



SBS partner strategico di:



News - 24/05/2021

## INDUSTRIA 4.0 TRA OPPORTUNITA' E OT CYBERSECURITY

I cambiamenti che la rivoluzione 4.0 porta con sé nell'industria sono radicali ed epocali. Negli ultimi anni infatti migliaia di aziende si sono dotate di tecnologie sempre più complesse ed avanzate che prevedono un modo di lavorare ed una sensibilità organizzativa completamente diverse rispetto ai metodi di lavoro tradizionali. Il lavoro quotidiano, la programmazione, la gamma dei servizi, l'assistenza, le soluzioni si sono dovute adeguare ai nuovi paradigmi stabiliti dal digitale, da tecnologie sempre più connesse e da intelligenze artificiali sempre più sofisticate. L'era 4.0 implica quindi nuove e vaste opportunità, ma anche molti rischi fino a pochi anni fa sconosciuti.

Sul fronte delle opportunità, l'elemento che fa la differenza, soprattutto nel settore dei costruttori di macchine e beni strumentali industriali, è dato dall'**interfaccia uomo-macchina**. In un mondo connesso e in un'industria 4.0 l'interfaccia uomo-macchina è sia l'elemento determinante per migliorare le performance delle linee esistenti, massimizzando il ritorno sull'investimento, sia l'elemento che stabilisce nuovi modelli di business e relazioni a lungo termine tra utilizzatore e produttore. L'utilizzo di wearable devices, dispositivi indossabili, anche in ambiente industriale, permette infatti di fornire modelli di sviluppo ed esempi innovativi di interfacce uomo-macchina fruibili dai tecnici e a valore aggiunto per il management aziendale. Implementando realtà aumentata ed algoritmi di machine learning, già oggi è possibile mostrare come l'HMI (Human Machine Interface) diventi l'elemento cruciale nell'esercizio di linee automatiche connesse ad alta efficienza.

Sul fronte dei rischi, il nuovo fronte imprescindibile per ogni azienda è dato dalla **cybersecurity**. Senza un sistema efficiente ed aggiornato di protezione dei dati, a partire dai sistemi di controllo industriali (Industrial Control System, ICS), l'impresa è esposta a rischi crescenti, non solo di vulnerabilità informatica, ma anche di responsabilità durante l'installazione e l'esercizio (anche in paesi remoti) delle macchine, dovendo prevedere anche variabili e normative degli stati dove gli strumenti sono utilizzati. La cybersecurity si cala così dalla sicurezza dei dati aziendali al funzionamento delle macchine, la cosiddetta OT (Operation Technology) con l'obiettivo di garantire sicurezza a partire dalla generazione del dato, nei sensori, nei controllori di impianto real-time, nei sistemi di Edge Computing, nei sistemi Scada che ne permettono supervisione, gestione degli allarmi e la comunicazione sicura al mondo dell'Information Technology.

“Le nostre aziende stanno crescendo all'interno del cambiamento epocale dell'Industria 4.0. Si sviluppano e si acquisiscono tecnologie sempre più complesse ed avanzate che prevedono un modo di lavorare ed una sensibilità organizzativa diverse rispetto al passato. In questi modelli di business avanzati la cybersecurity è fondamentale a partire dall'OT Operational Technology, ovvero dalla generazione del dato, fino alla tutela dello stesso”. Ing. Martino Caranti