AIS – ISA Italy Section

IIOT field applications and cybersecurity

Francesco Zucca

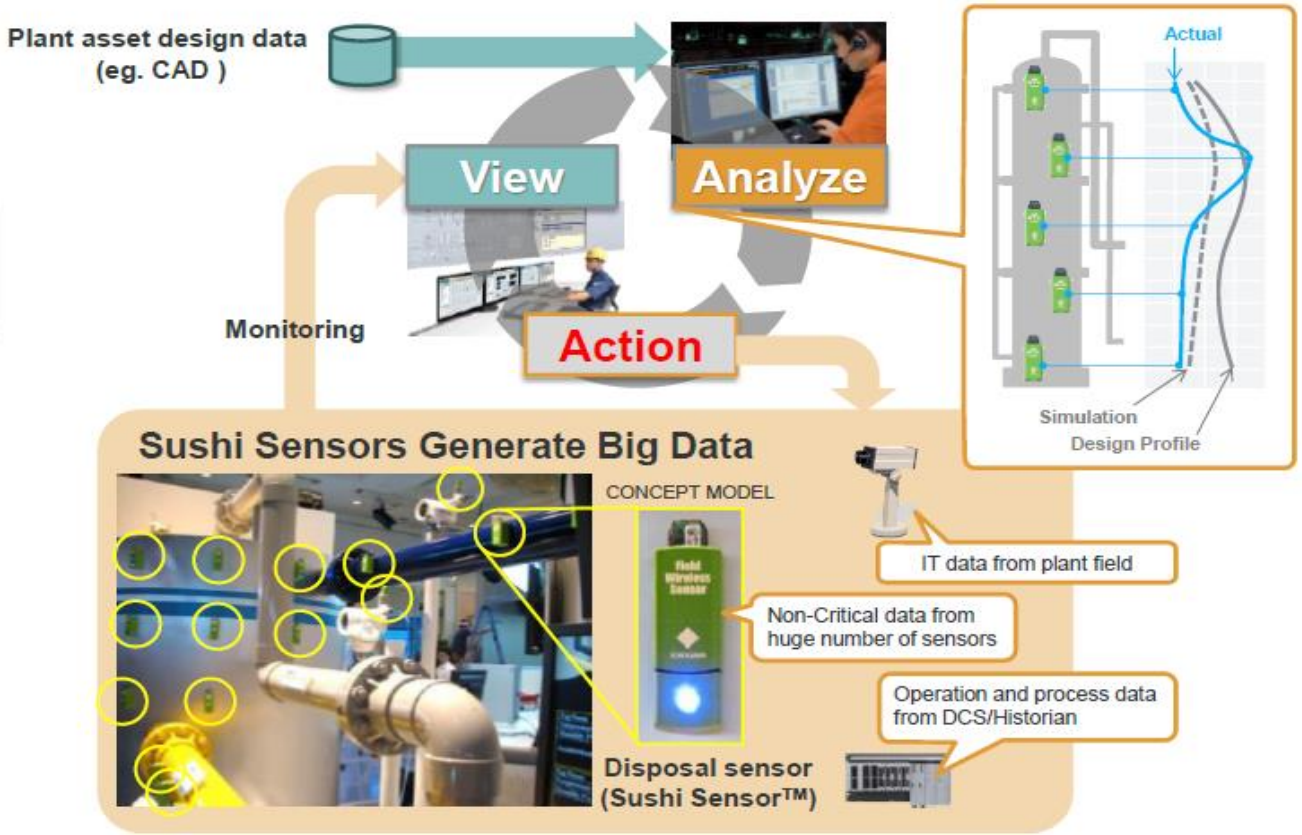
Wireless Expert

Tecnimont – 26 Ottobre 2017

Agenda

- Iiot – Introduzione
- Applicazioni Ilot – Monitoraggio Asset e Controllo Remoto
- Cybersecurity – Problematiche reti Wireless
- Contromisure – Cybersecurity

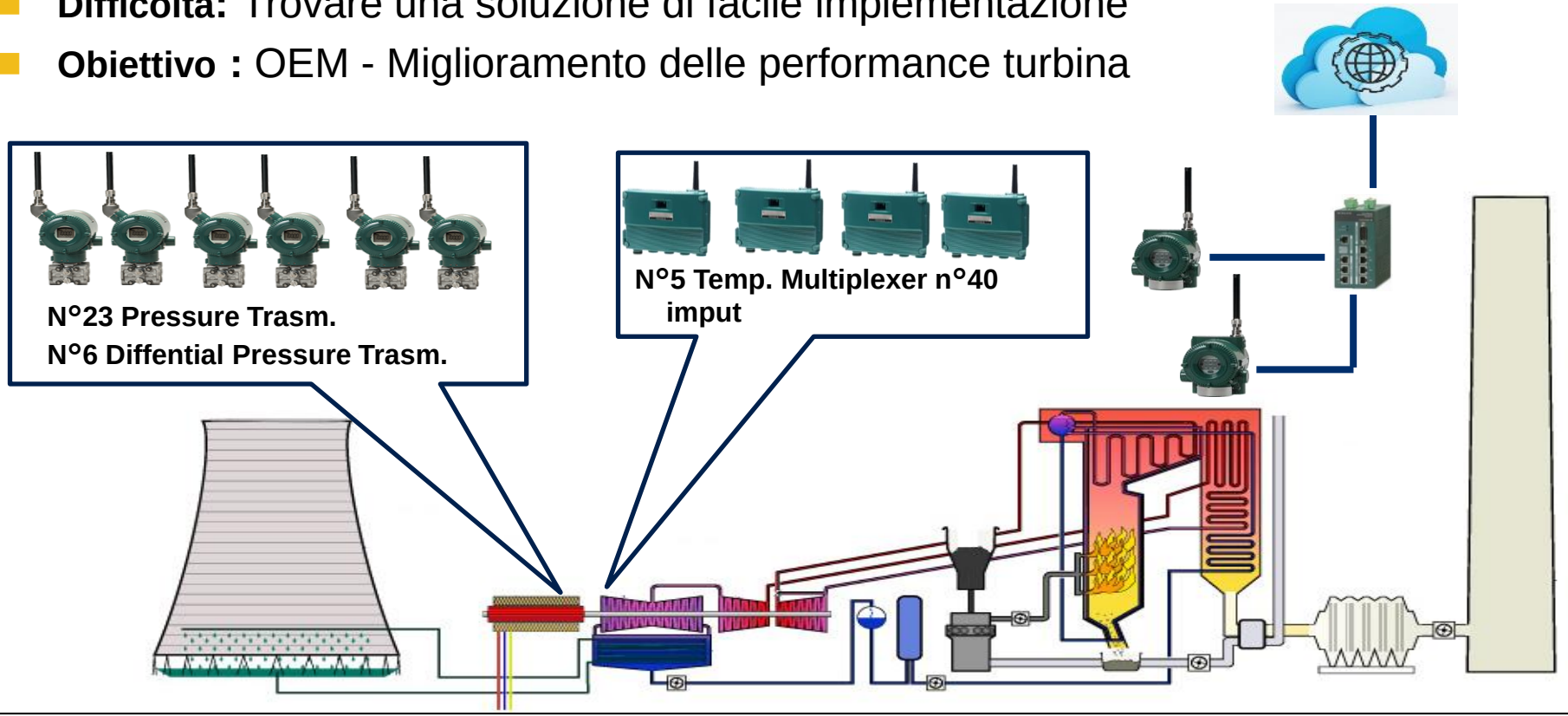
Yokogawa Iot



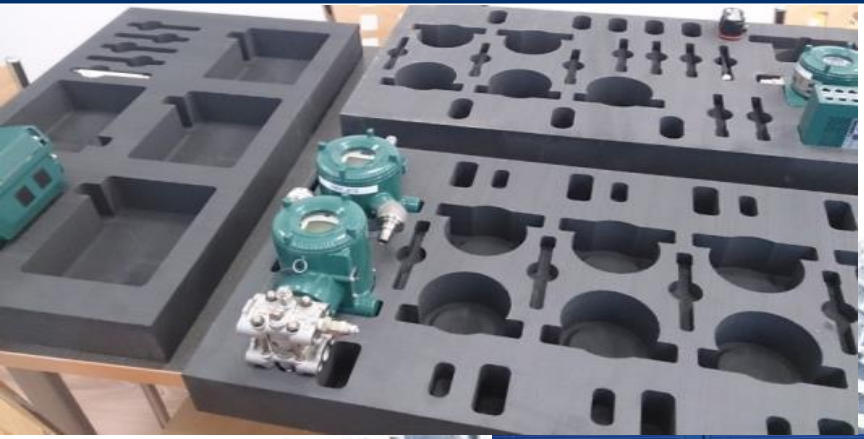
Applicazioni - Monitoraggio e ottimizzazione degli asset

Monitoraggio Temporaneo Performance Turbina

- **Difficoltà:** Trovare una soluzione di facile implementazione
- **Obiettivo :** OEM - Miglioramento delle performance turbina



Monitoraggio e ottimizzazione performance turbina



Benefit

Customer Benefit

- Ridurre costi di manutezione
- Verificare i componeti ed estendere la garazia
- Migliorare le performance
- Diminuire i consumi di energia

Wireless Benefit

- Facile installazione , Montaggio in parallelo alla strumentazione normale.
- No costi per canaline, cavi, ingegneria di dettaglio, Costi operatori DCS, etc
- Riutilizzo degli asset una volta finiti I mesi di test
- Strumentazione Multisensing digitale ,Strumenazione alta velocita 0,5 sec duo cast

IoT benefit

- Real time data
- Condivisione dei dati con società terze
- Accesso dati da remoto
- Simulazione da remoto

Monitoraggio remoto Piattaforma

Application note – Piattaforma Remota

Zuhal piattaforma offshore non presenziata ,Situata a 130 Km dalla costa in mar Cinese Meridionale , Sabah, Malaysia. Sabah. Zuhal dista 5 km dalla piattaforma presenziata Sumandak

Questo sito è stato scelto perchè:

- Nessun Gas detector Installato nella piattaforma.
- Ambiente off-shore e condizioni meteorologiche ridige.
- Possibilità di testare una Rete Wireless con lunga distanza 5km.

LINK PRESENTAZIONE COMPLETA

Project Execution and Installation

Timeline

- Installazione Offshore & commissioning - Maggio 2014
- Test & Monitoraggio – Gennaio 2015

Sfide

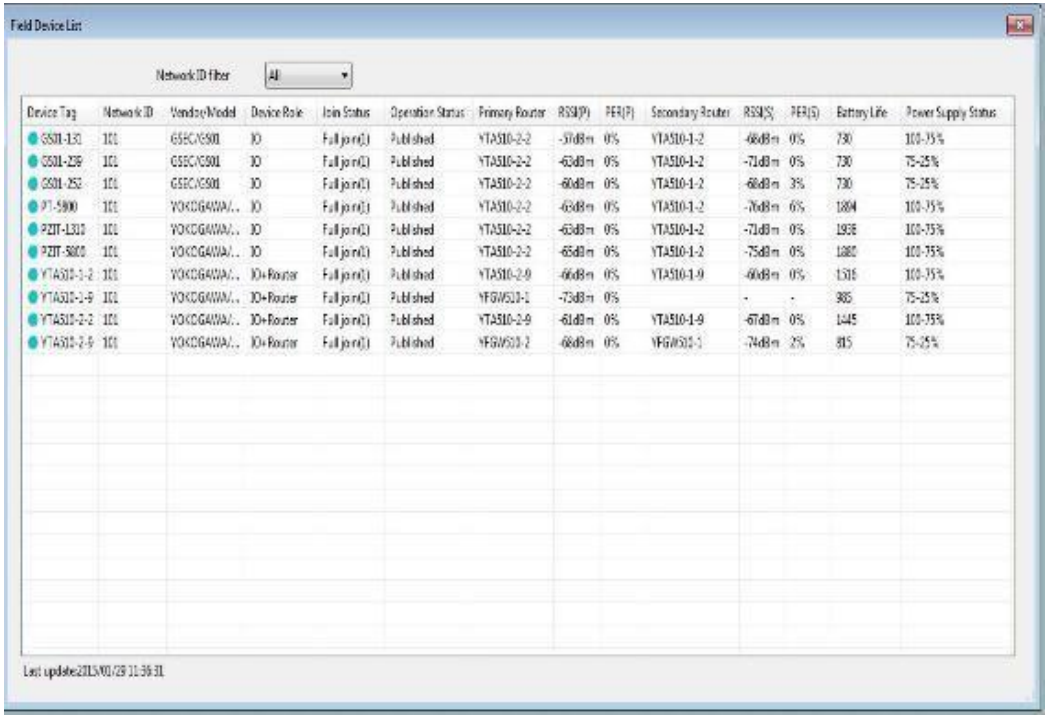
- Installazione Offshore
- Ambiente Rigido
- Strutture metalliche congestionate
- Lunga Distanza in ambiente offshore

LINK PRESENTAZIONE COMPLETA

Risultati del test

La rete ISA100 è stata testata per 6 mesi controllando due parametri principali Received Signal Strenght Indicator (RSSI) e Packet Error Rate (PER)

Risultati del Test :
Rete robusta e stabile
PER = 0%
RSSI = 60bbi



Benefit

Customer Benefit

- Ridurre costi di manutezione.
- Installazione semplice e veloce.
- Ridotti consumi di energia.

Wireless Benefit

- Facile installazione , Montaggio in parallelo alla strumentazione normale.
- No costi per canaline, cavi, ingegneria di dettaglio, Costi operatori DCS, etc.
- Strumentazione Multisensing digitale.

IoT benefit

- Real time data.
- Share dei dati con società terze.
- Accesso dati da remoto.
- Test strumenti da remoto.

Cyber Security

Perchè le WSN sono diventate un target ?

Distanze

100 m, 5 km , 60 km

Applicazioni

Monitoraggio, Controllo, Safety.

Interuzzione delle Utility

Shutdown Impianti

Daneggiamento Asset

Cybersecurity cosa ci dicono le statistiche

Deloitte.

High Technology | Online Media | Telecommunications | E-Commerce & Online payments | Insurance | Manufacturing | Retail | Contact

What are the top three threat vectors you are most concerned with?

Rank the top three, with "First" being the threat of highest concern.

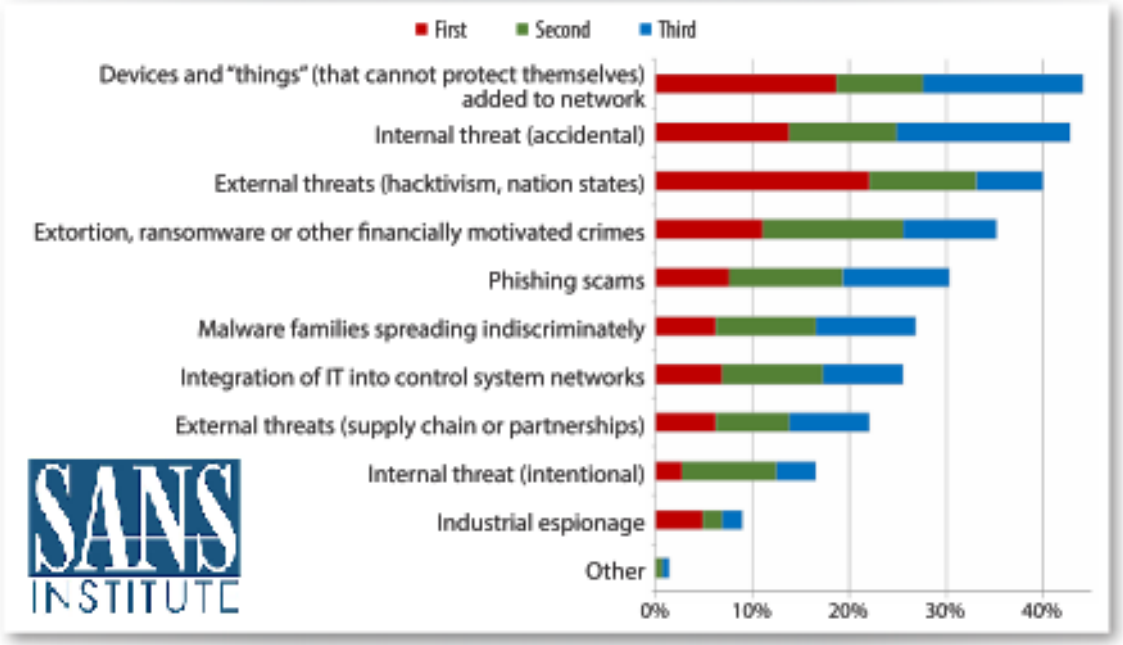


Figure 5. Top Threat Vectors

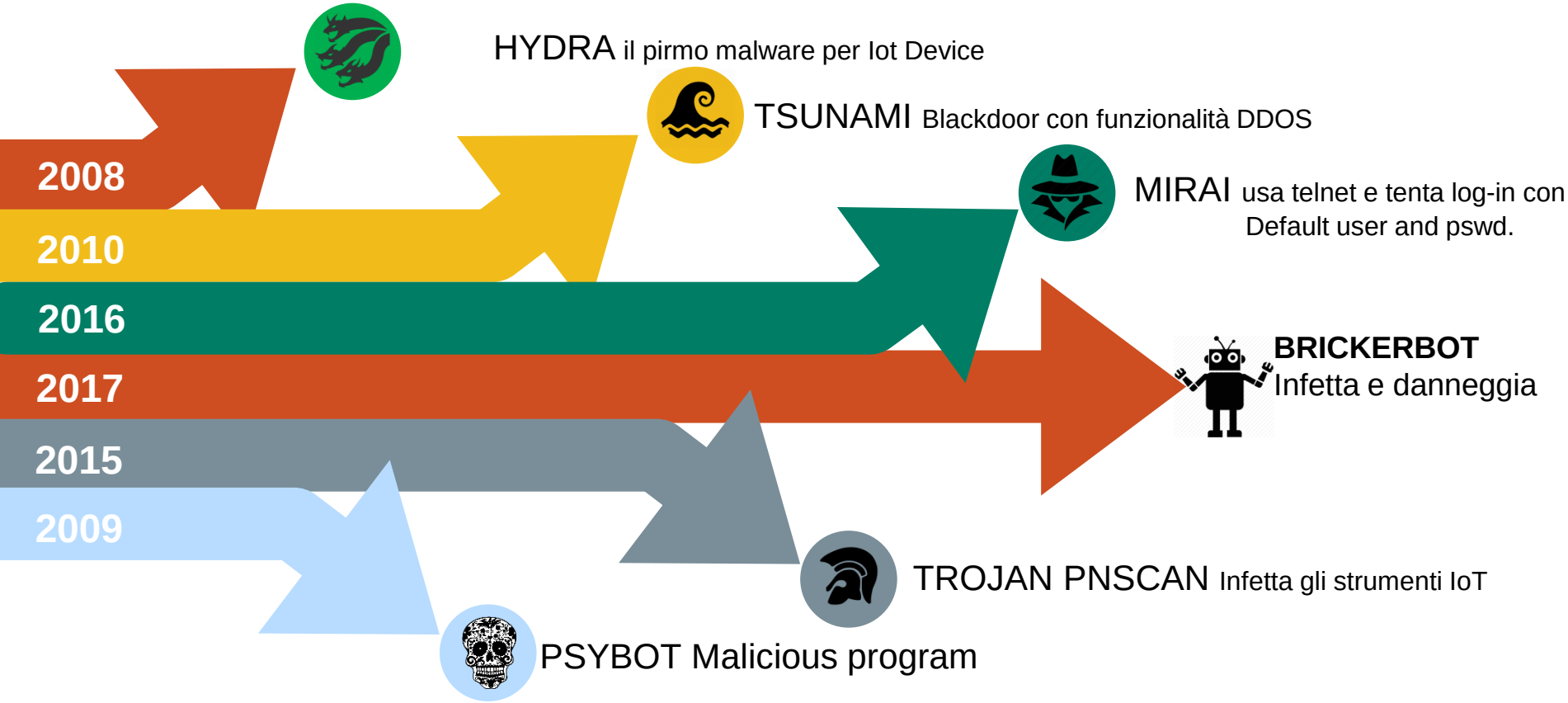
organization's mission.

IT Italian (Italy)

perative. It's a fundamental part of doing business. Yet for many C-suite
c agenda, what does it really mean? And what can your organization do to

Incident classification pattern	Percentage
Point of Sale System Intrusions	14%
Web App Attacks	35%
Insider Misuse	8%
Physical Theft/Loss	<1%
Miscellaneous Errors	2%
Crimeware	4%
Card Skimmers	9%
Denial of Service Attacks	<1%
Cyber-espionage	22%
Everything else	6%

Time line – Iot Malicious



Top five delle problematche sicurezza liot Device

Motore di ricerca IoT

ICS-CERT – Sistema Wireless Teste pozzo

Advisory (ICSA-[redacted])

[redacted] Vulnerabilities (Update A)

Print | Tweet | Send | Share

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

OVERVIEW

This updated advisory is a follow-up to the original advisory titled ICSA-[redacted] WIO Family Vulnerabilities [redacted], on the NCCIC/ICS-CERT web site.

--------- Begin Update A Part 1 of 2 --------

[redacted]

--------- End Update A Part 1 of 2 --------

AFFECTED PRODUCTS

The following [redacted] Products are affected:

[redacted] Wireless Gateway and

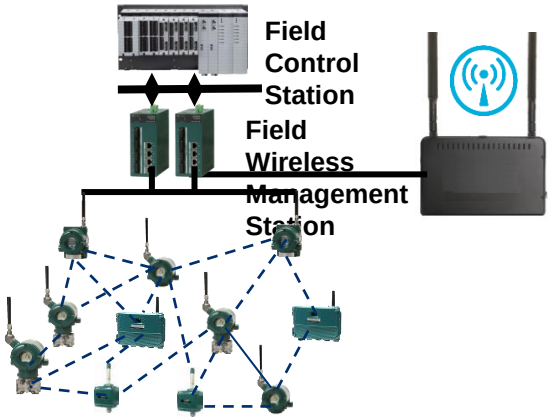
- All [redacted] Sensor Wireless I/O Modules versions.

IMPACT

Two identified vulnerabilities may potentially allow a Man-in-the-Middle (MitM) attack to either monitor for reconnaissance or insert specially crafted data packets into the data stream. The third vulnerability can lead to a denial-of-service (DoS) condition under the correct circumstances.

Attacchi alla WSN

Attacco al Rooter WI-FI



wireless network

Operator with
Tablet

L'operatore vuole testare i device con un tablet/pc, è richiesta la connessione mediante Rooter **WI-Fi**

Il PROBLEMA alcuni rooter usano protezioni obsolete **WPA o WEP**

Quindi, è facile per
Un haker craccare
Questi protocolli

Provisioning Sniffing

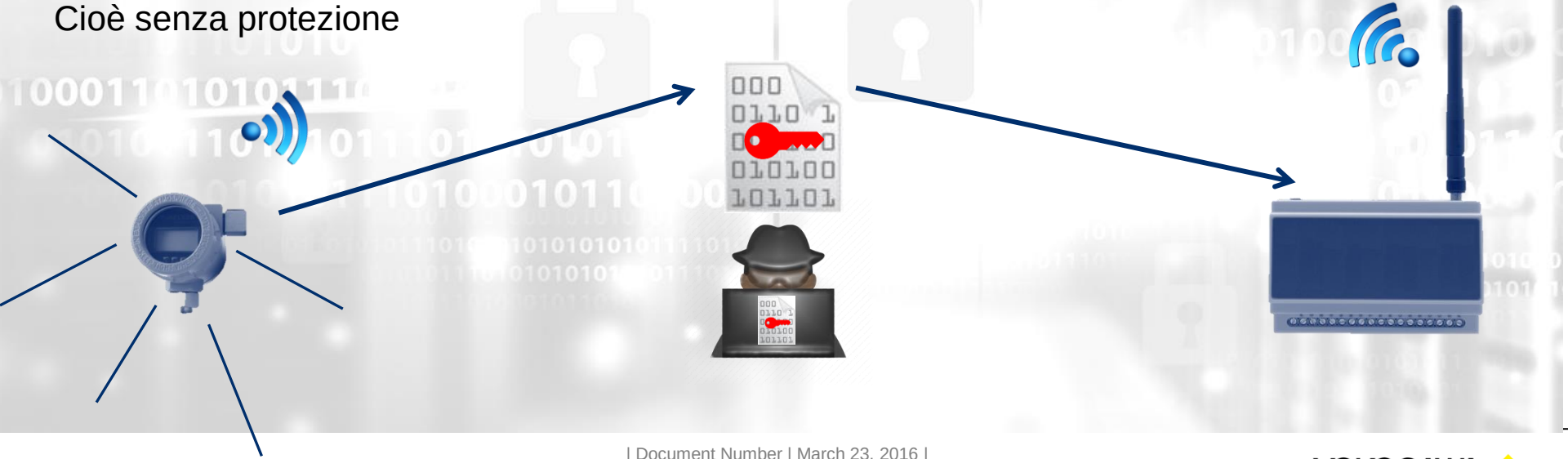
Quando si inserisce un nuovo strumento in rete si deve fare il << Provisioning>>>.

Quando si fa il provisioning >> Lo strumento riceve la cosidetta Join Key in alcuni casi la master key .

Il provisioning è fatto con diversi metodi il più utilizzato e insicuro è «OTA method» .

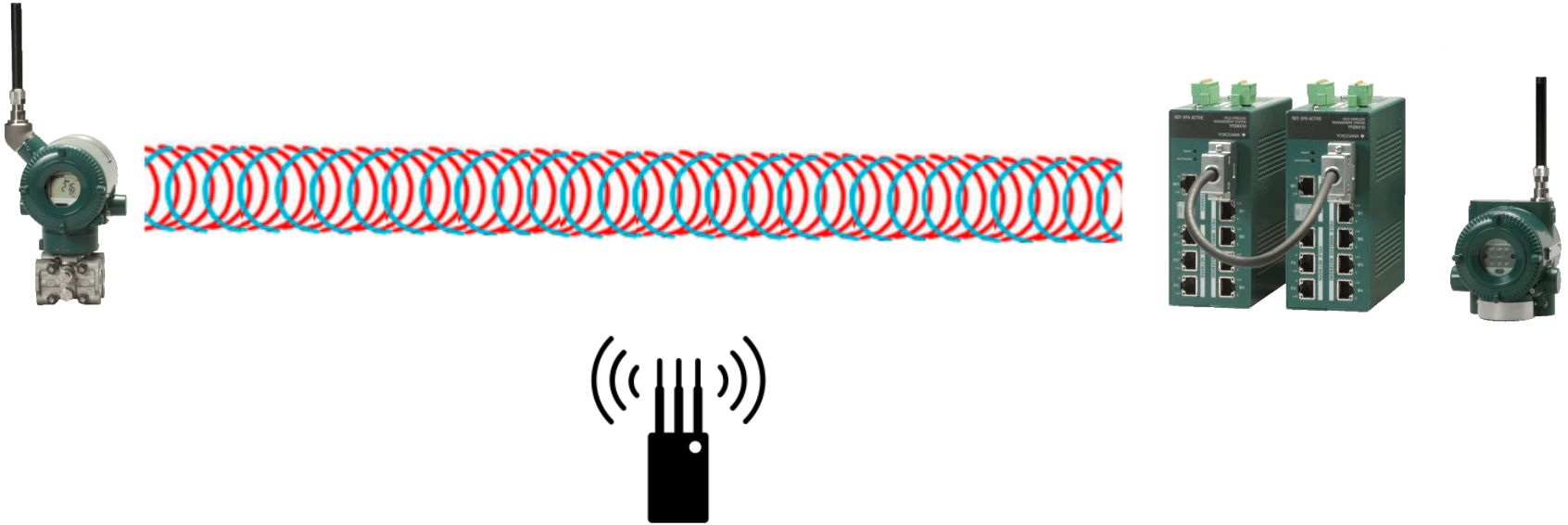
Problematica priocipale: Tutte le informazioni vengono spedite in testo non codificato

Cioè senza protezione



Jamming Reti Wireless

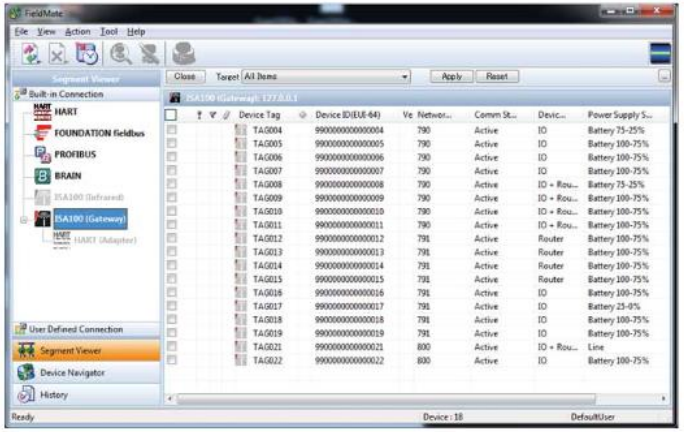
jamming è l'atto di disturbare volutamente le comunicazioni e reti wireless,
È un tipico attacco DoS .
Il Jamming porta alla perdita di dati o alla disconnessione completa dello strumento jamming continuo.

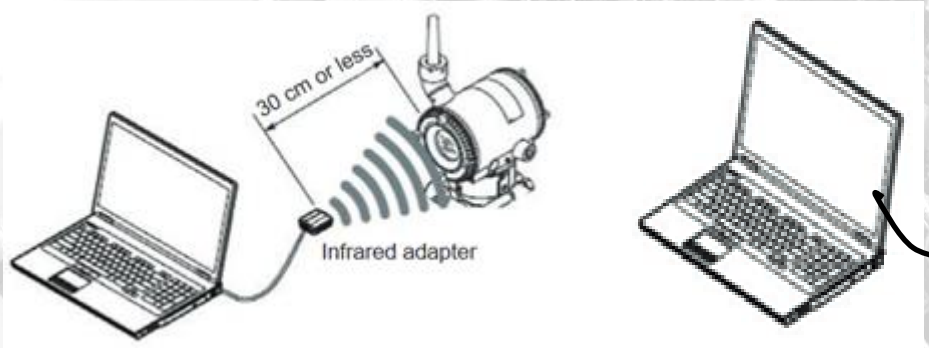


La sicurezza integrata nelle ISA100

Offline provissioning

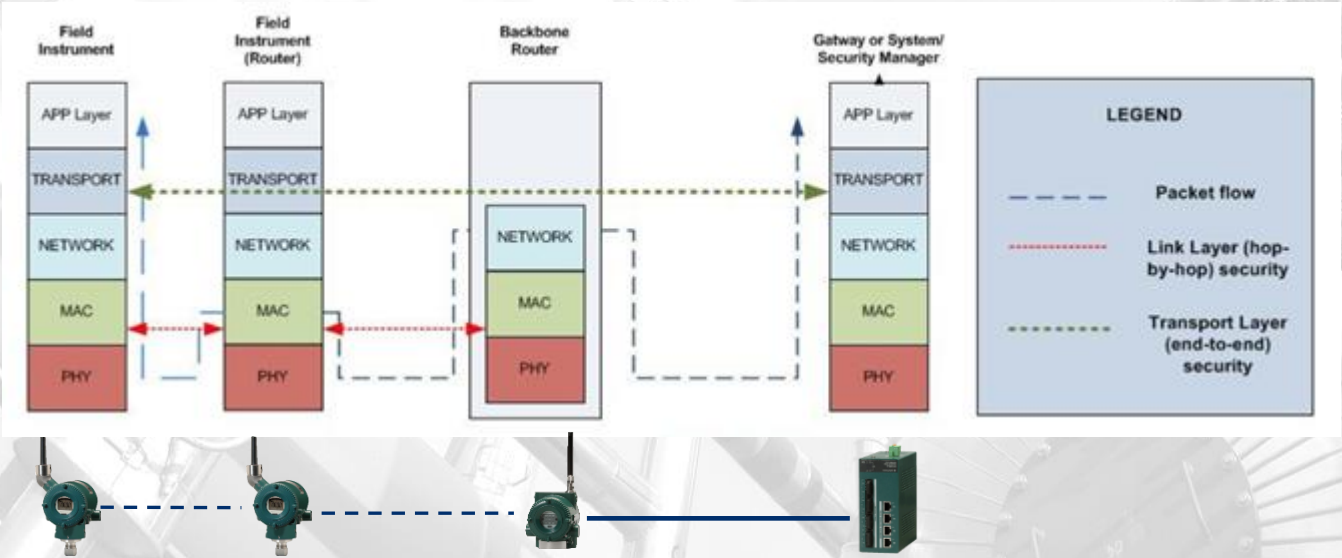
- Completamente OFFLINE
- Le chievi di accesso vengono create tramite software e trasmesse tramite porta infrarossi.



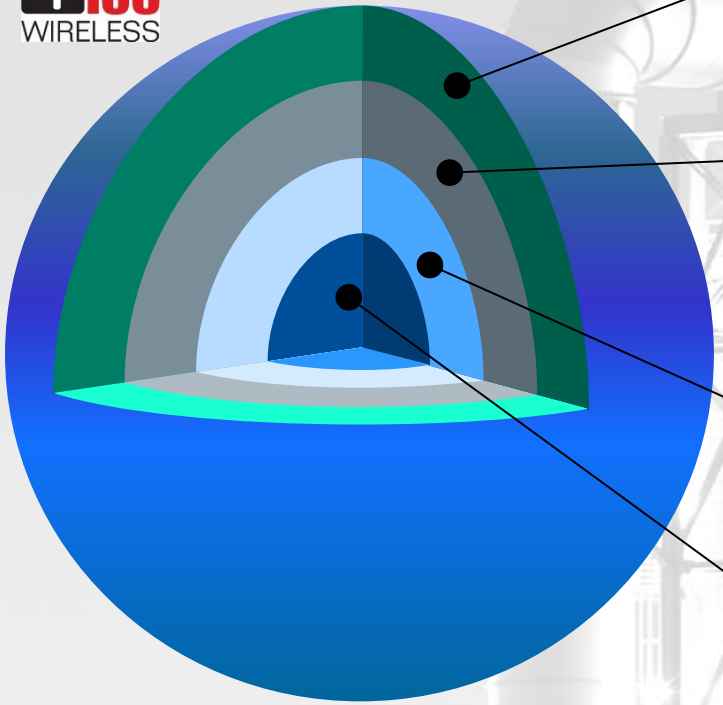


security design ISA100.11a

- Link Layer – Autenticazione Hop-to-hop criptata.
- Transport Layer – Autenticazione End-to-end criptata.



Security Keys in ISA100.11a



- Join Key

Chiave di tipo sincrona reata alla conclusione del provisioning

Usata per l'accesso nel WSN

- Master Key

Creata subito dopo che lo strumento è nel network.

Serve per comunicare con il security Manager .

Viene periodicamente aggiornata .

- DL Key

Usata per creare il Message Integrity Code (MIC)

A livello trasporto . Viene periodicamente aggiornata .

- Session Key

Usata per criptare e autenticare PDU (Protocol data unit) a livello trasporto. . Viene periodicamente aggiornata

Security integrated in ISA100.11a

ISA 100 WIRELESS

1 Crittografia

- Transpont/Data link Layers
- Motore AES-128

2 Mess. Integrity check

- Da. Link Layers
- Autentica I paccheti nel network

3 Security time Stamp

- Tran/Netw Layers
- La rete sincronizzata con il TAI.
- Tutti I paccheti dati che non sono sincronizzati vengo scartati
- Il TAI aggiorna tutte le chiavi

4 Adaptive Hopping

- Physical Layer
- Il Gateway la ricezione del segnale e adatta automaticamente la rete
- ISA100 usa 2.4 Ghz su 16 canali

Certificazione Cybersecurity

Certificate Of Compliance

This is to certify that the:

Field Wireless Management Station

Manufactured by:

Yokogawa Electric Corporation

Is in compliance with the requirements set forth by:

Achilles Level I Certification

CERTIFICATE NO. CERT-292-112415

YFGW410
MODEL NUMBER

R1.06.09
FIRMWARE VERSION

N/A
CONTROL PROTOCOL

Network Device
CATEGORY

This certificate is restricted to the specified version of the referenced Device (including model number, hardware/firmware/software version, and control protocols) set forth in this Certificate. Any change to the Device might impair the Device's ability to pass the standards referenced in this Certificate. This Certificate is based upon limited testing, and is not a complete or comprehensive certification of the security of the Device. The Device may contain security vulnerabilities and deficiencies that are not covered by the standards referenced in this Certificate. This Certificate is subject to revocation by Wurldtech Security Technologies Inc.

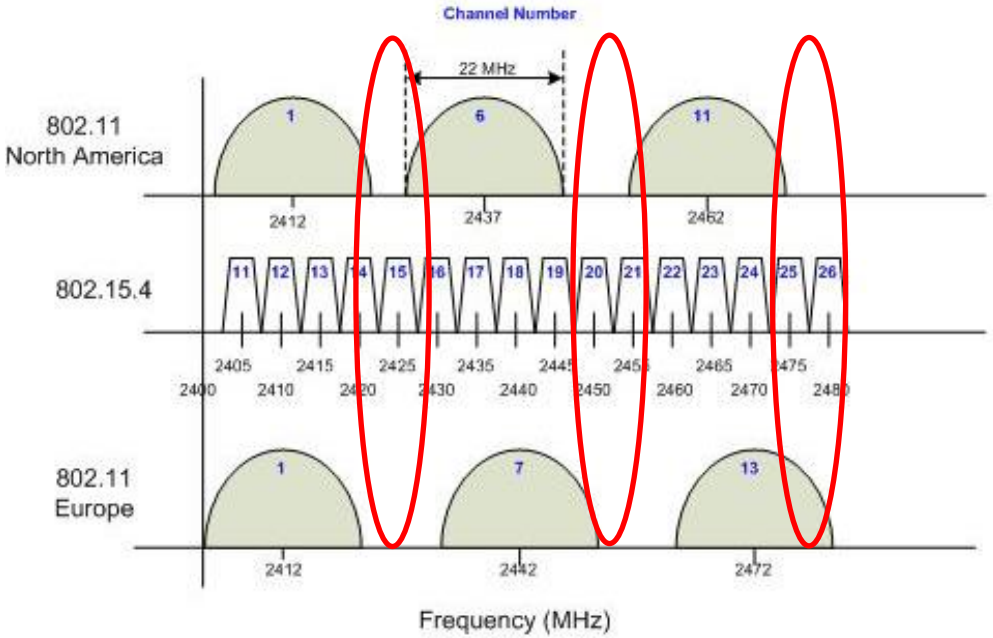
More information regarding this Certificate and the Achilles Communications Certification Standard is available at www.wurldtech.com and upon request from Wurldtech Security Technologies Inc.

Nate Kube, CTO

wurldtech
A GE Company

Contromisure

Conoscere il proprio spetro radio per proteggersi

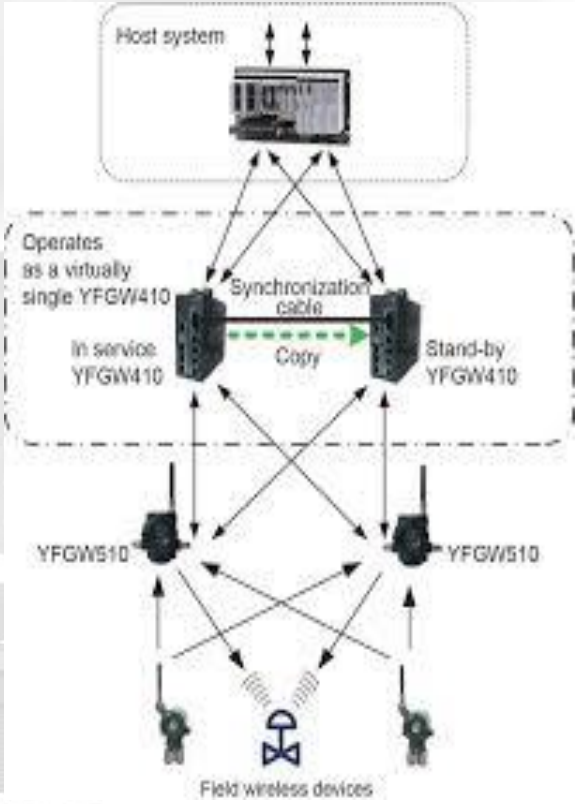


La frequenza 2.4-2.835 GHz è molto utilizzata da

- WiFi/WLAN Bluetooth ,802.15.4 (Industrial Wireless – ISA100, WirelessHART, ZigBee)
- Il target principale dei Jammer è la WiFi 802.11 nei canali WiFi 1,6,7,11,13
- Quindi la 802.15.4 dovrebbe essere canalizzata in **14,15,16,19,20,21,22,24,25,26**

Le contromisure in un WSN

- Inserire nelle RFQ la parte relativa alla Cybersecurity.
- Gli operatori devono essere formati per la parte IIoT e WSN.
- Scegliere soluzioni con Time Hopping e possibilità di blacklist canali.
- Usare protocolli conosciuti nati per l'automazione di processo.
- Le WSN connesse a DCS non devono avere un accesso WI-FI diretto.
- Cyber Security Life Cycle Management deve essere integrato nelle WSN.
- Spectrum survey deve essere introdotto nelle procedure di sicurezza.
- Loop rindondati sono richiesti per applicazioni di controllo (Gateway,Access points, strumenti).
- Le password devono essere complesse con lettere, numeri, caratteri spec.
- WSN connesse a VPN o WI-FI devono essere protette con firewall e protocolli sicuri (SSL , Ipsec)
- Tutte le user e password devono essere aggiornate allo start –up.
- Chiedere certificazione cyber security



Co-innovating tomorrow™

Thank you for you attention

francesco.zucca@it.yokogawa.com