sicurezza e la salute dei lavoratori in atmosfere esplosive; si applica negli ambienti a rischio di esplosione, dove impianti ed attrezzature certificate sono messe in esercizio ed è quindi rivolta agli utilizzatori.

Il nome deriva dalle parole *ATmosphères* ed *EXplosives*.

trasmissione dati), a partire da un insieme di risorse preesistenti, configurabili e disponibili in remoto sotto forma di architettura distribuita;

- ☐ **Fog computing:** è uno strato di intermediazione di dispositivi IoT rispetto a quelli di cloud.



Vantaggi dell'Edge computing

- ☐ Si hanno **tempi di risposta** molto più **rapidi**;
- ☐ Si ha una **riduzione del traffico di dati** (risiedono e vengono elaborati in primis sul dispositivo), trasferendo **solo dati composti**;
- ☐ Comportano **maggiore resilienza in caso di interruzione della connessione** dati: anche se manca, il sensore continua a rilevare.

È un modello computazionale largamente **adottato nell'ambito dell'IOT** in quanto:

- ☐ permette di elaborare grosse quantità di dati prodotti localmente ed eventualmente inviare a sistemi remoti una loro elaborazione molto più compatta;
- ☐ può anche essere sfruttato in architetture quali quella del **5G** per fornire ai dispositivi connessi servizi locali con risposte in tempo reale, difficilmente realizzabili con architetture Cloud.

Vantaggi del Cloud computing

- ☐ **Abbattimento di costi** di hardware, software e competenze specifiche;
- ☐ Disponibilità di **servizi flessibili su richiesta**:
 - ✓ **SAAS** (*software as a service*) - utilizzo di programmi installati su un server remoto, cioè fuori del computer fisico o dalla LAN locale, spesso attraverso un server web;
 - ✓ **DAAS** (*data as a service*) - con questo servizio vengono messi a disposizione via web solamente i dati, ai quali gli utenti possono accedere tramite qualsiasi applicazione come se fossero residenti su un disco locale;
 - ✓ **HAAS** (*hardware as a service*) - con questo servizio l'utente invia dati ad un computer messo a disposizione, i quali vengono elaborati e restituiti all'utente iniziale;

Quindi il **Cloud** può convenire perché:

- ☐ si paga in misura proporzionale all'utilizzo;
- ☐ si paga in relazione alla crescita;
- ☐ non ci sono costi di ammortamento;
- ☐ è semplice da gestire;
- ☐ serve per focalizzarsi sul business principale;
- ☐ si delega a terzi la gestione tecnologica e manutentiva e la sicurezza e privacy.

L'approccio usuale

Di solito, si tende ad utilizzare in contemporanea entrambe le modalità: con l'*Edge computing* si elaborano i **dati critici**, sensibili alla latenza, nel punto di origine tramite uno smart device, oppure inviandoli a un server intermedio localizzato in prossimità (le informazioni vanno elaborate in 'near real-time' o in 'real-time'); i **dati meno time-sensitive** possono invece essere trasmessi all'infrastruttura *cloud* o al Data Center dell'impresa, per:

- ☐ consentire elaborazioni più complesse, come l'analisi di big data;
- ☐ svolgere attività di *training* per affinare l'apprendimento degli algoritmi di machine learning (ML);
- ☐ fare lo storage di lungo periodo;
- ☐ analizzare dati storici.

Intelligenza artificiale nell'IoT

L'intelligenza artificiale si riferisce ad un livello di metodologie e processi replicanti più possibile l'intelligenza umana.

Artificial Intelligence is the science of making computer software that reasons [and learn] about the world around it. Humanoid robots, Google Goggles, self-driving cars, even software that suggests music you might like to hear are all examples of AI...
(Norvig & Thrun, 2011)

Nel corso del tempo, si è passati da un **approccio classico** della programmazione di software ("DATI e PROGRAMMI"), ad uno nuovo costituito da "**CONOSCENZA e RAGIONAMENTO**".

Agli albori dell'AI i successi principali in ambito commerciale sono state le applicazioni conosciute come **Sistemi Esperti**. Adesso, l'AI è rifulsa grazie alla grande disponibilità di dati e di risorse computazionali che hanno reso possibile l'implementazione delle cosiddette metodologie di **Deep Learning**, di cui si parlerà nel prossimo Modulo.

Il Machine Learning

L'**apprendimento automatico** (*Machine Learning*) è una branca dell'intelligenza artificiale che raccoglie metodi sviluppati negli ultimi decenni del XX secolo in varie comunità scientifiche, sotto diversi nomi:

- ☐ statistica computazionale
- ☐ riconoscimento di pattern
- ☐ reti neurali artificiali
- ☐ filtraggio adattivo
- ☐ teoria dei sistemi dinamici
- ☐ elaborazione delle immagini
- ☐ data mining
- ☐ algoritmi adattivi.

Machine Learning (o ML) è l'insieme di metodologie e metodi statistici per migliorare la performance di un **algoritmo** nell'**identificare pattern nei dati**.

Nell'ambito dell'informatica, l'apprendimento automatico è una variante alla programmazione tradizionale nella quale in una macchina *si predispone l'abilità di apprendere qualcosa dai dati in maniera autonoma, senza istruzioni esplicite*.

In altre parole, la macchina acquisisce **la capacità dei modelli di generalizzare**: si intende l'abilità di una macchina di portare a termine in maniera accurata esempi o compiti nuovi, che non ha mai affrontato, dopo aver fatto esperienza su un insieme di dati di apprendimento.

Esistono vari **tipi** di apprendimento automatico:

- ☐ apprendimento **supervisionato**, in cui al modello vengono forniti degli esempi nella forma di possibili input e i rispettivi output desiderati e l'obiettivo è quello di estrarre una *regola generale* che associ l'input all'output corretto;
- ☐ apprendimento **non supervisionato**, in cui il modello ha lo scopo di trovare una struttura negli input forniti, senza che gli input vengano etichettati in alcun modo.
- ☐ apprendimento per **rinforzo**, in cui il modello interagisce con un ambiente dinamico nel quale cerca di raggiungere un obiettivo (per esempio guidare un veicolo), avendo un insegnante che gli dice solo se lo ha raggiunto o meno.

L'**Output** dell'apprendimento automatico dipende dal tipo di analisi svolta:

- ☐ **Classificazione**. Gli output sono divisi in due o più classi e il sistema di apprendimento deve produrre un modello che assegni gli input non ancora analizzati ad una o più di queste (in genere tramite apprendimento supervisionato);
- ☐ **Regressione**. Anch'essa è relativa ad un problema supervisionato e l'output (come anche il modello) risulta continuo;
- ☐ **Clustering**. Si tratta di un insieme di input che viene diviso in gruppi. Diversamente da quanto accade per la classificazione, i gruppi non sono noti a priori, rendendolo tipicamente un compito non supervisionato.

Rispetto all'IoT, i **vincoli** del **ML** sono i seguenti:

- ☐ Potenza computazionale richiesta elevata e difficilmente ottenibile con i microcontrollori presenti su oggetti smart;
- ☐ Energia richiesta elevata a fronte di una limitata autonomia del dispositivo smart;
- ☐ Tempi di risposta richiesti variabili secondo l'esigenza (avere dati in real-time o meno), aspetto non sempre compatibile con il funzionamento di un dispositivo IoT;
- ☐ Rischi di privacy nel comunicare dati.

Esistono vari tipi di **architettura del ML** applicabili al mondo IoT:

- ☐ Inferenza (riconoscimento) e il training (addestramento) da **Cloud**. In questo modo il Cloud restituisce il modello (ottenuto dall'addestramento) che risiede nel dispositivo;
- ☐ Inferenza sul Cloud senza servizio di addestramento. L'applicazione sul dispositivo invia una richiesta al Cloud mediante una **API (Application Programming Interface)**⁵, inoltrando anche i dati. Il servizio sul Cloud restituisce una predizione.
- ☐ Inferenza sul dispositivo con modelli pre-addestrati. Si tratta di applicazioni IoT che richiedono latenza minima.

⁵ In un programma informatico, con Application Programming Interface (API) si indica un insieme di procedure (in genere raggruppate per strumenti specifici) atte all'espletamento di un dato compito; spesso tale termine designa le librerie software di un linguaggio di programmazione.

Il Deep Learning

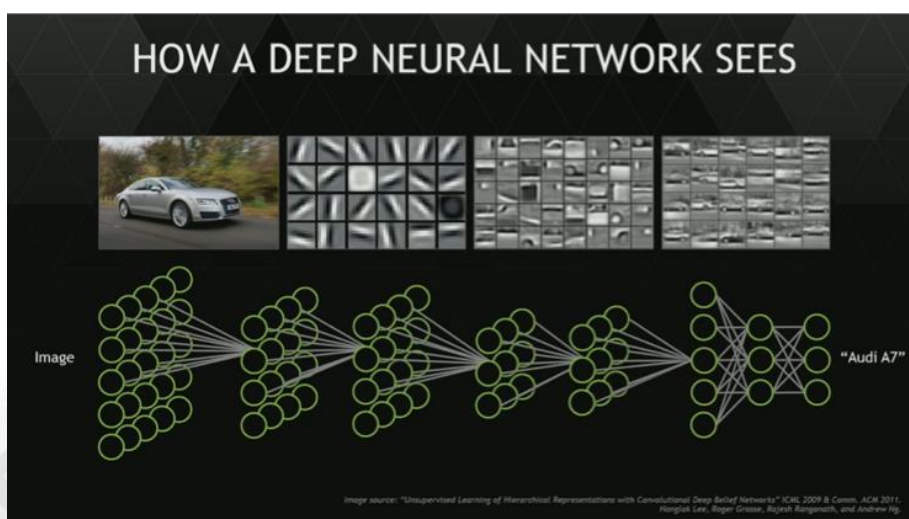
Si tratta di una **classe di algoritmi di apprendimento automatico** noti da anni, ma di cui non si avevano le risorse computazionali né le moli di dati odierni:

- usano vari livelli di unità non lineari a cascata per svolgere compiti di estrazione di caratteristiche e di trasformazione;
- ciascun livello successivo utilizza l'uscita del livello precedente come input;
- gli algoritmi possono essere sia di tipo supervisionato sia non supervisionato e le applicazioni includono l'analisi di pattern (apprendimento non supervisionato) e classificazione;

Esempio: abbiamo un'immagine come input sensoriale di una rete neurale e si vuole che questa rete riconosca il modello di auto Audi A7 (con precisione quasi al 100%).

Ogni stadio è molto complesso: i dati contribuiscono a elaborazioni sofisticate.

La rete impara a riconoscere dall'immagine degli stimoli (i contorni della macchina). A partire da ciò, gli altri strati della rete riconoscono componenti della macchina e, dalla composizione di questi sotto elementi, si possono riconoscere i vari modelli di auto.



È necessario però partire da un **presupposto**: gli **esempi in ingresso devono essere diversificati** (varie macchine con il modello e marca che si vuole distinguere, ma inserite in diversi scenari e angolature).

OSS: Il Deep Learning può utilizzare anche testi e audio. Anche in questo caso, i dati sensoriali diversi possono essere combinati fra loro per ottenere l'informazione giusta di classificazione, riconoscimento, clustering etc.

Gli Agenti Intelligenti nell'IoT

In sintesi, il **paradigma che sta dietro l'IoT** è di avere **Agenti Intelligenti**: un agente è un sistema computazionale, costituito da un programma software ed eventualmente da un supporto hardware, che:

- ☐ interagisce con l'ambiente circostante ed è **reattivo** agli stimoli di tale ambiente;
- ☐ è capace di prendere decisioni, e di conseguenza di agire, in modo autonomo, con il fine di raggiungere un obiettivo chiamato generalmente *goal* (che può essere predefinito o negoziato). Pertanto, può essere definito agente **proattivo**;
- ☐ è in grado di comunicare (coordinarsi, cooperare, negoziare) con altri agenti (e/o con esseri umani), quindi è capace di **interazione sociale**.

Ne esistono **varianti** incentrate sull'utilità, sull'apprendimento, operanti per obiettivi o con semplici riflessi ad input esterni.

Possono nascere anche dei **Sistemi multi-agente (MAS)**, ovvero costituiti da più agenti che interagiscono tra loro e che comunicano con messaggi per realizzare comportamenti sempre più sofisticati e complessi. L'evoluzione di tali sistemi porta agli **agenti 4.0**.

Un **agente intelligente embodied**, o robot (4.0) autonomo, dispone di:

- ☐ sensori per la percezione dell'ambiente e dell'uomo. In particolare, per le seguenti finalità:
 - ✓ navigazione autonoma
 - ✓ interazione sociale
 - ✓ esecuzione di compiti (task)
- ☐ moduli software per la pianificazione e apprendimento
- ☐ un modello di rappresentazione della conoscenza
- ☐ una connessione a risorse computazionali e conoscenze esterne.

ATT! Un robot è equivalente ad un **veicolo autonomo**, ma potenziato e reso *smart* (così come anche l'ambiente in cui si trova).

Piattaforme di elaborazione dei dati sensoriali

Per quanto riguarda l'**Edge Computing**, le **elaborazioni** possono avvenire sui **seguenti hardware**:

- ☐ **MCU (Microcontroller Unit)**. In elettronica digitale, è un dispositivo elettronico integrato su singolo circuito, nato come evoluzione alternativa al microprocessore e utilizzato generalmente in sistemi *embedded*, ovvero per applicazioni specifiche di controllo digitale.
- ☐ **SoC (System on a Chip)**. Si tratta di un circuito integrato che in un solo chip contiene un intero sistema, o meglio, oltre al processore centrale, integra anche un *chipset* ed eventualmente altri *controller* come quello per la memoria RAM, la circuiteria input/output o il sottosistema video.



Per quanto riguarda invece il **Cloud Computing**, ci sono **fornitori** con prezzi variabili a livello internazionale. Ognuno fornisce servizi specifici per l'intelligenza artificiale e di supporto all'IoT: software, dati, hardware, il tutto con interfacce semplificate, ma richiedendo conoscenza specifica dei costi e dei benefici del *Cloud* rispetto ad *Edge*. A seguire si riportano alcuni tra i più conosciuti fornitori e rispettive soluzioni.

FORNITORE	PIATTAFORMA
ABB	ABB Ability Platform
Amazon Web Services	AWS
Bosch	Bosch IoT Suite
C3.ai	C3 AI Suite; C3 AI Applications; C3 Integrated Development Studio (C3 IDS)
GE Digital	Predix Platform
Hitachi	Lumada
IBM	IBM Watson IoT Platform
Microsoft	Microsoft Azure IoT
Oracle	Oracle Internet of Things Cloud
PTC	ThingWorx
Samsung SDS	Brightics IoT
SAP	Leonardo IoT
Siemens	MindSphere
Software AG	Cumulocity IoT

Le reti di telecomunicazione

"Solo l'1% del PIL viene utilizzato per la ricerca e, di conseguenza, trasformato in idee"

La nascita di Internet

La conquista dello spazio causò la nascita di Internet. Il primo satellite fu lanciato dalla Russia nel 1957 (Sputnik) e, successivamente, anche gli Stati Uniti mandarono il proprio. L'Italia ha mandato il quinto, con il satellite San Marco.

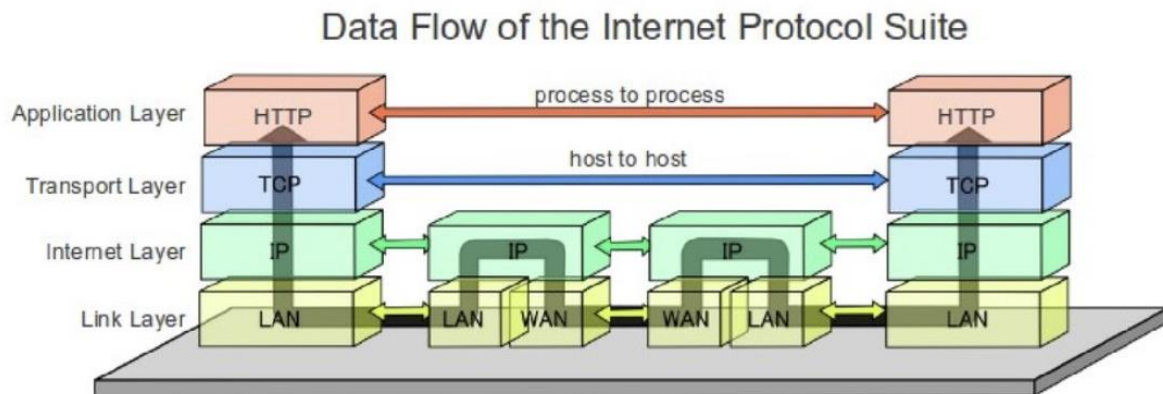
Jurij Gagarin fu stato il primo cosmonauta della storia ad andare nello spazio (1961). Gli americani, in risposta, fondarono un dipartimento intero (DARPA) dedicato ai progetti avanzati ("Il cervello del Pentagono"). Al DARPA nacque il progetto **ARPANET**⁶, dal quale, successivamente, vide la luce Internet.

ATT! Internet non è una **rete** fisica, ma **logica**, astratta, ovvero una virtualizzazione, un modo di spostare l'informazione.

⁶ ARPANET (acronimo di "Advanced Research Projects Agency NETwork", in italiano "Rete dell'Agenzia per i progetti di ricerca avanzati"), anche scritto ARPAnet o Arpanet, fu una rete di computer studiata e realizzata nel 1969 dalla DARPA, l'agenzia del Dipartimento della Difesa degli Stati Uniti responsabile dello sviluppo di nuove tecnologie ad uso militare di cui anche gli universitari potevano fare uso. Si tratta della forma per così dire embrionale dalla quale poi nel 1983 nacque Internet. Non era stata ideata, come solitamente si tende a pensare per scopi militari statunitensi, ma per collegare due università americane durante il periodo della guerra fredda. Gli sforzi per utilizzarla per la sicurezza nazionale avvennero molto dopo. Nacque così uno dei più grandi progetti civili, una rete globale che collega tutta la Terra.

I grandi dell'informatica progettarono una **struttura gerarchica** della rete internet:

- **TCP** (*Transmission Control Protocol*), ovvero un protocollo funzionante solo nella periferia della rete e avente funzione di valvola (controllore della rete);
- **IP** (*Internet Protocol*), protocollo container che “gira” su tutti i dispositivi, sia periferia che nodi intermedi (*router*⁷);
- **Hardware**, ovvero primo livello che cambia nel tempo e avente la funzione di trasportare bit in forma di blocchetti (“trame”).



ATT! Il **datagramma IP** è un'astrazione, ovvero un *container*. Esso rappresenta un integratore, un elemento di sviluppo della prima finalità che aveva la rete: l'interoperabilità (si voleva consentire a sistemi di interagire tra loro).

Le reti sviluppate dall'uomo

L'uomo ha dato vita a varie **tipologie di reti**:

- **Rete telefonica** (sviluppato a fine 1800, con anche trasmissione transoceaniche). Le sue caratteristiche:
 - monomediale (passa la voce);
 - tutte le sorgenti sono uguali fra loro;
 - ambito **interattivo**, ovvero, se la rete introduce ritardo superiore a 150 millisecondi, l'esperienza diventa sgradevole;
 - ormai digitale, trasmette bit che corrispondono alla nostra voce.

Se è presente un bit rate (ovvero la banda, cioè quanti bit escono dalla tua interfaccia al secondo, si può intervenire con modem più evoluti) più alto, non consegue che il ritardo si abbassa. Il **ritardo** è dovuto alla propagazione dei segnali nei mezzi trasmissivi e ad altri contributi.

⁷ Un router (lett. "*instradatore*") o commutatore, nelle telecomunicazioni e informatica, nell'ambito di una rete informatica a commutazione di pacchetto, è un dispositivo di rete usato come interfacciamento tra sottoreti diverse, eterogenee e no, che lavorando a livello logico come nodo interno di rete deputato alla commutazione di livello 3 del modello OSI o del livello 2 Internet nel modello TCP/IP, si occupa di instradare i pacchetti dati fra tali sottoreti permettendone l'interoperabilità (*internetworking*) a livello di indirizzamento.

ATT! Il *Tempo di trasmissione* è la quantità di bit diviso la velocità di propagazione (bit al secondo), mentre il *tempo di propagazione* è la distanza diviso la velocità della luce nel mezzo (non si può ingegnerizzare).

☐ **Rete televisiva.** Caratteristiche:

- ✓ è monodirezionale, opposta alla telefonia interattiva;
- ✓ non ha requisiti stringenti sul ritardo;
- ✓ ha requisiti sul bit rate, ovvero quest'ultimo dev'essere costante.

☐ **Rete di dati** (tra calcolatori). I calcolatori presentano la necessità di scambiarsi i dati, ma il **bit rate non occorre che sia costante.**

Rete telefonica

Tutti i laboratori di fisica occidentali sono da tempo a conoscenza che le onde elettromagnetiche si propagano in linea retta: Guglielmo Giovanni Maria Marconi (1874- 1937) capì che poteva sfruttarlo per realizzare il **telefono senza fili**. Però, pensare di usare l'ingegneria per la scienza all'epoca era assurdo: all'epoca si partiva sempre dall'astrazione.

La telefonia analogica divenne digitale, ma uno dei requisiti restò sempre **l'interattività**, successivamente risolto con il *voice constant* che filtra e capisce quando la sorgente vocale non sta generando parole, eliminando gli altri rumori e rendendo il bit rate variabile. La codifica della nostra voce è complessa, perciò il voice constant è necessario anche per risparmiare batterie. Tale funzionamento, però, risulta in contraddizione con il tradizionale **"tubo"** necessario per la trasmissione del bit rate: utilizzare un tubo per un bit rate variabile comporta uno spreco incredibile di risorse.

Rete di dati

La rete di dati, che poi è diventata la *Global Interaction Infrastructure*, inizialmente non era come la conosciamo.

Tutti coloro che ci hanno lavorato, sono partiti da un principio di progetto: hanno fatto la proposta per la rete sicura, flessibile, super operabile, capace di servire quel che conosciamo e quello che non conosciamo ancora.

Arpanet è nata con due servizi:

- ☐ *File transfer*,
- ☐ *Remote job entry* (condividere un programma da remoto).

Di conseguenza, anche **Internet è nato per questi due servizi.**

Sono morte diverse proposte al momento della nascita del **WORLD WIDE WEB**: la causa è da ricercarsi nel browser (MOSAIC), ovvero il primo browser creato, a cui non interessava la potenza di calcolo era facilmente utilizzabile da tutti. Arpanet, invece, era un progetto per pochi e utilizzabile da pochi.

Requisiti di internet

Internet presenta pochi ma fondamentali requisiti:

- ☐ **l'integrità dei dati.** Ad esempio: se ci rechiamo in banca e preleviamo 200 Euro, vogliamo avere la certezza dell'integrità di questa transazione;
- ☐ la **flessibilità**, ovvero un bit rate non costante;
- ☐ la **sicurezza**.

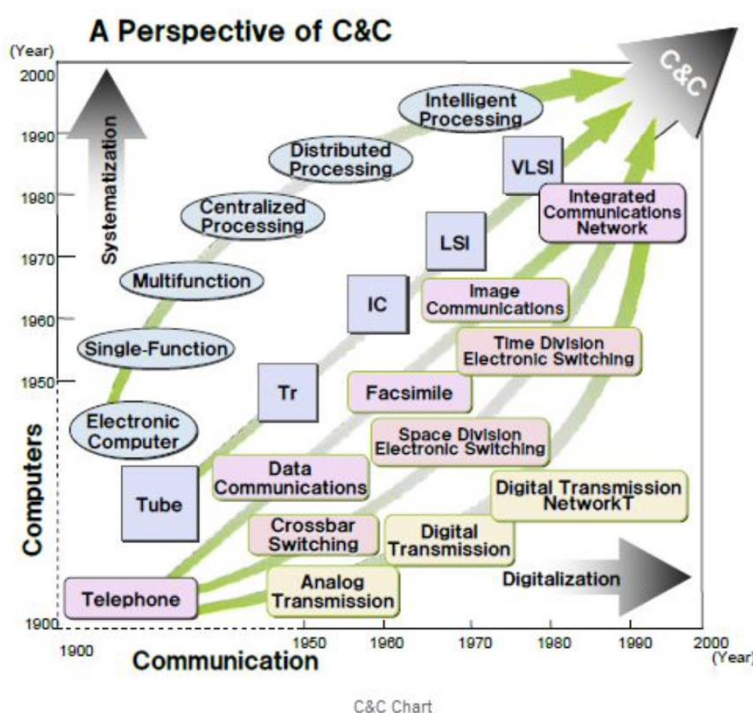
ATT! Internet funziona sia su reti mobili che fisse.

Ad oggi esistono **tantissimi protocolli**: nel tempo son stati aggiunti nel tentativo di migliorare (approccio evolutivistico).

Inoltre, ci sono delle proposte *disruptive* rispetto ad Arpanet o Internet (approcci “*clean slate*”): questo non significa che internet, in futuro, verrà cancellata, ma si costruiranno gateway, ovvero reti interoperabili con internet finalizzati a determinati settori.

Una di queste si chiama RINA, una *Name Data Networking*⁸ dove non si cerca l'indirizzo, ma direttamente il contenuto.

Le differenze tra le reti e la convergenza futura delle tecnologie



Sebbene fin dagli anni '50 esponenti del settore hanno predetto la convergenza delle reti di telecomunicazione, inizialmente queste ultime si sono sviluppate in maniera differente, come spiegato a seguire:

- ☐ **Rete Televisiva.** Essa affitta risorse e trasmette in prossimità della superficie terrestre: ha fatto più paura di tutti perché caratterizzata da un bit rate enorme.
- ☐ **Rete Internet.** È una rete complicata nella periferia e semplice all'interno (*Core Edge*).

⁸ Named Data Networking è una proposta di architettura Future Internet ispirata da anni di ricerca empirica sull'utilizzo della rete e una crescente consapevolezza dei problemi irrisolti nelle architetture Internet contemporanee come l'IP.

- **Rete Telefonica.** La rete telefonica risulta, invece, semplice nella periferia e complicata al suo interno: si tratta di una rete di organi di scambio (autocommutatori), ma sottende alla loro autoconfigurazione una rete di calcolatori (**rete di segnalazione** al canale comune).

Alcune specificazioni su questo tipo di rete:

- ✓ non è fatta solo dei nostri bit (PIANO DI UTENTE);
- ✓ è costituita da automatismi interni, ovvero da una parte che si configura da sola (PIANO DI CONTROLLO);
- ✓ esiste anche il PIANO DI GESTIONE che riguarda la comprensione di ciò che succede nella rete stessa.

L'aspetto più costoso e complesso della telecomunicazione è monitorare il piano di controllo.

La Commutazione

La prima vera rete di dati della storia fu in realtà il sistema **SAGE**, anche se non tutti lo sanno, realizzato dagli americani per paura di essere bombardati nel 1958: erano presenti sensori radar che rilevavano i bombardieri, li raffiguravano sui quadranti radar e comunicavano i dati via modem al centro di controllo tramite rete telefonica. Tuttavia, l'utilizzo di tale canale, ovvero di un circuito di telecomunicazioni all'epoca costosissimo per trasmettere solo dati sporadici dei calcolatori, era del tutto **inefficiente**. Per tale motivo, spesso SAGE non viene citata: è assurdo parlare di reti di sensori e intercettori con la modalità del "tubo" (**commutazione di circuito**⁹).

Un ingegnere, **Paul Baran**, nel '58 capì che la commutazione di circuito non aveva senso, però, neanche per la voce (dunque nella rete telefonica): la voce, quando viene trasmessa in modo digitale, costa troppo a causa dei silenzi e comporta quindi inefficienze. Allora propose di creare la rete a **commutazione di pacchetto**¹⁰: consiste nel mandare solo **pacchetti di bit** costanti ottenuti grazie al **Voice Detection**.

Tuttavia, nella rete telefonica, è necessario garantire uno specifico bit rate e interattività: tale problema si risolve con dei **store-and-forward buffer** (Voice over IP¹¹) per riempire i vuoti di uno coi pieni dell'altro, serializzando i telefoni per tenere il "tubo" sempre pieno (commutazione statistica, ovvero serializzare pacchetti uno dopo l'altro).

⁹ In una rete a commutazione di circuito la capacità del canale trasmissivo è interamente dedicata ad una specifica comunicazione. Essa si ha quando una parte della capacità trasmissiva totale in uscita al moltiplicatore è stabilmente assegnata a ciascun canale tributario in ingresso. Ciascun utilizzatore ha a disposizione un canale trasmissivo dedicato, con la garanzia di avere sempre disponibile tutta la capacità allocata ad ogni richiesta di servizio. Gli elementi intermedi, o centraline di comunicazione, creano circuiti fisici point-to-point. Le tariffazioni applicate alla commutazione di circuito sono tendenzialmente a tempo.

¹⁰ La commutazione di pacchetto si rivela molto più efficiente nonostante la maggior quantità di dati inviata, in quanto i canali fisici sono utilizzati solo per il tempo strettamente necessario. Inoltre, poiché ogni pacchetto porta con sé la sua identificazione, una rete può trasportare nello stesso tempo pacchetti provenienti da sorgenti differenti. Essa permette quindi a più utenti di inviare informazioni attraverso la rete in modo efficiente e simultaneo, risparmiando tempo e costi mediante la condivisione di uno stesso canale trasmissivo (cavo elettrico, ethernet, fibra ottica ecc.).

¹¹ Voice over IP (in italiano "Voce tramite protocollo Internet", in acronimo VoIP), in telecomunicazioni e informatica, indica una tecnologia che rende possibile effettuare una conversazione, analoga a quella che si potrebbe ottenere con una rete telefonica, sfruttando una connessione Internet o una qualsiasi altra rete di telecomunicazioni dedicata a commutazione di pacchetto, che utilizzi il protocollo IP senza connessione per il trasporto dati.

All'epoca, altri esponenti obiettarono che il buffer poteva riempirsi troppo e, di conseguenza, comportare la perdita di pacchetti. Oggi, per risolvere tale problematica, esiste infatti il **Congestion Control**¹².

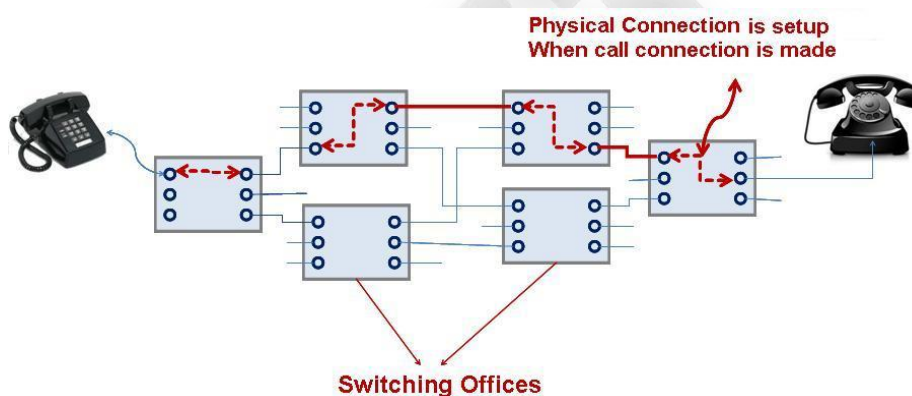
Fu chiaro fin da subito, però, che tale commutazione poteva essere applicata ai calcolatori, dove l'interattività non conta quanto nella rete telefonica: sono sorgenti a bit rate variabile, perciò la nuova modalità si prestava bene.

Ne deriva, dunque, che Internet si basa sulla **commutazione di pacchetto**.

Confronto sul trasporto dell'informazione

Prima di procedere, analizziamo la differenza tra le due commutazioni nel trasportare l'informazione:

- La rete telefonica si basava sulla **commutazione di circuito** ("tubo") che, inizialmente, era un circuito elettrico (analogico) e poi digitale (rullo trasportatore di bit *end to end*). Dato il costo ingente per costruirla, spesso si prevedeva al massimo un solo telefono per città.



Anche la successiva rete telefonica digitale allocava tubi per un servizio monodirezionale e interattivo.

Inizialmente si salvava un limitatissimo intervallo di frequenze per far entrare il più possibile nel tubo (4 kHz, da cui derivano 64 000 bit/s), tale per cui, ad esempio, una voce femminile era difficilmente distinguibile al telefono.

Per la rete di dati, questa commutazione sarebbe assurda avendo un flusso variabile di bit, ovvero non avendo il requisito di interattività.

Quindi, come anticipato, entra in gioco la **commutazione di pacchetto**: si possono "bufferizzare" le unità operative perché le sorgenti sono caratterizzate da bit rate variabile, ottenendo una elevata utilizzazione della linea che, di conseguenza, risulta sempre piena (quanto più è piena, tanto più viene ammortizzata la risorsa).

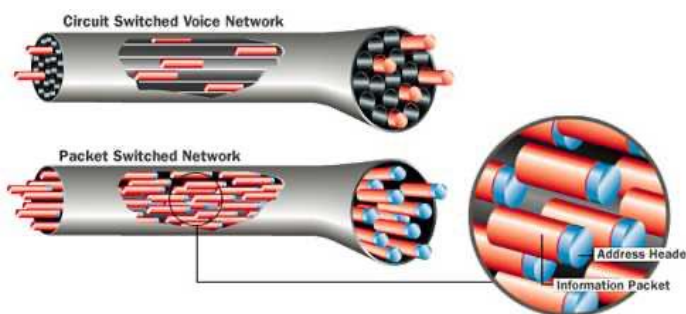
Come già detto, però, esiste il rovescio della medaglia: in tal modo, è necessario il controllo della congestione, ovvero una valvola che, se si rischia di perdere pacchetti di dati, trasmette

¹² In telecomunicazioni e informatica il controllo della congestione in TCP è una funzionalità di controllo di trasmissione da parte di TCP che permette di limitare la quantità di dati trasmessi sotto forma di pacchetti e non ancora riscontrati dal mittente, adattando il flusso dati inviato all'eventuale stato di congestione della rete. Tale stato è desunto indirettamente a partire da informazioni ricavabili dallo stato della trasmissione dei pacchetti da parte di un terminale, evitando così congestione nella rete stessa.

meno pacchetti al fine di riequilibrare il flusso. Tale ruolo di **valvola** è stato affidato al **TSP**: è il protocollo più complicato in assoluto.

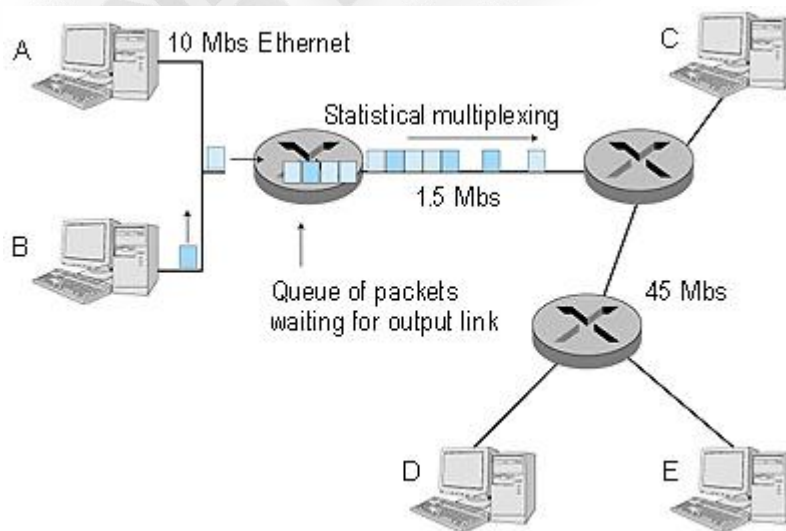
Perciò, il flusso di dati variabile tipico della rete internet deve essere controllato quest'ultimo e regolarlo in base al più lento delle sorgenti in comunicazione. Ne consegue che risulta difficile mantenere la trasmissione immediata per tutte le sorgenti: internet è di tutti, perciò nessuno ha la priorità. I router sono solo gli *end-system* che, quando si rendono conto di una perdita di pacchetti, rallentano a prescindere dal proprio ruolo trasportatore.

- Nella commutazione di circuito, esiste il concetto di **Time Division Multiplexing (TDM)**: il tubo fibra ottica viene diviso in tanti piccoli tubi, da cui si ottengono tanti spazi, cioè silenzi e quindi inefficienze. È come un'intermittenza: la comunicazione non è simultanea, si realizza una divisione del tempo della mia risorsa, con slot tutti uguali.



ATT! la rete telefonica digitale che utilizza la commutazione di circuito non è un circuito fisico, ma logico, con un rullo trasportatore di bit *end to end* necessario per non sopprimere i silenzi e avere al contempo flusso costante 64 mila bit/s.

La commutazione a pacchetti invece, facendo convergere tanti pacchetti sulla stessa fibra ottica, riesce a usarla al meglio, evitando i silenzi e vuoti tipici della commutazione di circuito.



Le reti e l'Internet of Things

Ad una fiera (*Interop*), è stato mostrato un tostapane collegato ad internet, primo oggetto IoT: esso utilizzava IP e SNMP, ovvero il protocollo di gestione. In generale, fin dal 2007 si sa cos'è l'Internet delle cose, ma si può affermare che sia effettivamente partito solo parlando di **identificatori**, cioè del tema di identificare un oggetto per costruire poi un sistema intero.

L'**RFID (RadioFrequency IDentification)**, come approfondiremo, è un oggetto passivo che non possiede batteria e contiene informazioni in un *tag* (dotato di antenna): il *reader* (dotato di antenna a sua volta) comunica a quest'ultimo l'energia nel momento in cui deve leggere la memoria al suo interno. Tale sistema viene chiamato **sistema bistatico** (due ricetrasmittitori necessari) e la parte difficile del funzionamento sono i protocolli di accesso.

Vediamo alcune **applicazioni** non convenzionali della tecnologia RFID:

- ❑ **Sensing:** limitatamente a certe grandezze (esempio: umidità, temperatura). L'antenna si deforma per la temperatura e quindi si può rilevare un segnale riflesso diverso per ogni temperatura.
ATT! In questo caso, gli RFID non avranno mai le caratteristiche di un sensore digitale specifico per quel dominio.
- ❑ **Localizzazione:** leggere e simultaneamente localizzare. Ad esempio: esiste un oggetto commerciale che riesce a localizzare oggetti aventi RFID nel raggio di 1 metro.
La parte complessa, in tal caso, è l'interfaccia per presentare il dato;
- ❑ **Tracking:** seguire oggetti in movimento, permettendo di trarre inferenze;
- ❑ **Delay tolerant networks:** diventare una pennetta usb, cioè l'RFID funziona come un nodo a reti dove serve solo che arrivino le informazioni, senza requisiti stringenti sulle tempistiche.

La seconda generazione dei RFID passivi è il caso delle **reti di sensori** (*wireless sensor networks*). Essa nega due dogmi:

- ❑ Internet è una rete *Core Edge* (complessa in periferia, semplice all'interno). Gli RFID, invece, sono **router wireless**: sono sia router (dentro) che *device* (ricevono e trasmettono in periferia), costituendo una rete ad hoc. Quindi non c'è più un dentro e un fuori, un centro e una periferia.
- ❑ La rete dei sensori non è il "postino di bit" come Internet: è il primo posto dove avviene il **network processing** e **storage**. La rete di RFID è un computer distribuito.

Tale tipologia di rete caratterizzante il mondo IOT, però, comporta alcuni **effetti collaterali**:

- ❑ Il **tema energetico** è un problema;
- ❑ **non c'è generalizzazione**, ovvero non è possibile standardizzare questo genere di rete, ma bisogna costruirla ad hoc in base al contesto e alle esigenze;
Ad esempio: nel mondo della agricoltura si usano specifiche tecnologie perché è chiaro l'obiettivo specifico. Ne consegue che non può essere utilizzato un IOT generalista.

La vera definizione di IoT

IoT è diverso dal **Machine to Machine Communication (M2M)**: M2M consiste nell'avere oggetti comunicanti ed esiste da anni.

Anche gli **Smart objects** esistono da tempo: un oggetto si chiama "smart" se possiede un microcontrollore.

IoT, invece, è stata sancita in modo rigoroso dall'**ITU**¹³: esso è un ente che realizza standard non proprietari per la telecomunicazione e afferma che l'IOT è un'**infrastruttura globale che abilita**

¹³ L'**Unione internazionale delle telecomunicazioni**, in acronimo **ITU** (dall'inglese *International Telecommunication Union*) è un'organizzazione internazionale che si occupa di definire gli standard nelle telecomunicazioni e nell'uso delle onde radio. Fondata il 17 maggio 1865 a Parigi da 20 membri con il nome di *International Telegraph Union*, cambia con il nome attuale nel 1932; dal 1947 è una delle agenzie specializzate delle Nazioni Unite e l'attuale sede è a Ginevra. Il 17 maggio viene festeggiata la giornata mondiale delle telecomunicazioni e della società dell'informazione.

nuovi servizi avanzati grazie all'interconnessione di oggetti fisici e virtuali, mediante l'impiego delle più recenti tecnologie dell'informazione e della comunicazione.

Il *presupposto* è che ci dev'essere **interoperatività** estrema (iper-connettività) per poter mettere insieme il **mondo virtuale** e lo **spazio cinetico (fisico)**.

Internet of Things, perciò, non è semplicemente un sistema di sensori connessi al Cloud, ma è una rete che esegue *processing*, *storing*, che inizia col dispositivo locale e finisce a chilometri di distanza. È la **piattaforma che abilita il web servicing dentro gli oggetti**.

Tuttavia, tale rete non presenta solo vantaggi e, come tutte le tecnologie, è caratterizzata da alcuni costi derivanti da:

- ☐ gli hardware;
- ☐ il servizio di gestione (rappresenta ben i due terzi del costo totale);
- ☐ *network services*, ovvero i costi dei servizi abilitati dalla rete.

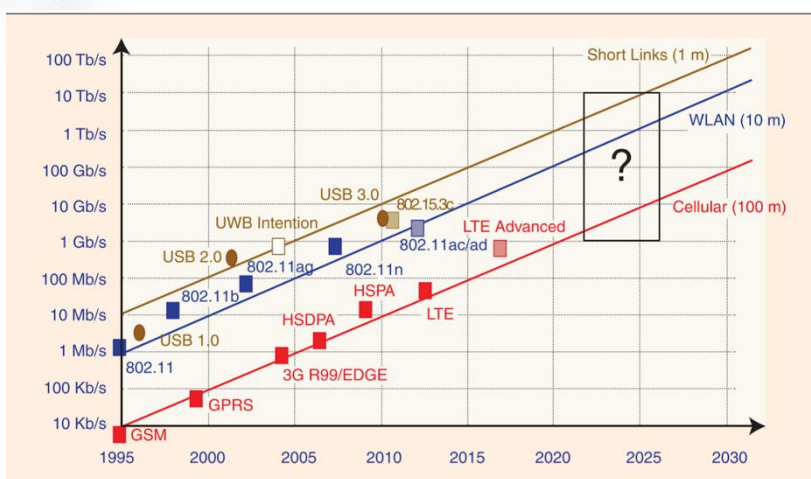
Inoltre, gli aspetti più complessi riguardanti l'IoT sono:

- ☐ la gestione;
- ☐ l'affidabilità;
- ☐ la sicurezza, ovvero riguardante attacchi che provocano *lateral movements*, i quali piano piano si spostano da un *device* all'altro per acquisire dati o inserire funzioni (il 55% del crimine è crimine informatico).

In sintesi, non sono le tecnologie gli aspetti realmente caratterizzanti l'IoT, ma è lo **sviluppo complessivo**, è il valore che sta nelle idee, nella fantasia di nuovi servizi ancora da intuire (applicabili a qualsiasi dominio) e nella gestione di questi ultimi. La necessità è quella di **estrarre conoscenza**: dai dati, alle informazioni, alla *knowledge*, fino ad arrivare alla saggezza.

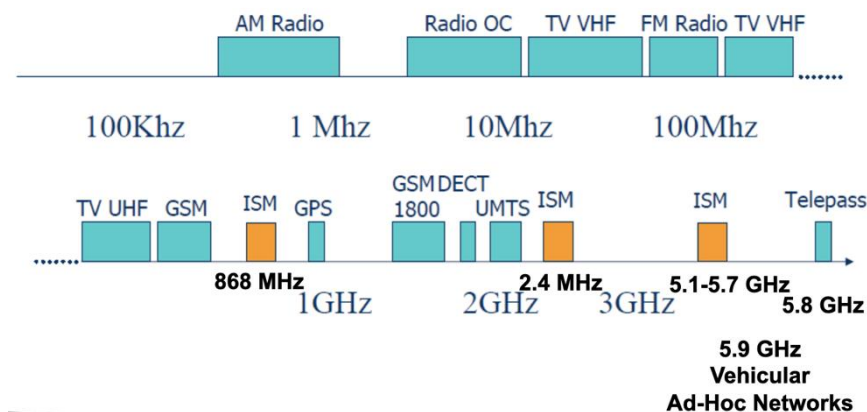
Le reti mobili cellulari

Se vediamo una retta in scala logaritmica, capiamo che siamo in presenza di trend esponenziali: come mostra il grafico, è successo al Wi-Fi, all'USB e lo vediamo anche per le reti mobili cellulari. Per ottenere una rete mobile cellulare standardizzata, ci sono voluti sempre 10 anni tra una generazione e l'altra. Finalmente, siamo arrivati a consolidare gli standard del **5G**, ma si tratta di una partita complicata che mette in concorrenza tecnologie diverse.

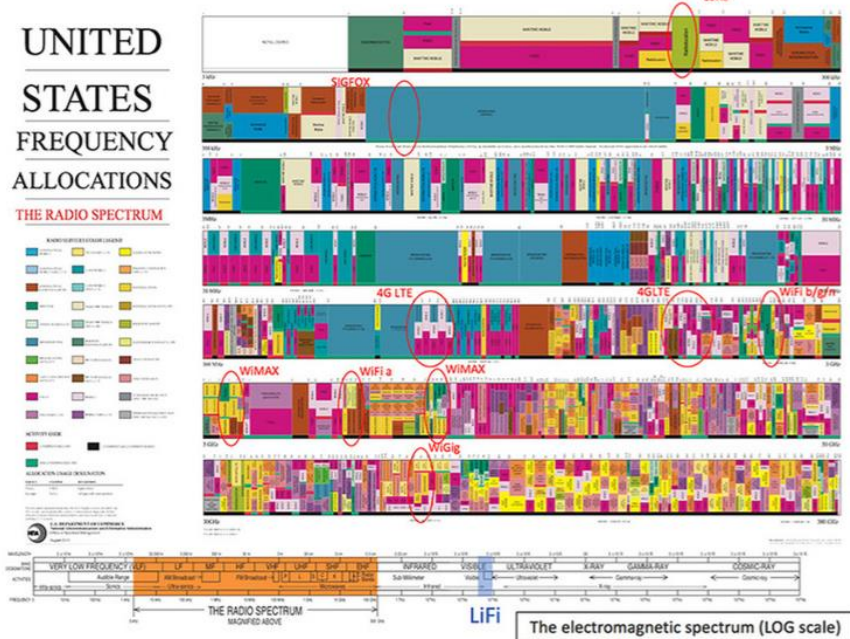


Digressione: i principi fisici alla base

Le comunicazioni fanno uso delle **onde elettromagnetiche**, ma non solo le onde radio, anche l'ottica (ad esempio l'infrarosso che usiamo per i telecomandi).



In passato le diverse porzioni dello spettro erano associate ad un servizio. Le zone gialle (nell'immagine soprastante) sono in banda non licenziata (molto congestionata), mentre nelle altre bande, gli operatori spendono molto per poter avere le licenze di utilizzo. Infatti, dal GSM¹⁴ in poi, gli operatori di reti radiomobili cellulari hanno complessivamente speso 20 miliardi di euro solo per le licenze delle reti.



Curiosità:

se guardiamo lo spettro trasmissivo in un Paese come gli Stati Uniti (in figura), ci accorgiamo di quanto è complicato allocare le risorse radio e che ci stiamo spingendo nel dominio delle onde millimetriche.

¹⁴ Global System for Mobile Communications 2G (in italiano *Sistema globale per comunicazioni mobili*, o GSM) è uno standard di seconda generazione di telefonia mobile approvato dall'Ente Europeo di Standardizzazione (ETSI). Si tratta di uno standard aperto sviluppato dalla conferenza europea delle amministrazioni delle Poste e delle Telecomunicazioni (CEPT), formalizzato dall'Istituto europeo di standard telecomunicativi (ETSI) e reso operativo dal consorzio 3GPP. Al 2017 era il più diffuso al mondo con più di 3 miliardi di persone in 200 Stati.

La storia delle reti radio mobili su cellulari

La **prima** rete mobile è stata **analogica**: lavorava con tecnica **FDM** (qualcuno si riusciva a collegare con gli scanner-radio).

È stata poi surclassata dalla seconda generazione (**GSM**). Con la seconda si cominciava a parlare di comunicazione dati (*edge* e *gps*), ma è nata, di base, per comunicazione voce digitale. Tutta l'Europa ha unito le forze, dando vita al successo più grande nelle telecomunicazioni.

Poi è arrivata la **rete 3G (UMTS)**, primo caso in cui gli utenti hanno cominciato a usare internet dal cellulare e si puntava alla videoconferenza che, tuttavia, non usava ancora nessuno.

Successivamente è nato il **4G** (detto **LTE**), diffuso tutt'ora, grazie al quale usiamo internet dal cellulare e, navighiamo superando le velocità trasmissive dell'ADSL. Il 4G viene a sua volta superato in molti casi da LTE ADVANCED (4G ADVANCED), che raggiunge i 200 megabit/s, ovvero velocità superiori alla rete fissa.

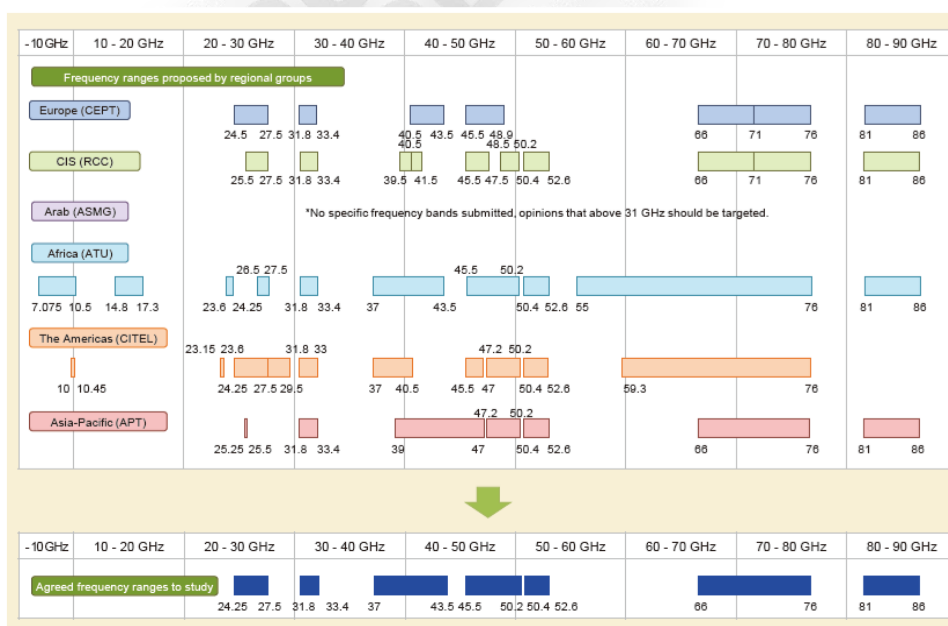
Oggi si sta affermando il **5G**: si fa riferimento al **bit rate** pari a **1 Gbit/s**, dunque anche in questo caso **più della rete fissa**.

ATT! È da specificare che, dal 3G in poi, si parla di *Packet switching* (**commutazione a pacchetto**).

Il 5G

Il 5G è una rete fortemente **densificata**: le coperture non sono macro-cellulari, ma *small-cells*, di qualche decina di metri.

Nell'immagine sottostante, si descrive la variabilità che sussiste nell'impiego di diverse bande per il 5G nei diversi Paesi.



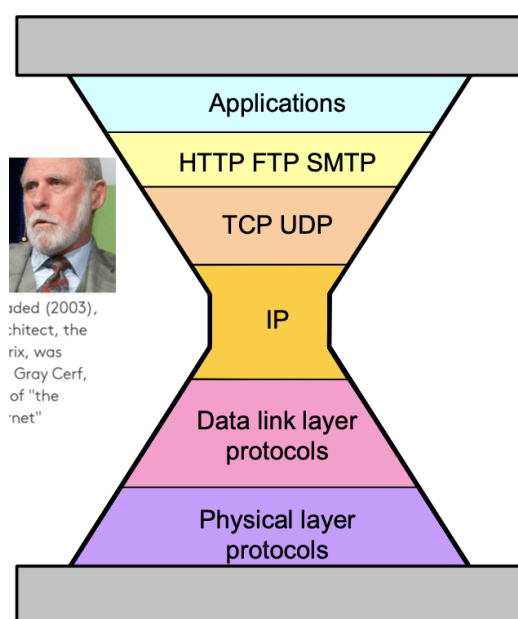
Uno degli aspetti straordinari del 5G è il **Beamforming**¹⁵: si utilizzano tecniche di realizzazione delle antenne che le rendono pannelli aventi 256 trasmettitori radio con cui si riesce a creare un segnale singolo per ogni utente (si parla anche di *pencil beamforming*).

¹⁵ Il "Beamforming" è una tecnica di elaborazione del segnale utilizzata negli array di sensori per la trasmissione o la ricezione del segnale direzionale.

Ovviamente, tale segnale deve essere in visibilità ottica per evitare che si scolleghi dalla rete: per tale motivo, è necessario porsi il **problema di sfruttare i rimbalzi degli edifici per raggiungere comunque il singolo** (si sentirà parlare di beta-materiale soprattutto in ambito urbano).

La possibile conseguenza del Beamforming sarà il minor inquinamento elettromagnetico e il risparmio energetico.

Un altro aspetto fondamentale è che le reti 5G sono **reti ALL-IP: IP on everything and everything over IP**. In altri termini, ogni applicazione può girare su ogni IP e IP può girare su qualsiasi tecnologia.



Ma in realtà, si sta creando una **sclerotizzazione della rete (ossification)**, grazie alla nascita di **due nuovi paradigmi delle telecomunicazioni**:

1. La rete (e di conseguenza il router) non è più fatta di scatole chiuse, di *black box* o silos.

Un router è una macchina costituita da software e hardware che, di norma, decide come agire autonomamente. Oggi, con la rete 5G, quello che fa il router lo decide un controllore generalizzato (**software define networking**).

In pratica si tratta dello **split di funzioni software e hardware del router** per poterle definire da un'applicazione che gira sul controllore, similmente a come accade con il sistema operativo di un calcolatore avente varie applicazioni: la rete esegue ciò che scrivono terze parti (PMI specializzate nel creare software sofisticati).

Il valore risiede, dunque, nella **programmabilità**: la rete diventa programmabile!

ATT! È chiaro che tale programmabilità comporti numerosi **problemi di debugging**: sbagliando un passaggio nel codice sul controllore che comanda tutta una rete, le conseguenze sono caotiche. Infatti, di solito sono previsti più controllori che intervengono per sicurezza sulla stessa rete.

- 2.** I pezzi di ferro diventano **macchine virtuali** che "girano" su *data centre (network function virtualization)*. Infatti, le centrali telefoniche diventano data centre e, in questo nuovo contesto, il **Cloud** risulta fondamentale.

In sintesi, nel 5G sono presenti:

- ☐ **Enhanced mobile broadband.** Si va da 100 mbit a 1 Gbit o addirittura 10 Gbit (anche se può farlo già LTE);
- ☐ **Massive IoT.** Si raggiunge una comunicazione massiva, con 1 milione di dispositivi per ogni metro (1000 bit al secondo, ovvero 1 Gbit). Tuttavia, tale caratteristica è presente anche in LTE;
- ☐ **Bassi ritardi.** Si tratta dell'unico aspetto completamente nuovo rispetto a LTE: un ritardo di 1 millisecondo.
- ☐ Possibilità di **Storage, Processing e Connection** e, per la prima volta, **Slicing**, cioè virtualizzazione della infrastruttura.

Infine, anche la rete 5G deve essere vista non come una rete di trasporto o postino di bit, ma come **piattaforma abilitante di nuovi servizi, cioè di soluzioni a problemi** (*smart city, smart hospital, etc*).

Applicazioni reali dell'IoT

A seguire sono raccontate alcune applicazioni dell'Internet of Things in casi reali.

Intelligent Transportation Service

Nel mondo delle super car, sono presenti geometrie variabili (come nei velivoli) grazie ad alcune componenti adattative.



Per poter controllare tale variabilità, è stato applicato al mondo della fluidodinamica adattativa il CPS (*Cyber-Physical System*, cooperazione mondo fisico e virtuale), ma quest'ultimo non è sempre intuitivo.

Si prenda, ad esempio, una moto: date certe condizioni di flusso, come si devono allocare gli alettoni al fine di avere la massima prestazione, sicurezza e comfort?

A seconda di cosa vuole l'utente, si possono ottenere **tre configurazioni diverse**, facendo lo studio di un set discreto di casi. Alla moto in esempio, sono stati aggiunti dei sensori wireless e dei nodi che parlano con gli attuatori (in questo caso alettoni): i sensori misurano le pressioni, i valori vengono passati alla centralina che comanda di modificare gli attuatori (e dunque gli alettoni della moto).

Potrebbe esserci alla base una rete neurale che esegue un'interpolazione per i casi non conosciuti. Relativamente a questo caso, è stato sviluppato anche il Cloud e la visualizzazione: è fondamentale ricordare che il primo modo per estrarre conoscenza è permettere a un esperto di visualizzare i dati in real-time.

Precision Agricultural Production

La Toscana è una delle regioni più avanti in ambito di Agricoltura di precisione. Ci son tanti aspetti da considerare: irrigamento, fertilizzanti, concimi e altri scenari specifici che richiedono competenze particolari.

Il primo problema (dopo la burocrazia) che assale l'agricoltura sono gli attacchi da fauna selvatica (uccidono anche decine di persone ogni anno sulle strade).

Un'azienda toscana, a tal proposito, non ha voluto soluzioni invasive: voleva allontanare gli animali con gli **ultrasuoni**, quindi si poteva risolvere utilizzando una piattaforma abilitante di nuovi servizi (IoT).

A seguire si elencano alcune soluzioni tradizionalmente implementate per risolvere tale problema:

- ☐ repellenti chimici;
- ☐ sistemi in banda acustica (che fanno sentire suoni di animali feroci come le tigri, etc.);

- ☐ reti metalliche;
- ☐ reti elettrificate.

Tutte queste soluzioni sono, tuttavia, poco efficaci, costano molto in termini di manutenzione e sono anche poco gestibili.

Soluzione Natech Escape

LoRa¹⁶ è una radio potente e proprietaria (solo un venditore al mondo la vende). È una radio dove, se il segnale è immerso in rumore, riesce comunque a ricevere. Si tratta di una trasmissione molto robusta ai disturbi e fornisce coperture geografiche straordinarie. Presenta un bit rate bassissimo: da 50 bit/s a 50 kbit/s. Inoltre, ha un consumo energetico bassissimo.

Grazie all'utilizzo di LoRaWAN¹⁷ (la rete rispettiva della radio LORA), Natech (PMI fornitrice dell'azienda toscana) ha creato un sistema autonomo dal punto di vista energetico e costituito da sensori (rilevanti immagini) ed attuatori per respingere gli animali. Tali immagini, grazie a reti neurali, vengono classificate in tempo reale. Il sistema si chiama Natech Escape.

Quindi è nata una **piattaforma abilitante**: i nodi parlano con i gateway, possono funzionare anche nel bel mezzo del nulla, ma, qualora ci fosse una copertura, diventerebbe ancora più semplice.

La parte costosa di tale piattaforma risulta essere la gestione del Cloud: esistono programmi che girano sul telefono e che, popolando dei database, permettono di passare i dati raccolti dal sistema al Cloud e, in questo modo, accedere a servizi terzi per fare altro (come ad esempio creare *dashboard*).

In conclusione, **IoT** è l'**equivalente di internet**: una piattaforma globale di servizi che ancora non immaginiamo e che non deve essere costruita da zero, ma partendo da elementi esistenti (ad esempio gli oggetti fisici).

¹⁶ **LoRa (Long Range)** è una tecnologia di modulazione di frequenza a spettro espanso derivata dalla tecnologia di Chirp Spread Spectrum (CSS) ed è la prima implementazione a basso costo dello spettro di diffusione chirp per uso commerciale. È stato sviluppato da Cycleo di Grenoble, in Francia, e acquisito da Semtech nel 2012, membro fondatore di LoRa Alliance.

¹⁷ LoRaWAN è uno dei numerosi protocolli sviluppati per definire gli strati superiori della rete. LoRaWAN è un protocollo di livello MAC (Media Access Control) basato su cloud ma funge principalmente da protocollo di livello di rete per la gestione delle comunicazioni tra gateway LPWAN (Low Power Wide Area Network) e dispositivi end-node come protocollo di routing, gestito da LoRa Alliance.

Appendice: Introduzione a Zerynth

Storia e presentazione azienda



Zerynth nasce come un'azienda statunitense grazie a una campagna di *crowd funding*.

La piattaforma offerta da Zerynth è utile a scopo *educational* e per la prototipazione (versione gratuita), ma anche in fase di industrializzazione (tramite licenze del software).

La notizia più importante che riguarda l'azienda è quella di aver ottenuto un investimento di due milioni euro che ha permesso di passare dalla fase di *startup* a *scaleup*, permettendole di crescere.

L'IoT in Zerynth

Per IoT si intende una rete di dispositivi fisici che presentano all'interno ("embeddato") elettronica, software, attuatori, sensori e connettività per estrarre dati da scambiare fra loro.

Gli **elementi hardware** si classificano in:

- ☐ *Sensori* (dispositivi di input)
- ☐ *Attuatori* (dispositivi di output)
- ☐ *Microcontrollori* (CPU)

Col passare degli anni, il costo dell'hardware è diminuito sempre di più e sono, di contro, aumentate le prestazioni.

Grazie ai microcontrollori si possono eseguire numerose azioni pur avendo RAM di pochi *megabite*: bisogna **programmarli**, ovvero creare dei veri e propri software appositi che gli permettano di controllare input e output.

Si distinguono **due tipi di linguaggi di programmazione**:

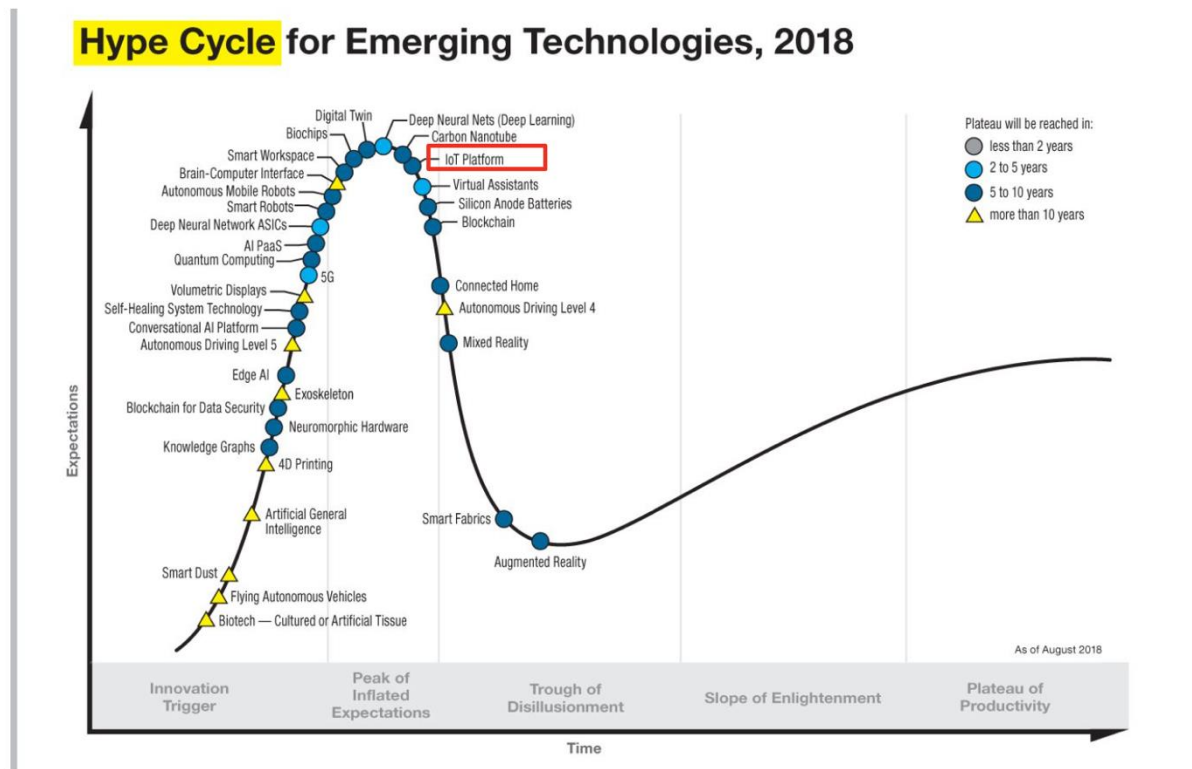
1. Linguaggio di programmazione di **alto livello** (come Python), ovvero più vicino al linguaggio naturale;
2. Linguaggio di programmazione di **basso livello** (come C, C++ o Assembly), ovvero più vicino al linguaggio macchina. Il testo del codice dice cosa fare alla macchina.

Il codice del programma, in ogni caso, deve essere sempre mantenuto: lo sviluppatore deve rivederlo frequentemente, sebbene spesso non possa ricordare tutto ciò che ha scritto. Tale problematica, infatti, comporta la nascita del linguaggio di alto livello (spesso anche ben commentato), così da permettere al programmatore di orientarsi più facilmente in un secondo momento.

I microcontrollori sono i veri elementi che popolano tutti i dispositivi *smart*, ma, grazie alla facilitazione del linguaggio di alto livello per programmarli, si ottiene una vera **rivoluzione del mondo IoT**: diventa accessibile anche a chi non conosce il linguaggio di basso livello.

In particolare, Zerynth ha scelto il linguaggio Python perché molto diffuso e anche comprensibile. Altre aziende prediligono Java o Java script (sempre alto livello). Sussiste una **certa resistenza** alla conversione, però, da parte di chi è *old school*, abituato a C e Assembly (basso livello).

Nella figura sottostante si osserva l'**andamento** delle **aspettative degli utenti** rispetto a varie tecnologie: Edge, AI (intelligenza artificiale sul microcontrollore), etc.



Appena uscite dalla fase di Ricerca e Sviluppo (R&D), c'è un picco di aspettative e se ne parla tanto. Successivamente si va verso una fase discendente, ovvero di disillusione: si intuisce che si può fare tanto con tali tecnologie, ma che alcune promesse saranno disattese. Infine, si arriva a un plateau di produttività (regime).

Si nota dal grafico che le **piattaforme IoT** hanno appena superato il massimo delle aspettative, andando incontro alla fase discendente: ci sarà una diminuzione di startup che offrono piattaforme per programmazione IoT (come Zerynth).

Parlando di numeri, oggi sono presenti nel mondo miliardi di dispositivi IoT.

Le **opportunità** derivanti dall'utilizzo di una **piattaforma IoT** sono le seguenti:

- ☐ Si può aumentare il numero di clienti.
Ad esempio, un'azienda che produce lo spazzolino elettrico dovrebbe utilizzare IoT perché migliora le funzionalità e la *Customer experience* e, quindi, la fidelizzazione;
- ☐ Abilita la *Servitization*. Permette di creare nuove fonti di ricavo: i prodotti generano dei dati che possono essere sfruttati ed elaborati per generare altri servizi;
Ad esempio, le macchinette del caffè che indicano quando stanno per finire le cialde o che le ordinano in automatico;
- ☐ I dati possono servire per capire come il prodotto viene utilizzato e fare meglio R&D poiché descrivono come i prodotti interagiscono col cliente, evitando sondaggi soggettivi.

Come si può intuire, è lo stesso concetto dietro internet: le aziende che possiedono i social network ottengono ricavi dai dati. Un e-commerce sa come gestire un prodotto perché è a conoscenza di quale prodotto ha ricevuto più *click* e lo mette in vetrina.

Perciò, in particolare traggono **beneficio** dall'IoT:

- ☐ Aziende di prodotto
- ☐ Aziende manifatturiere (IoT nei macchinari industriali)
- ☐ Consulenti e *system integrator*.

Tuttavia, esiste un **problema dell'IoT**: il mercato attuale è estremamente frammentato, dunque complesso. Per ogni elemento della catena ci sono milioni di aziende che offrono i propri servizi, il che diventa complesso e causa l'aumento del rischio.

Alcuni **pilastri** del concetto di piattaforma IoT per affrontare il rischio sono i seguenti:

- ☐ Completa (hardware, software e cloud);
- ☐ Poche frizioni, facile da usare;
- ☐ Resiliente (*future-proof*, ovvero quello che si realizza oggi dev'essere adeguato ad integrare tecnologie che usciranno tra un anno);
- ☐ Sicura.

In particolare, **quella di Zerynth** è una **piattaforma completa**:

- ☐ **Hardware**. Si tratta di uno "scatolotto" (chiamato **4zerobox**) che si installa sulle macchine delle aziende, in quanto le macchine sono vecchie e di per sé non producono dati. Tale *device* serve a disaccoppiare l'OT dall'IT creando un ponte tra la macchina e il gestionale dell'azienda: la scatola parla la lingua dell'elettricista, l'IT parla il linguaggio dei *data scientist* (python etc);
- ☐ **Software**, per programmare l'hardware (Zerynth SDK);
- ☐ **Cloud** (Zerynth Device Manager). Serve per rendere i dati fruibili per le terze parti, quali quelle che offrono la costruzione di grafici, analisi, dashboard (ad esempio Grafana, Ubidots), etc.

Il sistema Zerynth, in sintesi, presenta il ruolo di **middleware**, cioè ponte tra parte hardware (prodotte da altre aziende) e Cloud.

Caso d'uso

Smart Agriculture: si tratta di un lampante esempio di **servitizzazione**.

È stato creato un sistema IoT che permette di rilevare lo stato di salute delle piante (direzione del vento, temperatura, umidità, etc.) e del sistema di irrigazione.

Il cliente è **l'azienda che produce e vende concimi**: ha capito che andando a installare questo sistema sulle piante dei suoi rispettivi clienti, può monitorare meglio il loro stato e offrire un altro servizio di consulenza consistente nel suggerire quando sia più opportuno usare il concime.

L'azienda è passata ad essere tecnologica e innovativa. Zerynth fornisce la tecnologia, mentre l'azienda in questione la rivende mettendoci il suo brand e creando una rete di aziende che lo aiutano nell'installazione del sistema IoT, dando vita ad un **circolo virtuoso**.