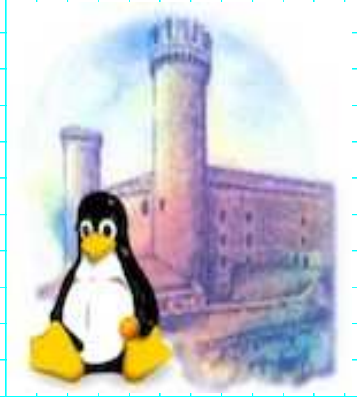


LinuxDay-2017 Ivrea

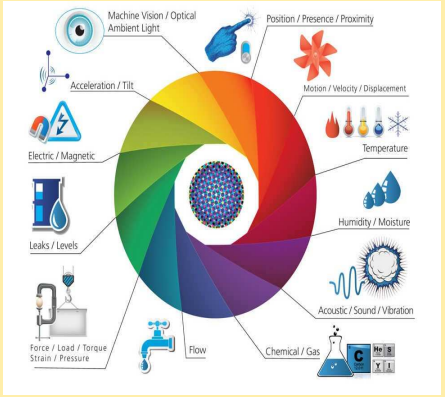
# Sicurezza di IoT:

# l'Internet delle cose.

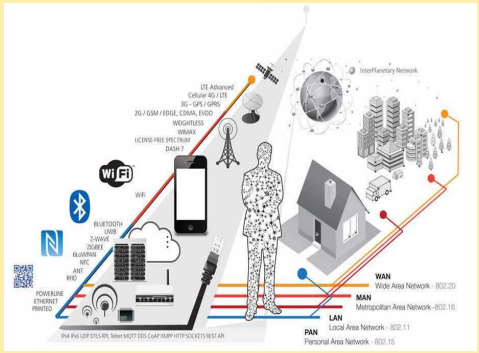
Luigi D. Capra & Norberto Patrignani

# IoT può essere presentata in molti modi

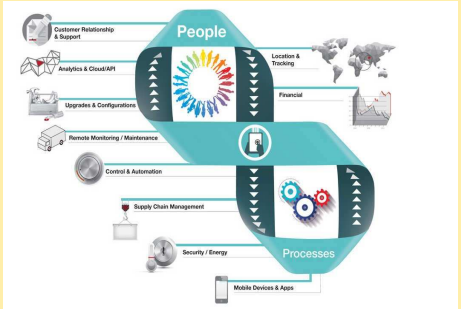
## Sensors & Actuators




## Connectivity

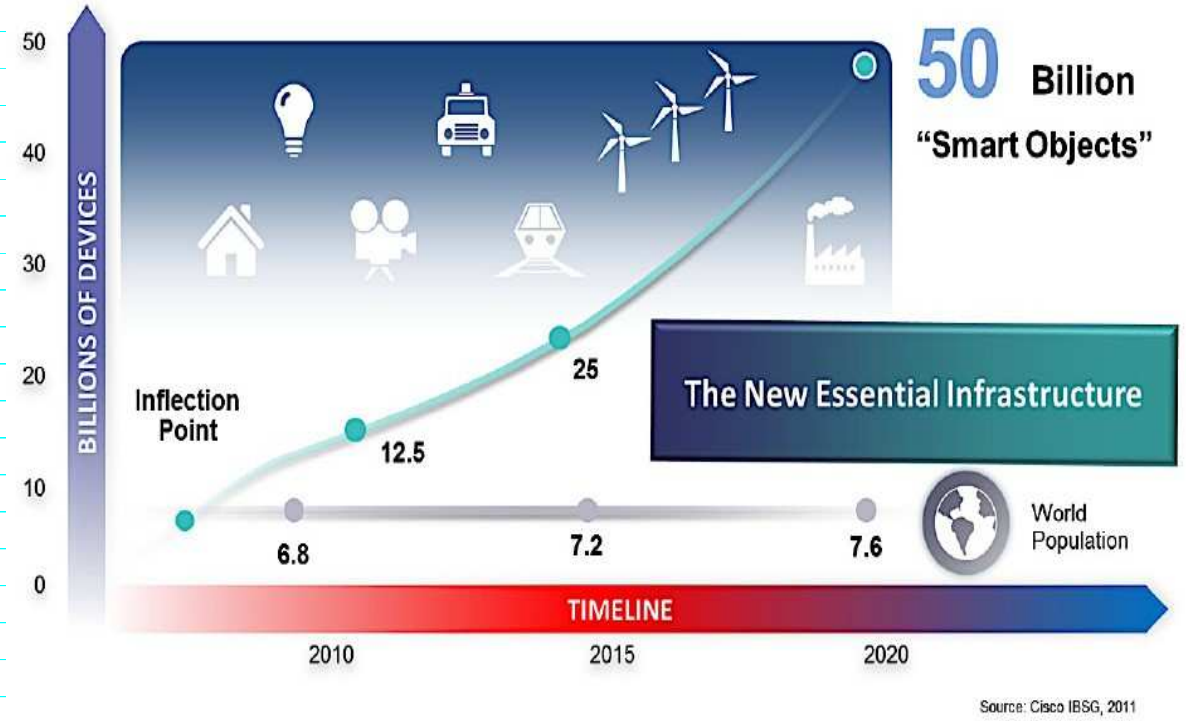


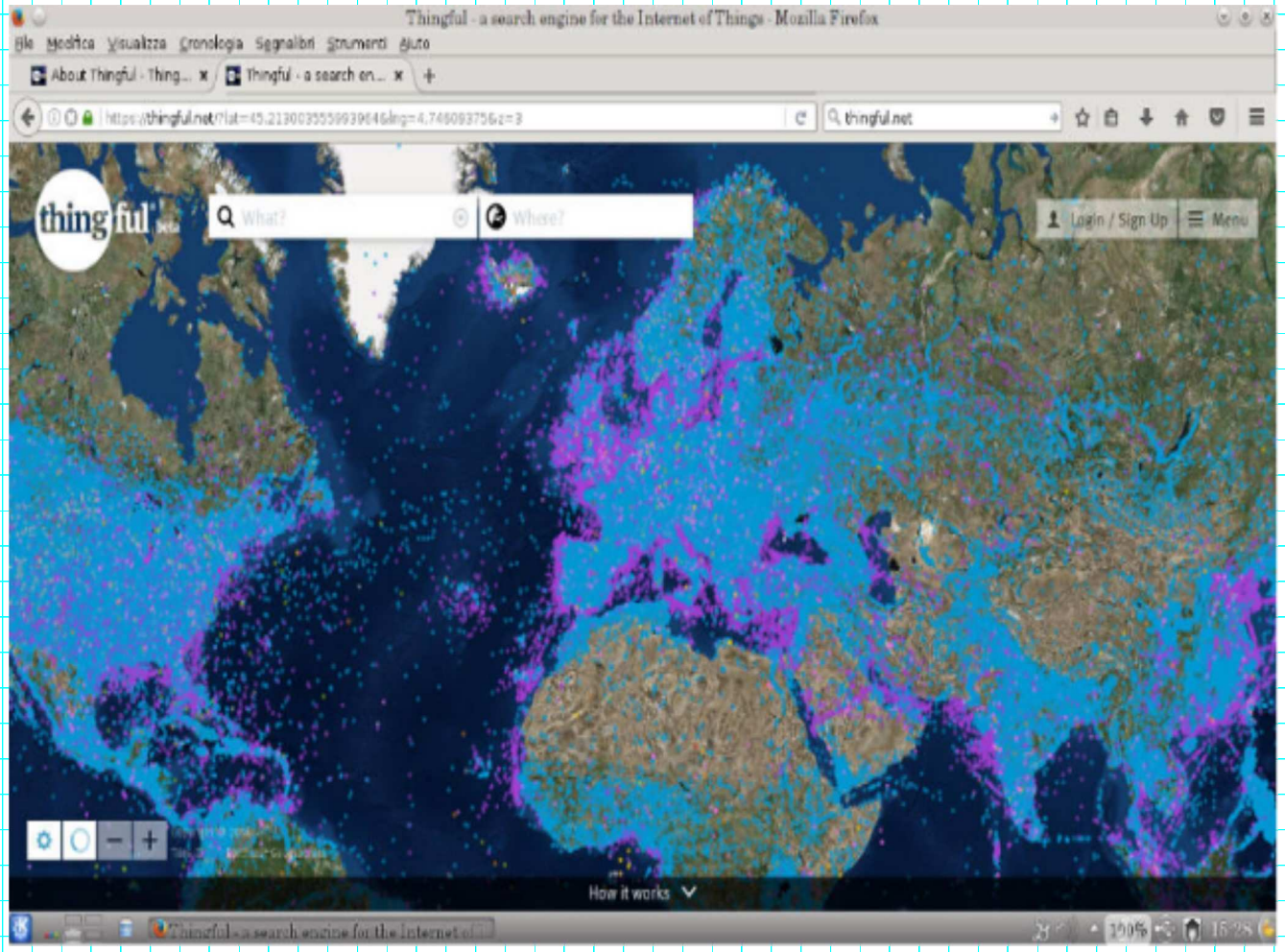

## People & Process



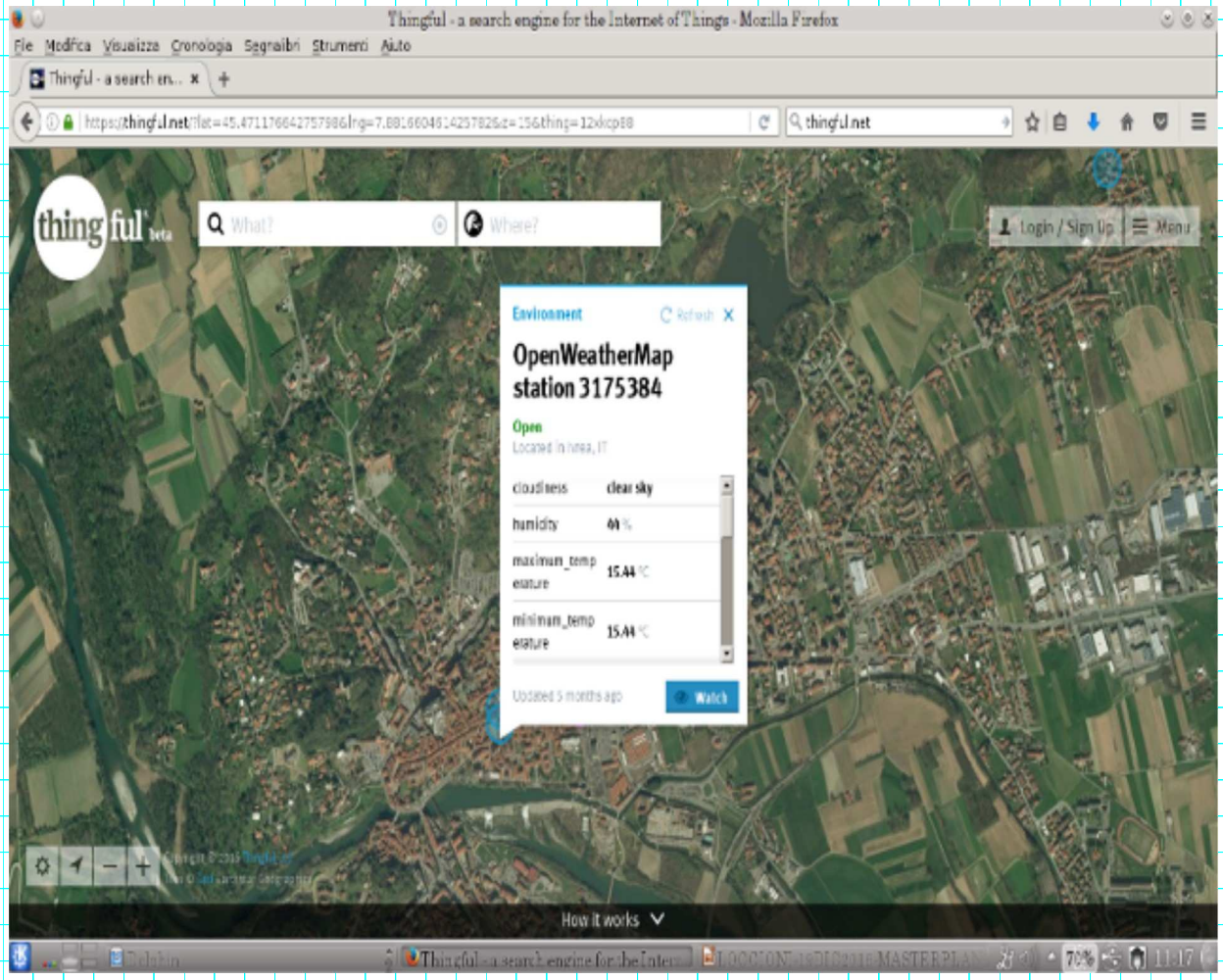

Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea

*Internet of Things* (IoT) è già fra noi:
il numero di dispositivi collegati in rete è in continua crescita
tanto da aver già da tempo superato quello della popolazione mondiale.



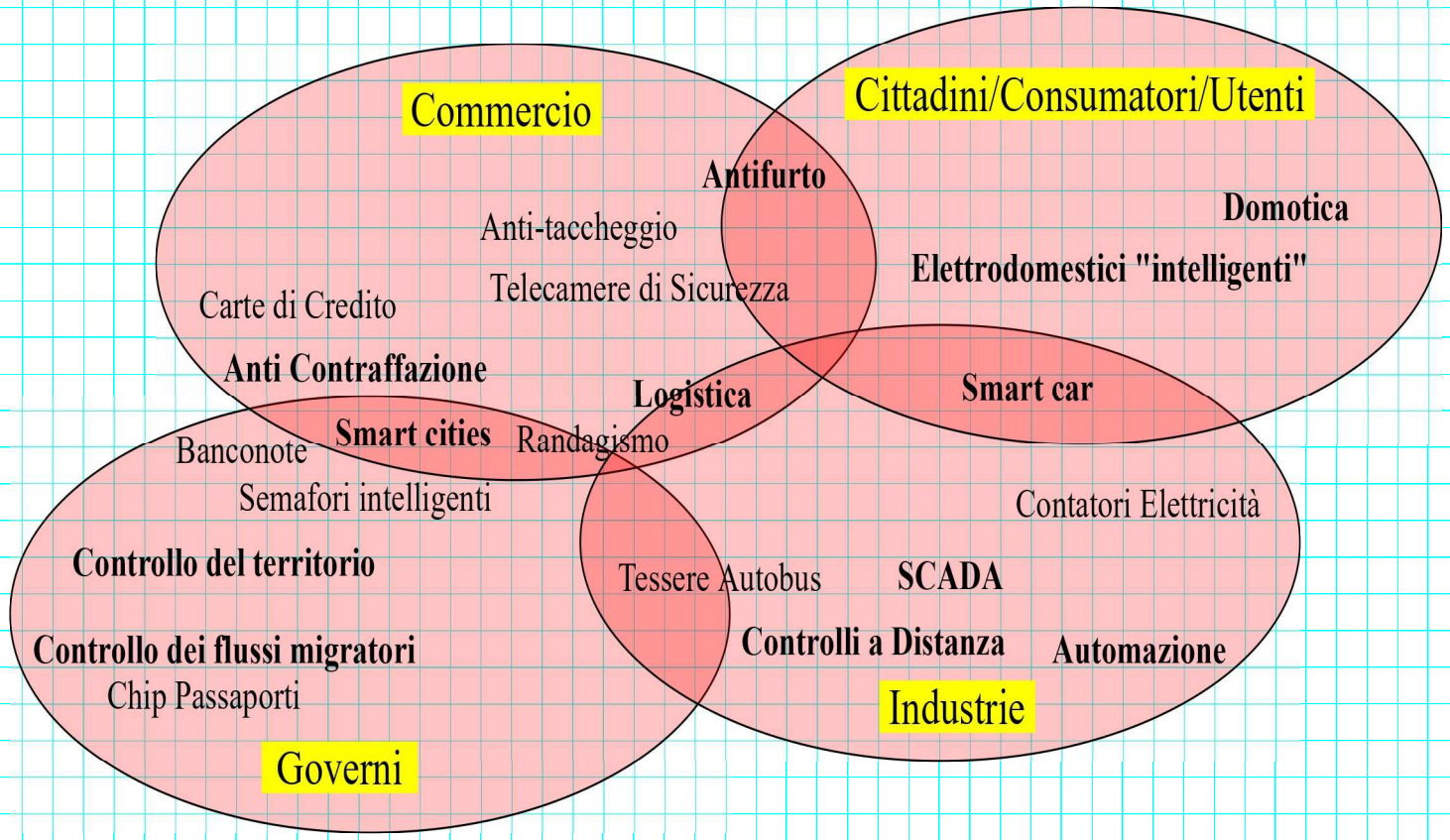



Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea




Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea

# IoT sta permeando ogni ambiente e ogni tipologia di applicazione




Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea

# ed è qui per restare!


Commercio

Cittadini/Consumatori/Utenti

Industrie

Governi

Antifurto

Domotica

Anti-taccheggio

Elettrodomestici "intelligenti"

Telecamere di Sicurezza

Carte di Credito

Anti Contraffazione

Logistica

Smart car

Smart cities

Randagismo

Banconote

Chip Passaporti

Impresa 4.0

Contatori Elettricità

Semafori intelligenti

Automazione

Controllo del territorio

Controlli a Distanza

Controllo dei flussi migratori

Auto Connesse

fabbrica 4.0

La transizione in corso prospetta degli auspicabili benefici



ma desta anche preoccupazioni sul piano della sicurezza

non soltanto per quanto concerne il possibilie abuso dei dispositivi IoT

da parte di gruppi criminali, ma anche gli usi legittimi da parte di

governi, istituzioni, privati cittadini

per non parlare delle ripercussioni sociali.

Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea


## Security of IoT

"While the benefits of IoT are undeniable,
the reality is that security is not keeping up
with the pace of innovation.
As we increasingly integrate network connections
into our nation's critical infrastructure,
important processes that once were performed manually
(and thus enjoyed a measure of immunity against
malicious cyber activity) are now vulnerable to cyber threats.
Our increasing national dependence
on network-connected technologies
has grown faster than the means to secure it...
IoT security is now a matter of homeland security"

Strategic Principles for Securing the Internet of Things,
US Department of Homeland Security,
November 2016


IoT
Realtà o
Fantascienza?

## Industry 4.0: Tecnologie abilitanti e pericoli

- Internet of Things (IoT)
- Cyber-Security
- Cyber-Physical Systems
- Cloud Computing
- Big Data - Data Science
- Machine Learning
- Realta' Aumentata
- Robotica
- Connessione Impianti
- Manifattura Additiva
- Prototipazione 3D

...


2020: 5G, +100 Mb/sec + IoT! (congestion management)

Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea

A questo proposito può essere interessante partire
dalla discussione del rapporto intercorrente fra
sicurezza Informatica e sicurezza IoT

Secondo alcuni autorevoli esperti di sicurezza informatica
non c'è assolutamente nessuna differenza fra i due concetti,
secondo altri il tema della sicurezza IoT è completamente nuovo,
ragione per cui lo si dovrebbe affrontare partendo dai fondamentali...

Nel mondo anglosassone i fautori di questa seconda ipotesi si spingono
a sostenere la necessità di superare la tradizionale distinizione
fra i concetti di security e di safety
adottando il punto di vista "continentale" ovvero un approccio olistico.

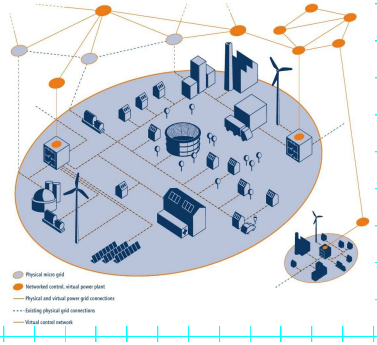
Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea

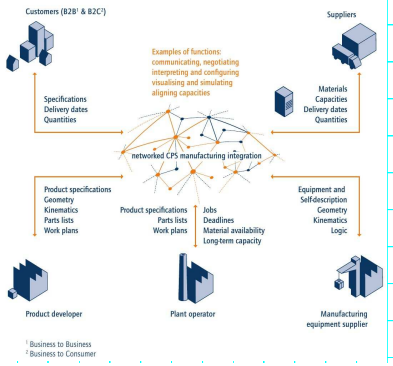

## Security of IoT

Strategic Principles for Securing the IoT

1. Incorporate Security at the Design Phase
2. Advance Security Updates and Vulnerability Management
3. Build on Proven Security Practices
4. Prioritize Security Measures According to Potential Impact
5. Promote Transparency across IoT
6. Connect Carefully and Deliberately

Il tema della sicurezza IoT si differenzia da
quello della sicurezza informatica
per il fatto di non riguardare solo il controllo delle informazioni,
ma anche e sopratutto la possibilità di impiegare dispositivi IoT
per agire nel mondo fisico a danno di qualcun altro,
monitorando in tempo reale cose e persone o addirittura
avvalendosi di attuatori remoti per atti di sabotaggio o attentati.




Source: Geisberger, E., & Broy, M. (Eds.). (2015). Living in a networked world: Integrated research agenda Cyber-Physical Systems (agendaCPS), p.159. Herbert Utz Verlag

Sotto queste premesse

la legittimità di certe applicazioni potrebbe essere una questione di punti di vista

1) Acquistando un apricancello IoT idealmente vorremmo avere la garanzia di essere gli unici a poterlo usare per aprire l'ingresso di casa nostra, analoghe consisderazioni valgono per le telecamere di sicurezza, il baby monitor, la nostra auto connessa, eccetera, ...

2) ma se dovessimo scoprire che un gruppo di terroristi stesse pianificando di far scoppiare delle bomba o investire la folla con dei camion guidati remotamente saremmo molto più propensi a concedere alle forze dell'ordine la possibilità di prendere il controllo degli stessi dispositivi.

Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea

3) I "teorici del complotto" potrebbero, a loro volta, interpretare queste ultime considerazioni in maniera del tutto diversa ipotizzando che i rischi paventati o addirittura alcuni eventi di cronaca utilizzabili per avvalorare la tesi della pericolosità sociale delle tecnologie IoT siano stati orchestrati ad arte per indurre i cittadini a rinunciare ad una parte delle loro prerogative in fatto di *privacy* a favore dei governi o gruppi di potere occulti.

## Quelli che "giocano" a *guardie e ladri*,...

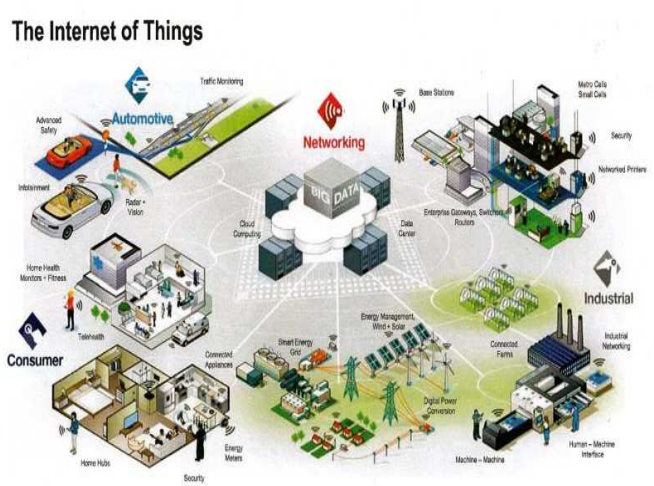
I dispositivi IoT attualmente sul mercato sono caratterizzati da livelli di sicurezza molto bassi, inoltre vige un clima di incertezza circa la proprietà dei dati raccolti e i corrispettivi diritti di sfruttamento. I dati raccolti appartengono:
- all'utilizzatore,
- al proprietario dell'apparecchio cioè di chi lo ha acquistato,
- all'azienda che ha sviluppato e prodotto il dispositivo IoT?

In una simile situazione è relativamente facile per terze parti non autorizzate "prendere visione" dei dati raccolti ed eventualmente impartire comandi ai dispositivi IoT.

Il rovescio della medaglia è che spesso è altrettanto facile a chi gioca in difesa cogliere sul fatto i malintenzionati (almeno i più sprovveduti) e adottare delle contromisure.

Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea

## Le istituzioni.




Il problema della sicurezza informatica in riferimento alle reti IoT è un tema molto serio che coinvolge anche governi, organismi amministrativi, grandi enti ed aziende, in particolare le reti di servizi pubblici (elettricità, gas, telecomunicazioni, controllo del traffico cittadino, ferroviario, aereo, sanità, eccetera.

Simili contesti sfuggono al controllo dei cittadini per cui si può solo confidare che le istituzioni preposte alla salvaguardia della sicurezza pubblica assolvano diligentemente i propri incarichi (senza abusare dei nuovi strumenti che sono messi loro a disposizione).

Se non ci si fida, si può tentare di opporsi alla modernizzazione restando finché è possibile ancorati al passato, ma probabilmente è una sfida persa, poiché difficilmente alcuni individui isolati potranno contrastare gli interessi economici in gioco. Le questioni connesse agli abusi della tecnologia sono problemi politici e come tali debbono essere affrontati.

Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea

# Consumatori e Prodotti IoT/Industria 4.0

personalizzazione di massa

Prodotti Industriali classici

10% applicazioni
90% degli utenti

Utente medio per cui sono pensate le *soluzioni standard*

Desideri e i bisogni della gente

90% applicazioni
100% degli utenti

NOI

Le esigenze degli utenti finali sono molto più ampie di quelle coperte dalle aziende.

Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea

# Consumatori e Prodotti IoT/Industria 4.0

Gli impieghi delle tecnologie IoT nell'ambito di Impresa 4.0 se da un lato prospettano la possibilità di andare incontro alle nostre esigenze di cittadini/clienti/consumatori soddisfacendole in maniera più adeguata, dall'altro spalancano le porte a tutta una serie di abusi da parte delle istituzioni (governi totalitari), imprese industriali (fabbricanti) e furfanti più o meno smaliziati.

Da che mondo è mondo il concetto di "casa" è stato associato ad un luogo sicuro, per sé e per la propria famiglia, in cui è possibile godere della *privacy* e custodire i propri averi.

Oggi questo presupposto sta venendo meno come conseguenza della diffusione di una serie di tecnologie che si prestano al monitoraggio a distanza delle nostre vite:

le reti telefoniche e i computer possono essere hackerati esponendo i nostri dati e il contenuto delle nostre missive e conversazioni ad occhi e orecchi indiscreti.

Ed in prospettiva un simile problema si porrà per i nostri gusti alimentari, le attività che svolgiamo dentro casa e quant'altro.

Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea

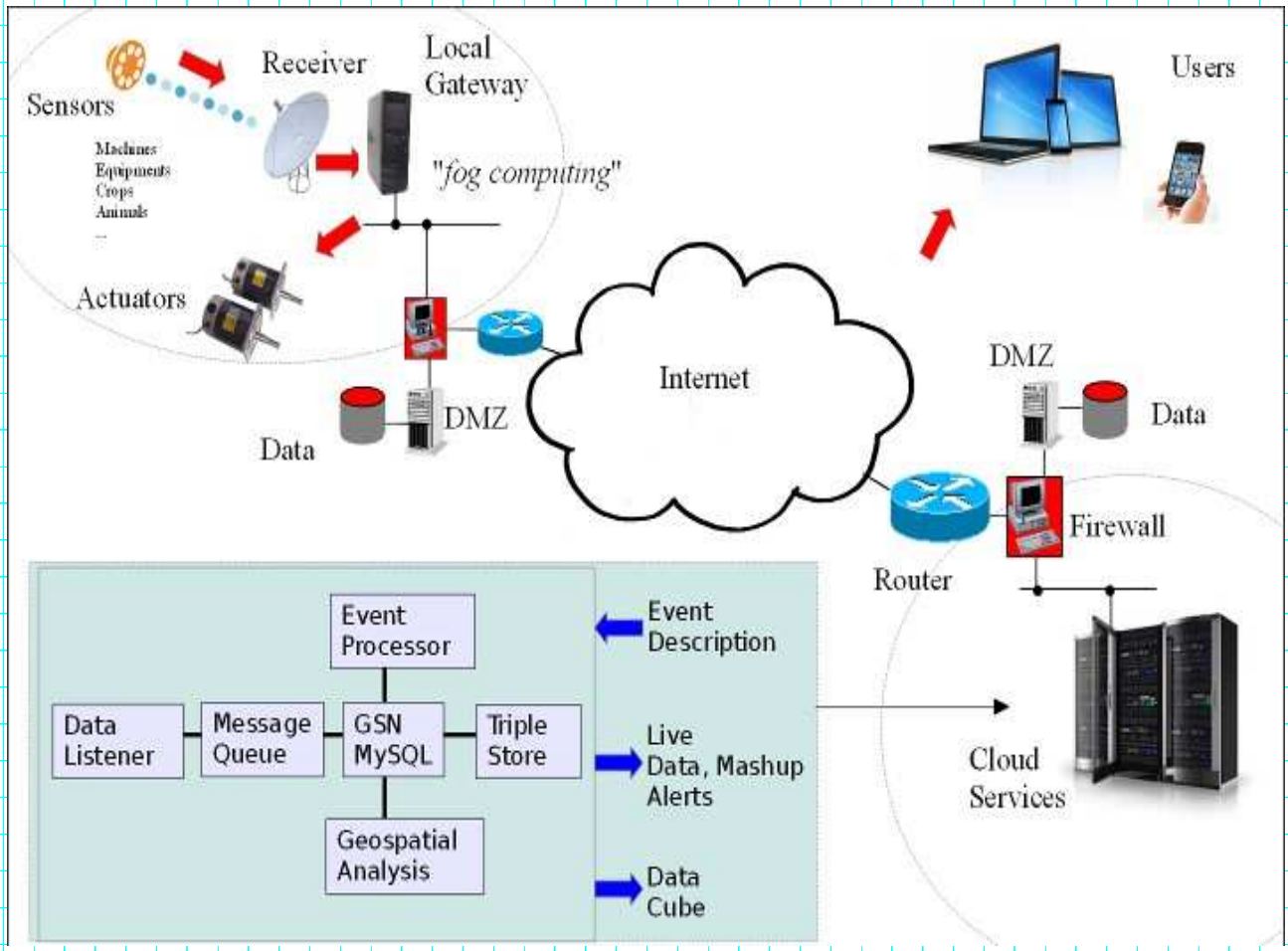
Sebbene, dal punto di vista tecnico, varie azioni di monitoraggio ai nostri danni si potessero già fare da anni (come mettere i telefoni sotto controllo o installare delle "cimici"), sino a tempi recenti i suddetti interventi costavano tempo, fatica e richiedevano competenze professionali di tutto rispetto e possibilmente l'autorizzazione di un magistrato.

Condizioni che oggi stanno venendo meno per cui le nostre vite e i nostri segreti si trovano esposti alla curiosità di chiunque da Google all'impiegato del supermercato che potrebbe studiare i dati risultanti dalle tessere (elettroniche) dei punti fedeltà per ricavare informazioni circa il tenore di vita dei clienti e il fatto che questi siano presenti a casa osiano in vacanza e passarle quindi ad una banda di "topi d'appartamento".

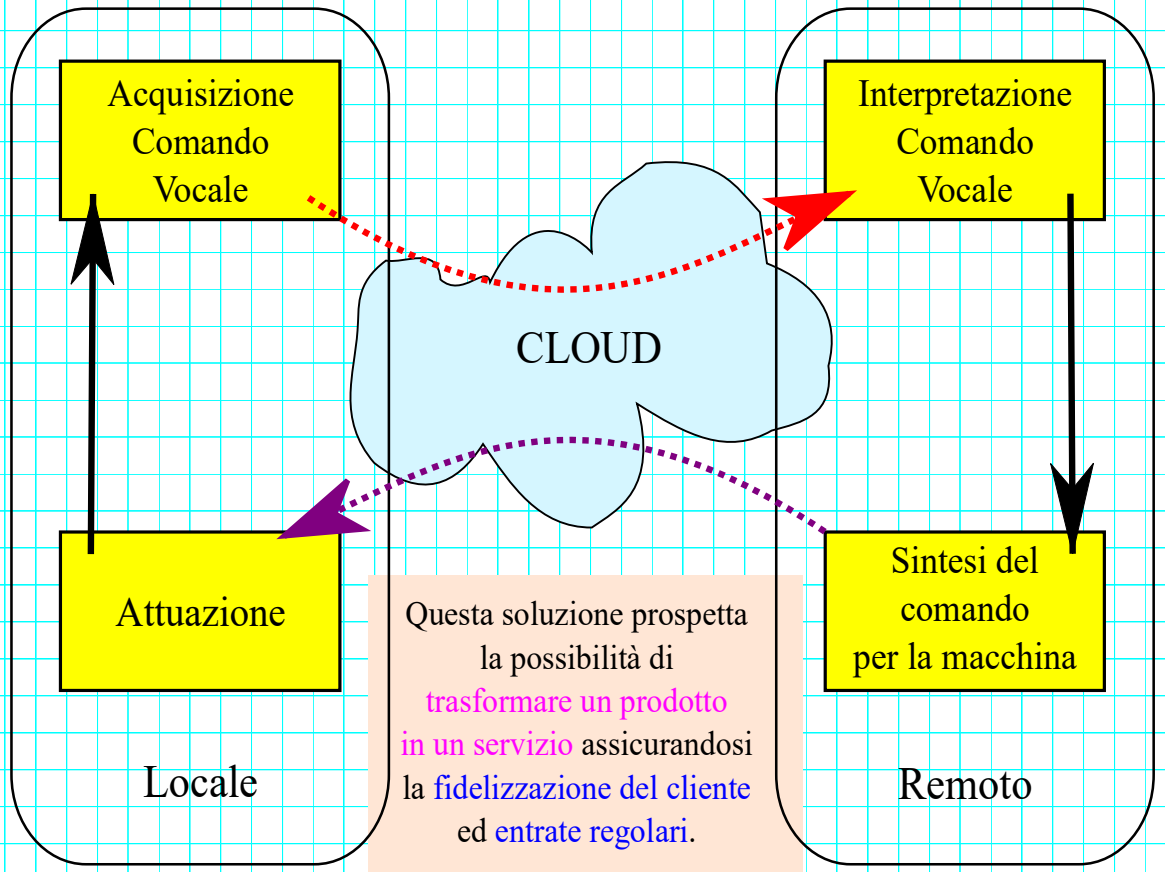
Dal punto di vista tecnico i suddetti problemi potrebbero essere messi in relazione con due modelli operativi concernenti gli apparecchi che si stanno diffondendo sempre più a causa dei loro evidenti vantaggi (anche per i malintenzionati):
il ricorso a servizi basati sul cloud e le memorie di prodotto.

Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea

# IoT System Architecture

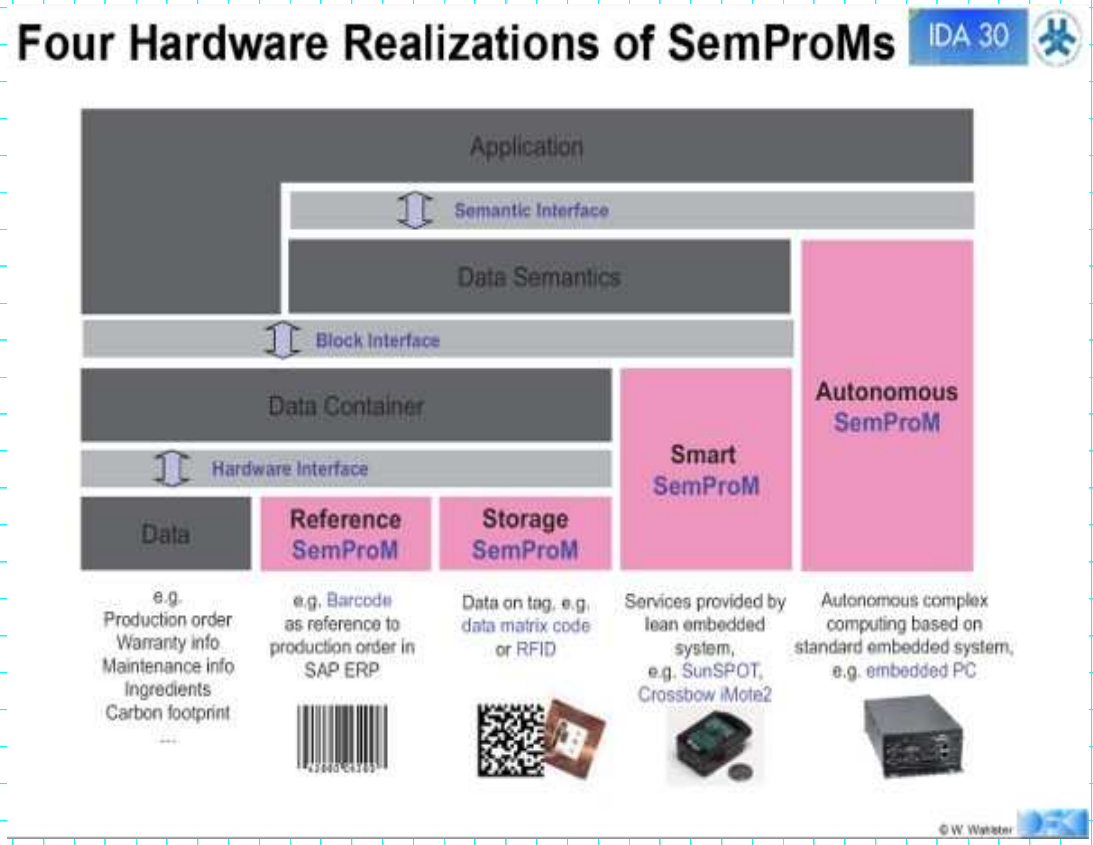


Ciclo decisionale dei prodotti IoT che utilizzano servizi Cloud




Questa soluzione prospetta la possibilità di trasformare un prodotto in un servizio assicurandosi la fidelizzazione del cliente ed entrate regolari.

# Active Product Memory



Infine c'è il punto di vista dei programmatori ovvero degli sviluppatori

In un recente sondaggio organizzato nella primavera di quest'anno dalla IEEE,
oltre la metà degli intervistati hanno ammesso di non avere preso alcuna precauzione particolare nei loro progetti IoT.
E si osservi che gli intervistati costituivano un campione qualificato di addetti ai lavori!

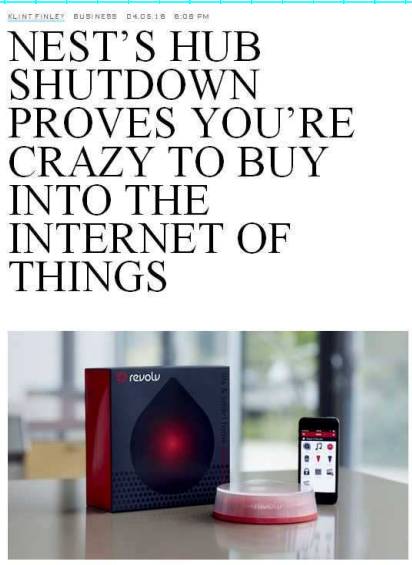
Di fronte ad una simile evidenza, chiaramente, ci si potrebbe limitare ad osservare che
gli interessati non ci fanno una bella figura! Ma sarebbe un giudizio affrettato che non tien conto della realtà in cui ci si trova ad operare ed in particoilare:
- delle limitazioni delle tecnologie attualmente disponibili;
- della scarsa esperienza nello sviluppo di questo tipo di applicazioni;
- ma soprattutto della pressione delle aziende che mirano ad essere le prime ad immettere sui mercato dei prodotti che non molto tempo fa avebbero potuto passare per il frutto dell'immaginazione di un autore di fantascienza!

Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea

Le aziende, che aspirano a proporsi come *leader*, sono attualmente impegnate ad occupare ogni possibile nicchia di mercato, rilasciando dei prodotti HARDWARE equipaggiati di SOFTWARE provvisorio, con la promessa che verrà aggiornato alla prima occasione!

Agendo in tal modo i produttori stanno accumulando un debito tecnologico insanabile, che prima o poi si riperquoterà sulle spalle dei clienti che si sono prestati a ricoprire il ruolo di early adopters. Come del resto è già accaduto l'anno scorso.




KLINT FINLEY BUSINESS 04.05.16 8:08 PM

NEST'S HUB SHUTDOWN PROVES YOU'RE CRAZY TO BUY INTO THE INTERNET OF THINGS




mercoledì 6 aprile 2016 di Gaia Bottà

Commenti (234)

Domotica, utenti in ostaggio del mercato

*Nest renderà inservibili dei controller per la casa connessa lanciati meno di 3 anni fa: l'ennesima dimostrazione del fatto che l'utente non possiede le cose connesse*

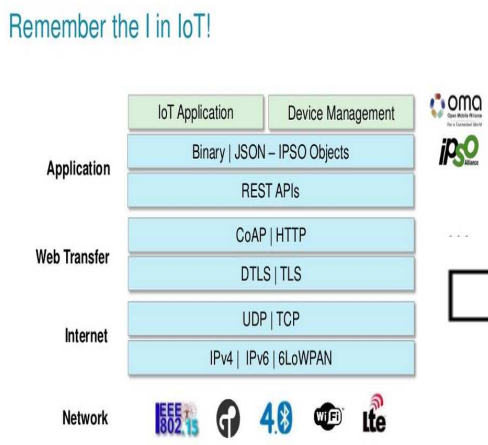
home

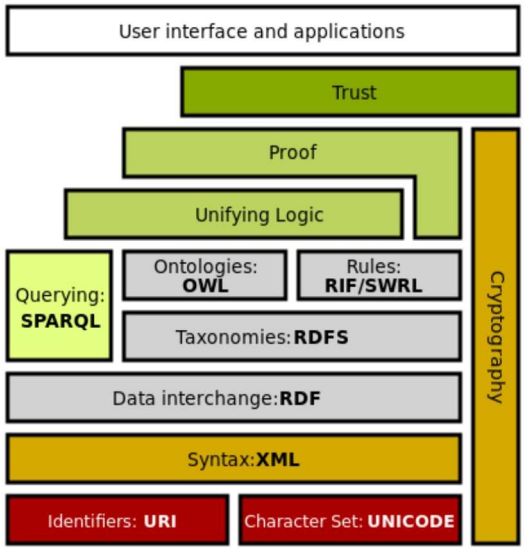
Roma - Revolv era stato presentato come un controller per la casa automatizzata, popolata da dispositivi connessi per l'intrattenimento, l'illuminazione, il riscaldamento, la sicurezza: a seguito di sommovimenti di mercato, lo smart hub smetterà a breve di funzionare, lasciando orfani i dispositivi che operavano nella sua orbita, e gli utenti che li hanno acquistati.

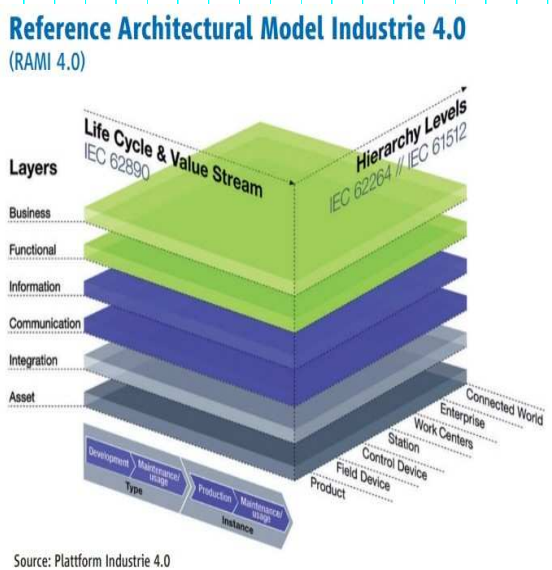


Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea

# Un'ovvia soluzione: il ricorso a Standard Aperti



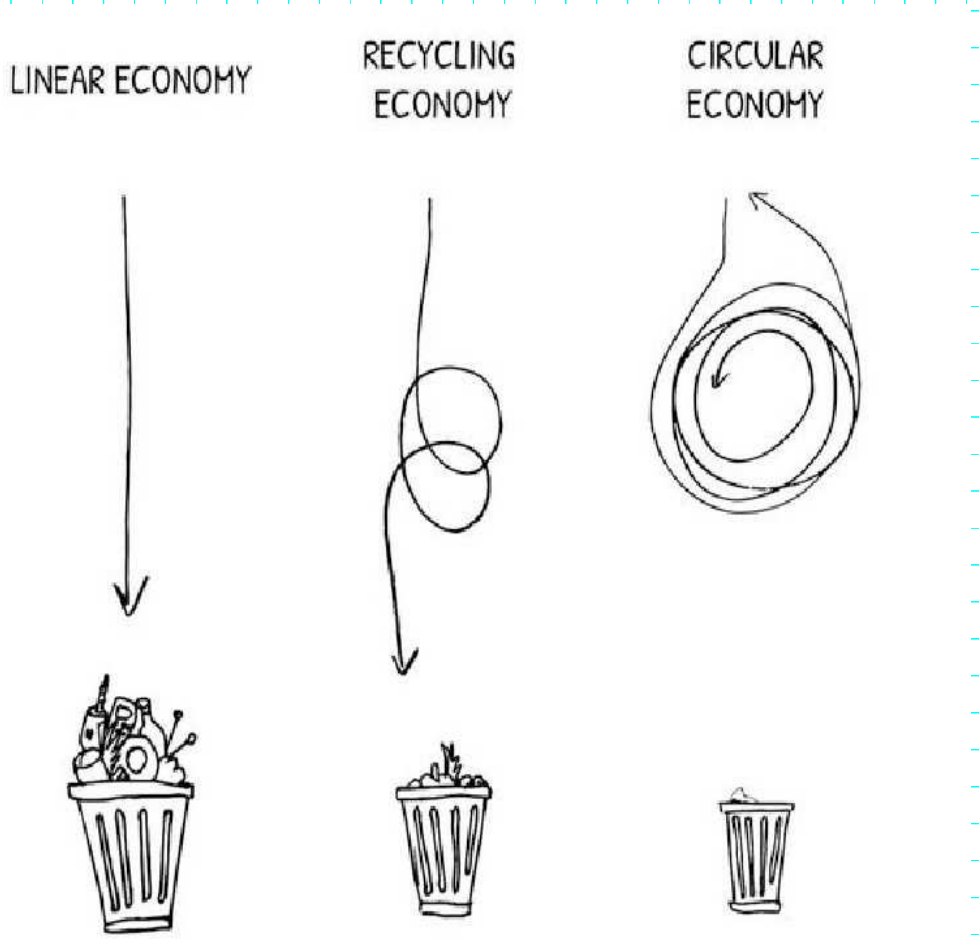



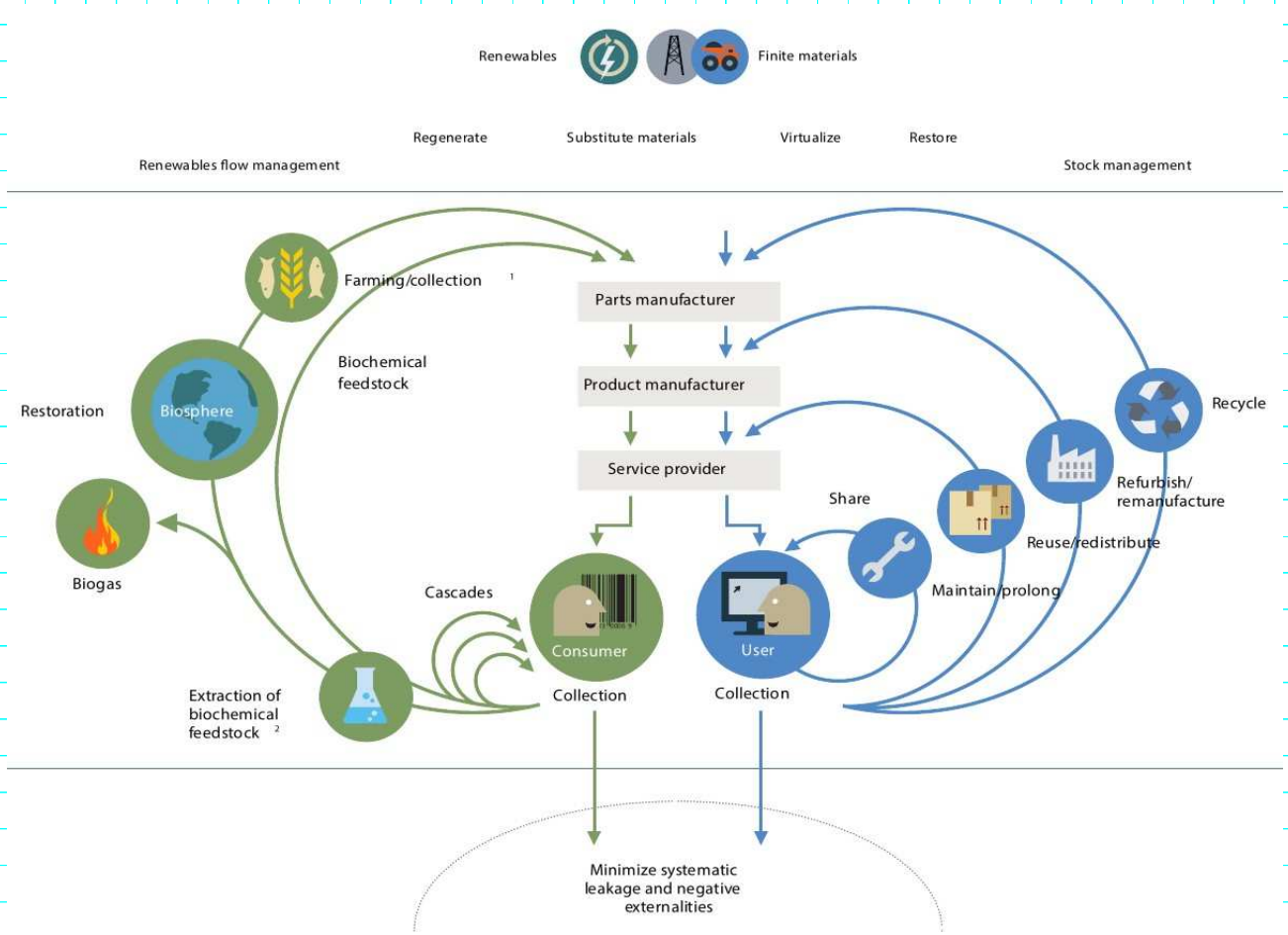




Luigi D. Capra & Norberto Patrignani, "Sicurezza IoT", LinuxDay 2017, Ivrea

Un messaggio di speranza

# Internet of Things enabler of Circular Economy?


LINEAR ECONOMY
RECYCLING ECONOMY
CIRCULAR ECONOMY


Renewables
Finite materials
Regenerate
Substitute materials
Virtualize
Restore
Renewables flow management
Stock management
Farming/collection
Biochemical feedstock
Restoration
Biosphere
Biogas
Extraction of biochemical feedstock
Parts manufacturer
Product manufacturer
Service provider
Cascades
Consumer
Collection
User
Collection
Share
Maintain/prolong
Reuse/redistribute
Refurbish/ remanufacture
Recycle
Minimize systematic leakage and negative externalities

| | INTELLIGENT ASSET VALUE DRIVERS | | |
|---|---|---|---|
| **CIRCULAR ECONOMY VALUE DRIVERS** | Knowledge of the **location** of the asset | Knowledge of the **condition** of the asset | Knowledge of the **availability** of the asset |
| **Extending** the use cycle length of an asset | • Guided replacement service of broken component to extend asset use cycle<br>• Optimised route planning to avoid vehicle wear | • Predictive maintenance and replacement of failing components prior to asset failure<br>• Changed use patterns to minimise wear | • Improved product design from granular usage information<br>• Optimised sizing, supply, and maintenance in energy systems from detailed use patterns |
| Increasing **utilisation** of an asset or resource | • Route planning to reduce driving time and improve utilisation rate<br>• Swift localisation of shared assets | • Minimised downtime through to predictive maintenance<br>• Precise use of input factors (e.g. fertiliser & pesticide) in agriculture | • Automated connection of available, shared asset with next user<br>• Transparency of available space (e.g. parking) to reduce waste (e.g. congestion) |
| **Looping/ cascading** an asset through additional use cycles | • Enhanced reverse logistics planning<br>• Automated localisation of durable goods and materials on secondary markets | • Predictive and effective remanufacturing<br>• Accurate asset valuation by comparison with other assets<br>• Accurate decision-making for future loops (e.g. reman vs. recycle) | • Improved recovery and reuse / repurposing of assets that are no longer in use<br>• Digital marketplace for locally supplied secondary materials |

Source: World Economic Forum report: Intelligent Assets, Unlocking the Circular Economy Potential, 2016


Grazie
per la cortese
attenzione

## Per approfondire:

### Capra-Patrignani : Sicurezza IoT

- Fabbrica 4.0 - Home Page
- Dizionario di IoT e Fabbrica 4.0