DATA INTEGRITY, SAFETY E SECURITY NELL'INDUSTRIA

Tavola rotonda

COME MANTENERE UN IMPIANTO IN ESERCIZIO, MITIGARE GLI INCIDENTI E GARANTIRE LA CONFORMITÀ A NORMATIVE E REGOLAMENTI? CHE AIUTO PUÒ ARRIVARE ALLA DIFESA DIGITALE DALL'INTELLIGENZA ARTIFICIALE?

Micaela Caserza Magro, Ilaria De Poli

Foto Shutterstock

Le tre dimensioni della sicurezza industriale, data integrity, safety e cybersecurity, sono fondamentali per mantenere in esercizio un impianto, evitare incidenti e garantire conformità normativa

Negli ultimi anni, l'industria manifatturiera e di processo è al centro di una trasformazione senza precedenti, guidata dalla convergenza tra tecnologie OT e IT, dalla crescente digitalizzazione dei processi e dalla progressiva automazione spinta da algoritmi di intelligenza artificiale (AI). In parallelo, l'aumento delle minacce informatiche e la necessità di garantire continuità operativa, sicurezza funzionale e affidabilità dei dati stanno imponendo nuovi standard di gestione del rischio e della conformità.

Il panorama normativo europeo e internazionale si sta rapidamente evolvendo per affrontare queste sfide. Nello specifico, la Direttiva NIS2 (Direttiva UE 2022/2555) ha ampliato gli obblighi di cybersecurity per gli operatori di servizi essenziali e introdotto requisiti vincolanti su analisi del rischio, resilienza operativa, gestione degli incidenti, supply chain e governance; il Cyber Resilience Act (CRA), attualmente in fase di finalizzazione, stabilirà obblighi specifici per la cybersecurity dei prodotti con elementi digitali, impattando fortemente sui dispositivi industriali smart e i sistemi embedded; il Regolamento UE 2021/155 per la cybersecurity dei veicoli, anche a due ruote, vincola l'omologazione alla dimostrazione di una gestione efficace della sicurezza informatica durante l'intero ciclo di vita del prodotto. Inoltre, standard internazionali come ISO/IEC 27001:2022 e la serie IEC 62443 sono ormai imprescindibili per una gestione sistematica della sicurezza delle informazioni e della cybersecurity OT, soprattutto in ambienti regolati o a rischio elevato. A questo si aggiungono GMP Annex 11 e FDA 21 CFR Part 11, fondamentali nei settori farmaceutico e alimentare per la data integrity, che richiedono che i dati digitali siano completi, accurati, protetti da alterazioni e auditabili, e i regolamenti ambientali e di processo, come Seveso III, che richiedono che safety e risk assessment tengano conto anche delle minacce derivanti da incidenti digitali.

In questo contesto, l'integrità del dato (data integrity), la sicurezza operativa (safety) e la protezione dei sistemi digitali (security) diventano tre dimensioni interconnesse e fondamentali per mantenere in esercizio l'impianto, evitare incidenti e garantire conformità normativa.

Il ruolo dell'AI

Parallelamente, l'intelligenza artificiale sta assumendo un ruolo crescente nella gestione industriale: dal rilevamento delle anomalie nei sistemi Scada e DCS, alla manutenzione predittiva, fino al supporto nelle decisioni critiche in caso di deviazioni operative o potenziali attacchi cyber. Tuttavia, anche il dominio dell'AI è oggi soggetto a regolamentazioni emergenti. Il Regolamento sull'Intelligenza Artificiale (AI Act), in fase di adozione finale da parte dell'UE, definisce un quadro normativo basato sul rischio per lo sviluppo, la validazione e l'impiego di sistemi AI. I sistemi utilizzati in ambito industriale o critico, per esempio per il controllo di infrastrutture o impianti, possono ricadere nelle categorie ad alto rischio, soggette a requisiti obbligatori di trasparenza, sicurezza, affidabilità e tracciabilità.

Le Linee Guida dell'Enisa e i contributi del Nist propongono approcci per la cybersecurity dei sistemi AI evidenziando i nuovi vettori di attacco introdotti dall'impiego di algoritmi, come data poisoning, adversarial attack, model inversion. Infine, le nuove versioni dei framework di sicurezza, come Nist CSF 2.0, includono ormai esplicitamente il tema della gestione del rischio associato all'AI.

In questo quadro complesso e sfidante, questa tavola rotonda si propone di affrontare tre grandi domande: come mantenere l'impianto in esercizio continuo e sicuro? Come mitigare gli incidenti e proteggere l'integrità dei dati? Come può l'AI contribuire, senza introdurre nuovi rischi, a sostenere la resilienza digitale industriale?

Percorsi sicuri per i dati

In che modo l'integrità del dato può essere garantita in ambienti OT ibridi, dove coesistono sistemi legacy e nuove soluzioni digitali? Quali sono gli approcci più efficaci per mantenere la tracciabilità e la validazione del dato lungo tutta la catena operativa e decisionale?

Chiara Rovetta, Regional communication specialist di **Omron** (*https://omron.it/it/home*): "In ambienti OT ibridi, dove coesistono sistemi legacy e nuove soluzioni digitali, garantire l'integrità del dato è una sfida complessa ma cruciale per assicurare continuità operativa, tracciabilità e conformità normativa. La chiave sta nell'integrare automazione, controllo dei processi e qualità dei dati lungo tutta la catena produttiva e decisionale.

Per esempio, in Omron proponiamo un approccio a tre livelli, qualità del prodotto, del packaging e dei dati, in cui l'integrità viene salvaguardata in ogni fase del ciclo produttivo, dalla stampa preliminare all'aggregazione finale. Questo modello prevede la stampa e la validazione puntuale dei dati

prima del confezionamento, una corretta applicazione e leggibilità, tracciabile durante il packaging, e l'aggregazione e la conservazione dell'informazione post confezionamento. L'adozione di questi standard consente di estendere la qualità fino agli stadi più a valle, contribuendo alla sostenibilità e alla riduzione degli sprechi. Un elemento strategico fondamentale è la digitalizzazione dei processi ancora gestiti manualmente. Le operazioni basate su carta espongono l'impianto a errori, perdite di dati, difficoltà di auditing e rischio di non conformità. L'automazione, invece, consente di gestire in modo centralizzato le informazioni degli operatori, registrare e sincronizzare automaticamente le modifiche ai parametri di sistema e proteggere i dati tramite back-up regolari e crittografia. Questo approccio riduce la dipendenza dall'input umano, elimina il rischio di manomissioni e migliora la capacità di risposta ai requisiti normativi.

Chiara Rovetta, Regional communication specialist di Omron

Infine, la tracciabilità e la validazione del dato lungo l'intera filiera possono essere assicurate attraverso sistemi digitali interconnessi, capaci di aggregare e storicizzare le informazioni in modo coerente e accessibile. In questo modo, ogni decisione, sia essa operativa o strategica, si fonda su dati affidabili, verificabili e prontamente consultabili. Integrare sistemi legacy con tecnologie avanzate fa sì che la qualità dei dati diventi un asset competitivo, oltre che un requisito essenziale per l'efficienza e la resilienza dell'industria manifatturiera moderna".

Andrea Faeti, sales director Enterprise Accounts di **Vertiv Italia** (*www.vertiv.com*): "Per migliorare i processi produttivi, le imprese del settore manifatturiero puntano sempre più sugli investimenti in automazione, come la robotica, il machine learning e le applicazioni di AI. Servirà concentrarsi poi sulla semplificazione della gestione della supply chain per poter operare in modo efficiente, gestire meglio le scorte e ridurre i costi operativi. La digitalizzazione della supply chain avviene attraverso l'uso di Rfid, BI e strumenti per ottimizzare logistica, inventario e approvvigionamento. Di certo, non c'è più spazio per i tempi di inattività in un impianto di produzione, poiché questi comportano perdite finanziarie e possono compromettere gli impegni contrattuali.

Andrea Faeti, sales director Enterprise Accounts di Vertiv Italia

Vertiv è in grado sia di supporta l'implementazione di nuove infrastrutture, sia l'ammodernamento di impianti esistenti con soluzioni efficienti, adatte a garantire ridondanza e resilienza, e certificabili secondo gli standard di settore".

Chris Grove, director Cybersecurity Strategy di **Nozomi Networks** (*www.nozominetworks.com*): "Negli ambienti OT ibridi, l'integrità dei dati è cruciale. Dati di processo e letture dei sensori sono immediatamente rilevanti e la loro accuratezza è vitale per il funzionamento continuo. Garantire l'integrità significa assicurare che questi dati ad alta velocità si muovano solo tra dispositivi autorizzati e siano sempre precisi.

Un approccio efficace per la tracciabilità e la validazione dei dati include un inventario completo degli asset OT, IT e IoT, un monitoraggio costante della rete e un'analisi comportamentale in tempo reale. Queste tecniche, automatizzabili con AI e machine learning, proteggono sia i sistemi legacy, sia le nuove soluzioni digitali".

Chris Grove, director Cybersecurity Strategy di Nozomi Networks

Matteo Ripamonti, sales engineer di **Trend Micro** (*www.trendmicro.com*): "In un ecosistema industriale sempre più eterogeneo, in cui sistemi legacy, tecnologie proprietarie, dispositivi edge e piattaforme di orchestrazione coesistono, la fiducia nel dato diventa un requisito imprescindibile. Non basta più proteggerlo solo durante il transito: ogni fase del suo ciclo di vita, dalla sensoristica alla componente decisionale, deve essere monitorata e sicura.

Il primo passo è proteggere ciò che non può essere aggiornato: PLC, Scada, HMI. Soluzioni come TXOne EdgeIPS permettono di segmentare logicamente questi asset, ispezionare il traffico e bloccare anomalie in tempo reale, senza impattare la produzione. In parallelo, l'analisi passiva dei protocolli OT offre visibilità completa senza introdurre rischi o interruzioni. Il controllo delle modifiche è altrettanto cruciale per garantire l'integrità del sistema: rilevare alterazioni non autorizzate su configurazioni, firmware e dati operativi è fondamentale. In questo contesto, TXOne StellarProtect protegge gli end-point OT anche in ambienti air-gapped, grazie a tecniche non invasive di application control e protezione runtime. Non va sottovalutato il rischio legato a reti isolate e operatori esterni. Monitorare queste interazioni, identificare vulnerabilità e analizzare lo stato di salute degli asset è cruciale per eseguire audit efficaci su dispositivi non gestiti e controllare l'introduzione di file tramite storage sicuro. TXOne Portable Inspector consente tutto questo senza installare agent o modificare l'ambiente: una soluzione ideale per scenari critici.

Matteo Ripamonti, sales engineer di Trend Micro

Infine, la visibilità centralizzata offerta da Trend Vision One consente di aggregare eventi, tracciare modifiche e costruire una vista unificata tra ambienti OT e IT. È il principio della trustworthy pipeline: ogni anello della catena deve essere verificabile, per garantire sicurezza e continuità operativa".

Fabrizio Corti, sales specialist Industrial Automation di **Softing Italia** (*www.softingitalia.it*): "L'integrità del dato in ambienti OT ibridi, caratterizzati dalla coesistenza di sistemi legacy e nuove soluzioni digitali, rappresenta una sfida cruciale, infatti la garanzia dell'integrità non si limita alla mera accuratezza del dato, ma include anche la sua tracciabilità, validazione e protezione lungo l'intera catena operativa e decisionale. Diventa dunque importante utilizzare soluzioni che supportano e gestiscono sistemi sia digitali che legacy. La soluzione dataFeed OPC Suite di Softing, con la sua

Fabrizio Corti, sales specialist Industrial Automation di Softing Italia

capacità di convertire dati da OPC Classic a OPC UA, gioca un ruolo fondamentale nell'armonizzazione dei dati provenienti dai sistemi legacy. Anche i dispositivi APL Switch, FG200 e smartLink sono essenziali per integrare i sistemi di campo più datati, Profibus PA, Hart, FF, PA in ambienti basati su OPC UA. Queste soluzioni non solo consentono la connettività, ma offrono anche l'opportunità di 'iniettare' maggiore sicurezza e integrità nel flusso di dati. La garanzia dell'integrità dei dati in un ambiente OT ibrido si basa su un approccio che sfrutta le capacità dei nuovi sistemi (come la sicurezza intrinseca di OPC UA), mitiga le limitazioni dei sistemi legacy attraverso una conversione intelligente, e implementa pratiche di governance e monitoraggio robuste lungo l'intera infrastruttura".

Filippo Petrolese, key account manager e referente Digital Transformation, e **Fabio Sarti**, sales engineer e referente Digital Transformation, di **Axis Communications** (*www.axis.com/it-it*): "Negli ambienti OT ibridi garantire l'integrità del dato rappresenta una delle sfide più complesse, che Axis affronta attraverso un mix di tecnologie innovative, standard di sicurezza consolidati e una filosofia progettuale orientata alla trasparenza e alla resilienza.

Filippo Petrolese, key account manager e referente Digital Transformation di Axis Communications

Un primo elemento chiave è Axis Signed Video, una tecnologia proprietaria che consente di firmare digitalmente ogni singolo frame generato da una telecamera. Quando abilitata in una telecamera, la funzione video firmato permette di autenticare il video e rilevare eventuali manomissioni. In secondo luogo, per garantire la sicurezza del trasporto dei dati, Axis utilizza protocolli crittografici standard e collaudati come Https (basato su TLS) e Mqtt con supporto TLS, garantendo la protezione dei dati anche in ambienti industriali complessi.

Dal nostro punto di vista, l'integrità del dato non è solo un requisito tecnico, ma anche culturale. Axis promuove attivamente la formazione degli operatori, mostrando come il dato video possa supportare la sicurezza e l'efficienza: si pensi a impianti in cui gli operatori modificano i comportamenti rischiosi in seguito a segnalazioni ripetute generate proprio da alert video, che si attivano al verificarsi di una data azione a rischio, contribuendo alla creazione di una cultura più consapevole e sicura".

Fabio Sarti, sales engineer e referente Digital Transformation di Axis Communications

Paolo Cecchi, sales director Mediterranean Region di **SentinelOne** (*https://it.sentinelone.com*): "Ogni giorno, i team di sicurezza ricevono in media oltre 1.000 avvisi che richiedono approfondimenti, pur considerando che, negli anni, gli attacchi informatici alle infrastrutture critiche (reti elettriche, impianti petroliferi e del gas, trasporti, telco e servizi sanitari) sono cresciuti sensibilmente. Un aumento principalmente dovuto alla maggiore interconnessione e interoperabilità tra le tecnologie operative e quelle informatiche.

Una delle principali lacune degli strumenti OT è che non dispongono di funzionalità di sicurezza informatica, in quanto i device sono progettati per svolgere compiti specifici senza l'interazione diretta dell'uomo. Anche l'adozione della tecnologia 5G offre l'opportunità di una connettività più veloce e affidabile, estendendone ulteriormente le capacità e le vulnerabilità.

Paolo Cecchi, sales director Mediterranean Region di SentinelOne

La sicurezza informatica non può più limitarsi alla difesa, ma deve poter anticipare e bloccare le minacce prima ancora che queste si verifichino. Il futuro è una sicurezza proattiva e autonoma, che si evolve alla stessa velocità del contesto delle minacce. Sfruttando l'AI e l'apprendimento automatico, le soluzioni di cybersecurity possono anticipare e identificare i comportamenti dannosi prima che questi causino danni. Nello settore industriale, le imprese dovrebbero esaminare tutte le vulnerabilità dei sistemi OT e analizzare le molteplici minacce informatiche, con le rispettive probabilità e conseguenze. Un piano di gestione del rischio strutturato contribuirà a dare priorità alle misure di sicurezza e ad allocare le risorse in modo oculato. A seguire, l'approccio di 'network segmentation', che consiste nel dividere la rete OT in segmenti più piccoli e isolati, aiuterà a contenere il malware e le altre minacce. Serve poi un controllo rigoroso degli accessi ai sistemi OT (tutti gli accessi devono essere periodicamente aggiornati), così come sono indispensabili continue attività di monitoraggio e rilevamento, unitamente all'implementazione di un Incident Response Plan, e alla sensibilizzazione dei dipendenti sui processi necessari a garantire la sicurezza dei sistemi OT".

Mario Testino, managing director di ServiTecno

Mario Testino, managing director di **ServiTecno** (*www.servitecno.it*): "Ci sono un paio di caratteristiche che permettono di migliorare l'approccio per la gestione dell'integrità del dato: l'autenticazione (authentication) e il non-ripudio (non repudiation). L'autenticazione è la capacità di dimostrare che un utente o un'applicazione sia veramente ciò che dichiara di essere. Più l'autenticazione è 'forte', per esempio mediante il riconoscimento multi-fat-

tore, migliori sono le garanzie di sicurezza per il trattamento del dato. A completamento di questa capacità è estremamente importante l'assegnazione dei diritti e delle autorizzazioni che ogni utente ha per accedere a risorse e funzionalità specifiche dei sistemi.
Il non-ripudio si riferisce alla garanzia che il titolare di credenziali di accesso a determinati dati non possa negare in modo convincente di averli modificati. Questa caratteristica è associata alla tracciabilità delle operazioni effettuate sul dato: maggiori e più dettagliate sono tali informazioni memorizzate, più difficilmente confutabili sono le evidenze associate alle operazioni sul dato".
Alberto Ascolti, product manager ctrlX Automation di **Bosch Rexroth** (*www.boschrexroth.it*): "Negli ultimi anni si è cercato di creare piattaforme IoT che unissero le funzioni aziendali alle funzioni macchine. Sappiamo bene che ciò comporta un rischio perché rendere visibile, trasparente, un dato significa 'giocoforza' aprire una connessione verso l'esterno. Conseguentemente, vediamo il futuro segnato da piattaforme progettate già sulla base di requisiti di sicurezza avanzati (Secure by Design, ovvero concepite all'origine prevedendo in primis policy di accesso, gestione delle password, gestione degli utenti e tracciamento della loro attività) e tali da essere resilienti, fornendo risposte efficaci a possibili attacchi informatici.

Alberto Ascolti, product manager ctrlX Automation di Bosch Rexroth

In quest'ottica, la chiave di volta per Bosch Rexroth si chiama ctrlX Automation, una piattaforma per l'automazione industriale già concepita sulla base dei requisiti previsti dalla IEC62443, norma che contempla una serie di standard internazionali che trattano la cybersecurity per i sistemi di controllo industriale (ICS) e l'automazione industriale. Delle app permettono di governare con efficacia l'accesso da remoto; attraverso una VPN vengono creati dei tunnel sicuri, crittografati, con cui è possibile accedere al sistema e chiudere la comunicazione quando la sessione è finita. E ancora: dei firewall permettono di inserire nel dispositivo edge delle policy che fanno in modo di stabilire con chi comunicare, con quale protocollo e attraverso quale porta, bloccando di default tutto quello che è altro. Per concludere, la app 'Security Scanner' consente di inventariare i componenti all'interno di una macchina, scansionandone la rete alla ricerca di dispositivi; si possono anche scansionare i componenti alla ricerca di porte aperte".
Christoph Behler, business development manager di **CIpa Europe** (CC-Link Partner Association - *cc-link.org*):"Nelle architetture OT eterogenee, in cui coesistono sistemi legacy e soluzioni moderne, garantire l'integrità dei dati rappresenta una sfida centrale. Mentre le tecnologie attuali integrano nativamente approcci Security by Design, i sistemi obsoleti richiedono misure di hardening mirate, come l'impiego di switch Industrial Ethernet con funzionalità di Deep Packet Inspection, segmentazione Vlan e controllo degli accessi basato sulle porte, per proteggere la comunicazione di rete.

Christoph Behler, business development manager di CIpa (CC-Link Partner Association) Europe

Un approccio particolarmente efficace per garantire la tracciabilità e la validazione dei dati lungo l'intera catena operativa e decisionale è l'utilizzo di protocolli di comunicazione aperti e realtime, come CC-Link IE TSN, che consente la convergenza di diversi flussi di dati, dai segnali di motion e safety, fino agli I/O classici e alla comunicazione IP, su un'unica infrastruttura di rete. Grazie alla compatibilità con lo standard Ethernet è possibile integrare sia i sistemi moderni che quelli esistenti. La piattaforma OT risultante può connettersi in modo trasparente a sistemi IT, applicazioni edge o cloud di fabbrica, rendendo i dati disponibili per reportistica, manutenzione predittiva o analisi basate su AI. Il risultato: un'architettura semplificata, che non solo rafforza l'integrità dei dati, ma migliora anche trasparenza e tracciabilità su tutti i livelli produttivi e decisionali. Un passo fondamentale verso una produzione resiliente e a prova di futuro".
Denis Cassinerio, senior director & general manager South Emea di **Acronis** (*www.acronis.com*): "Garantire l'integrità del dato in am-

Denis Cassinerio, senior director & general manager South Emea di Acronis

LEGGI LA RISPOSTA ALLE ALTRE DOMANDE

- Safety e cybersecurity vengono ancora gestite troppo spesso come domini separati. Quali sono le esperienze o i framework più efficaci per un'integrazione sinergica tra funzioni di sicurezza funzionale e sicurezza informatica negli impianti industriali?
- Considerando gli obblighi normativi, come NIS2, ISO/IEC27001, IEC62443, regolamenti di settore ecc., quali strategie adottate per mantenere un impianto in esercizio continuo senza compromettere la compliance e la resilienza? È possibile coniugare efficacemente 'uptime' e 'compliance'?
- L'intelligenza artificiale può essere un game-changer nella protezione dei sistemi industriali, oppure rischia di introdurre nuove vulnerabilità? Quali sono gli ambiti in cui oggi l'AI offre reale valore aggiunto nella difesa digitale OT?
- Quanto è importante il fattore umano nell'equilibrio tra automazione intelligente, sicurezza operativa e risposta agli incidenti? Quali competenze sono oggi più critiche per i team OT e quali cambiamenti formativi servono per preparare le figure chiave alla gestione integrata di safety, security e AI?

Leggi online l'articolo integrale

bienti OT ibridi richiede una visione unificata e multilivello della protezione. In contesti dove convivono sistemi legacy e nuove tecnologie digitali è fondamentale adottare soluzioni capaci di interagire con entrambi gli ambienti, senza compromettere la continuità operativa".

Pasquale Lambardi, presidente e CEO di **Relatech** (*https://relatech.com*): "L'integrità del dato in ambienti OT ibridi, dove convivono sistemi legacy e nuove tecnologie digitali, rappresenta una sfida complessa ma imprescindibile. In Relatech, attraverso **EFA Automazione** (*www.efa.it*), società Relatech con oltre trent'anni di esperienza nel mondo della connettività e della smart industry 5.0, affrontiamo questa complessità abilitando una convergenza sicura tra IT e OT, adottando una logica di Secure by Design. Questo significa progettare architetture in grado di garantire tracciabilità end-to-end, con soluzioni che integrano sensori, PLC, sistemi Scada e piattaforme di edge computing. Le architetture proposte adottano protocolli nativamente industriali standardizzati e interoperabili, come OPC UA, per assicurare che ogni scambio informativo avvenga con garanzie di autenticità e integrità, anche nei contesti legacy, ma sono anche aperte oltre i confini dello stabilimento grazie a framework come lo Sparkplug B. L'obiettivo è abilitare una supply chain digitale trasparente, dove la fiducia nel dato rappresenta il fondamento dell'efficienza e della resilienza operativa".

Pasquale Lambardi, presidente e CEO di Relatech

Alberto Griffini, product manager Modular PLC di **Mitsubishi Electric** (*www.mitsubishielectric.com/fa/index.html*): "La presenza simultanea di sistemi legacy e nuove soluzioni digitali rappresenta oggi la normalità negli impianti industriali. Se le nuove soluzioni digitali integrano già contromisure molto efficaci per garantire l'integrità del dato, per quanto riguarda i sistemi legacy è invece necessario investire in aggiornamenti per rendere la soluzione più sicura, per esempio tramite l'introduzione di switch con funzioni integrate di sicurezza informatica. Un approccio che si rivela molto utile per mantenere la tracciabilità e la validazione del dato lungo tutta la catena operativa e decisionale è l'utilizzo di protocolli come CC-Link IE TSN. Essendo compatibile con tutto ciò che può girare su Ethernet, CC-Link IE TSN offre il vantaggio della convergenza delle reti, consentendo di unificare su una singola infrastruttura di comunicazione quello che tradizionalmente veniva gestito attraverso reti separate, semplificando significativamente le architetture e introducendo funzionalità avanzate per la tracciabilità dei dati lungo tutta la catena operativa".

Alberto Griffini, product manager Modular PLC di Mitsubishi Electric

Marco Marella, general manager di **FasThink** (*www.fasthink.com*): "Assicurare l'integrità del dato in ambienti OT ibridi, in cui coesistono sistemi legacy e nuove soluzioni digitali, è una challenge che può senz'altro entrare a progetto, e che si risolve con metodologie anche differenti, ugualmente efficaci. Innanzitutto, è importante l'integrazione tra i diversi sistemi IT e le tecnologie OT, in modo che i due mondi comunichino in modo sicuro e affidabile. Il modo più agevole che conosciamo e applichiamo correntemente è l'adozione di una piattaforma digitale, un orchestrator dotato di AI, che non si limiti a fare solo da bridge, ma che orchestri le diverse risorse disponibili e si occupi della raccolta, formattazione e gestione dei dati, e ne assicuri l'indispensabile coerenza e conformità lungo l'intera catena produttiva/operativa.

Marco Marella, general manager di FasThink

Per tenere sotto controllo la tracciabilità e la validazione del dato è consigliabile adottare una strategia di audit trail, in modo da registrare costantemente ogni modifica o accesso ai dati, istituendo un registro completo e immutabile.

Altro punto fondamentale è il controllo qualità e validazione dei dati nei punti chiave del processo, in modo da poter disporre delle informazioni corrette e utili per poter prendere decisioni sempre più mirate e organizzate, al riparo il più possibile da errori di valutazione preventiva. L'automazione e la digitalizzazione di questi controlli, tramite moderni sistemi di monitoraggio e alert, aiuta a individuare tempestivamente anomalie o incoerenze.

Infine, la formazione del personale, sempre più digitalizzato ai diversi livelli nei rispettivi ambiti operativi, e l'applicazione di procedure standard sono essenziali per mantenere alta l'attenzione sulla qualità delle performance e sull'integrità dei dati, soprattutto in ambienti complessi e ibridi".

Umberto Cattaneo, Eura Cybersecurity business consultant lead di **Schneider Electric** (*www.se.com*): "Sebbene possa sembrare un tema di secondo piano, in certi contesti industriali con ambienti severi, i problemi di integrità possono derivare più dalle condizioni operative ambientali, che dalle infrastrutture IT. È quindi necessaria una solida protezione fisica dei mezzi di trasporto dei dati, che si può ottenere adottando soluzioni come, per esempio, sistemi di comunicazione schermati da radiazioni elettromagnetiche. È importante anche selezionare tecnologie di rilevamento delle intrusioni di tipo industriale, in grado di controllare protocolli e dati in circolo sulla rete, che si andranno ad affiancare ai sistemi anti-malware. Per avere la più ampia capacità di gestione di ogni evento di sicurezza si può adottare a livello di impianto un sistema Siem (Security Information Event Management), che vada a integrare tutto questo e consenta di verificare gli eventi che possono portare a rischi, segnalare problematiche, distinguere tra falsi allarmi e situazioni da esaminare.

Umberto Cattaneo, Eura Cybersecurity business consultant lead di Schneider Electric