FORUM
TELECONTROLLO 2019
RETI DI PUBBLICA UTILITÀ

# ServiTecno, Mario Testino – Sergio Leoni

## Tecnologie per Sicurezza, Qualità ed Efficienza dell'Acqua 4.0: dai Big-Data agli Analytics passando per Continuità Operativa, IIoT, Edge-Computing ed OT-Cyber Security

ANIE AUTOMAZIONE

messe frankfurt

# Digital Journey

*L'industria dell'Acqua e le Multiutility sono costantemente alla ricerca di modi possibili per adattarsi alle mutevoli condizioni in cui si trovano ad operare nel tentativo di trovare soluzioni efficaci a sfide globali come i cambiamenti climatici e l'urbanizzazione. Sfide che stanno aumentando costantemente la domanda delle scarse risorse idriche disponibili o altresì richiedono il contenimento di risorse eccessive.*

*La sempre crescente Digitalizzazione e l'applicazione, anche in questo settore, di termini come "Big Data", "Internet of Things", "Analytics", "KPI" o "Realtà Aumentata", con gli ovvi risvolti legati alle problematiche di "Cyber Security", hanno permesso di immaginare un nuovo filone di Industria 4.0: il Water 4.0.*

*Scopo di questo "Digital Journey" è esplorare alcune delle nuove tecnologie e architetture informatiche che, integrandosi con sistemi di automazione e di telecontrollo, permettono un miglioramento della Continuità Operativa attraverso il costante monitoraggio degli indicatori critici e la gestione di possibili "Early Warning" nel quadro di un Ciclo Idrico Integrato.*

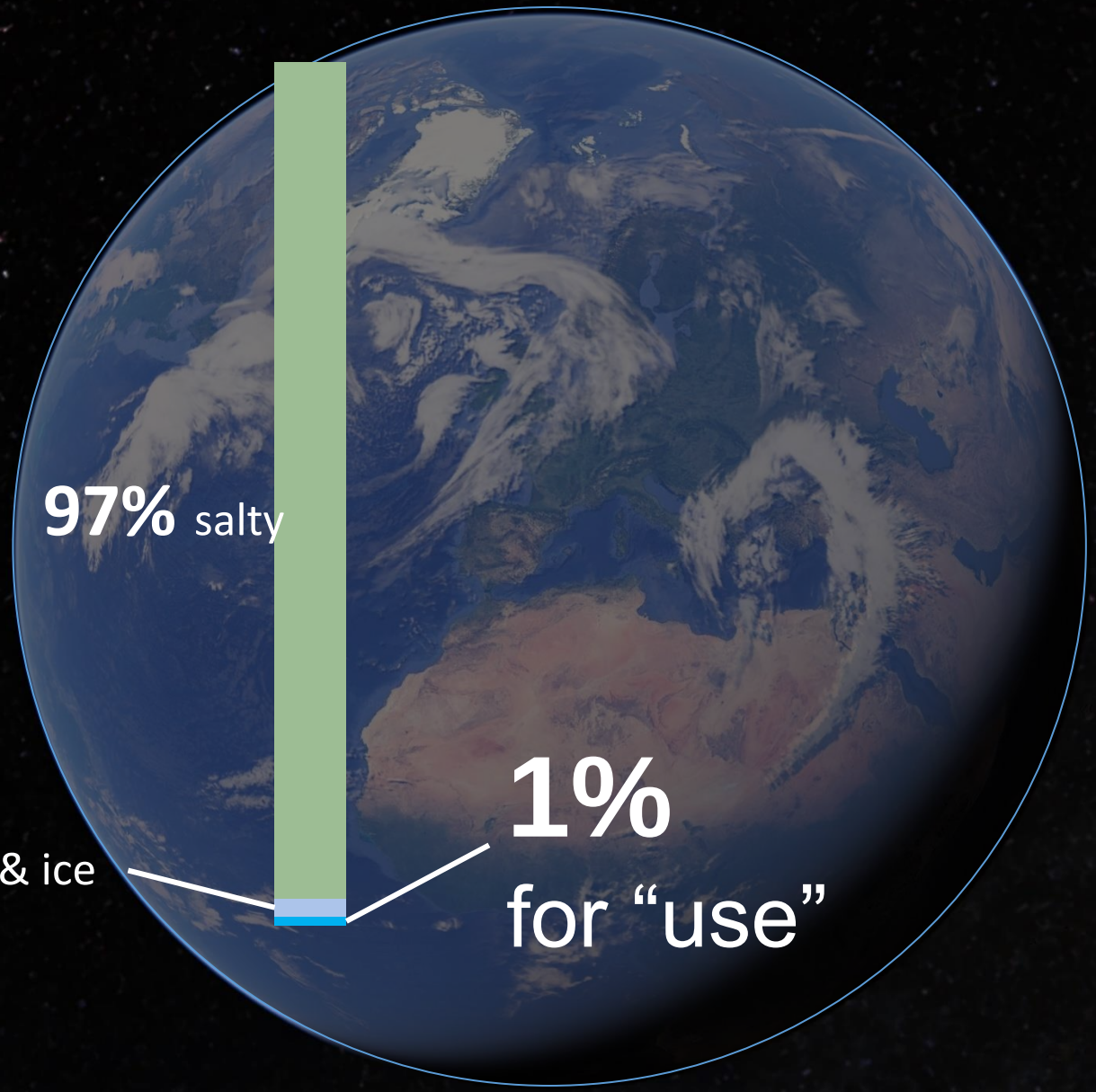



Image: Google Earth

# Tanti dati ma poche informazioni


Data Rich Information Poor

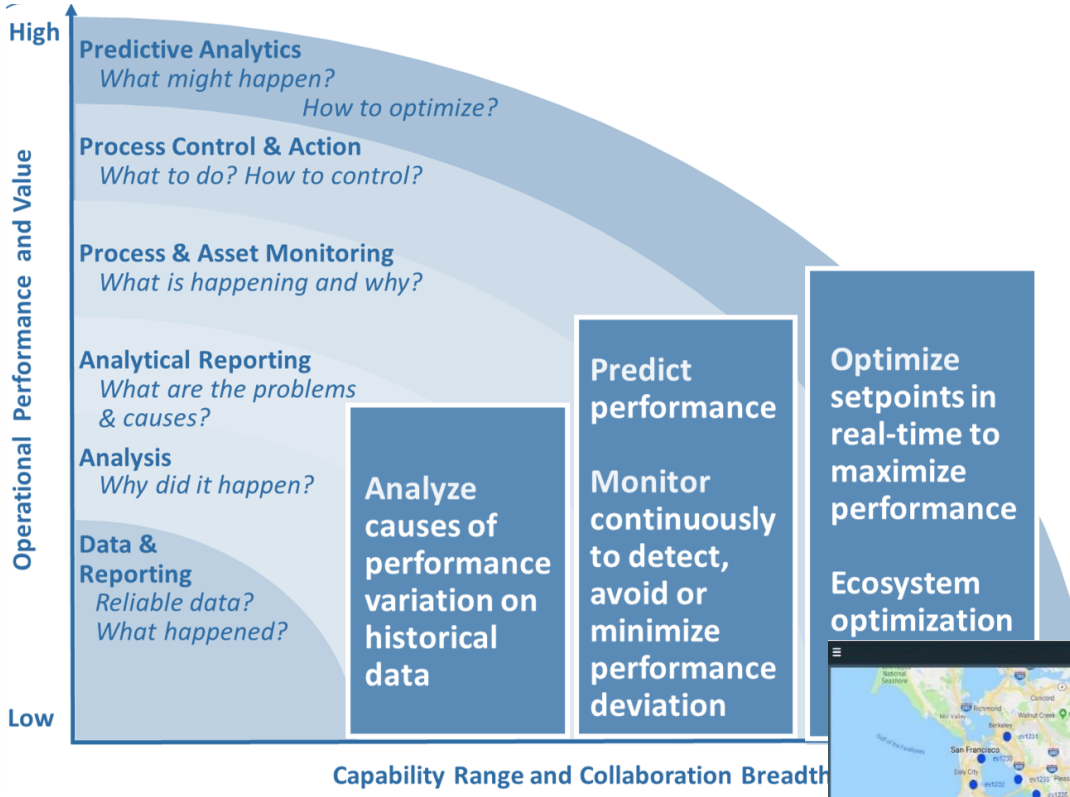
Big Data

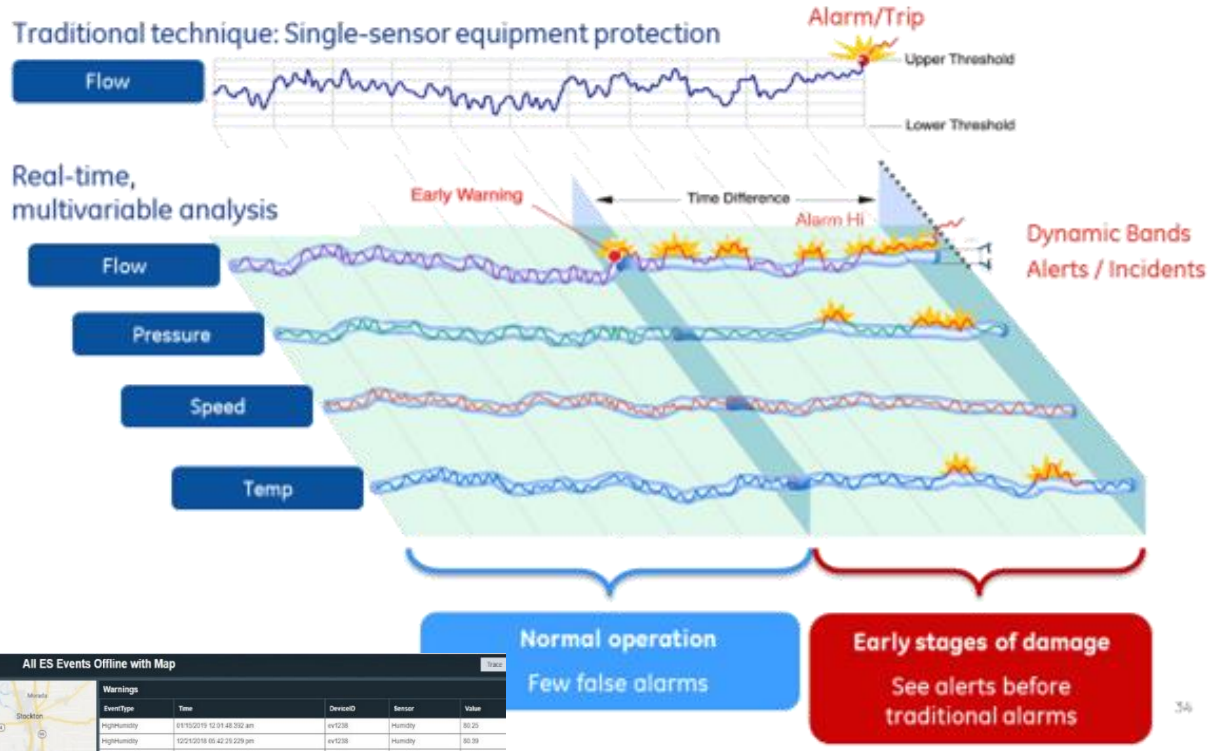

Real Time Alarms

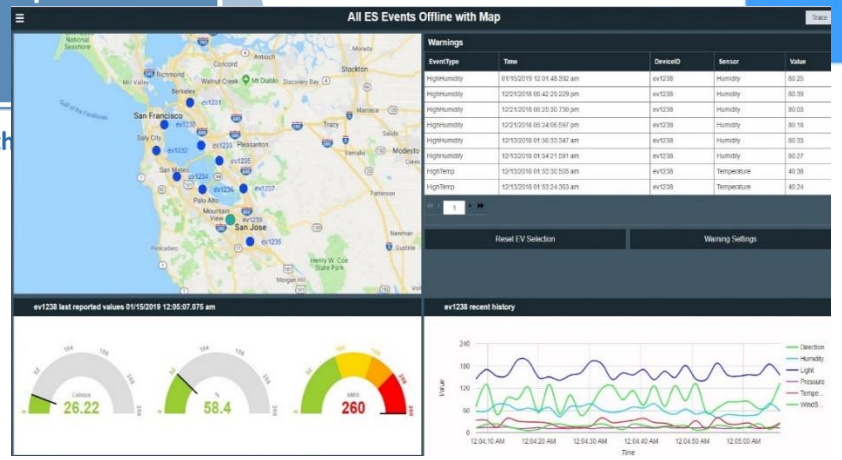
ANIE AUTOMAZIONE

messe frankfurt

# Dato, Informazione, Tempestività e Consapevolezza



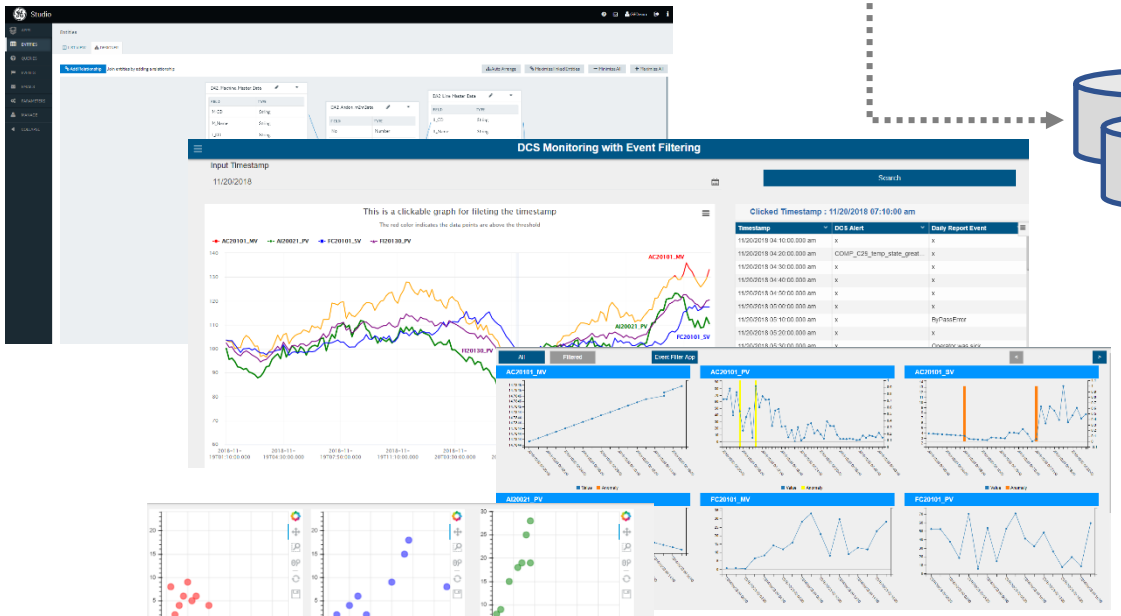



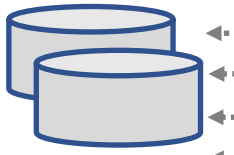



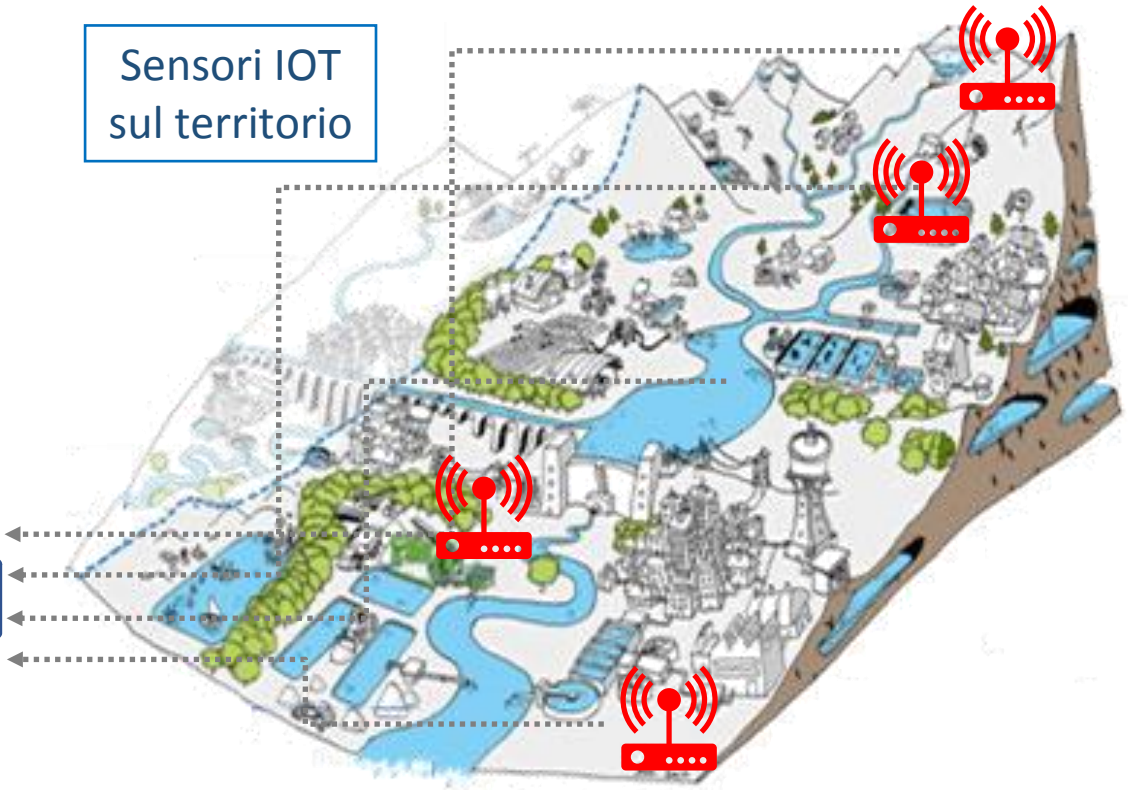
# Sistemi di Supporto alle Decisioni

Previsioni in Tempo reale

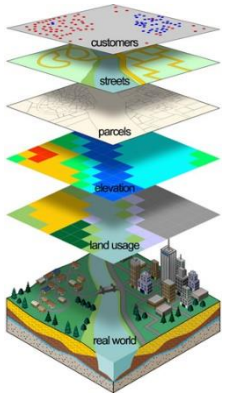

Sensori IOT sul territorio





GIS




Algoritmi di Machine Learning e Analisi

# Nuovi Strumenti RAD (Rapid Application Develp.)

**Asset 1** (OPC UA, MQTT)
- Model
- Tags
- Alarms

**Asset 2** (OPC UA, MQTT)
- Model
- Tags
- Alarms

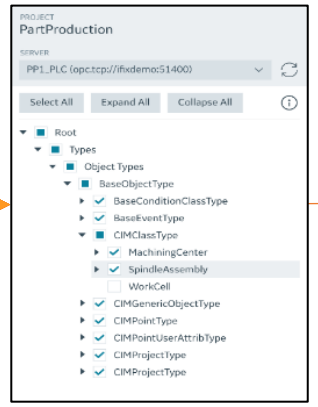
**SCADA**

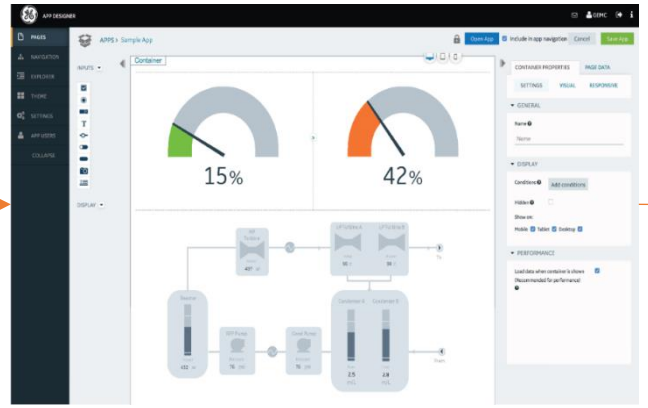
**Historian**

**SQL**

**JSON & URLs**

**MES**




# L’evoluzione della manutenzione

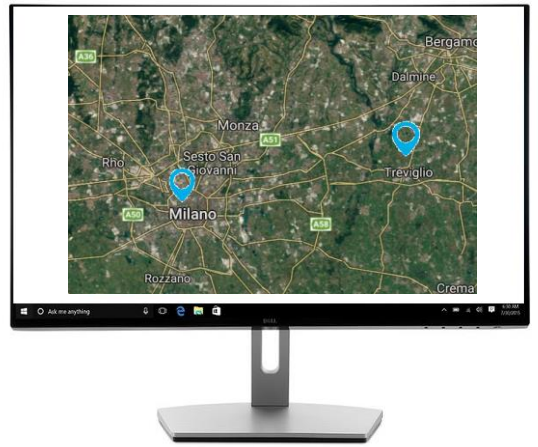
Monitor

Microfono

Telecamera Anteriore

Manutentore Sul Campo

Operatore Remoto



# Continuità Operativa di Servizio (SLA)

| Livello SLA Uptime [%] | Tempo annuo di Dowtime (Fermo) |
|---|---|
| 99 | 3 giorni 15h 39m 29.5s |
| 99.9 | 8h 45m 57.0s |
| 99.99 | 52m 35.7s |
| 99.999 | 5m 15.6s |
| 99.9999 | 31.6s |

→ Sito Web

→ PC Office

→ Server Fault Tolerant

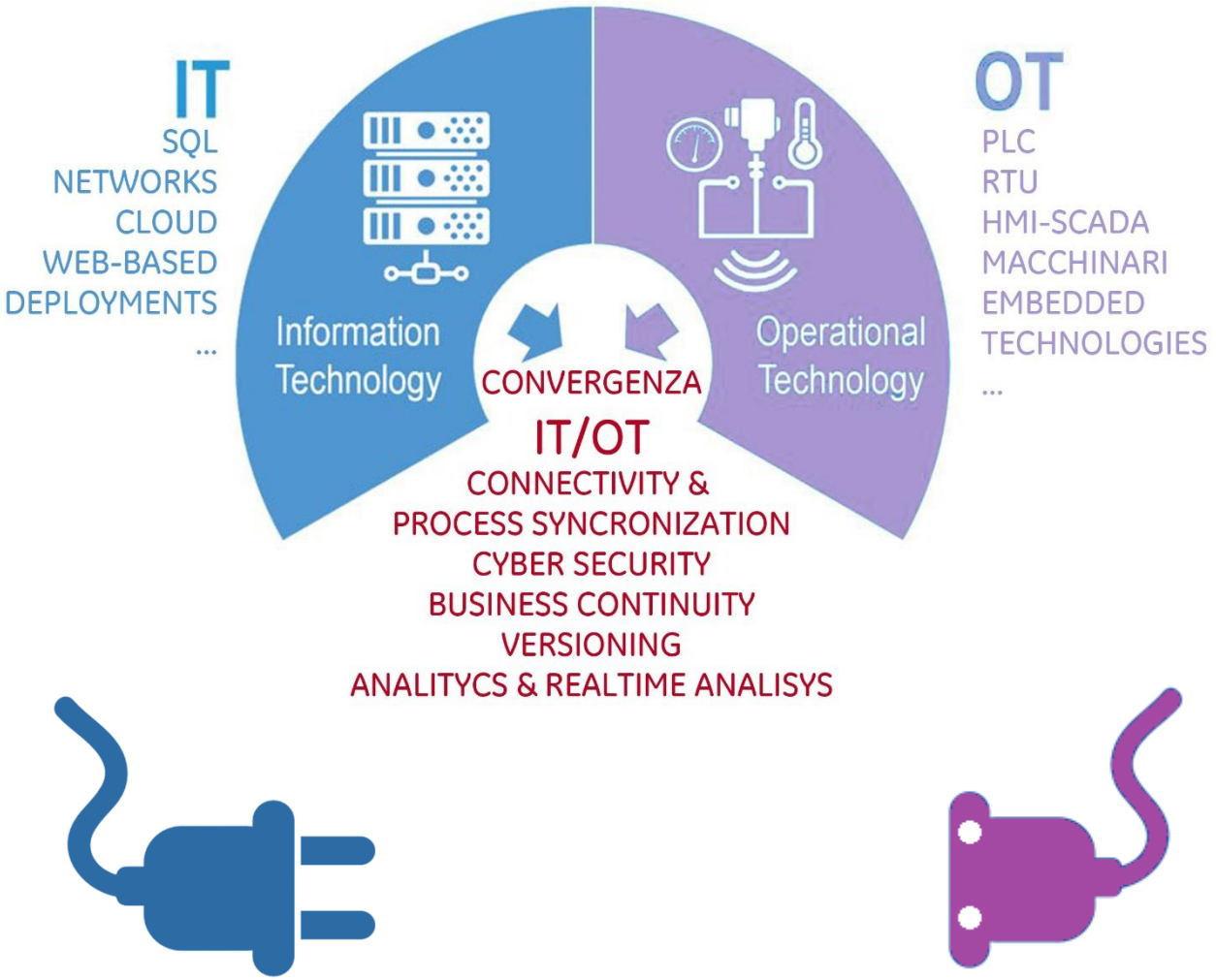
Requisiti sempre più stringenti!

# Convergenza IT - OT

**Tutti gli standard informatici aziendali, network, gestionale, cloud, analytics.**

- **Sistemi non-deterministici**
- **Sistemi non-realtime**
- **O al piu'near-realtime**

- **Data Integrity**
- **Data security**
- **Patent Infringement**
- **Business Continuity**




**Le interfacce informatiche primarie con macchine e impianti, attuatori e trasduttori fisici delle logiche programmabili.**

- **Sistemi deterministici**
- **Sistemi strettamente realtime**
- **Brand specifici**

- **People Safety**
- **Business and Service Continuity**

ANIE AUTOMAZIONE

messe frankfurt

# Industrial Cyber Security Incidents Are Costly…
# … in dollars, production impact, reputation & trust

*"Cyberattacks on critical infrastructure and strategic industrial assets are now one of the top five global risks."*

**World Economic Forum**
**Global Risk Report, 2018**

**Average estimated cost of cyberattack**

**$1.7M**

| | Organization | Issue/Attack | Cost | Impact |
|---|---|---|---|---|
| 2019 | Norsk Hydro | LockerGoga Ransomware | $70m | Equipment replacement, Production loss |
| | Duke Energy | Compliance Violation | $10m | …s and reputation |
| 2018 | Saudi Petrochem | Triton | *Unknown* | |
| | UK NHS | WannaCry | 92m GBP | |
| 2017 | Merck | NotPetya | $870m | |
| | FedEx (TNT Express) | NotPetya | $400 | |
| | Maersk | NotPetya | $3… | |
| | Mondelēz | NotPetya | $… | |
| 2016 | Ukrenergo | Industroyer/Crashoverride | | |
| 2012 | Saudi Aramco | Shamoon | $1 Billion | |

Sour…


ANIE AUTOMAZIONE

messe frankfurt

# Cyberattacks on Manufacturing are Increasing

IndustryWeek

### Ransomware Attack Hits Manufacturing – Are You Vulnerable?

**Mar. 2019**

Norsk Hydro, a multinational manufacturer headquartered in Norway and one of the world's largest aluminum producers, reported last week that it was hit by a ransomware that affected its production and IT systems.

CIO DIVE

### Mondelez in $100M Court Battle with Insurer Over Cyberattack-related Damages

**Jan. 2019**

NotPetya malware left 1,700 servers and 24,000 laptops "permanently dysfunctional" after the attack hit Mondelez twice. Impact included loss of electronic data, software and physical damage.

REUTERS

### Cyber Attack Hits U.S. Newspaper Distribution

**Dec. 2018**

A cyber attack believed to originate outside the U.S. impacted the back-office systems used to publish and produce multiple newspapers sharing a Los Angeles-based production platform.

AdAge

### How Much Did Cyberattack Cost Reckitt Benckiser? Try $117M

**Jul. 2017**

The cyberattack caused widespread disruptions to shipping terminals, corporate information-technology networks and other vital infrastructure around the world.

# Manufacturing: #2 of Top Five Most Targeted Industries

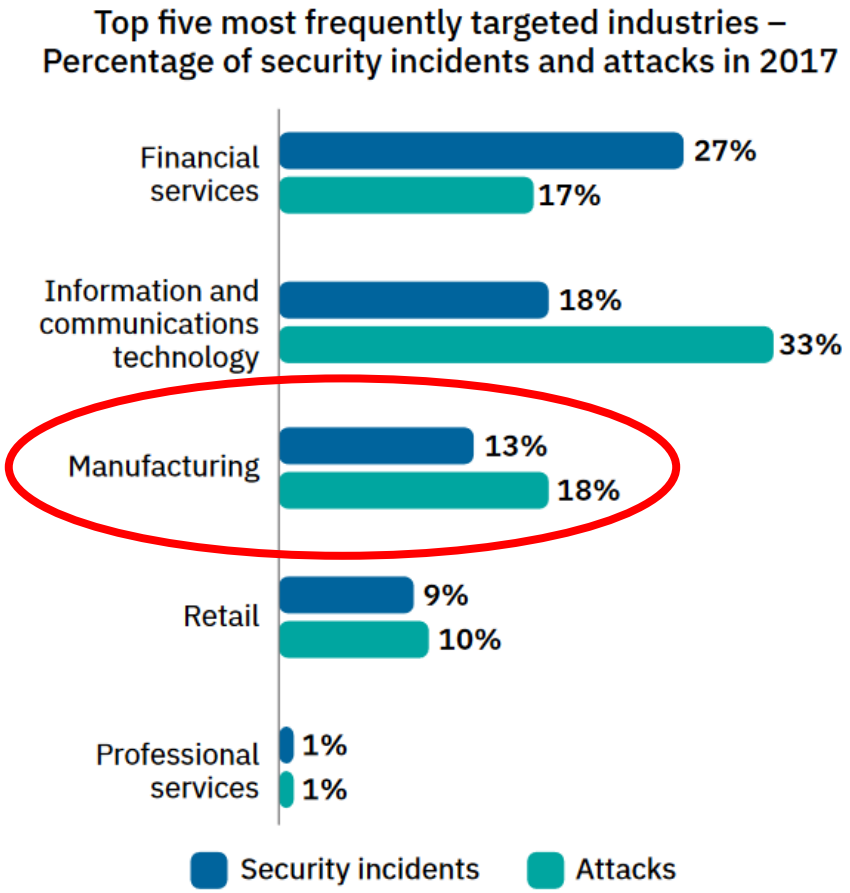


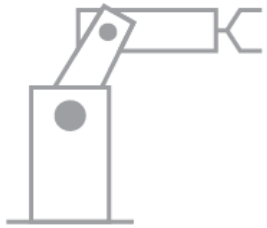

*Figure 3: Top five most frequently targeted industries – Percentage of security incidents and attacks in 2017.*

> *"Manufacturers experienced **13% of security incidents in 2017, and 18% of attacks**, slightly more attacks than the number-one targeted industry financial services."*
>
> *"The manufacturing sector was also hit by various ransomware attacks in 2017, which notably caused downtime after disruptive cases of **WannaCry** and **NotPetya infections**."*

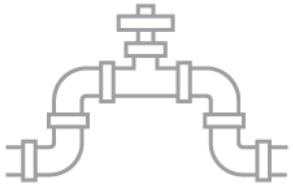
Source: IBM X-Force Threat Intelligence Index 2018

# Networks: Engaged with Global Industry Leaders

Electric Utilities



Automotive Manufacturing



Oil & Gas

Pharmaceuticals

Mining

Chemicals

Food & Consumer Goods

Water/Waste water

ANIE AUTOMAZIONE

messe frankfurt

# Market Drivers

**IT/OT Convergence**
Interconnectedness of non-homogenous systems, applications and platforms

**Corporate Espionage**
State-sponsored or independently led IP theft, corporate espionage and sabotage

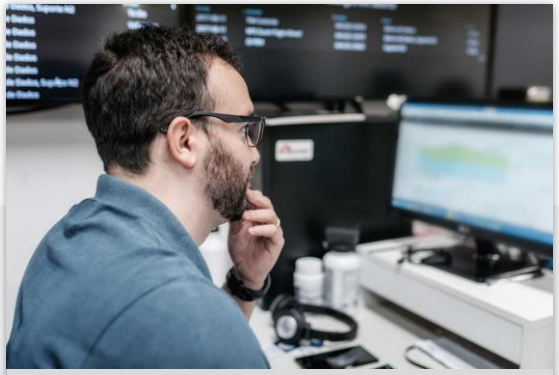
**Resilience & Uptime** (direct loss of revenue)
Cyber-born or preventative maintenance issues that result in system failure / downtime

**Reputation Risk** (indirect loss of revenue)
Degradation of company reputation due to data-loss, system shutdown and safety negligence

**Safety** (Personnel and Environmental)
Failure of cyber-physical system maintenance and a safety systems (i.e. SIS)

**National Security Responsibility**
Regulatory and tort responsibility to adhere to regional and vertical standards and practice

# Common Operational & Cyber Challenges for Manufacturing

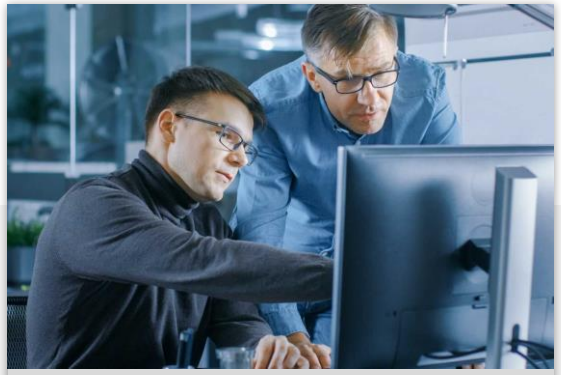


### Effectively Monitoring My ICS Network

To stay on top of what's happening, you need real-time visibility into assets, connections, communications and more.

### Keeping Production Lines Running

Unplanned downtime can cost millions in lost production capacity, and create inventory headaches that hit your bottom line



### Integrating IT/OT Security Efforts

To close security gaps and protect manufacturing processes against disruption, you need to leverage the expertise of IT.


### Applying Cyber Security Best Practices

To build cyber resiliency and reduce risk, you need to embrace standards like the NIST cyber security framework, IEC 62443 and more.

# The Nozomi Networks Solution for Manufacturers

**Real-time operational visibility and cyber security protects your products and production capacity against disruption while driving digital transformation**.

## Superior Operational Visibility

Accurately **visualize** your industrial networks and improve **resilience** with **real-time asset inventory** and **network monitoring**.

## Advanced ICS Threat Detection

Rapidly **manage** cyber threats and process risks with **a solution that correlates multiple, advanced detection techniques.**

## Rapid Global Deployment

Centrally **monitor** hundreds of facilities with a solution proven to **scale** across continents and **integrate** with IT/OT systems.

FORUM

TELECONTROLLO 2019
RETI DI PUBBLICA UTILITÀ

# GRAZIE PER L'ATTENZIONE

ANIE AUTOMAZIONE

messe frankfurt