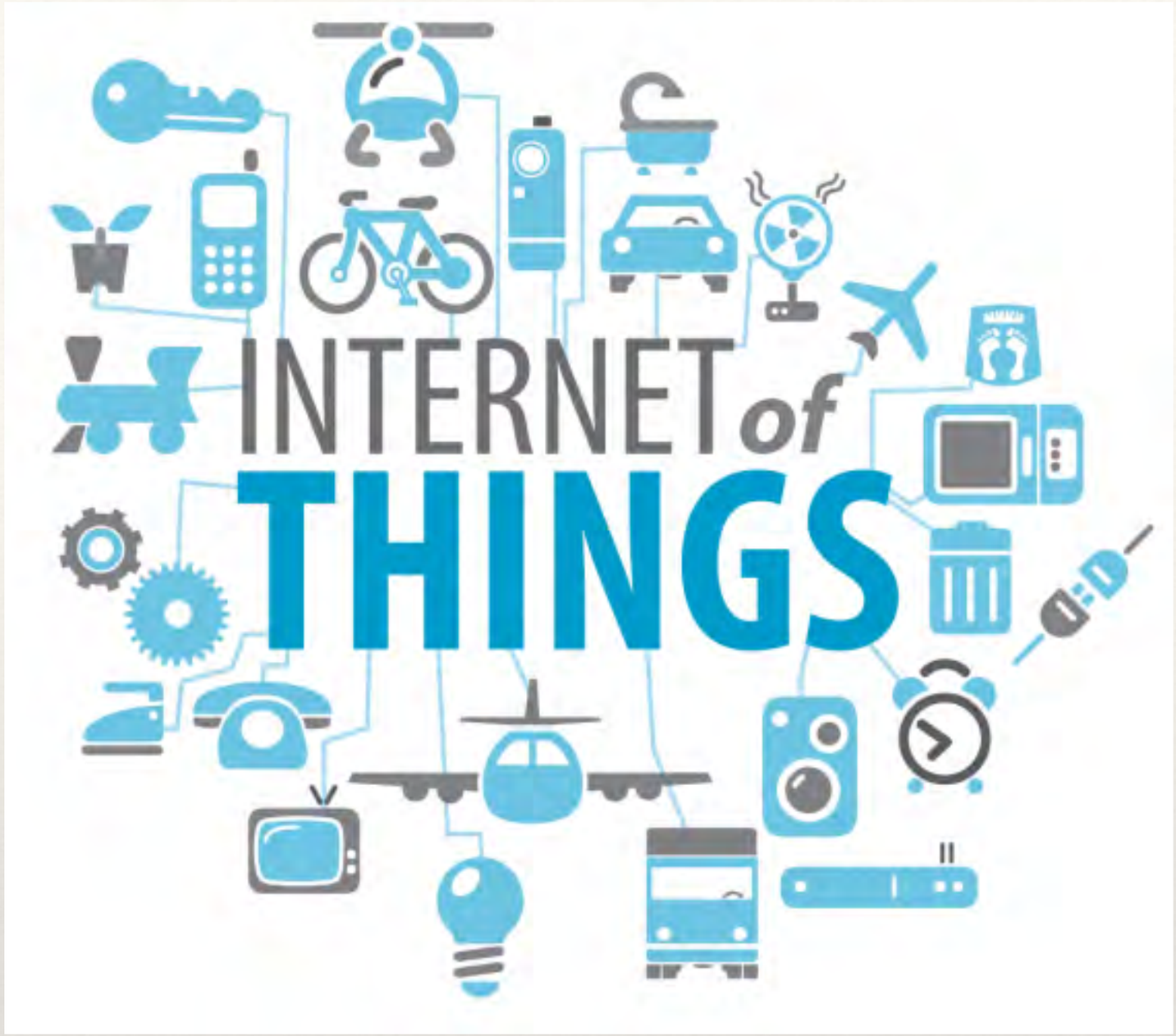


ASSI Bologna
1 luglio 2015
Marco Muratori

La sicurezza oltre l'azienda : Internet of Things

Implicazioni di sicurezza sulla vita quotidiana e lavorativa

Agenda

- ***Definizioni***
- ***Contesti di applicazione***
- ***Chi sono i protagonisti ?***
- ***Vantaggi e rischi***
- ***Impatto sulla sicurezza: gli aspetti chiave***
- ***Aspetti di sicurezza logica***
- ***Aspetti di sicurezza fisica***
- ***Il fattore umano***
- ***Contesti normativi ed evoluzioni possibili***
- ***Conclusioni***

IoT - Definizioni

Estensione di Internet

al mondo degli oggetti e dei luoghi concreti

Tutti gli oggetti possono acquisire un **ruolo attivo**
grazie al collegamento alla Rete.

L'obiettivo dell'internet delle cose è di **far sì che il mondo elettronico tracci una mappa di quello reale**, dando un'identità elettronica alle cose e ai luoghi dell'ambiente fisico.

IoT - Definizioni

Internet of Things : **è un percorso (in divenire)**

- **crea valore per gli individui, le aziende e le nazioni**
- **rivoluziona la concorrenza portandola anche in ambiti finora separati**
- **rende possibili funzioni e servizi prima non immaginabili o troppo onerosi**

è un percorso che coinvolge:

- la definizione di standard di protocolli
- lo sviluppo dei contesti normativi attuali e futuri

che pone altresì nuove questioni di sicurezza nelle possibili applicazioni

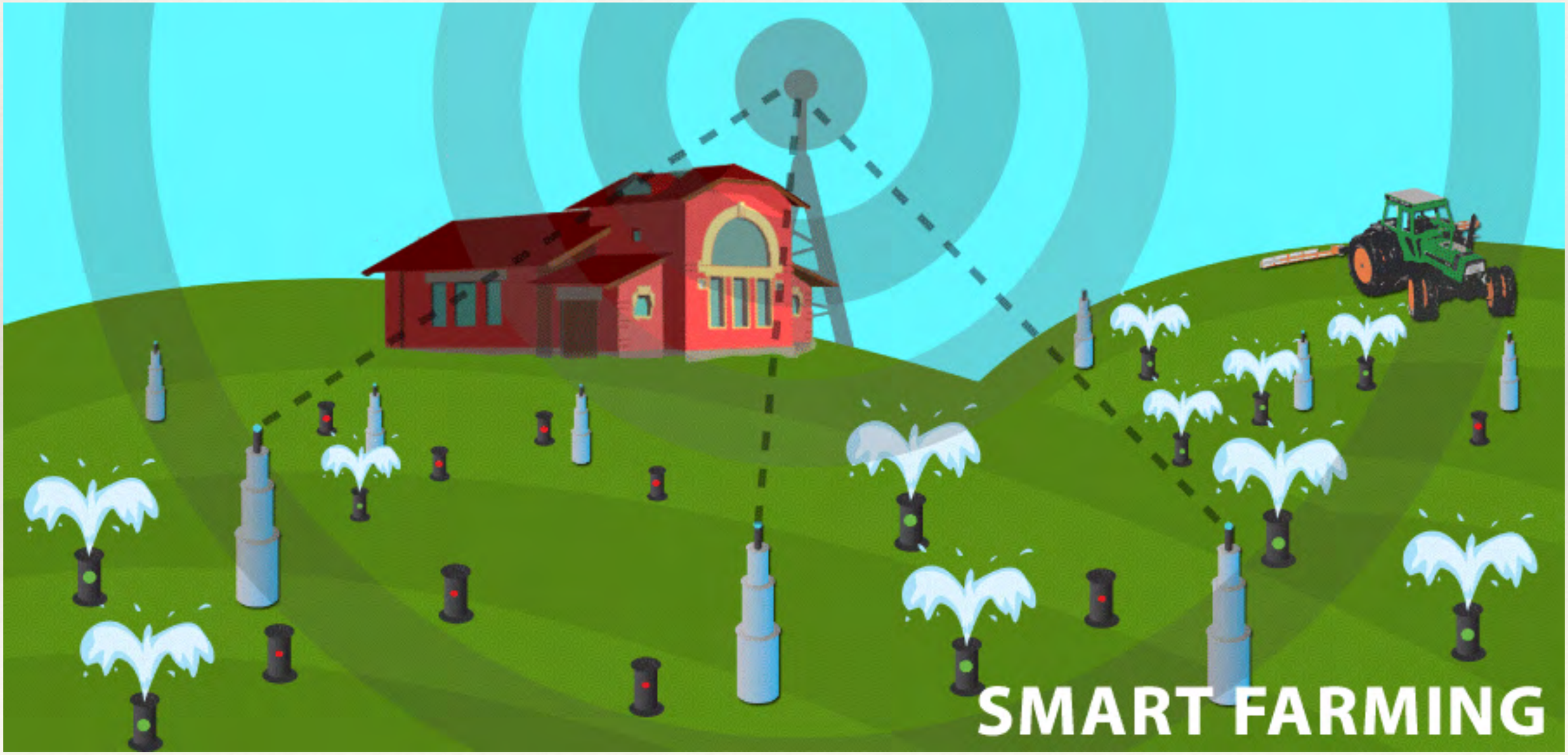
IoT - contesti di applicazione

I principali domini applicativi ed ambiti operativi interessati dallo sviluppo della IoT sono :

- Domotica
- Robotica
- Avionica
- Industria automobilistica
- Biomedicale
- Monitoraggio in ambito industriale
- Telemetria
- Reti wireless di sensori
- Sorveglianza
- Rilevazione eventi avversi
- Smart grid e Smart City
- Sistemi Embedded
- Telematica

IoT - contesti di applicazione

"Agricoltura 2.0" …



IoT - contesti di applicazione

Predictive maintenance

Energy Saving

Improve Productivity

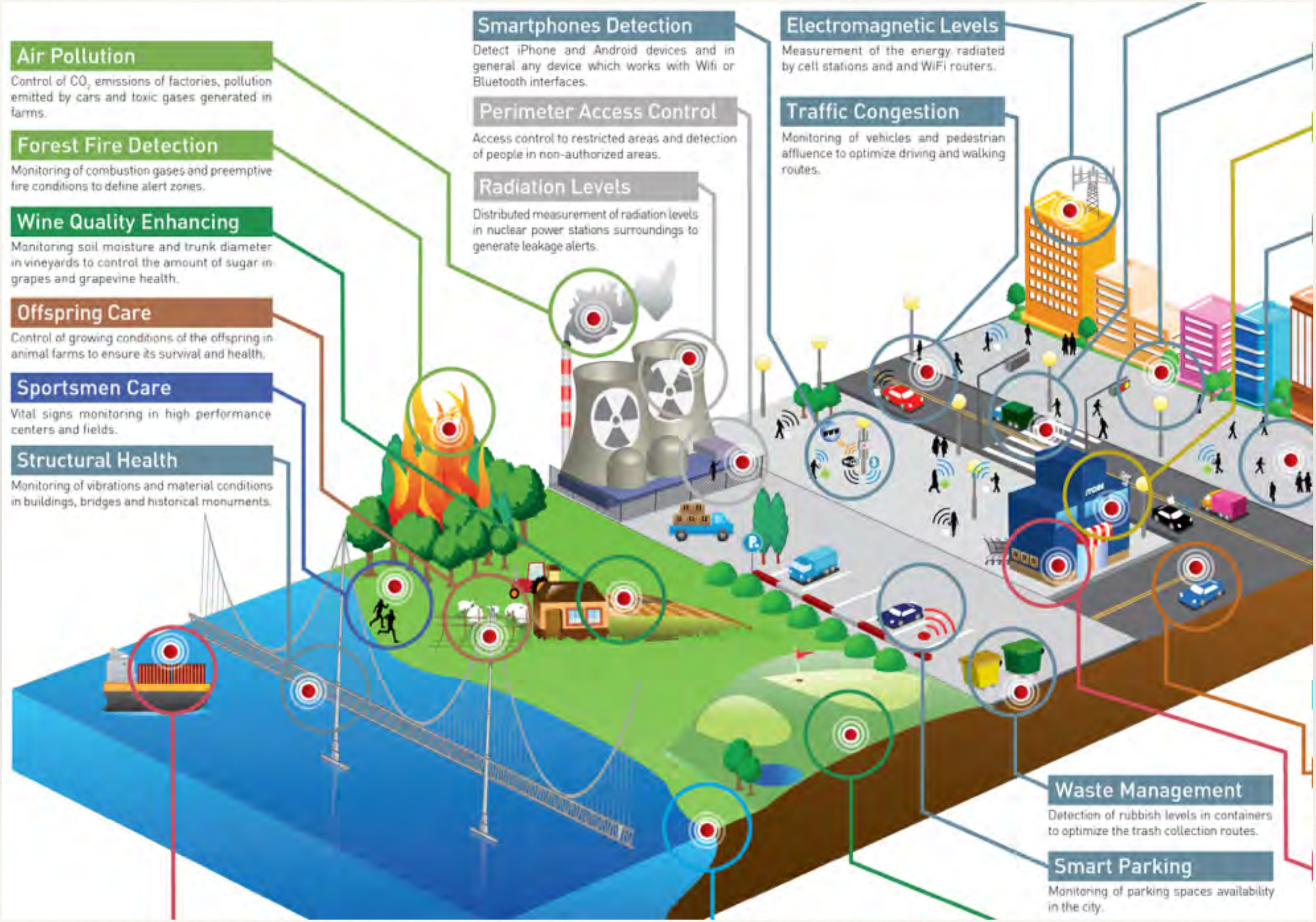
Smart Cities

Intelligent Building

Industrial Automation

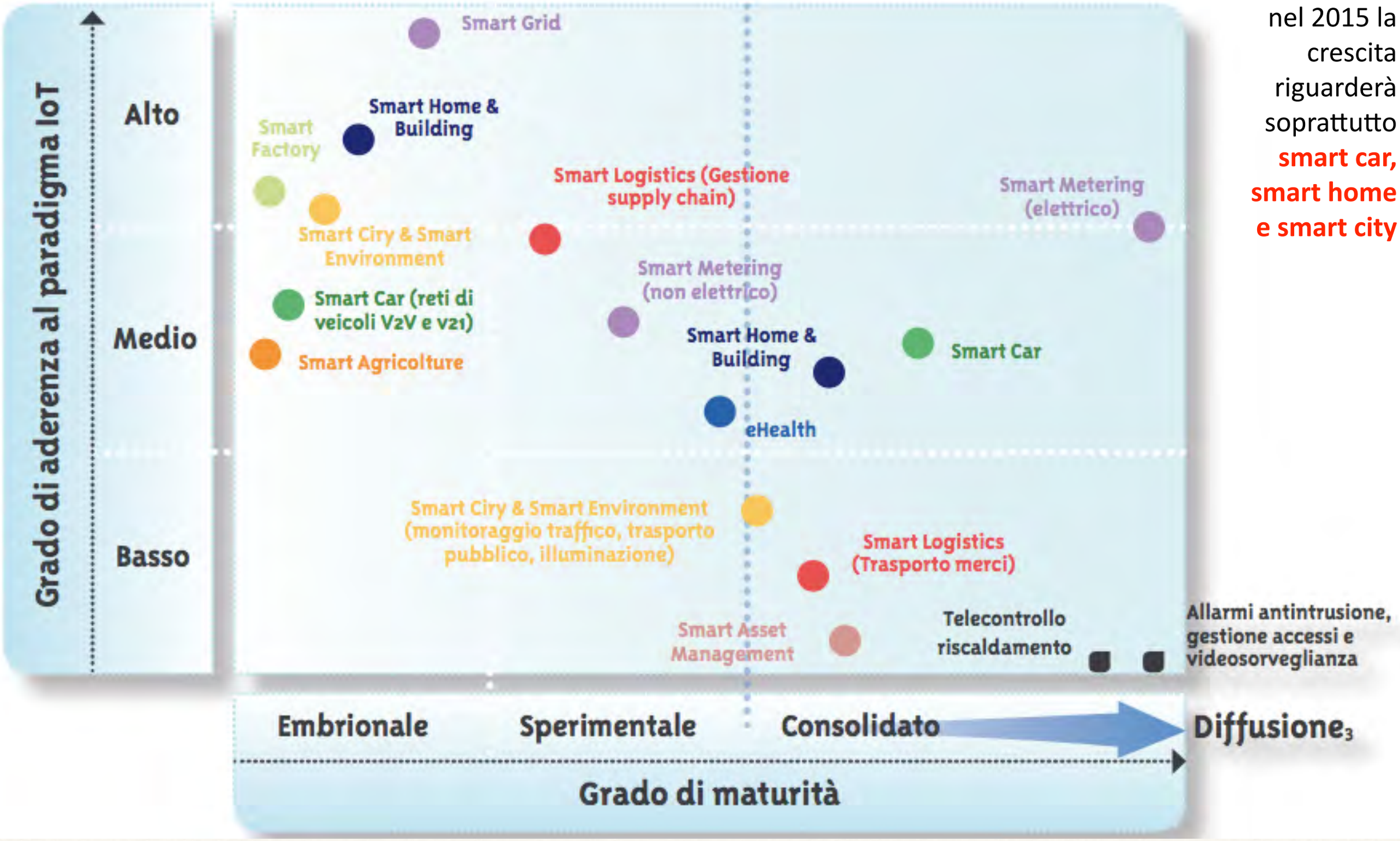
Health Care

Smart Home



IoT : la sicurezza oltre l'azienda - Marco Muratori

IoT - applicazioni in Italia

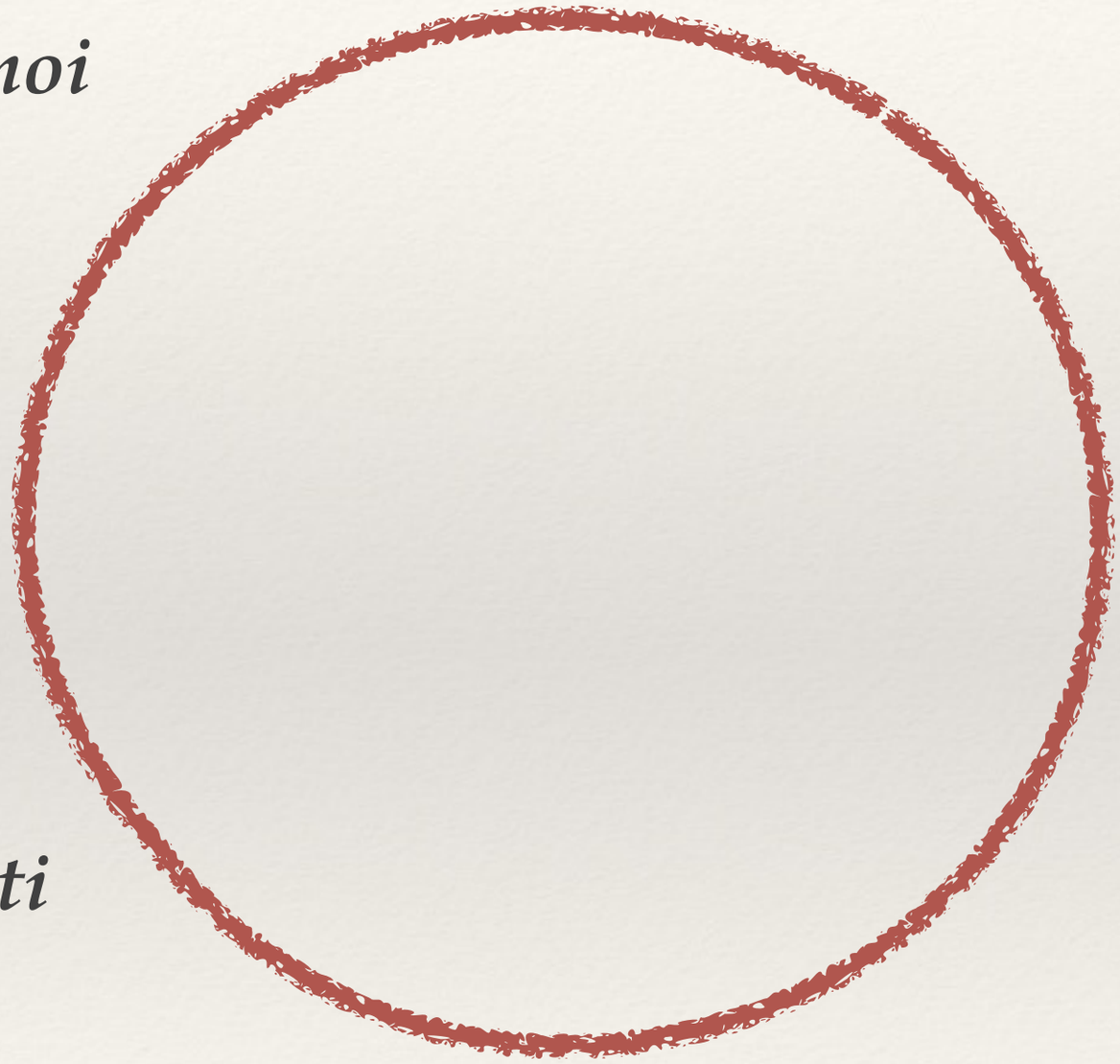


nel 2015 la crescita riguarderà soprattutto **smart car, smart home e smart city**

Fonte : analisi Osservatorio IoT, Politecnico di Milano

Chi sono i protagonisti ?

Tutti noi



Grandi aziende IT (ma non solo)

Gli oggetti

Chi sono i protagonisti ?

Tutti noi

PERCHE' TUTTI NOI ?

Noi interagiamo con gli oggetti

Produciamo e raccogliamo dati

Perché ad oggi sono gli esseri umani a generare la quasi totalità delle informazioni in rete, circa 50 petabytes (un petabyte è 1,024 terabytes). Dati che sono generati dalla digitazione di testo, upload di foto e video, scansioni di codici a barre e codici QR, registrazioni audio, ecc.

Da un lato c'è l'identità delle persone dall'altro i cinque sensi associabili alle possibili interazioni con gli oggetti: fisicamente o da remoto

Limiti a raccolta di dati attraverso l'uomo

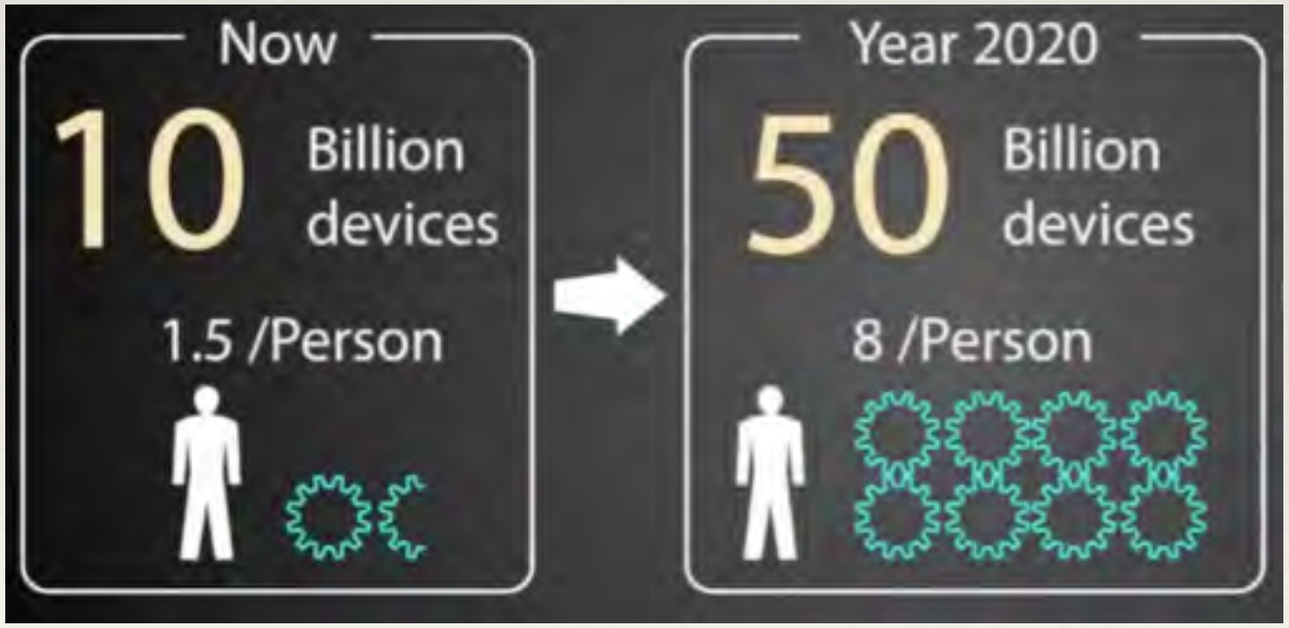
Per nostra natura possiamo raccogliere dati dalla realtà che ci circonda solo per alcune ore al giorno e il nostro livello di attenzione varia così come l'accuratezza.

Chi sono i protagonisti ?

Gli oggetti

Potranno essere…

- quelli che conosciamo, “aggiornati” per comunicare in rete
- **molti altri nuovi** che verranno sviluppati nei prossimi anni e che avranno loro “sensi”



Benson Houghland, TEDxTemecula

Potranno comunicare fra di loro.

E agire anche senza l’uomo.

Chi sono i protagonisti ?

Gli oggetti

COSA LI RENDE “SMART” ?

“AUTO CONSAPEVOLEZZA”	INTERAZIONE CON L’AMBIENTE CIRCOSTANTE	ELABORAZIONE DATI
• Identità univoca	• Acquisizione dati distinta in: Sensing (misura variabili di stato) e Metering (misura variabili di flusso)	• Elaborazione base ovvero il trattamento del dato primitivo raccolto
• Localizzazione		
• Diagnosi stato	• Attuazione ovvero eseguire comandi da remoto o derivati da elaborazione dati in loco	• Elaborazione avanzata ovvero l’estrazione di informazioni dal dato primitivo

Chi sono i protagonisti ?

Grandi aziende IT
(ma non solo)

Disruptive players ?

"Game of acquisitions…"

Nuove startup

Waze

Nest Labs

Deepmind

(quelli di WeChat)

Chi sono i protagonisti ?

Ha appena rilasciato una versione Android per IoT : **OS Brillo** (pesa 30 MB)
Fine maggio 2015

Da due anni ha rilasciato il microchip **Galileo**, ottimizzato per applicazioni IoT

Ha presentato la gamma di microchip **Artik** (tre modelli per ora), compatibili con il software open source di Arduino

Windows 10 supporterà hw pensato per IoT quali Galileo, Arduino, Minnowboard

Chi sono i protagonisti ?

Ha già sul mercato il suo **HomeKit** per la domotica, con diversi prodotti in commercio controllabili direttamente dai dispositivi iOS.

Ha appena introdotto **Agile IoT,** architettura che prevede:
Agile IoT gateway, Agile Controller e LiteOS. Quest'ultimo pesa solo 10KB, non necessita di configurazione e supporta auto-discovery e auto-networking. E' aperto a tutti gli sviluppatori ed è adatto a diversi ambiti applicativi, tra questi smart home, wearable e i veicoli interconnessi.

Fine maggio 2015

La piattaforma cloud **Bluemix**, ha arricchito la componente IoT,
Ci sono poi altri prodotti come **Tivoli Netcool** che riesce a gestire alcuni protocolli industriali e **MessageSight** progettata per gli ambienti machine to machine e mobile. Inoltre i laboratori IBM cercano **algoritmi** sempre più innovativi per l'analisi dei dati in tempo reale

Chi sono i protagonisti ?

Ha presentato il suo sistema operativo **YunOS**

XIAOMI a presentato il suo sistema operativo **Miui**

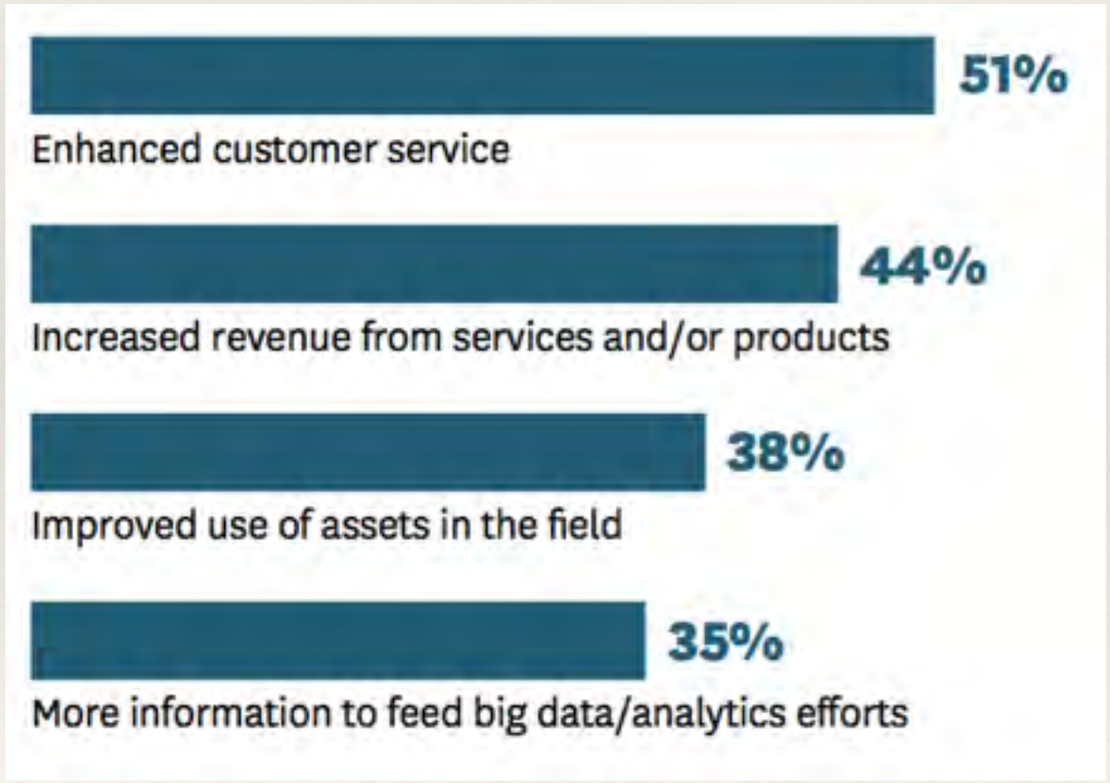
(quelli di WeChat)

Ha introdotto **Tos+**, sarà un connettore per una piattaforma aperta per collegare persone, dispositivi e servizi

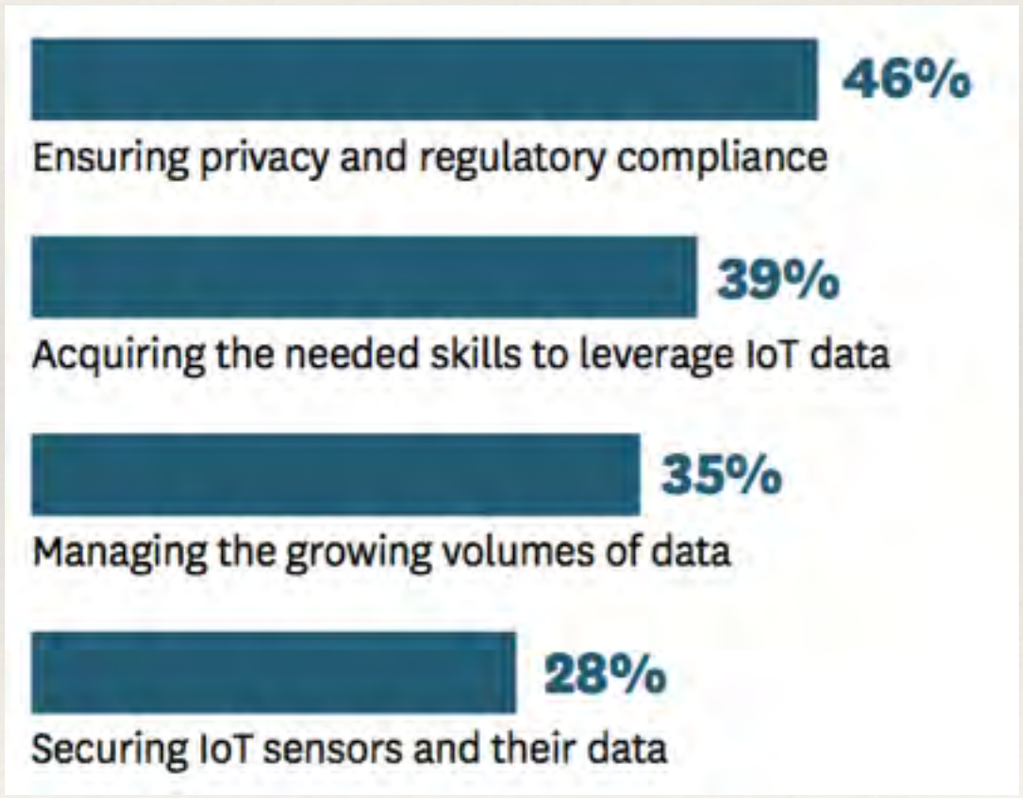
IoT - vantaggi per le aziende

Con tante possibili applicazioni, quali benefici e ostacoli per le aziende ?

Ambiti con i maggiori benefici misurabili :



Cosa frena l'adozione di soluzioni IoT :



Fonte : Harvard Business Review, dicembre 2014

Vantaggi nel mondo industriale

AZIENDE CHE HANNO SVILUPPATO APPROCCI E PRODOTTI IOT IN ITALIA

KEB Italia
Tex Computer,
Siemens Industry Software
ESA Automation
Trend Micro Italia
Schneider Electric
Bosch Rexroth
EFA Automazione
Belden, Industrial IT
neXo
Panasonic Electric Works Italia
Advanced PLC Solutions & SCADA di Mitsubishi Electric
Technical Sales & Business Development Italy, PTC (*)
RFID Global
Rockwell Automation
Embedded Processing di Texas Instruments
SICK
Autodesk
National Instruments

PROCESSI COINVOLTI E BENEFICI OTTENUTI

- Minori tempi morti degli impianti
- Abbattimento costi manutenzioni e post vendita (impianti e prodotti)
- Ingegnerizzazione prodotti (grazie alle analisi)
- Nuovi servizi per impianti industriali
- Ottimizzazioni energetiche
- Riduzione dei costi operativi
- Miglioramento la sicurezza nelle aree di produzione.

(*) PTC ha acquisito la startup ThinkWorx un anno e mezzo fa

Vantaggi e rischi

PERCHE' CON L'INTERNET OF THINGS SI CAMBIA PARADIGMA ?

(anche a livello di sicurezza)

INTERNET OF THINGS

- Oggetti esistenti
- Oggetti nuovi

CRESCENTE POTENZA DI CALCOLO

- per analizzare i Big Data, ora alimentato ulteriormente dalla crescente mole di dati forniti o semilavorati dagli oggetti

..SERVE UN "BIG UNDERSTANDING"

- L'uomo non basta più, si ricorre all'intelligenza artificiale per poter prendere decisioni sensate
- Gli sviluppi dell'AI sono rapidissimi..

Chi detiene la capacità di analizzare queste informazioni

oggi ha la chiave dell'economia e dello sviluppo.

Vantaggi e rischi

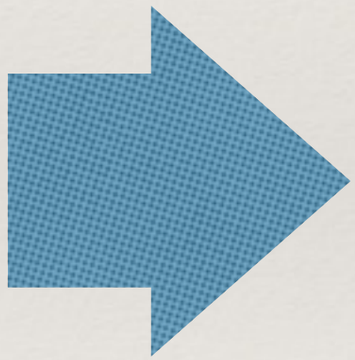
PERCHE' CON L'INTERNET OF THINGS SI CAMBIA PARADIGMA ?

(anche a livello di sicurezza)

INTERNET OF THINGS

CRESCENTE POTENZA DI CALCOLO

INTELLIGENZA ARTIFICIALE



Serve un nuovo modo di gestire la condivisione dei dati,

spesso legata a contesti che variano rapidamente,

per bilanciare privacy e interesse della comunità

Impatto sulla sicurezza: gli aspetti chiave

PRIVACY

- Degli individui
- Delle organizzazioni

CONTESTI NORMATIVI

INTEROPERABILITA’

- Protocolli di comunicazione
- Sistemi operativi
- Framework e architetture

TEMPI DI RISPOSTA

EVOLUZIONI DELLA SICUREZZA FISICA

ASPETTO ORGANIZZATIVO

La sicurezza …oltre l’azienda

Aspetti di sicurezza logica

INTEROPERABILITA’

- Protocolli di comunicazione
- Sistemi operativi
- Framework per IoT

Protocolli di comunicazione

- Tag RFID e codici QR , ormai consolidati
- IPv6 —> indirizzi IP assegnabili ad ogni atomo della Terra e di altri 100 pianeti come la Terra… *(Steve Leisbon)*
- IEEE 802.15.4e, in grado di incrementare notevolmente l'affidabilità dei collegamenti a radio frequenza e l'efficienza energetica, grazie all'adozione del meccanismo di accesso al mezzo *Time Slotted Channel Hopping.*
- IETF 6LoWPAN, RPL, e CoAP, in grado di creare operativamente una rete IP di oggetti che può dialogare con la rete Internet per creare nuovi servizi in molteplici domini applicativi.
- Per l’ultimo miglio : ZigBee, Wireless M-BUS, WiFi e Bluetooth
- Per il backend : tecnologia cellulare 2G, 2G+, 3G, Wireless Mesh o Power Line.

Aziende come B-Scada, ThingWorx, IoT-Ticket.com, Raco Wireless, nPhase, Carriots, EVRYTHNG, Apio e Exosite stanno sviluppando dei **framework per l'internet delle cose**.

Sistemi operativi: Brillo, Arduino, iOS, LiteOS, YunOS, Miui..

Aspetti di sicurezza logica

ARCHITETTURA PREVALENTE IoT IN AMBITO BUSINESS

L'architettura di rete si articola in tre livelli : primo e secondo

Interfaccia con il mondo fisico

A questo primo livello un elevato numero di nodi (tag o unità sensoriali) interagisce con l'ambiente fornendo un codice identificativo, acquisendo informazioni o comandando un attuatore.

Tali nodi hanno ridotta capacità di elaborazione e memoria

Comunicazioni wired o wireless con le unità del secondo livello.

Costi : dai pochi centesimi fino ai 30-150 euro per i nodi con capacità attuative

Vita operativa : da alcuni anni fino a oltre 10

Mediazione

Le unità di secondo livello, di cui fanno parte i lettori di tag RFId e i gateway, hanno il compito di raccogliere le informazioni dai nodi di primo livello per veicolarle ai centri di controllo.

Hanno maggiore capacità di elaborazione e memoria

Costi : può variare molto, dai 50 euro di un nodo gateway ai 2.000 euro di un reader RFId;

i nodi sensore e i gateway non sono ancora caratterizzati da soluzioni standardizzate né in termini di hardware (Mica Motes, Sunspot, Jennic, etc.), né di software (Tiny OS, SOS, Mantis, Contiki, FreeRTOS, etc.), né di middleware (Tiny DB, GSN, DNS, SWORD, ecc.)

Aspetti di sicurezza logica

ARCHITETTURA PREVALENTE IoT IN AMBITO BUSINESS

L'architettura di rete si articola in tre livelli : terzo livello

Centro di controllo

le unità del terzo livello, di cui fanno parte i sistemi di acquisizione centrale e le sale operative, hanno il compito di ricevere le informazioni dalle unità di secondo livello per le successive fasi di memorizzazione, elaborazione e la messa in fruibilità dei dati.

Il costo di queste unità può variare da 1.000 a 10.000 euro trattandosi di calcolatori di fascia medio-alta.

Aspetti di sicurezza fisica

EVOLUZIONI DELLA SICUREZZA FISICA

L'introduzione di oggetti SMART nei controlli fisici consentirà di
- migliorare quelli esistenti
- consentire nuove forme di controllo
- tutelarsi dalle nuove minacce

Controllo accessi

I fattori di autenticazione sono in base a:

- Qualcosa che so
- Qualcosa che ho
- Qualcosa che sono
- Qualcosa che faccio
- Una qualsiasi combinazione degli stessi

Esempi

riconoscimento targhe veicoli

+

riconoscimento volti e comportamenti

+

sensori che analizzano
temperatura veicoli e/o peso
in appositi punti di transito

Aspetti di sicurezza fisica

EVOLUZIONI DELLA SICUREZZA FISICA

La sicurezza fisica vede come potenziali minacce
sia gli uomini
sia dispositivi ..che potranno essere diretti dai primi o autonomi..

Quali sotto sistemi sono coinvolti ?

- Controllo accessi (a livello applicativo)
- Sistemi anti intrusione
- Impianti speciali
- Dispositivi IoT

I rilevatori

È il mezzo attraverso il quale viene prodotta l'informazione di pericolo

Deve poter rilevare una serie di eventi (PD ossia probabilità di detezione) e comportamenti.

Non deve generare falsi allarmi

Quanto è sabotabile o eludibile?

Aspetti di sicurezza fisica

IL MONDO (ATTUALE) DEI RILEVATORI

Contatti elettromeccanici
Contatto magnetico
Sensori a filo teso
Pesatura oggetti
Infrarosso passivo
Filo o serigrafia
Sensore inerziale
Microfono selettivo
Sensori capacitivi
Tappeti sensibili
Microfono acustico
Rottura vetro con apposito sensore

Barriera infrarosso attivo
Barriera bistatica a microonde
Doppler a microonde o ultrasuoni
Fibra ottica
Fili tesi
Devo fence
Elettro fence
GPS (pressione differenziale)
Cavo microfonico
Cavo fessurato
Sensore tattico portatile a microonde
Campo elettrostatico
Sismici

Aspetti di sicurezza fisica e logica

TEMPI DI RISPOSTA

Equazione minima per la sicurezza

Triv + Ttx + Tint < = Tabb

- Triv è tempo di rilevazione dell'intrusione
- Ttx è il tempo per trasmettere l'informazione
- Tint è il tempo necessario per intervenire
- Tabb è il empo necessario per abbattere i mezzi passivi posti a difesi del bene da proteggere

- **Tempi di rilevazione**: già in molti attacchi informatici i malintenzionati non lasciano traccia delle loro "osservazioni"
- Ora si aggiungono altre minacce legate agli "oggetti".. ad esempio i droni (UAV)

Aspetti di sicurezza fisica : i droni

DRONI: 40 USI CIVILI

SERVIZI DI EMERGENZA
1. Monitoraggio di merci pericolose
2. Servizi di emergenza (medicine e attrezzature mediche)
3. Coordinamento delle emergenze
4. Valutazione post-disastri
5. Salvataggio

SERVIZI DI SICUREZZA
6. Investigazione e scene del crimine
7. Sorveglianza
8. Polizia
9. Sorveglianza per la sicurezza
10. Gestione evento di pericolo

AGRICOLTURA
11. Trattamenti chimici e biologici
12. Monitoraggio incendi
13. Inventari
14. Salvataggio animali
15. Operazioni di precisione

GESTIONE AMBIENTALE
16. Pericoli e impatti ambientali
17. Controllo conformità ambientale
18. controllo delle specie e dei parassiti invasivi
19. Ricerca scientifica
20. Monitoraggio habitat e protezione animale

URBANISTICA, PATRIMONIO IMMOBILIARE, ARCHITETTURA E INGEGNERIA
21. Costruzione
22. Architettura, ingegneria, paesaggio urbano e design
23. Mapping (risorse topografiche)
24. Marketing
25. Pianificazione, progettazione

MEDIA E COMUNICAZIONI
26. Pubblicità e marketing
27. Arte (progettazioni commerciali)
28. Intrattenimento (cinema, televisione, internet...)
29. Giornalismo investigativo
30. Notizie e fotografia

BUSINESS E COMMERCIO
31. Aero-tecnologia, robotica, ricerca e sviluppo
32. Reporting
33. Esplorazione (acqua, olio, gas, minerali...)
34. Inspezioni: (infrastrutture e industrie)
35. Servizi di consegna

RICREAZIONE E INTRATTENIMENTO
36. Esplorazioni
37. Eventi
38. Hobby
39. Fotografia e video
40. Controllo remoto del volo

Aspetti di sicurezza logica

ASPETTO ORGANIZZATIVO

Gli oggetti connessi AMPLIFICANO i rischi esistenti : molte vulnerabilità saranno **VULNERABILITA' INDOTTE** sia per la possibile esposizione a rischi degli oggetti sia per le aumentate possibilità di interazioni (normali o malevole) con gli esseri umani

Quale risposta efficace per le aziende ?

L'unica risposta permanente efficace per le aziende, a prescindere dalla tecnologia, è quello di **definire un solo responsabile della sicurezza, a tutto tondo. Che interagisce con tutte le funzioni aziendali e che riporta direttamente al board.**

Costui effettuerà un assessment sui rischi inerenti ai processi aziendali, assegnerà un valore economico ai rischi inerenti le attiva svolte, definirà i mezzi adatti per avere il rischio considerato accettabile e implementa un processo continuo di miglioramento

Il fattore umano

L’uomo è l’artefice delle rivoluzioni possibili con l’IoT nel bene come nel male.

Ecco i temi chiave esistenti che l’adozione dell’IoT amplifica :

Formazione PERMANENTE sugli impatti della tecnologia su uomo e ambiente
Per chi produce e sviluppa
In alcuni contesti saranno sviluppate

Etica nell'uso dei dati raccolti
Normative, **policy aziendali** e …
personali

Termini d'uso per applicazioni e servizi
--> necessità **dirompente** di consulenze multi disciplinari (es. risarcimento danni..) ?

Coscienza critica nell’uso degli oggetti connessi
Esempio dei termini e condizioni dell'hot spot Wi-Fi all'aeroporto di Londra attivato da F-Secure

Contesti normativi ed evoluzioni possibili

Ci sono 28 Autorità per la privacy in Europa, si coordinano ma ci sono contesti normativi diversi..

ARRIVA IL REGOLAMENTO EUROPEO…

A dicembre 2014 è stata approvata la prima versione del Regolamento Europeo per la Privacy che consentirà una normativa uniforme a livello di Unione Europea…

Dovrebbe essere emanato tra la fine del 2015 e il primo semestre del 2016

SOSTITUISCE NORME ESISTENTI

Abrogherà la direttiva 95/46 in materia di protezione dei dati personali e anche parte del Codice italiano della privacy *(rimanendo inalterate le norme di attuazione della Direttiva 2002/58 e quelle della Direttiva 2009/136)*.

REGOLE ANCHE SOGGETTI EXTRA UE

Il regolamento conterrà una clausola tramite la quale si ovvierà all'applicazione di due normative diverse, stabilendo un'unica disciplina alla quale dovrà sottostare qualsiasi soggetto che offre beni e servizi a cittadini dell'Unione europea, anche se non stabilito nel suo territorio.

Contesti normativi ed evoluzioni possibili

COMPARE UNA NUOVA FIGURA : IL DATA PROTECTION OFFICER

Per gestire i nuovi adempimenti sarà introdotta anche la figura (nuova nell'ordinamento italiano) del Responsabile della protezione dei dati personali (c.d. Data Protection Officer, Dpo)

Potrà essere un soggetto interno o esterno con compiti di informazione, sorveglianza e controllo in merito agli adempimenti tecnico-organizzativi e di sicurezza.

Per ora non sembra sarà obbligatorio, tuttavia.
probabilmente sarà una figura dirigenziale o equivalente.

Contesti normativi ed evoluzioni possibili

QUALI COMPITI PER IL DATA PROTECTION OFFICER ?

1) sorvegliare la corretta applicazione della normativa sulla protezione dei dati, incluse le misure e le procedure tecniche e organizzative
2) sorvegliare la corretta applicazione della protezione dei dati sin dalla progettazione degli applicativi (privacy by design), garantendo per gli stessi delle impostazioni privacy predefinite (privacy by default) nonchè la sicurezza dei dati
3) effettuare ispezioni, consultazioni, attività di documentazione
4) partecipare alla redazione dei Data protection impact analysis (c.d. Dpia)
5) fungere da contact point e collaborare con l'Autorità Garante
6) controllare che le violazioni dei dati personali siano documentate, notificate e comunicate (c.d. Data Breach Notification Management).

Contesti normativi ed evoluzioni possibili

QUALI REQUISITI PER IL DPO ?

IL REGOLAMENTO EUROPEO CITA SOLO CHE E' :
"necessaria una "conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai compiti".

REALISTICAMENTE CHI POTRA' FARLO ?

Chi ha una conoscenza in ambito tecnico-informatico **funzionale alla natura delle attività che svolge il titolare del trattamento**

Chi ha **certificazioni che verificano le competenze effettive** quali quelle internazionalmente riconosciute e rilasciate da organismi che operano da anni nel settore come per esempio da Isaca e da Iapp (p.e. Cissp, Cisa, Cism, Cipp et similia)

Conclusioni

ENTRO IL 2018… **non ci sarà un ecosistema IoT dominante, i leader IT avranno ancora bisogno di comporre soluzioni da provider multipli". Una piattaforma unica: questa è la sfida futura, da cui dipenderà il successo dell'Internet of Things nel lungo periodo**

(fonte: Gartner)

Chi consentirà di sfruttare appieno l'IoT ?

Chi offre soluzioni a livello di servizio ossia per la mediazione dei protocolli e tutte le applicazioni per la gestione delle funzionalità di business

Chi offrirà strumenti per un uso intelligente dei dati ossia estrarre diverse tipologie di dati **per tradurli in informazioni di business utili all'azienda e ai partner** per differenziarsi rispetto alla concorrenza

Conclusioni - nel concreto…

Fruibilità delle applicazioni in nuovi contesti e con nuovi dispositivi
—> opportunità su tutti i fronti (clienti, partner, personale dipendente)

Rischi amplificati a livello di individui (metà dei dispositivi smart home hanno lacune) e di organizzazioni (un altoforno bloccato quali danni provoca ?)

“Human factor”
Gli strumenti per gestire la sicurezza ci sono ma i benefici dell’adozione di soluzioni che integrano l’Iot saranno tali solo se il fattore umano sarà indirizzato correttamente ossia:
—> politica di sicurezza delle aziende come processo strutturato che tocca tutte le funzioni (non solo staff IT): a livello di selezione del personale, processi, analisi dei rischi e policy adottate (comitati, deterrenti, sanzioni, ecc)
—> DEDICARE TEMPO E RISORSE