SICUREZZA DEI MACCHINARI IN PRESENZA DI SISTEMI COMPLESSI E INTERCONNESSI

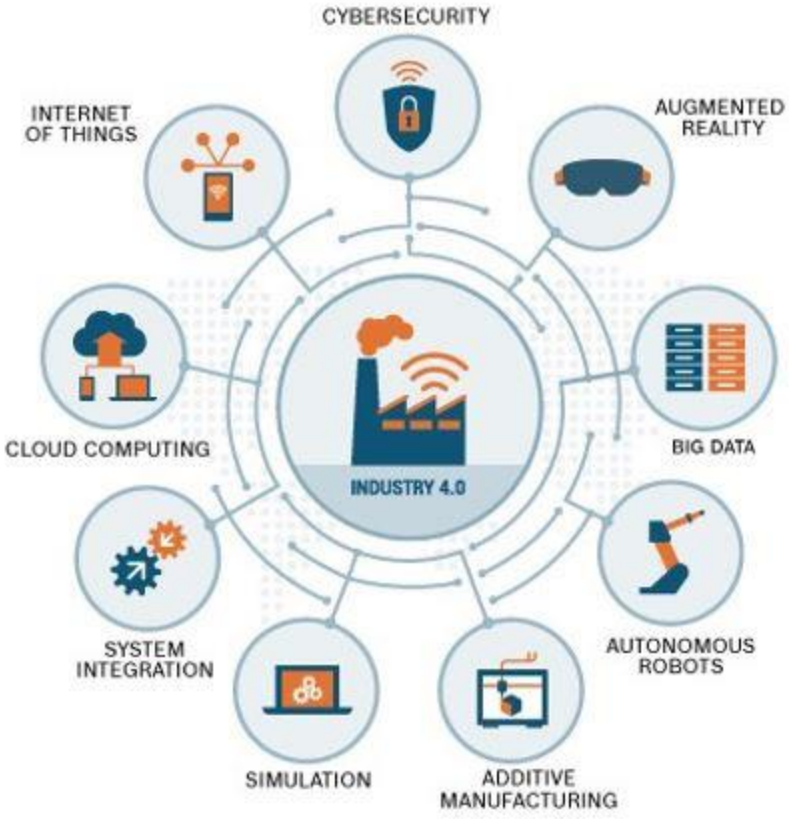
Ing. Luigi Zerella
Membro Sotto-Commissione Sicurezza Igiene del Lavoro e Cantieri
Ordine Ingegneri della Provincia di Milano
Ispettore e consulente Direttiva Macchine
luigi.zerella@certitudo.it

9-10 Settembre 2021

Presentazione

- Breve introduzione I4.0 e tecnologie abilitanti
- Automazione ed interconnessione
- Perché parlare di sicurezza delle macchine in I4.0 è importante?
- Brainstorming sicurezza in I4.0 (Stato dell'arte)
- Cosa sono i sistemi complessi
- Sistemi interconnessi nell'ambito macchinari
- Come si può fare sicurezza: tecniche e metodi
- Riferimenti normativi per la sicurezza in I4.0
- Cosa dobbiamo fare
- Discussione e saluti

Generalità e definizioni I4.0



ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI MILANO

Ing. Luigi Zerella

Membro Sotto-Commissione Sicurezza Igiene del Lavoro e Cantieri

Ordine Ingegneri della Provincia di Milano

Le tecnologie abilitanti

- Le 9 tecnologie abilitanti :
- ***Advanced manufacturing solution***: sistemi avanzati di produzione, ovvero sistemi interconnessi e modulari che permettono flessibilità e performance. In queste tecnologie rientrano i sistemi di movimentazione dei materiali automatici e la robotica avanzata, che oggi entra sul mercato con i robot collaborativi o *cobot*.
- ***Additive manufacturing***: sistemi di produzione additiva che aumentano l'efficienza dell'uso dei materiali.
- ***Realtà aumentata***: sistemi di visione con realtà aumentata per guidare meglio gli operatori nello svolgimento delle attività quotidiane.
- ***Simulazioni***: simulazione tra macchine interconnesse per ottimizzare i processi.

Le tecnologie abilitanti

- ***Industrial internet****:* comunicazione tra elementi della produzione, non solo all'interno dell'azienda, ma anche all'esterno grazie all'utilizzo di internet.
- ***Cloud***: implementazione di tutte le tecnologie *cloud* come l'archiviazione online delle informazioni, l'uso del *cloud computing*, e di servizi esterni di analisi dati, ecc. Nel *cloud* sono contemplate anche le tecniche di gestione di grandissime quantità di dati attraverso sistemi aperti.
- ***Sicurezza informatica***: l'aumento delle interconnessioni interne ed esterne aprono la porta a tutta la tematica della sicurezza delle informazioni e dei sistemi che non devono essere alterati dall'esterno.
- ***Simulazioni***: simulazione tra macchine interconnesse per ottimizzare i processi.
- ***Big Data Analytics***: tecniche di gestione di grandissime quantità di dati attraverso sistemi aperti che permettono previsioni o predizioni.

Le direttrici di sviluppo I4.0

- L'industria 4.0 scaturisce dalla quarta rivoluzione industriale, il processo che **porterà alla produzione industriale del tutto automatizzata e interconnessa**.
- 4 le **direttrici** di sviluppo in cui muoversi:
- La prima riguarda **l'utilizzo dei dati**, la potenza di calcolo e la connettività, e si declina in big data, open data, Internet of Things, machine-to-machine e cloud computing per la centralizzazione delle informazioni e la loro conservazione.
- La seconda è quella degli **analytics**: una volta raccolti i dati, bisogna ricavarne valore. Oggi solo l'1% dei dati raccolti viene utilizzato dalle imprese, che potrebbero invece ottenere vantaggi a partire dal "machine learning", dalle macchine cioè che perfezionano la loro resa "imparando" dai dati via via raccolti e analizzati.

Le direttrici di sviluppo I4.0

- La terza direttrice di sviluppo è l'**interazione tra uomo e macchina**, che coinvolge le interfacce "touch", sempre più diffuse, e la **realtà aumentata**.
- La quarta direttrice è data dal settore che si occupa del passaggio dal digitale al "reale" e che comprende la **manifattura additiva, la stampa 3D, la robotica, le comunicazioni, le interazioni machine-to-machine e le nuove tecnologie** per immagazzinare e utilizzare l'energia in modo mirato, razionalizzando i costi e ottimizzando le prestazioni.

Sicurezza ed I4.0 – Perché?

- Motivo pratico:
  - Legato alla conformità della presentazione della domande per il credito di imposta, uno dei requisiti per il buon esito della domanda è la «**conformità alle più recenti regolamentazioni europee**» (**Direttive di prodotto**)* e parlando di combinazione di macchine e sistemi complessi, il riferimento è agli **assiemi di macchine****.
- In realtà il motivo più importante:
  - Nelle 9 tecnologie abilitanti **sono celati** risvolti che hanno a che fare direttamente o indirettamente con la sicurezza (safety e security) e che possono ripercuotersi sulla salute dei lavoratori - alcuni esempi:
    - Cybersecurity e rapporto con la **sicurezza funzionale delle macchine;**
    - Connessione con SW non tipicamente di sicurezza (funzionale);
    - Gestione big data per intelligenza artificiale e auto-apprendimento delle macchine;

Automazione ed interconnessione

- Dal 2016 data di entrata in vigore del primo Decreto I40, anche grazie agli incentivi industria 4.0 ora Transizione 4.0, moltissime aziende hanno connesso le loro macchine alla rete aziendale.
- In parte sicuramente solo per garantire la rispondenza ai requisiti della norma (ed ottenere i vantaggi dell'Iperammortamento oggi Credito di imposta), in parte con una visione più a lungo termine, di trarre un oggettivo vantaggio da questa interconnessione e nell'ottica della digitalizzazione dell'azienda.
- Quasi tutte le aziende, però, hanno seguito la strada dell'interconnessione delle macchine senza pensare alla sicurezza. Questo significa che la maggior parte delle macchine sono oggi raggiungibili con strumenti come VNC (Virtual Network Computing), FTP, client specifici per marca del PLC, client OPC-UA senza alcuna protezione. (Open Platform Communications (OPC) e OPC UA (Unified Architecture) sono standard che facilitano lo scambio di dati tra PLC, interfacce uomo-macchina (HMI), server, client e altri macchinari ai fini dell'interconnettività e della circolazione delle informazioni).

Automazione ed interconnessione

- Con un VNC aperto, una macchina può essere fermata o riconfigurata per creare un danno alla produzione.
- Spesso si è sottovalutato questo problema in quanto le macchine sono in **una rete interna**, quando va bene in una sotto-rete propria, e quindi la raggiungibilità dall'esterno è oggettivamente improbabile.
- Ma gli attacchi possono avvenire anche dall'interno, sia per mano degli stessi dipendenti sia utilizzando questi ultimi come testa di ponte attraverso i loro PC o smartphone.
- Quindi Il punto più debole sono le stesse macchine o meglio, la configurazione della loro interconessione.
- I «sistemi di produzione interconnessi» sono creati da tecnici che sanno tutto di meccanica ed automazione, ma non molto di interconnessione e sicurezza informatica. Gli stessi strumenti che utilizzano (PLC, HMI, PC industriali) non hanno la sicurezza «interna» come priorità, anzi, spesso sono considerati dei fastidi perché rendono più lungo lo sviluppo del SW.

Automazione ed interconnessione

- Una macchina, quindi, una volta che viene collegato il cavo ethernet diventa un punto di accesso, libero ed attaccabile, sia in lettura che in scrittura.
- Anni di fatica per far digerire che la sicurezza funzionale fosse fondamentale per la sicurezza dei lavoratori ed uno switch, potrebbe rappresentare un problema.
- Ogni macchina che viene interconnessa deve obbligatoriamente richiedere delle credenziali per poterne modificare i parametri di funzionamento, eppure ancora oggi la psw per le modifiche che i costruttori rilasciano è 0000.
- Se l'accesso alla macchina in lettura non è probabilmente un gravissimo problema, l'accesso in scrittura lo è.
- E' quindi indispensabile chiedere al produttore di inserire un blocco in questo senso rappresentato almeno dalla richiesta di credenziali per operazioni di modifica e di progettare in ottica di sicurezza informatica.
- Quasi mai viene fatto perché il produttore stesso, nel momento della teleassistenza, dovrebbe avere a disposizione le credenziali che, come succede a tutti, nel tempo vengono perdute o rimosse per comodità.

Teleassistenza

- Teleassistenza permanente: attraverso una VPN il produttore può accedere alla macchina in qualsiasi momento su richiesta del cliente. Questa incredibile comodità paga un prezzo: se il produttore subisce un attacco, le macchine del cliente risultano esposte.
- La teleassistenza non si fa ogni giorno, ma solo su richiesta: modifiche al software, diagnostica, riconfigurazione. E' uno strumento molto importante anche considerando l'aumento dello «smartworking», ma pericoloso se fatto in modo non sicuro e quanto a casa hanno un sistema protetto.
- Il produttore deve garantire che l'accesso in teleassistenza possa agire sulla macchina solo se viene permesso sulla macchina stessa nel momento della necessità ed in presenza (fisica) di un tecnico competente della macchina oppure che all'interno della fabbrica possa accedere da remoto un tecnico interno con le credenziali e sbloccare l'accesso in teleassistenza.

Brainstorming Sicurezza Macc. in I4.0

- Riferimento per la sicurezza dei macchinari è la Direttiva CE 2006/42/CE – Direttiva Macchine, ma anche le altre direttive (EMC, LVD, ATEX, PED..), che però sono ferme a prima dell'avvento dell'industria 4.0 (le ultime direttive importanti sono del 2014 e non c'è nessuna traccia di quanto detto finora).
- Gli standard correlati sono le Norme armonizzate che, come tutte le norme non sono obbligatorie, solo in alcuni casi danno la presunzione di conformità, **ma non sono ancora pronte per l'integrazione** e tanto meno per l'interconnessione di macchine ed apparecchi;
- Per la sicurezza informatica ci sono stati dei passi avanti notevoli negli ultimi anni ,ma le norme della serie IEC 62443 e la norma ISO 27001 sono volontarie e non sono ancora state recepite a livello di CEN e CENELEC.
- Lo scopo delle Direttive di Prodotto (non solo la Direttiva Macchine) è fare in modo che attraverso il soddisfacimento dei Requisiti di Salute e Sicurezza i prodotti possano essere utilizzati con un livello di rischio accettabile, possibilmente basso, con un percorso in cui l'analisi dei pericoli e la **valutazione del rischio tengano conto dei fattori noti**.

Brainstorming Sicurezza Macc. in I4.0

- Macchinari vengono interconnessi quasi sempre non dai fabbricanti, ma dagli utilizzatori; le macchine spesso non sono state pensate per la difesa da «attacchi» esterni, sia a livello di sicurezza informatica, che dal punto di vista dell'introduzione di nuovi sensori o circuiti di sicurezza «adattati» allo scopo dell'utente.
- Peraltro se si analizza scenario attuale (o solo di qualche anno fa) la maggior parte delle linee produttive e delle aziende manifatturiere posseggono macchine non sempre adeguate all'Allegato V del Dlgs.81/08 che come riferimento ha norme e principi che derivano dal DPR 547 del 1955!
- I4.0 – deriva verso una pseudo digitalizzazione solo in funzione degli incentivi economici per l'industria?

Tecniche generali di Sicurezza

- Se si vuole che I4.0 sia veramente un'opportunità di sviluppo delle aziende e delle tecnologie non a discapito della sicurezza dei lavoratori, ma soprattutto se si vuole che questo rappresenti non un dominio di pochi, ma un'evoluzione, appunto la 4a rivoluzione industriale, è necessario re-indirizzare gli obiettivi e pianificare in ottica di una vera e propria «cultura della sicurezza».
- Da dove cominciare? Consolidando quello che si ha, utilizzando gli strumenti normativi attuali e... Spingere (qualcuno di noi partecipa ai CT di UNI e CEI) per nuove norme in ottica i4.0.
- Innanzitutto mettere a punto delle **tecniche di sicurezza** dei macchinari che siano congiunte: la prevenzione degli infortuni passa sempre attraverso un'attenta analisi dei pericoli e valutazione dei rischi che quindi deve tenere in conto di due fattori della sicurezza: la **sicurezza funzionale** (safety) e la **sicurezza** (security) contro gli «attacchi» dall'esterno, visto l'elevato livello richiesto di interconnessione;

Tecniche generali di Sicurezza

- Progettare la nuova macchina interconnessa o la nuova linea I4.0 a cominciare dalle specifiche tecniche verso i produttori delle singole macchine.
- Evitare di pensare che si possano mettere insieme due macchine qualsiasi e creare una linea interconnessa con il «softwarista che cura le buste paga», non saprà niente di sicurezza macchine.
- Si possono individuare tre strategie, al di là dell'attesa dell'adeguamento del quadro normativo (es. il Nuovo Regolamento Macchine introduce la questione della sicurezza informatica e delle nuove tecnologie ma è ancora una proposta):
- Al momento attuale appare più importante agire sui fabbricanti e sulla nuova esigenza di flessibilità delle macchine che possono combinarsi in modi molto diversi (progettazione di macchine predisposte alla scalabilità, flessibilità, ai nuovi sensori, all'interconnessione) senza dimenticare la sicurezza intrinseca della macchina stessa ma in ottica di futuri assemblaggi;
- Sviluppare competenze interdisciplinari per cui la valutazione del rischio safety sia sviluppata in contemporanea alla valutazione del rischio security;

Tecniche generali di Sicurezza

- Puntare sull'uso di strumenti di comunicazione collaudati e progettare in sicurezza gli scambi di informazioni tra le macchine del sistema produttivo e le altre reti informatiche dell'azienda (sistema cyberfisico).
- A questo proposito alcuni riferimenti normativi possono aiutarci:
  - Le norme di nuova generazione della serie IEC 62443 che sono state preparate per rendere sicure le reti di comunicazione industriale e i sistemi di automazione e controllo industriale (IACS) attraverso un approccio sistematico.
    Sono inclusi inoltre Sistemi di Controllo e Acquisizione Dati (SCADA) che sono comunemente usati dalle organizzazioni che operano in settori di infrastrutture sensibili, come la generazione, la trasmissione e la distribuzione di energia e le reti di distribuzione di acqua e gas.
  - La norma volontaria ISO 27001:2005 che stabilisce i requisiti per il Sistema di Gestione della Sicurezza delle Informazioni (ISMS).
    L'obiettivo principale è quello di stabilire un sistema per la gestione del rischio, la protezione delle informazioni e degli asset aziendali, ivi inclusi gli asset IT.

Sicurezza dei sistemi complessi ed interconnessi

1. Progetto del sistema cyberfisico sulla carta, con specifiche per tutti i componenti (fisici ed immateriali) frutto di scambio di informazioni tra i componenti del sistema in funzione della sicurezza (safety e security);
2. Analisi dei pericoli e valutazione dei rischi:
   - Pericoli dovuti all'interferenza non solo di tipo meccanico tra le macchine componenti – con gli strumenti che si hanno (EN 12100, metodo ibrido, metodo dei grafi);
   - Simulazione degli scenari possibili;
   - Progetto delle misure di adeguamento, sia a livello di «meccanica» e «automazione» con incremento del livello di sicurezza funzionale con le norme esistenti (IEC 61508 e EN 13849) che a livello di scambio e sicurezza delle informazioni (security) con le norme della serie IEC 62443;

Sicurezza dei sistemi complessi ed interconnessi

3. Progettazione dell'interconnessione con i livelli gestionali secondo standard di sicurezza «interna» ed «esterna» per esempio secondo le norme (IEC 62443) e considerando livelli di responsabilità, accessibilità.
4. Progettazione del sistema di monitoraggio delle macchine:
   - la macchina deve sempre essere in grado di comunicare con l'esterno per fornire i propri parametri di funzionamento, ma deve rimanere protetta dalla possibilità di essere riconfigurata. La comunicazione deve essere solo un trasferimento di dati dalla macchina ad un altro sistema, non viceversa.
   - il trasferimento di dati ottimale è realizzato con la macchina che trasmette non con la macchina che viene "letta" da qualcuno.
   - Il trasferimento dati avviene dalla macchina al sistema esterno ed è controllato dalla macchina.

Sicurezza dei sistemi complessi ed interconnessi

- Aspetti importanti per la progettazione del sistema cyberfisico, in ottica I4.0 e sicurezza:
  - Fotografia dello stato attuale della fabbrica;
  - Mappatura dei processi e del flusso di informazioni (prestazioni del processo attuale, criticità del processo, individuazione delle opportunità di miglioramento);
  - Individuazione delle specifiche di progetto in ottica I40, mettendo al primo posto come indice di miglioramento la sicurezza del lavoratore.
  - Formazione degli attori che utilizzeranno (anche i manutentori per intenderci) il sistema cyberfisico in termini di sicurezza a 360° includendo quindi gli aspetti della sicurezza informatica.

Breve introduzione: IEC 62443-4-2

- È lo strumento per la Cybersecurity ma in realtà garantisce la safety del sistema interconnesso grazie alla confidenzialità disponibilità ed integrità dei dati che vengono utilizzati nello stesso.
- Ha come obiettivo quello di regolare la conformità tecnica agli standard di sicurezza informatica dei singoli endpoint quali PLC, sensori, attuatori, ecc.
- Nella norma 4 livelli di sicurezza di complessità crescente:
  - Security Level 1 (SL1): protezione contro la violazione casuale o occasionale;
  - Security Level 2 (SL2): protezione contro la violazione intenzionale con mezzi scarsi, con risorse scarse, competenze generiche del sistema e motivazione scarsa.
  - Security Level 3 (SL3) Protezione contro la violazione intenzionale con mezzi sofisticati, con risorse moderate, competenze specifiche del sistema e motivazione moderata.
  - Security Level 4 (SL4) Protezione contro la violazione intenzionale con mezzi sofisticati con risorse ingenti, competenze specifiche del sistema e forte motivazione.

✓ Appare evidente il parallelo con le IEC 61508/61511 e i livelli SIL (Safety Integrity Level) di integrità della Sicurezza.

IEC 62443-4-2

- I requisiti di sicurezza per ogni installazione variano a seconda della criticità dell'impianto e adempiono agli eventuali requisiti cogenti di legge.
- La componente Internet of Things (IoT) dei sistemi industriali sta espandendosi in modo decisamente marcato; a questo si affianca una affermazione del paradigma "Industry 4.0". Conseguenza sulla **cyber security** delle installazioni → **la superficie di attacco degli impianti industriali sta aumentando sensibilmente**.
- Quindi diventa vitale proteggere le singole apparecchiature da manipolazioni di terzi malevoli senza però compromettere le funzionalità proprie dei devices e degli impianti.

IEC 62443-4-2

- Fornisce una serie di indicazioni (già note da decenni nell'informatica), che stanno prendendo piede nella progettazione dell'esercizio di impianti industriali:
  - Importanza dei log;
  - Tenere traccia degli eventi di sicurezza;
  - Integrità del messaggio;
  - Validazione delle sessioni di comunicazione;
  - Sistemi di protezione perimetrale (VPN).

Conclusioni

- Come spesso accade le innovazioni corrono di più di quanto si riesca ad inseguirle, ed anche nell'ambito Transizione 4.0 prima si è pensato agli obiettivi di sviluppo economico e all'impatto per il benessere e solo dopo, alle eventuali conseguenze per i lavoratori.
- È compito dei legislatori fare in modo che I40 sia rivolto alla sostenibilità non solo in ambito energetico, e, di chi lavora nell'ambito della sicurezza, sostenere l'importanza del fattore umano (salute, capacità, invecchiamento, ecc.) di chi avrà a che fare in prima persona con la fabbrica digitalizzata.

GRAZIE per l'attenzione

Ing. Luigi Zerella
luigi.zerella@certitudo.it

Membro Sotto-Commissione Sicurezza Igiene del Lavoro e Cantieri
Ordine Ingegneri della Provincia di Milano
Ispettore e consulente Direttiva Macchine
Presente nell'elenco degli esperti industria 4.0 - OIM

ORDINE DEGLI INGEGNERI
DELLA PROVINCIA DI MILANO

9 Settembre 2021 | ore 14.00 - 15.00