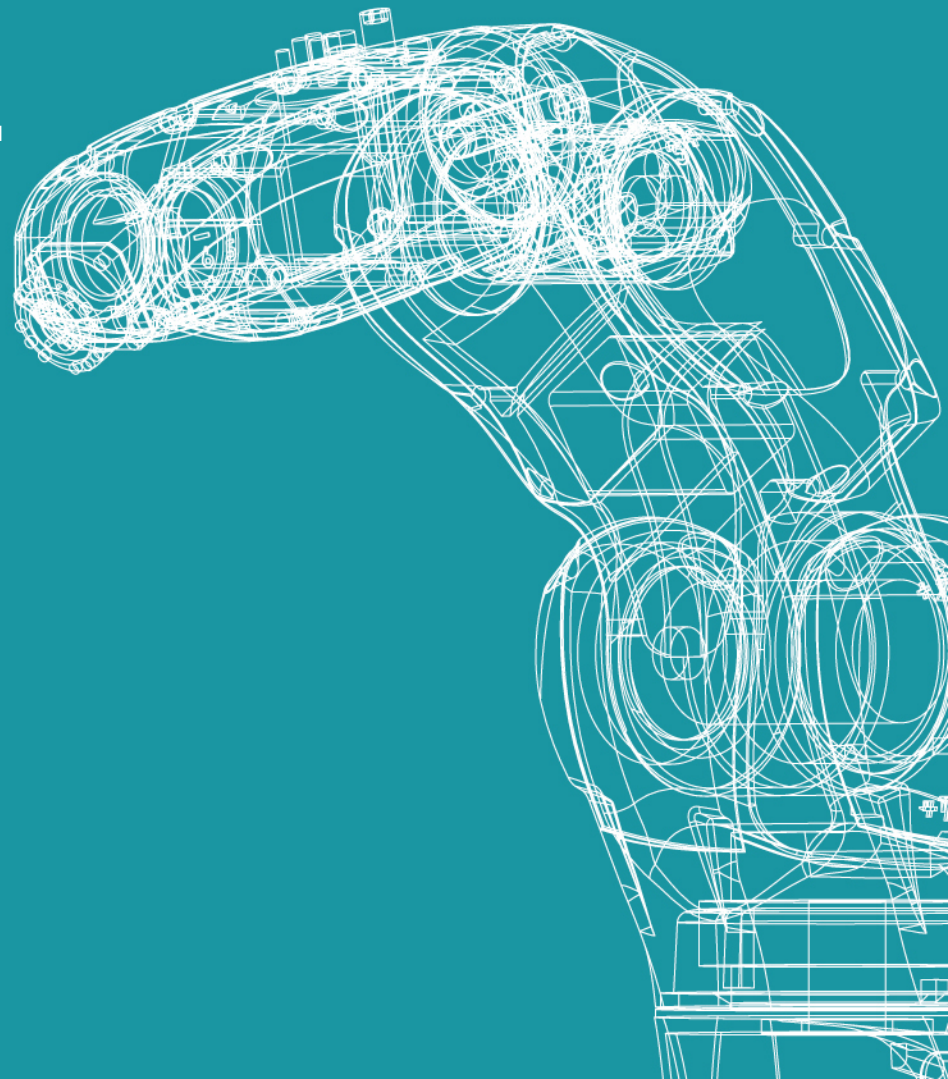
DIHP DIGITAL INNOVATION HUB PIEMONTE

# La convergenza di IT e OT Problema di cultura e competenze

Torino, 8 Ottobre 2018



DIH Digital Innovation Hub

# Situazione Contatti ed Incontri con Aziende

- Partecipazione a **59** Eventi collettivi (oltre **2500** aziende)
- Incontri individuali con aziende: circa **300** (418 registrate nel CRM)
- Digital Readiness Assessment: **60** aziende partecipanti
- Presentati ed approvati **3** progetti misura A per finanziamenti con Voucher Digitali I4.0 da CCIAA Torino per **23** aziende (finanziamento di circa 230,000€)

# Riscontri su sensibilità al tema Cybersecurity

- Abbiamo il **firewall**…
- Abbiamo l'**antivirus**…
- Ci è arrivato un **ransomware** ma per fortuna era venerdì e abbiamo tirato giù tutto…
- Ci è arrivato un **virus** ma avevamo il **back up** di due giorni prima e abbiamo ricaricato tutto…
- Facciamo il **back up** tutti i giorni e il responsabile lo porta a **casa**

## Riscontri su sensibilità al tema Cybersecurity

- Abbiamo il **firewall**…
- Abbiamo l'**antivirus**…
- Ci è arrivato un **ransomware** ma per fortuna era venerdì e abbiamo tirato giù tutto…
- Ci è arrivato un **virus** ma avevamo il **back up** di due giorni prima e abbiamo ricaricato tutto…
- Facciamo il **back up** tutti i giorni e il responsabile lo porta a **casa**
- Il DIHP **non** è riuscito a trovare aziende disposte ad effettuare un penetration test **finanziato** da CCIAA (voucher digitalizzazione I4.0)

# Problematiche legate all'integrazione IT OT

- I **dispositivi OT** (CNC, robot controllers,…) sono stati inizialmente concepiti per lavorare in modalità **stand alone**
- A lungo sono stati collegati ai controller centralizzati (i cosiddetti livelli 2) utilizzando collegamenti **punto a punto** o **reti industriali dedicate** (profinet, modbus, devicenet,…) per cui la tematica della sicurezza del device non era importante
- Infine **Ethernet** è diventato pervasivo, collegando su un'**unica rete** (**Ethernet IP**), tanto i dispositivi **IT** che i dispositivi **OT**, senza dotare questi ultimi di opportune caratteristiche di sicurezza
- E' necessario tenere in conto sia i rischi di sicurezza (**Security**) che i rischi per la sicurezza (**Safety**) in quanto i dispositivi per la safety condividono la **stessa rete**

# I problemi in officina (che ci accompagneranno a lungo)

- Ampia diffusione di apparati con **OS obsoleti** non predisposti per la **gestione remota**
- Complesso (impossibile?) certificare la **backward compatibility** di un sistema **cyberfisico**
- La gran parte delle PMI si affida a **consulenti esterni** per la gestione del proprio sistema informativo: tipicamente chi si occupa di **IT** non ha competenze sulle **reti industriali**
- Per ovviare ai problemi le aziende tendono a **non collegare** lo shop floor ad **Internet,** ma in questo modo limitano il range delle possibili applicazioni
- Eventuali attacchi **malevoli** ai dispositivi OT possono **non essere rilevati** (vedi youtube **Rogue Robots: Testing the Limits of an Industrial Robot's Security** https://www.youtube.com/watch?v=BxHYtFlKruY)

DIGITAL INNOVATION HUB PIEMONTE

# Grazie per l’attenzione

www.dih.piemonte.it

info@dih.piemonte.it

@dihpiemonte

Digital Innovation Hub Piemonte

@DihPiemonte