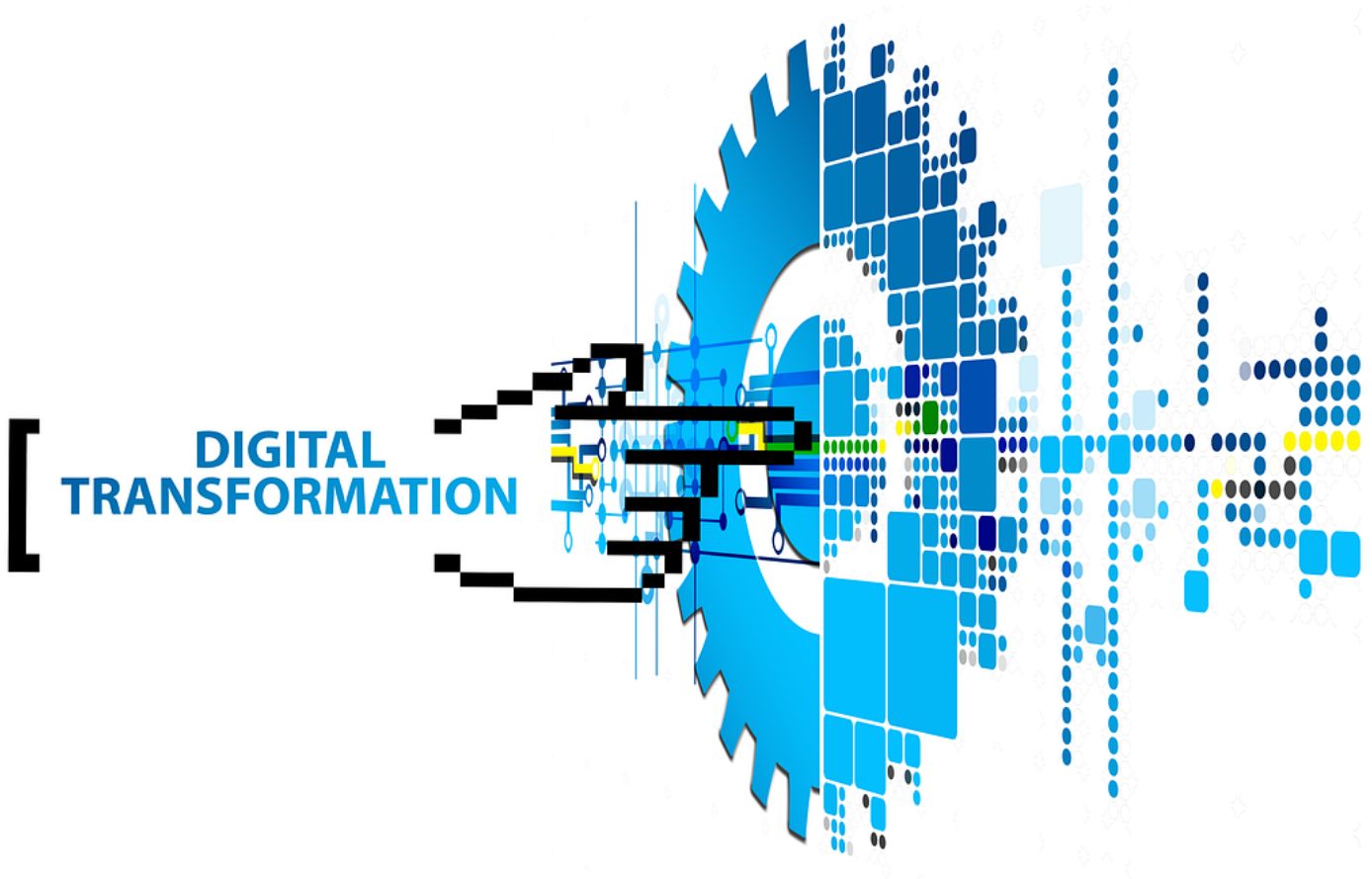
Trasformazione digitale e sicurezza dell'IIoT



Vincenzo Calabrò

“The internet of things (to be hacked)”

Anno 2014

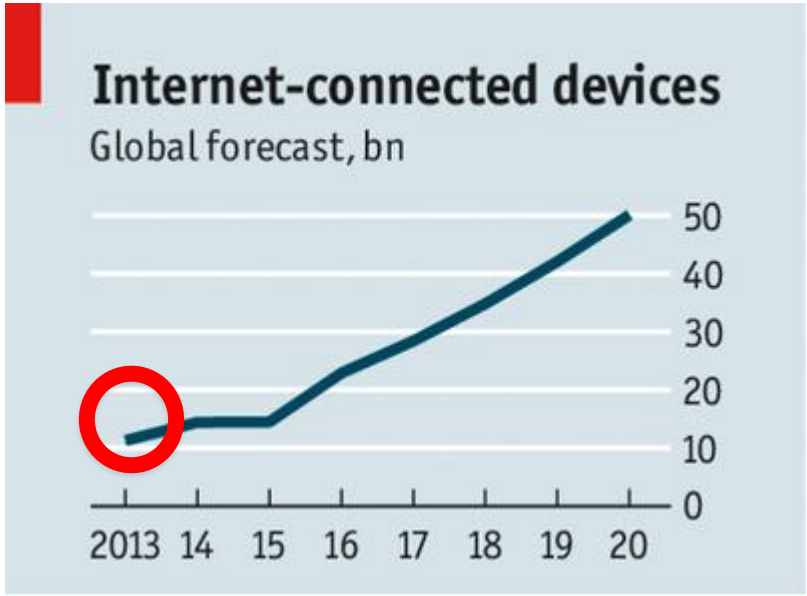
“Hooking up gadgets to the web promises huge benefits. But cyber security must not be an afterthought

A new phase is emerging: “the internet of things”: miniature computers embedded in objects and connecting them to the internet using wireless technology.

These small, embedded computers at the centre of the internet of things do not have as much processing power or memory, so security software tends to be rudimentary.

For the companies building the internet of things, its vulnerabilities could be costly. Tech firms will surely have to embrace higher standards.”

[The Economist, 2014]



“A cyber-attack on an American water plant rattles nerves”

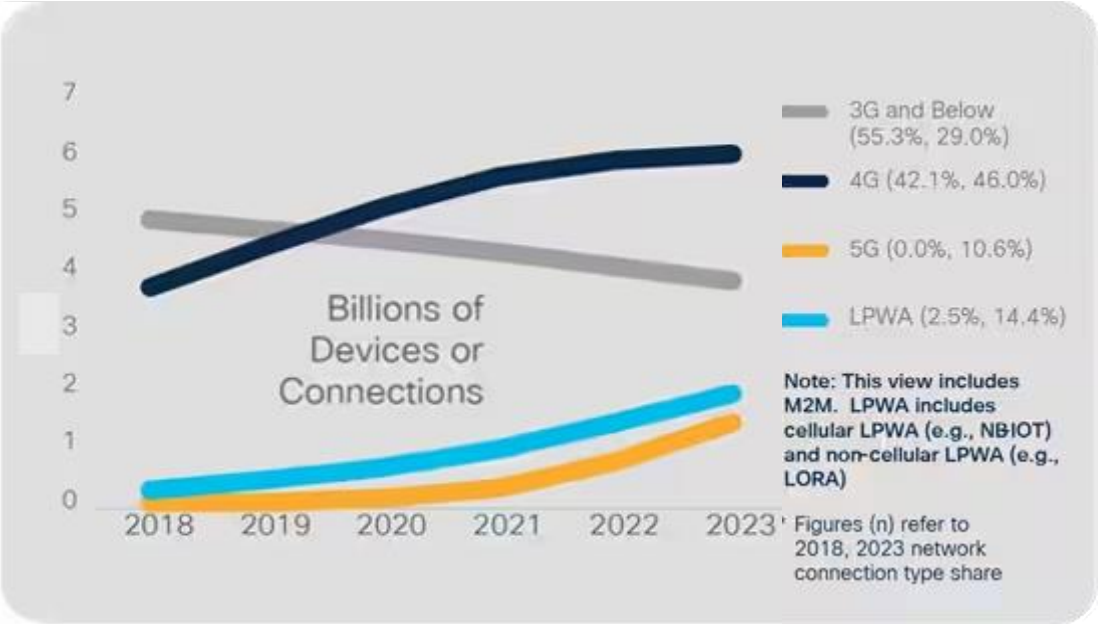
Anno 2020

Nel 2020, qualcuno avvelena l’impianto idrico di una città della Florida. La progressiva digitalizzazione dell’infrastruttura l’ha resa vulnerabile: l’attacco avviene a causa di un dipendente che installa TeamViewer.

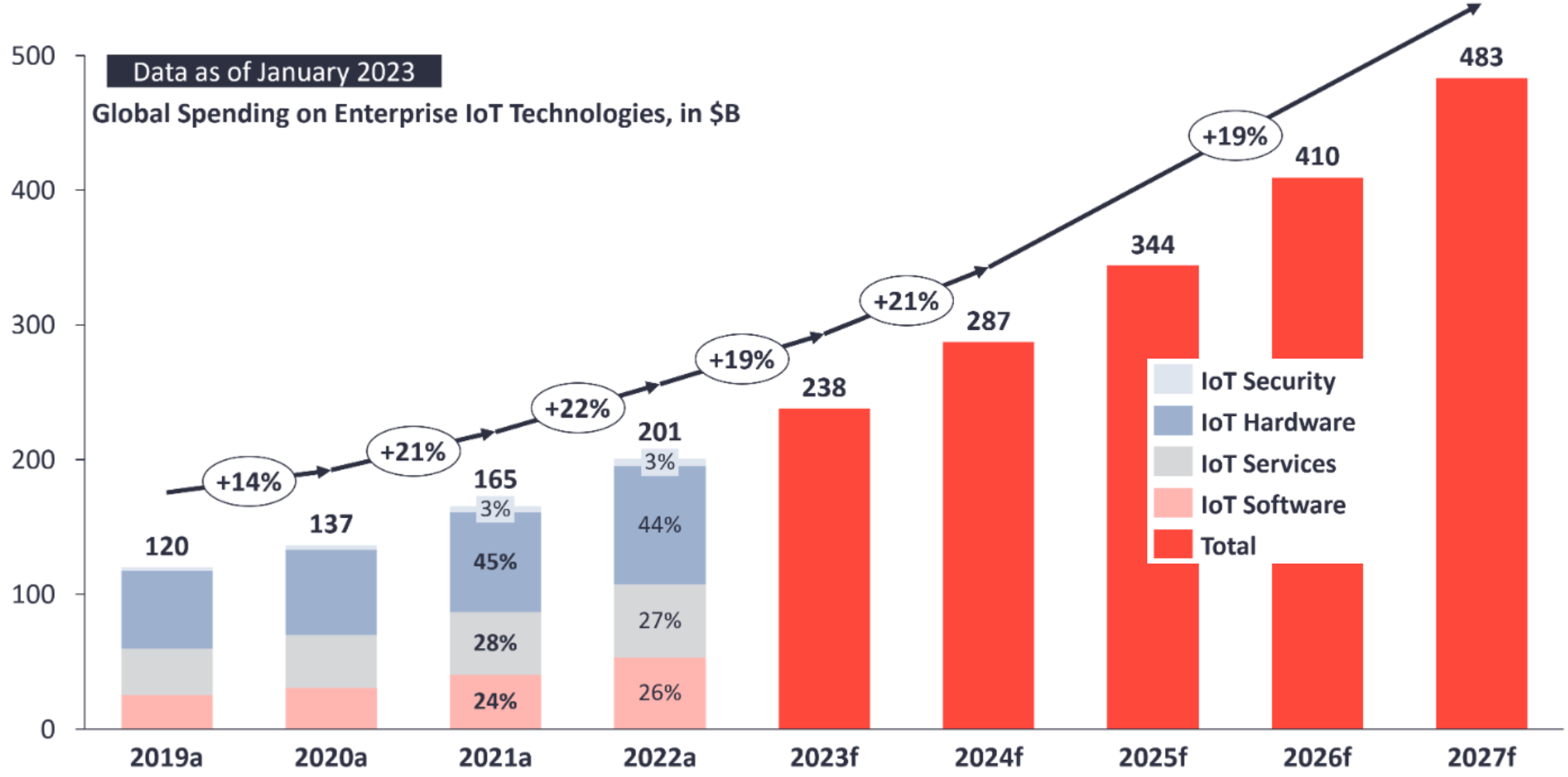
Già nel 2020, ci sono più di 112.000 sistemi di controllo industriale aperti ad internet.

Le 70.000 utilities idriche degli USA mettono su reti digitali “with dramatic variations in capacity and sophistication”, e “remaining ill-prepared to defend their networks.”

Gli Stati comprendono che possono penetrare le infrastrutture critiche degli altri a basso costo.



Industrial Internet of Things (IIoT) oggi

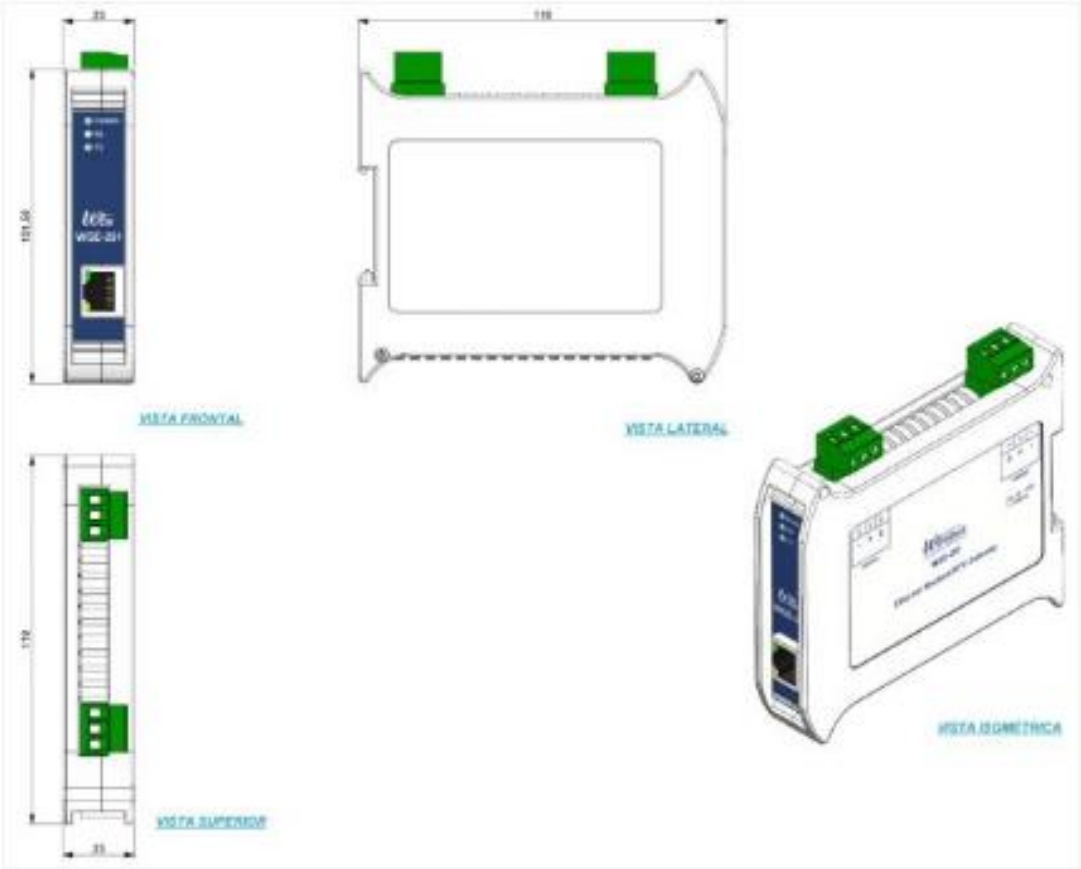


La Trasformazione Digitale: Industrial Internet of Things (IIoT)

Cyber-physical systems (CPS)

Cloud computing
Edge computing
Big data analytics

Cybersecurity
Artificial intelligence

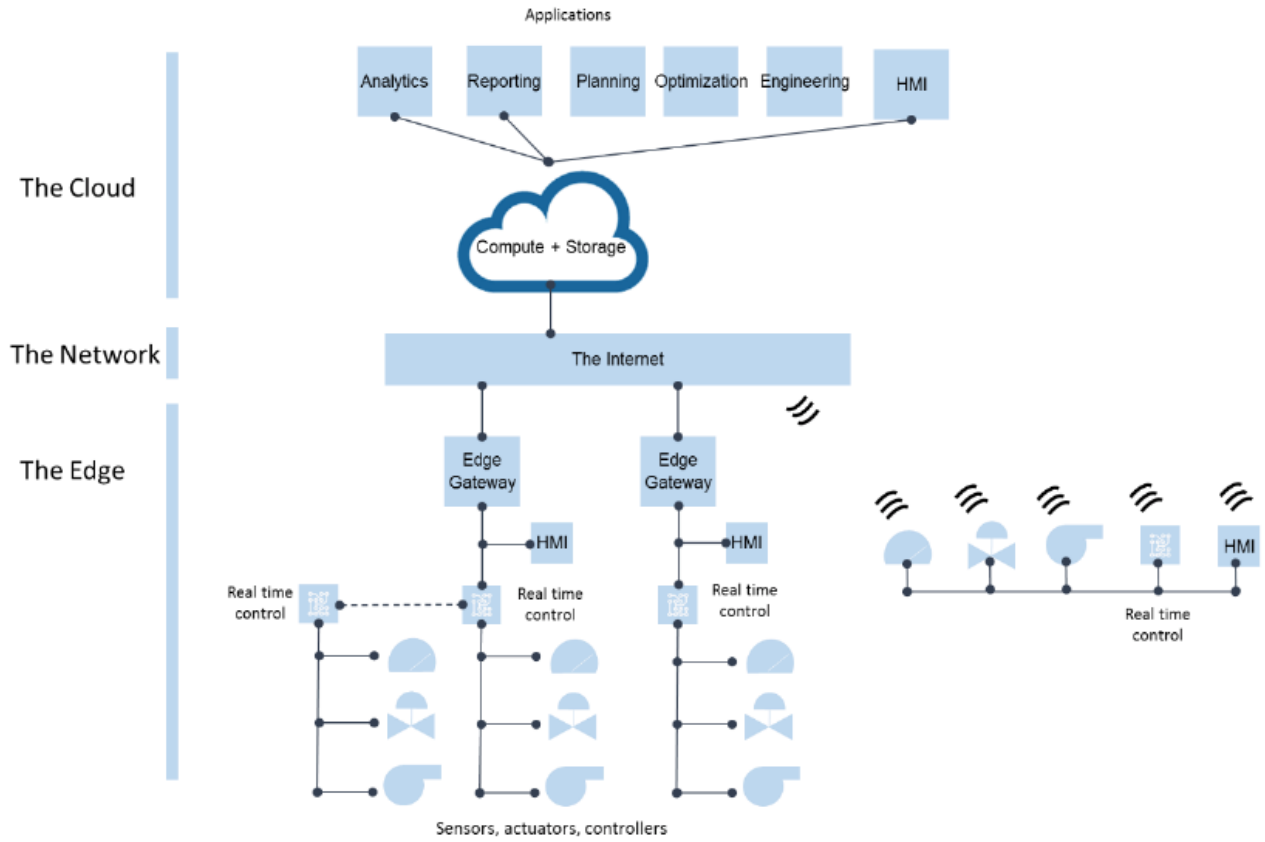


La Trasformazione Digitale: Industrial Internet of Things (IIoT)

Cyber-physical systems (CPS)

Cloud computing
Edge computing
Big data analytics

Cybersecurity
Artificial intelligence



Industrial IoT direttrici di sviluppo

Based on proven and mature technologies

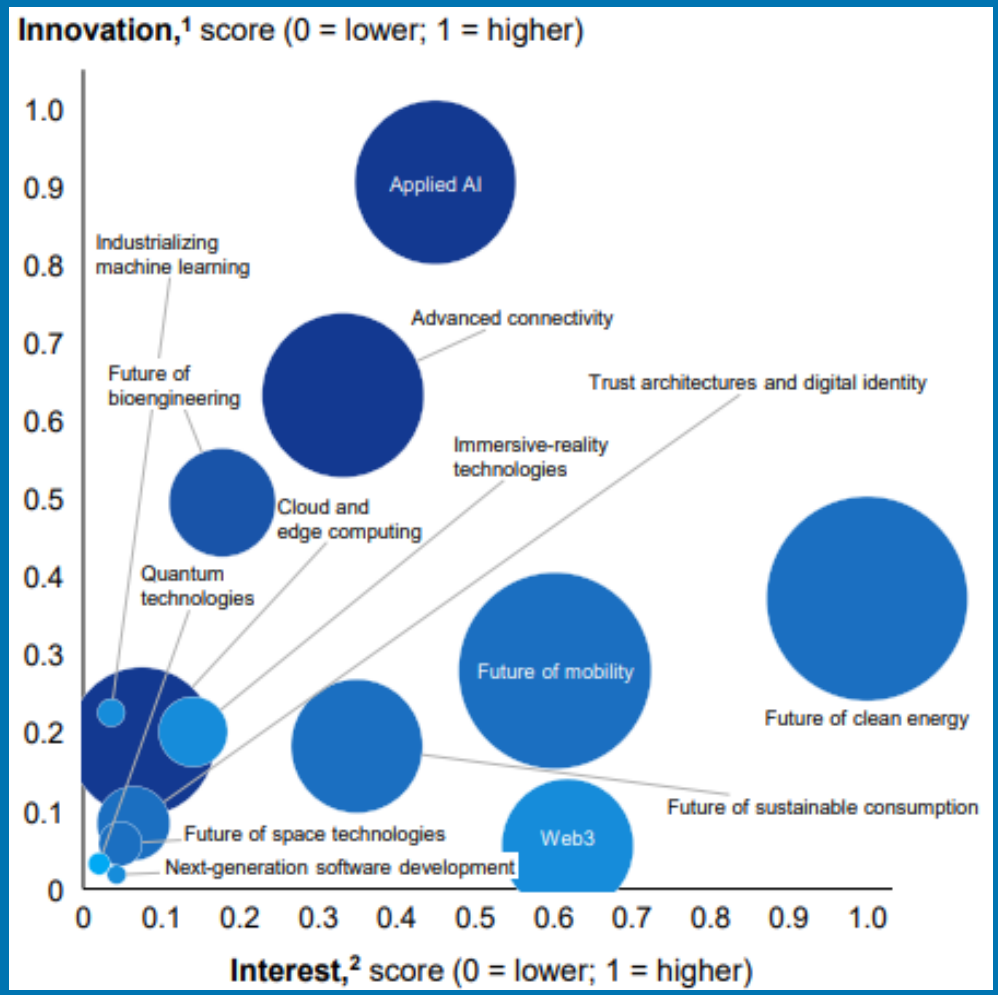
- applied AI
- advanced connectivity
- bioengineering
- cloud and edge computing

Sustainability priorities

- clean energy
- sustainable consumption
- mobility

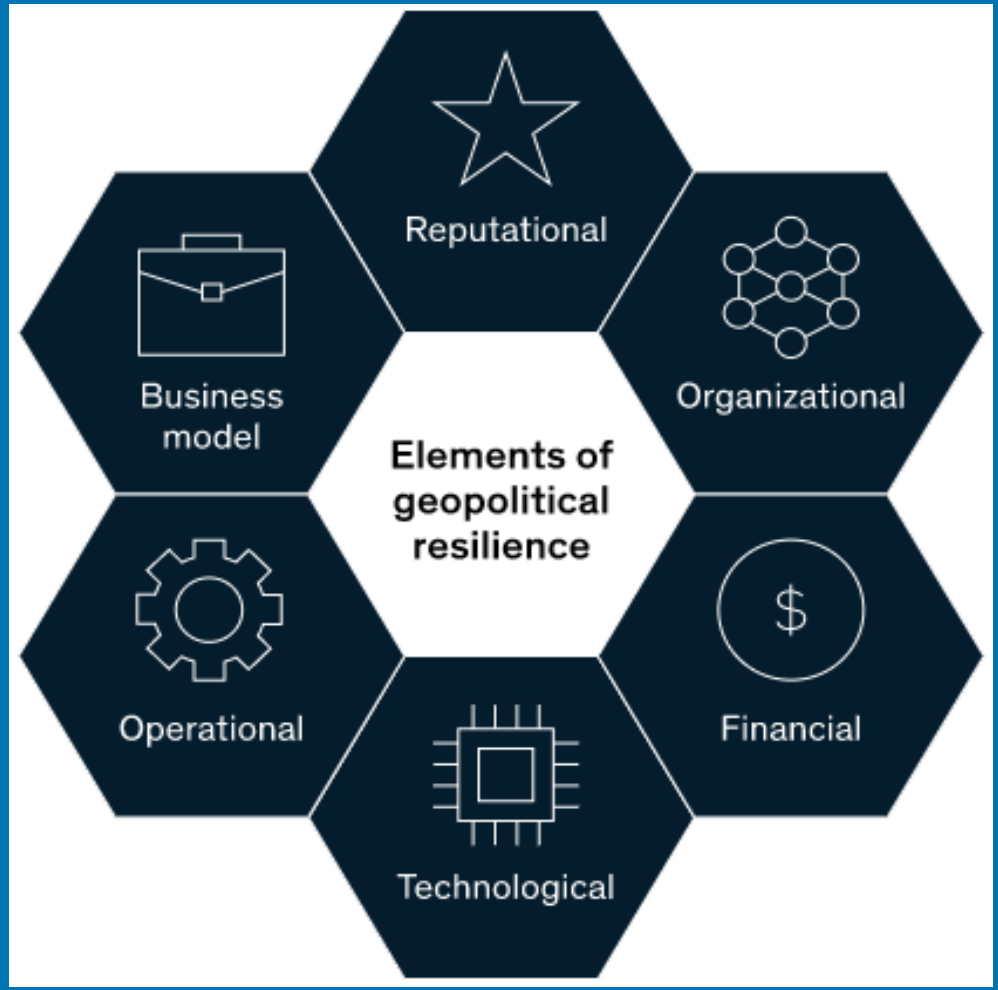
Emerging

- industrializing machine learning
- immersive-reality technologies
- trust architectures and digital identity
- next-generation software development
- quantum technologies



Industrial IoT
aree di intervento

- Business model
- Reputation
- Organizzazione
- Operations
- Technology
- Financials



Industrial IoT
fattori critici

- Capacità
- Competenze
- Componenti

Industrial IoT fattori critici

- Capacità
  - Opere civili
  - Permessi, autorizzazioni
  - Interventi, installazioni e collaudi
- Competenze
- Componenti

Industrial IoT fattori critici

- Capacità
- Competenze
  - Data scientist
  - Cyber esperti
  - Esperti di Intelligenza Artificiale
  - Esperti di Firmware e Programmatori
- Componenti

Industrial IoT
fattori critici

- Capacità
- Competenze
- Componenti
  - End of life
  - Disponibilità e tempi
  - Provenienza e controlli

MMSZ4697T1G
ON Semiconductor Limited
ZEN SOD123 REG 0.5W 10V
RoHS(10)-Conforme(1)

Codice Prodotto Fornitore:	MMSZ4697T1G
Vs. codice articolo:	**E1003179B**
Vs. Riferimento/Posizione:	**MRP 17-01.xlsx**
Codifica doganale:	8541100(
Confezione:	3.000 PCL
Confezionamento Prodotto:	Reel
Consegna Standard (sett.) (2):	53

Scheduli di consegna

Data richiesta	Quantità richiesta	Data prevista
06.02.2023	3.000	01.10.2025

Un possibile approccio per contribuire a proteggere i dispositivi IIoT già in campo

Rilevare e correggere i firmware già a bordo:

- monitorare le versioni dei firmware dei device IIoT già esistenti, rilevando i firmware "non autorizzati" o mal gestiti;
- analizzare i firmware manomessi usando l'IA per riconoscere connessioni indesiderate o possibili exploit che potrebbero essere utilizzati per hackeraggi;
- eventualmente sostituire i firmware delle tipologie di dispositivi compromessi.

Trasformazione Digitale Sostenibile
Convergenze e sinergie in atto

Italia e Unione Europea

- Sinergie tra industria civile, difesa e spazio;
- Investimenti comuni in tecnologie breakthrough;
- Cloud/Edge, microprocessori, cyber security, AI, Quantum computing.

Civile e Difesa

- Sinergie con le realtà civili che fanno innovazione tecnologica;
- Approccio “trasversale” per usare basi tecnologiche comuni
- Sviluppo applicazioni civili, militari e duali.

MINISTERO DELL’INTERNO

MINISTERO DELLA DIFESA

Pubblico e Privati

- Coordinamento tra i soggetti pubblici coinvolti nella materia;
- Coinvolgimento dei privati del sistema produttivo nazionale;
- Coinvolgimento del mondo dell’università e della ricerca.

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

Il mondo IOT: Multisettore

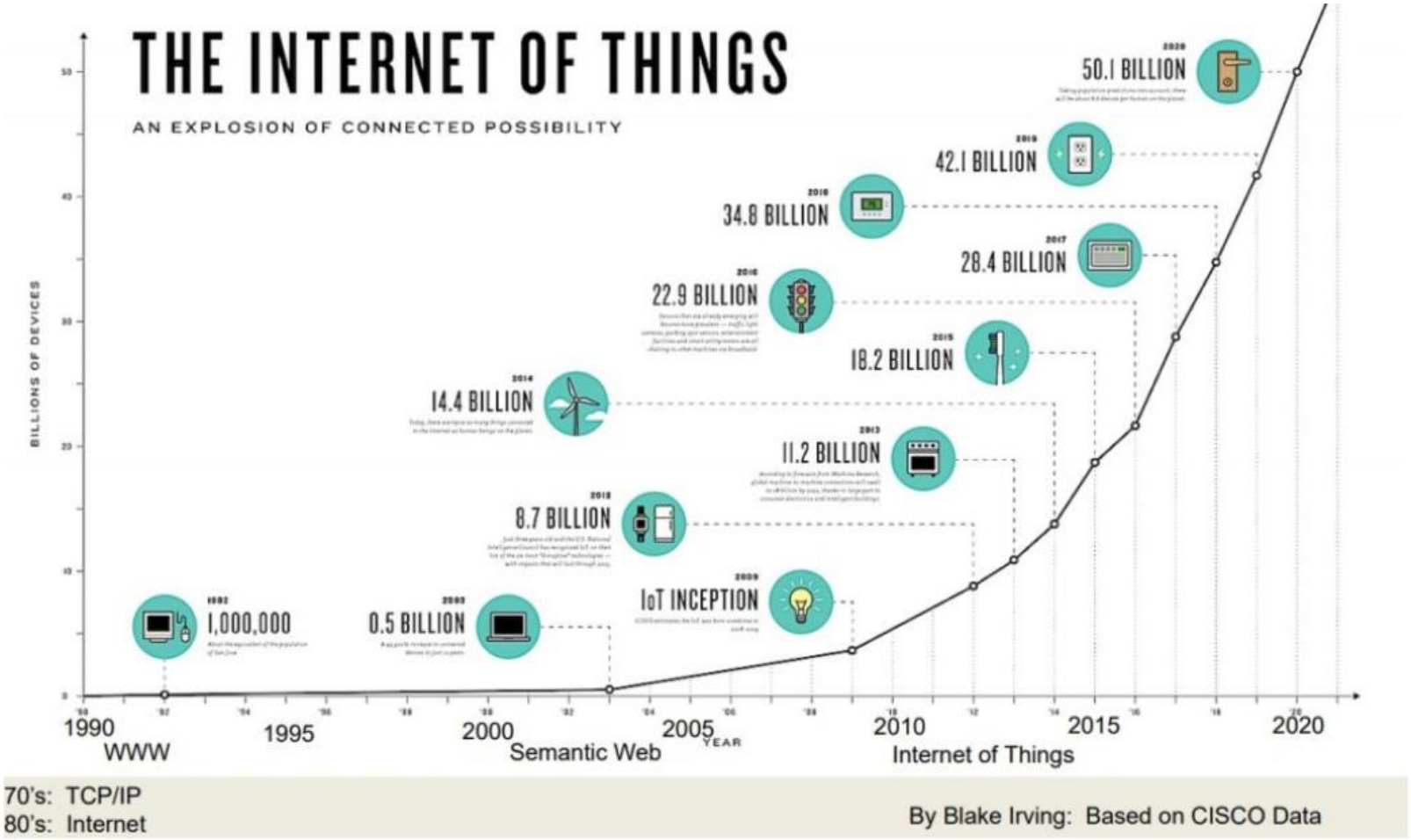
Il mondo IOT: Multi-device

IoT Cyber Security

IoT

- Nel 2020 sono stati censiti circa **50 miliardi di device IOT** a livello worldwide. I device IOT sono progettati per essere connessi ad una rete e molti di loro sono connessi a Internet.
- Questi device devono essere identificabili, manutenuti e monitorati dai team di sicurezza nelle grandi aziende e nelle grandi organizzazioni.
- Alcuni (pochi) di questi prodotti IOT comunicano una telemetria di base al produttore del device oppure hanno i mezzi per ricevere degli update software; nella gran parte dei casi questo e' impossibile ed il Cliente finale IT non sa nemmeno che esse esistano sulla rete.

I numeri dell'IoT



I numeri dell'IoT

EXHIBIT 3

IoT ADOPTION AND VALUE BY COUNTRY

	Global	US	UK	FR	DE	SP	IT	BNLX	CH	JP	AUS
% IoT Adopters	90%	94%	91%	91%	88%	89%	95%	91%	85%	88%	96%
% Projects in Use phase	25%	27%	25%	23%	25%	22%	26%	25%	25%	23%	18%
Time to Use stage (months)	12	11	13	12	14	11	10	12	16	12	16
Plan to use IoT more in 2 years	66%	78%	69%	67%	53%	76%	69%	59%	65%	51%	56%

Principali Applicazioni IoT

- Industria
- Agricoltura
- Automotive e Domotica
- Retail
- Medical
- Military ,Drones ,Soldiers,Sensors
- Energy, Oil and Gas
- Smart Grids
- Smart Cities

Perchè adottare l'IoT

EXHIBIT 7

TOP REASONS FOR IoT ADOPTION BY INDUSTRY

Manufacturing		Power & Utilities		Oil & Gas		Mobility		Smart Places	
Quality and compliance	47%	Smart grid automation	44%	Workplace safety	45%	Inventory tracking and warehousing	48%	Productivity enablement/ workplace analytics	47%
Industrial automation	45%	Grid asset maintenance	43%	Employee safety	43%	Manufacturing operations efficiency	40%	Building safety	42%
Production flow monitoring	43%	Remote infrastructure maintenance	40%	Remote infrastructure maintenance	39%	Surveillance and safety	34%	Predictive maintenance	41%
Production planning and scheduling	38%	Smart metering	37%	Emissions monitoring and reduction	35%	Remote commands	34%	Regulations and compliance mgmt	36%
Supply chain and logistics	38%	Workplace safety	37%	Asset and predictive maintenance	35%	Fleet management	32%	Space mgmt and optimization	34%

IoT Signals aka.ms/IoTsignals

Microsoft | hypothesis

Le sfide dell'IoT

- Cybercrime, Botnet, Shadow IoT, Data Theft;
- Weak authentication (passwords and more);
- Intellectual Property Rights;
- Tech standard spesso inconsistente o non del tutto definite;
- Sicurezza insufficiente per i dati e la loro protezione.

Superficie d’attacco

- Questi device possono essere usati da attori malevoli che possono utilizzarli come porte di ingresso ed, una volta all’interno della rete, possono muoversi alla ricerca di accounts e dati di valore; una volta entrati su ogni IoT device della rete possono, attraverso un “**tcpdump**”, sniffare tutto il traffico della rete e delle sottoreti locali;
- I device IoT sono usati in molti mondi applicativi dai sistemi di gestione delle citta’, alla sanita’, alle fabbriche, alle imprese fornitrici di servizi di utilita’ come Gas, Acqua, Elettricita’, Trasporto ed in genere nelle **infrastrutture critiche**;
- Questa espansione allarga in maniera drammatica la **base di attacco di attori malevoli**.

5 step per l'IOT Cybersecurity

1. **Proteggere i processi strategici:** non si può proteggere tutto ma si possono proteggere i più importanti;
2. **Mappare il terreno digitale:** quello della rete interna in prima battuta e poi le terze parti e i manutentori con accesso remoto;
3. **Analizzare il rischio:** valutando vulnerabilità attraverso modelli di threat intelligence o red-team che cercano altri vettori di attacco;
4. **Mitigare e Proteggere:** riducendo il numero degli entry points accessibili della rete usando zero trust policy di accesso e segregando i device IoT e OT dalle altre reti;
5. **Rimuovere tutti i Silos tra IT,OT,IoT e le CPS:** deviando tutti gli alerts verso il Soc e poi verso il Siem e la Soar per rispondere rapidamente agli incidenti OT/IoT.

AI IoT

L'obiettivo dell'AIoT è creare operazioni IoT più efficienti, migliorare le interazioni uomo-macchina e migliorare la gestione e l'analisi dei dati. (Artificial intelligent Internet of Things), in sostanza la combinazione fra un sistema di *machine learning* di intelligenza artificiale e l'infosfera degli oggetti connessi in rete IOT.

Sulla carta l'AIoT risolve l'operazione 1+1=3 ed è reciprocamente vantaggiosa per entrambi i tipi di tecnologia, in quanto l'AI aggiunge valore all'IoT attraverso le capacità di apprendimento automatico ed il miglioramento dei processi decisionali, mentre l'IoT aggiunge valore all'AI attraverso la connettività, la segnalazione e lo scambio di dati. L'AIoT può migliorare le aziende ed i loro servizi creando più valore dai dati generati dall'IoT.

Nei dispositivi AIoT, l'intelligenza artificiale è incorporata nei componenti dell'infrastruttura, tutti collegati tramite reti IoT.

Grazie.

www.vincenzocalabro.it