La tecnologia wireless nel monitoraggio degli impianti

Oil & Gas e Energia

Fabio Camerin
Gruppo Wireless – ANIE Automazione

Federazione ANIE

Federazione Nazionale Imprese Elettrotecniche ed Elettroniche

- ✓ 13 Associazioni
- ✓ Oltre 1.200 Aziende
- ✓ Membro permanente di Confindustria

Il settore elettrotecnico ed elettronico
Fatturato: 56 Mld di €
Esportazioni: 29 Mld di €
Addetti: 410.000
Incidenza della spesa in R&S intra-muros sul fatturato: 4%

Il settore dell'Automazione di fabbrica e di processo
Fatturato: 4 Mld di €
Esportazioni: 1 Mld di €
Addetti: 25.000

ANIE Automazione

ANIE Automazione rappresenta i fornitori di componenti e sistemi per l'automazione industriale manifatturiera, di processo e delle reti.

I Gruppi operanti in ANIE Automazione lavorano su tre aree principali:

Prodotto

1. **PLC - I/O**
2. **AZIONAMENTI**
3. **HMI-IPC-SCADA**
4. **COMPONENTI E TECNOLOGIE PER LA MISURA E IL CONTROLLO**
   - ✓ **Wireless, Networking, Safety, Visione, RF-ID**
5. **UPS**
6. **CONTROLLO DI PROCESSO**

Soluzioni

7. **MECCATRONICA**
8. **TELECONTROLLO**
9. **ITS**

Software

10. **SOFTWARE INDUSTRIALE**
11. **DATA CENTER**

Il Gruppo Wireless

Gli obiettivi

- Diffondere informazioni chiarificatrici su caratteristiche e applicabilità della tecnologia wireless
- Promuovere la tecnologia tra gli utilizzatori
- Contribuire agli sviluppi della normativa e della regolamentazione del settore
- Quantificare e studiare il mercato

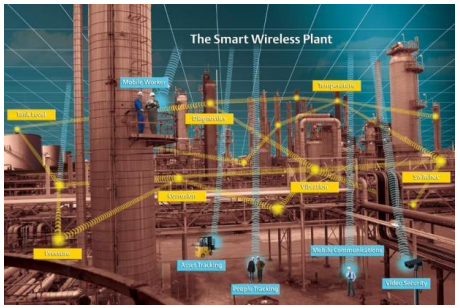
Le azioni

- Partecipazione alle principali fiere di settore con iniziative dedicate
- Promozione di giornate di studio e di approfondimento tecnologico
- Collaborazione con la stampa specializzata per la redazione di articoli tecnici e divulgativi
- Redazione di white paper e guide esplicative
- Interfacciamento con enti deputati alla regolamentazione dell'uso delle varie apparecchiature wireless
- Partecipazione ai tavoli di lavoro normativi nelle opportune sedi
- Periodiche rilevazioni statistiche e analisi di mercato

Le aziende

autec safety remote control
EATON Powering Business Worldwide
EMERSON Process Management
HEIDENHAIN
Panasonic ideas for life
PHOENIX CONTACT
NATIONAL INSTRUMENTS
OMRON
Rockwell Automation
Schneider Electric
TURCK
BANNER
SIEMENS
Weidmüller
YOKOGAWA

Wireless: alcuni ambiti applicativi industriali



Misure nell'industria di processo

Superamento di ostacoli e asperità del terreno

Copertura aree distese/ remote production

Eliminazione costi manutenzione

Factory automation

Asset mobili/service

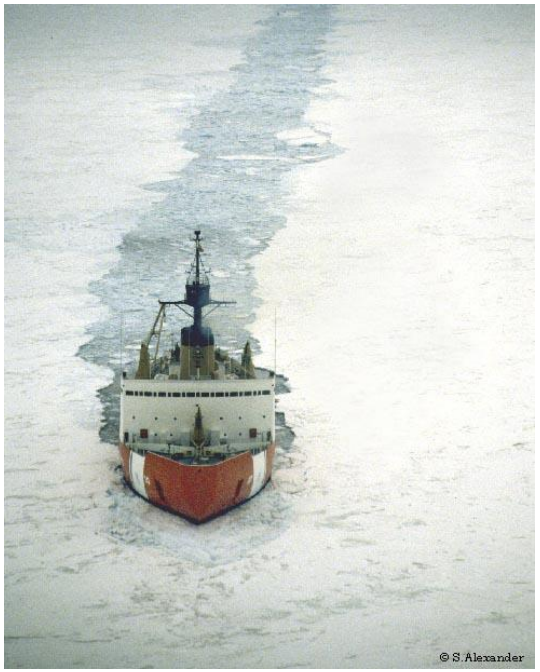
Il wireless di utilizzo quotidiano e per l'industria di processo

Wireless nell’industria di processo

Sebbene la tecnologia wireless sia oggi largamente diffusa in qualsiasi ambito, è bene suddividere e distinguere prodotti appositamente sviluppati per operare in ambito industriale da prodotti adatti ad ambiente residenziale o office. Affidabilità, resistenza ad ambienti critici, certificazioni per utilizzo in aree pericolose, immunità a disturbi, sicurezza del dato sono alcuni degli aspetti caratteristici delle soluzioni wireless per l’industria di processo

Feedback del mercato: le resistenze e i dubbi

- Mercato dell'industria di processo è conservativo
- Spesso le specifiche tecniche si basano su know-how e best practice vetuste
- Scenario economico e dinamiche progettuali spesso limitano la "vision" ad ampio raggio
- Sicurezza del dato wireless
- Dubbi sulla durata delle batterie
- Frequenza di aggiornamento del dato
- Resistenza al cambiamento: l'essere umano soffre di *metatesiofobia*

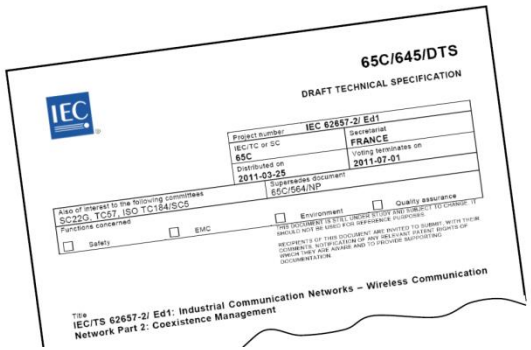


Feedback del mercato:
come trasformare resistenze in opportunità

- Centinaia di clienti nel mondo hanno adottato la tecnologia wireless (stimate oltre 6 miliardi di ore di funzionamento e 25.000 reti)
  - il 98% di essi* ha dichiarato di aver risparmiato M$ e persino fatto profitto (vedi energy saving)
- Rinomate compagnie petrolifere hanno adottato questa tecnologia e modificato le loro GP/specifiche
- La sicurezza del dato wireless è comprovata e garantita e ha permesso di effettuare installazioni in ambienti ad alta criticità e densità di segnali (es. aereoporti) e di ottenere persino la certificazione fiscale del dato

Wireless Field Instrumentation

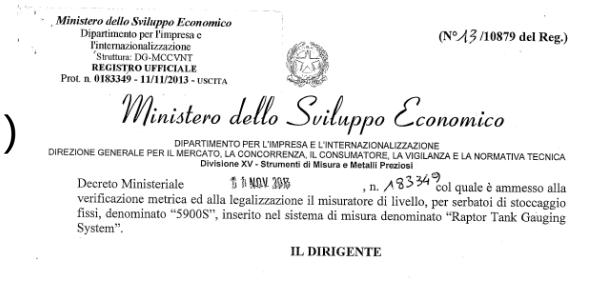
GP 15-01-05



* Fonti ARC,VDC,Harris, Country regions survey

Feedback del mercato: come trasformare resistenze in opportunità

- L’adozione della tecnologia in fase FEED ha permesso di utilizzare il wireless in macro progetti (Zubair, Exxon West Qurna, BP Quad 204 FPSO,TCO etc.)
- Sono stati introdotti strumenti wireless che hanno permesso applicazioni a volte irrealizzabili con il cablato (es. Acoustic transmitters, discrete input, strumenti per parti rotanti e non intrusivi)
- Tempi di update rate lenti: sono numerosi i punti di monitoraggio negli impianti. Comando, regolazioni e controllo sono comunque percorribili (http://www.wirelesscontrolfoundation.com)
- Sistemi di harvesting sono disponibili per garantire durate di batteria elevate contemporaneamente ad aggiornamenti rapidi del dato
- La tecnologia Wireless coesiste con il cablato e sistemi ibridi permettono gestioni migliori di impianti con acquisizione di diagnostica aggiuntiva



Ministero dello Sviluppo Economico
Dipartimento per l'impresa e l'internazionalizzazione
Struttura: DG-MCCVNT
REGISTRO UFFICIALE
Prot. n. **0183349 - 11/11/2013** - USCITA

(N°13 /10879 del Reg.)

Ministero dello Sviluppo Economico

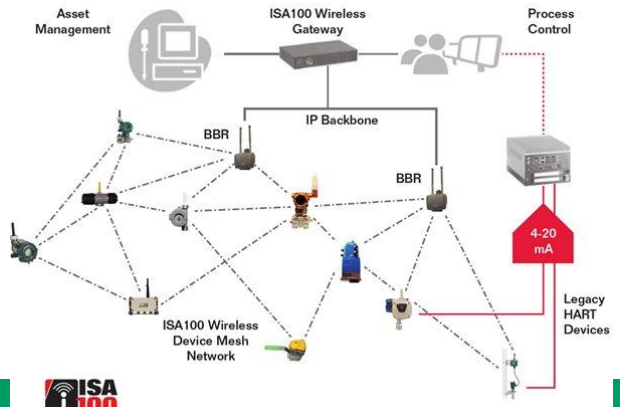
DIPARTIMENTO PER L'IMPRESA E L'INTERNAZIONALIZZAZIONE
DIREZIONE GENERALE PER IL MERCATO, LA CONCORRENZA, IL CONSUMATORE, LA VIGILANZA E LA NORMATIVA TECNICA
Divisione XV - Strumenti di Misura e Metalli Preziosi

Decreto Ministeriale 11 NOV 2013 , n. 183349 col quale è ammesso alla verificazione metrica ed alla legalizzazione il misuratore di livello, per serbatoi di stoccaggio fissi, denominato “5900S”, inserito nel sistema di misura denominato “Raptor Tank Gauging System”.

IL DIRIGENTE

Le tecnologie wireless più utilizzate nell'industria

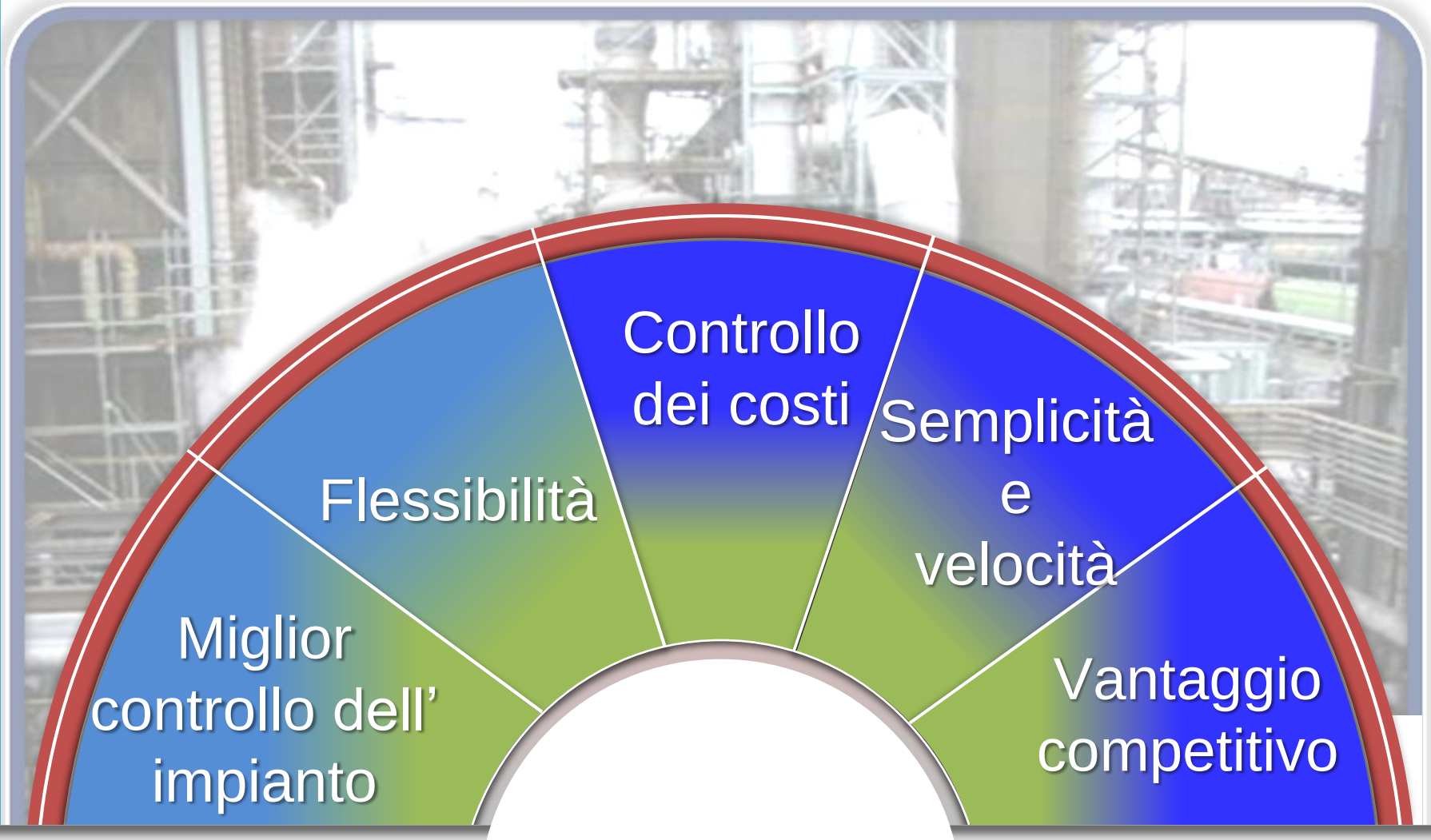
Standard	Coverage	Examples
IEEE 802.11 a/b/g/n	Local Area Networks (LAN)	Wi-Fi, WLAN
IEEE 802.15.1	Personal Area Networks (PAN)	Bluetooth
IEEE 802.15.4	Personal Area Networks (PAN)	IETF 6LowPAN ISA 100.11a WIA-PA WirelessHART ZigBee
IEEE 802.16	Metropolitan Area Network	WiMAX



Il quadro normativo esistente
Certificazioni e caratteristiche

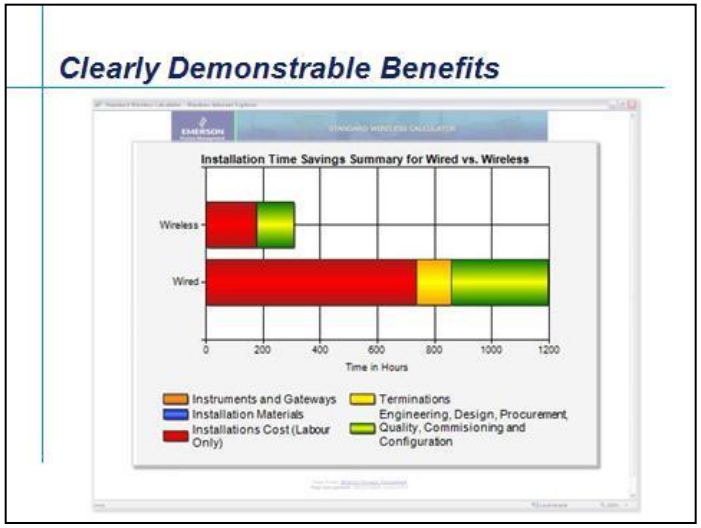
- Stesse peculiarità dei sensori cablati (certificazioni per aree pericolose, EC declaration, PED etc.)
- Standard IEC 6xxxx: vengono stabiliti i requisiti generali per le reti di comunicazione a filo e wireless
- *Electro Magnetic Compatibility (EMC) (2004/108/EEC)*
- Immunità ad emissioni EN 61326-1; 2006
    - EN 61326-2-3; 2006*R*
- *Radio and Telecommunications Terminal Equipment Directive (R & TTE) (1999/5/EC)*
- *EN 300 328 V 1.8.1: Electromagnetic compatibility and Radio spectrum Matters*

Perchè Wireless?



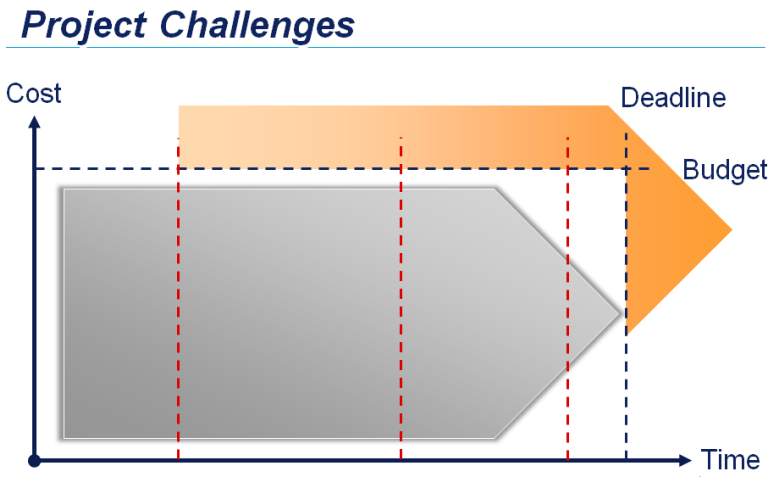
Perchè Wireless?
Oltre il risparmio dei cavi e accessori

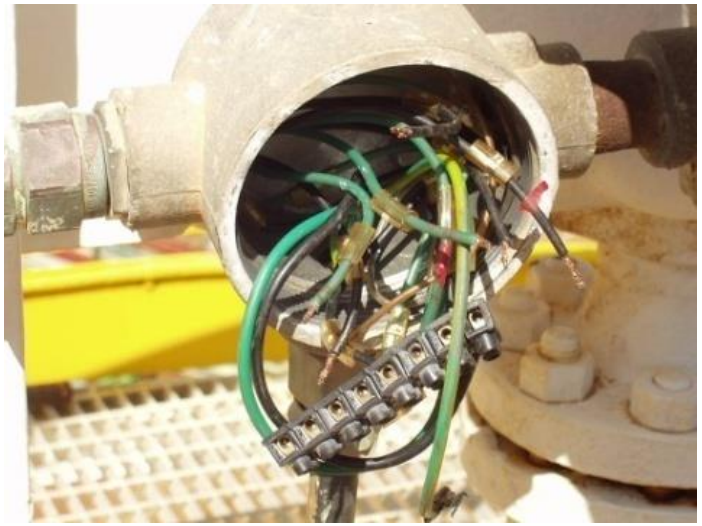
- Miglioramento costi manutenzione
  - Riduzione significativa per:
    - Migliore gestione assets
    - Acquisizione dati di diagnostica aggiuntivi
    - Ricerca guasti (grounding, schermatura,CC, disturbi EMC etc.)
- Miglioramento nei costi sicurezza
  - Riduzione dell'esposizione del personale in aree a rischio/remote
  - Riduzione dei cavi=riduzione dei rischi (incendi, tenute, roditori etc.)
- Flessibilità
  - Coesistenza con cablato esistente di qualsiasi brand e ridondanza segnali
  - Installazioni temporanee e non intrusive



Perchè Wireless?
Oltre il risparmio dei cavi e accessori

- Tempistiche di esecuzione
  - Semplicità e flessibilità nello sviluppo e modifiche dei progetti
  - Riduzione dei tempi di commissioning e startup
- Riduzione dei pesi e ingombri
  - Minor peso, maggior sfruttamento delle infrastrutture utilizzabili per il cablato, minor consumo
- Costi e budget
  - Riduzione del Capex e Opex
  - Scalabilità in esecuzione progetto e successiva
- Produttività, affidabilità ed efficientamento energetico:
  - Controllo costante motori,pompe,ventilatori,compressori
  - Efficienza scambiatori di calore, air cooler e monitoraggio scaricatori di condense





Topologie reti e industria di processo: teoria

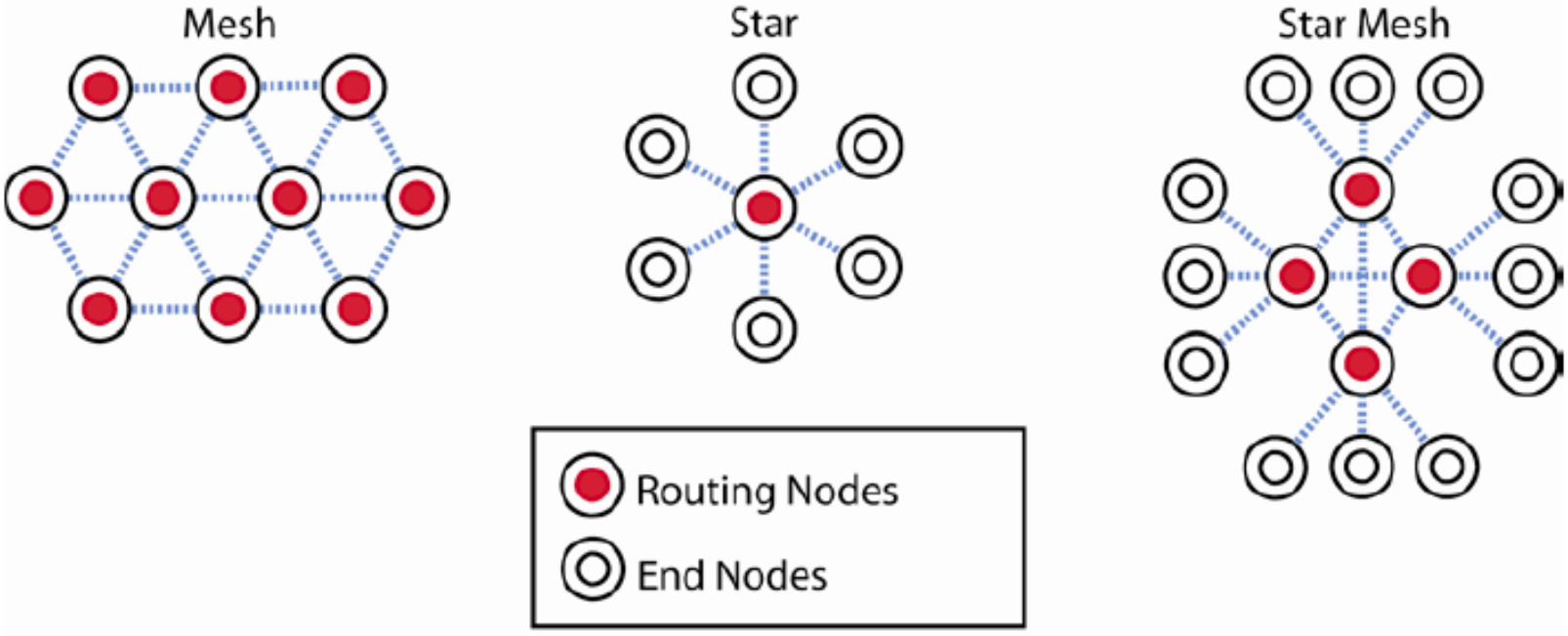


Figure 7: Network Topologies

In telecomunicazioni la topologia di rete è il modello geometrico finalizzato a rappresentare le relazioni di connessione, fisica o logica, tra gli elementi costituenti la rete stessa (detti anche *nodi*).

Topologie reti e industria di processo: pratica

Sicurezza nelle comunicazioni

La comunicazione sicura non è un concetto nuovo ed è la capacità di passare i dati verificabili da una fonte attendibile di un destinatario di fiducia senza interferenze di terzi.

SENDER

TRANSMISSION

RECEIVER

- **Re**: scrive un messaggio contenente l'ordine da trasmettere al suo comandante di fiducia
- **Messaggero**: trasporta il messaggio in territorio ostile
- **Comandante**: interpreta il messaggio del re ed esegue gli ordini

Sicurezza nelle comunicazioni

Un sistema di comunicazione sicura consente di:

Autenticare sia il mittente sia il destinatario - in altre parole, confermano che sono chi dicono di essere.
Verificare che il messaggio sia valido - ovvero che le informazioni ricevute sono le stesse che sono state inviate.
Crittografare i dati - ovvero rendere indecifrabile il messaggio se questo è intercettato da terzi.

Sicurezza nelle comunicazioni

CRITTOGRAFARE: il re cripta un messaggio, o lo scrive in un codice che solo lui e il comandante comprendono.
VERIFICARE: il re sigilla la lettera con la cera in modo che il destinatario può vedere che il messaggio non è stato manomesso, verificando così il suo contenuto.
AUTENTICARE: infine, il re, il messaggero e il comandante utilizzano password prestabilite per autenticare la persona che sta dare o ricevere il messaggio.
Il comandante di campo quindi decodifica il messaggio, ed esegue le istruzioni.

Sicurezza nelle comunicazioni: possibili attacchi

- Un attacco «**denial of service»** inonda i canali di comunicazione con messaggi indesiderati per evitare che il sistema funzioni. Questo include disturbi, o la creazione di interferenze sulle vie di segnalazione.
  - Ad esempio, i nemici del re potrebbe bloccare la strada con alberi e le rocce per evitare che il messaggero arrivi in tempo per consegnare il suo messaggio.

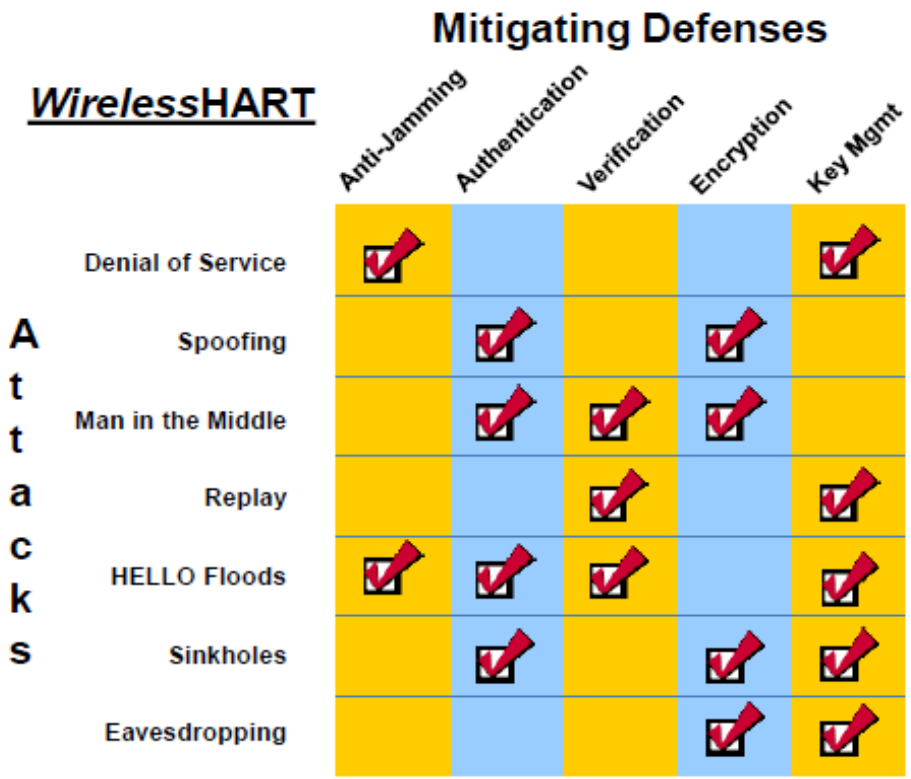
- «**Spoofing»** si verifica quando qualcuno assume l'identità di un altro in un tentativo di ottenere l'accesso al sistema.
  - In questo caso, qualcuno finge di essere il re e potrebbe inviare il proprio Messenger per fornire informazioni inesatte al comandante sul campo.
    Esempio: muovere le truppe del comandante di campo 5 miglia a ovest, quindi ogni volta che l'ordine sia rispettato le truppe saranno più lontano rispetto alla reale posizione.

Sicurezza nelle comunicazioni: possibili attacchi

- **«Men in the middle»** è il metodo che utilizza un utente malintenzionato per intercettare, modificare e / o controllare i messaggi senza che il mittente o il destinatario sappiano che il collegamento tra loro è stato compromesso.
  - Ad esempio, potrebbe accadere che il re dia il messaggio al suo messaggero che, si scopre, non essere fidato. Questo messaggero dà il messaggio a qualcun altro, che modifica il messaggio. Il messaggero poi consegna il nuovo messaggio al comandante sul campo.

- «**Replay»** è una forma di attacco alla rete in cui le informazioni vengono memorizzate senza autorizzazione e ripetutamente trasmesso senza la conoscenza del mittente.
  - Ad esempio, il messaggero inaffidabile potrebbe consegnare il messaggio del re per il comandante sul campo, poi consegnare lo stesso messaggio di nuovo il giorno dopo - e il successivo. Se l'ordine è stato quello di spostare le truppe del comandante di campo 5 miglia a ovest, quindi ogni volta che l’ordine sia rispettato le truppe saranno più lontano e fuori posizione.

Sicurezza nelle comunicazioni: possibili attacchi e contromisure



Crittografia.
La crittografia a 128 bit evita che dati sensibili possano essere intercettati.

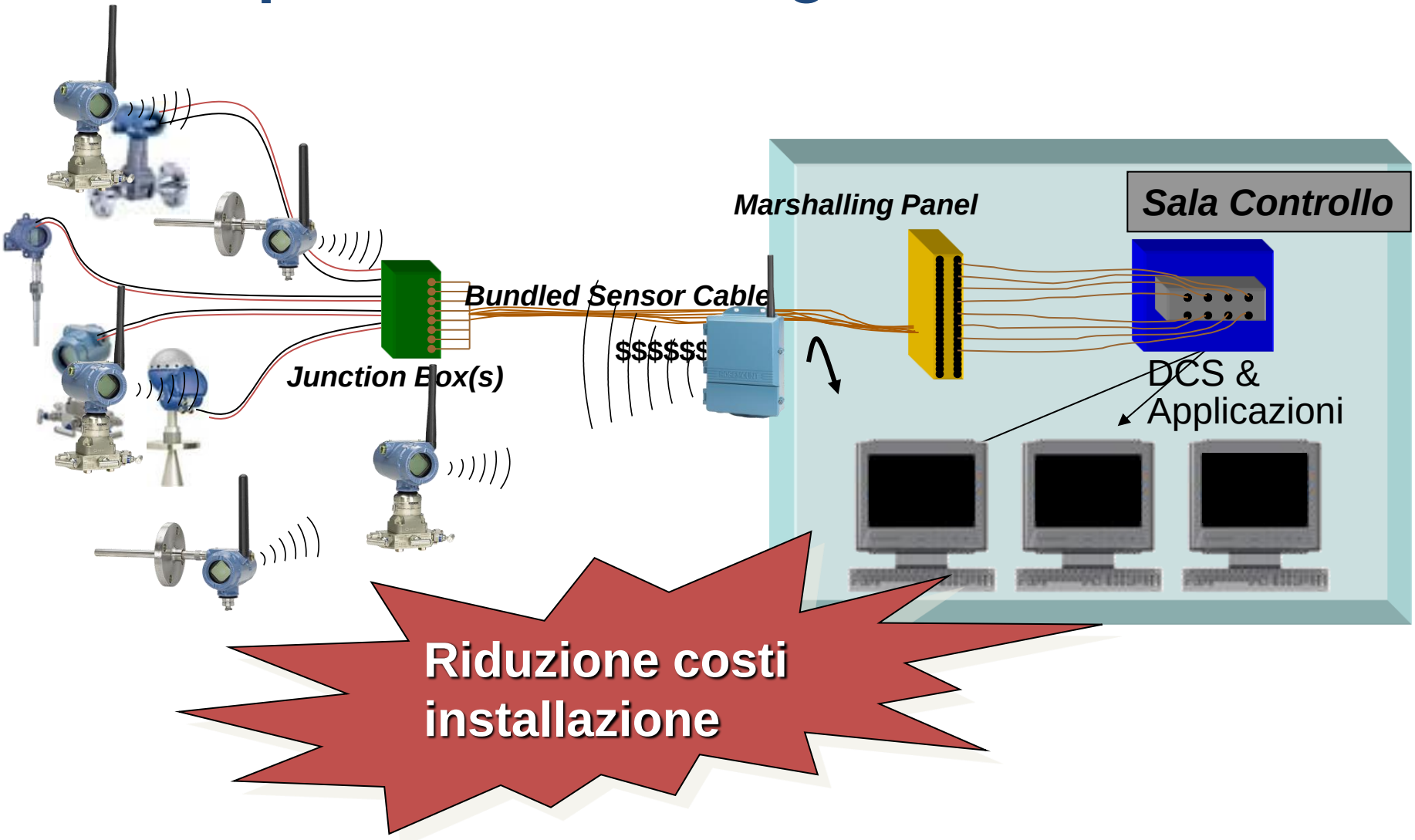
Verifica.
La presenza di Codici di Integrità del Messaggio (Message Integrity Codes) consente la verifica di ogni blocco di trasmissione.

Robustezza operativa.
Il Channel Hopping e la Mesh Infrastructure mitigano gli effetti di attacchi di jamming o di denial-of-service.

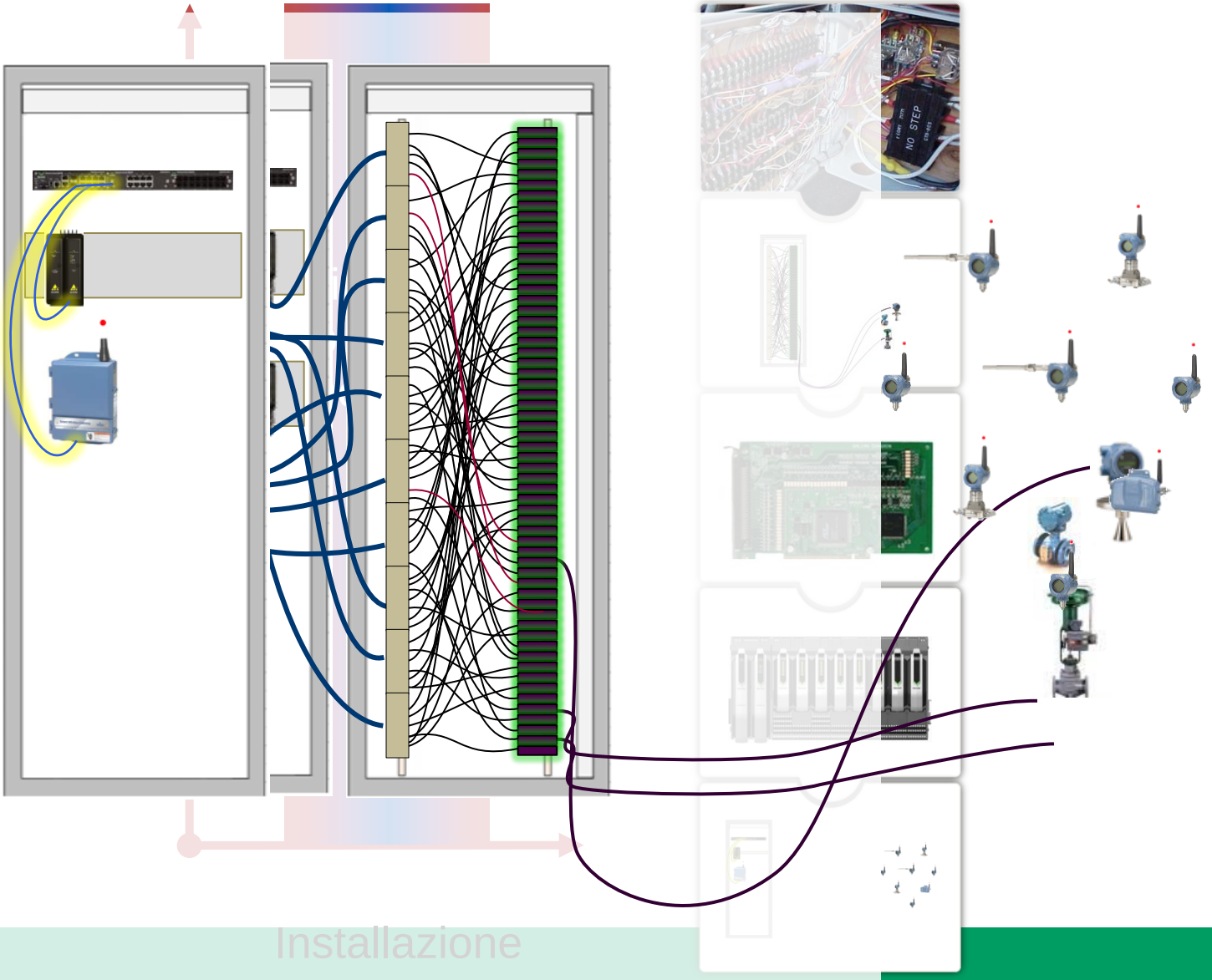
Key management.
Una rotazione delle password può prevenire la connessione o la comunicazione di strumenti non autorizzati sulla rete.

Autenticazione.
Gli strumenti non sono ammessi nella rete senza un’autorizzazione.

Benefici pratici
Start-up&commissioning



Riduzione significativa delle complessità di impianto



Conclusioni

- Nello scenario industriale attuale la tecnologia wireless rappresenta sicuramente **una scelta ottimale per numerose misure**
- Wireless non è una semplice opzione, una proposta alternativa, bensì un **valore aggiunto** per la competitività aziendale
- L'aggiornamento della misura non sempre rappresenta un ostacolo e numerose sono le applicazioni che non richiedono aggiornamenti veloci
- Durata batterie limitata: **sistemi di harvesting** risolvono eventuali problemi di durate limitate
- **Diagnostica integrata**: generalmente il wireless offre la possibilità di disporre di dati aggiuntivi a volte indispensabili l'impianto
- Wireless non necessariamente significa escludere il cablato: l'integrazione nel medesimo strumento cablato della tecnologia wireless (**sistema ibrido**) è oggi possibile

Buon proseguimento !