Pilz GmbH & Co. KG
Felix-Wankel-Strasse 2
73760 Ostfildern
Deutschland/Germania
www.pilz.com

Protezione per aziende, macchine e prodotti

Safety e Industrial Security – Tutto in uno e da un unico fornitore

Ostfildern, ottobre 2025 - **Gli incidenti di security non coinvolgono più solo i sistemi informatici (IT) ma sempre più spesso anche l’ambiente di produzione (OT). In ambito Industrial Security gli incidenti non sono solo gli attacchi mirati ma anche manomissioni e manipolazioni involontarie. Il compito dell’Industrial Security nella produzione è garantire la disponibilità di macchine e impianti, così come l’integrità e la riservatezza di dati e processi meccanici. Tuttavia, l'obiettivo di protezione massimo è la sicurezza funzionale. Perché, in definitiva, vale il principio secondo cui se le aziende non hanno controllo totale sui propri dati, sono in gioco l’azienda stessa e la sicurezza del suo personale: non c'è safety senza security e senza la prima viene a mancare anche la protezione delle persone.**

All'interno dell'UE si è preso atto di una crescita costante degli scenari di minaccia e, conseguentemente, si è adattata la legislazione in materia: a livello aziendale, la **direttiva NIS 2** richiede l’implementazione di misure volte a garantire un livello elevato comune di cybersicurezza all’interno dell’Unione, ad esempio attraverso una sistema di gestione della sicurezza delle informazioni (ISMS).

Il **Regolamento Macchine (UE) 2023/1230** prevede ora la protezione contro l’alterazione di macchine e impianti e obbliga a misure di Industrial Security per le parti della macchina che hanno effetti sulla sicurezza funzionale.

Il **Cyber Resilience Act (CRA)** prevede misure di security per i prodotti con elementi digitali. Tra questi rientrano anche i sistemi di controllo, i sistemi IO e altri componenti installati nelle macchine.

Aziende, macchine e prodotti – A ogni livello, i fabbricanti e gli operatori di macchine devono affrontare sfide diverse e attenersi a quadri giuridici differenti.

Sicurezza allo stato dell’arte

Indipendentemente dall’obbligo di implementare l’Industrial Security imposto dalla legislazione, esiste una serie di buoni motivi per cui occuparsi con tempestività dell'argomento e richiedere una consulenza in tempi brevi. I processi collaudati e le condizioni consolidate legati al funzionamento delle macchine possono favorire manipolazioni e manomissioni se non vengono periodicamente analizzati. Una vita utile lunga delle macchine, ad esempio, si ripercuote sui relativi sistemi che spesso cominciano a mostrare i segni del tempo e, prima o poi, a non soddisfare più gli standard di security attuali. Questi sistemi presentano gap nella sicurezza che non possono più essere colmati in quanto il loro provider non fornisce più gli aggiornamenti per la security. Analogamente, spesso risulta impossibile implementare sui dispositivi finali anche la protezione da malware: talvolta sono obsoleti con ripercussioni sulle prestazioni che possono sfociare in perdite di produzione.

Introduzione graduale di una maggiore Industrial Security

In ultima istanza, si tratta di mantenere al sicuro e protette le operazioni aziendali; tuttavia, per raggiungere questo obiettivo, le aziende devono superare sfide diverse che spaziano dall'identificazione delle disposizioni di legge vigenti, dall’individuazione ed eliminazione delle vulnerabilità nei sistemi,

passando per la sensibilizzazione e la formazione del personale fino a includere la successiva implementazione di controlli. La security è un “moving target”, ovvero un “bersaglio mobile”: ciò implica la necessità di controllare regolarmente lo stato dell’Industrial Security delle macchine. È quindi importante che, in azienda, le responsabilità siano chiare e occorre disporre di una procedura sistematica che preveda la creazione strutturata delle competenze necessarie.

Pilz, azienda leader in automazione, si è preparata per soddisfare queste esigenze realizzando un portfolio di servizi, di livello internazionale, su misura per fabbricanti di macchine e utenti con un approccio olistico rispetto a ogni aspetto inerente alla protezione di uomo e macchina. Gli esperti Pilz conoscono i requisiti legali e normativi più recenti e sono in grado di integrarli nel proprio servizio di consulenza. L’offerta è completata dai corsi di formazione con l’obiettivo di strutturare o aggiornare le conoscenze e le competenze in materia di security nelle aziende. L'implementazione pratica avviene anche con l’ausilio delle soluzioni di prodotto Pilz, come ad esempio la gamma per Identification and Access Management (IAM) per un plus in materia di Safety e Industrial Security.

Porre le basi giuste

Per garantire l’Industrial Security sulle proprie macchine, i professionisti che operano nella costruzione di macchine e impianti necessitano di conoscenze di base approfondite, in particolare riguardo alla legislazione e alle norme vigenti. Nel corso “Fondamenti di Industrial Security”; gli esperti Pilz condividono questo know-how e queste competenze. I partecipanti apprendono le minacce che la security deve affrontare, le misure di protezione idonee da implementare e le best practice da adottare nell’ambito della sicurezza di macchine e reti. In questo modo, anche i partecipanti ai

corsi di livello propedeutico sul tema Security potranno apprendere con quali misure proteggere efficacemente le macchine da attacchi informatici e manipolazioni o manomissioni a livello di produzione automatizzata.

Con la qualifica “CESA - Certified Expert for Security in Automation”, Pilz offre un corso di specializzazione avanzato (durata: 2 giorni) che eroga ai partecipanti conoscenze approfondite in materia di security e in linea con la situazione normativa più recente, in particolare per quanto riguarda la serie di norme IEC 62443 (“Industrial communication networks - Network and system security”). Altri contenuti del corso sono le misure pratiche per la riduzione del rischio, come il controllo degli accessi, l’incremento della sicurezza della rete con mezzi tecnici e anche le misure organizzative per la riduzione dei rischi in materia di Security. I partecipanti apprenderanno come applicare correttamente la norma e ad attestare che i propri sistemi di automazione soddisfano i requisiti in materia di cybersicurezza. Una volta superato l'esame, i partecipanti riceveranno l'attestato rilasciato da TÜV-NORD e riconosciuto a livello internazionale di “CESA - Certified Expert for Security in Automation”.

Mettere in pratica le conoscenze teoriche

Partendo dalle basi teoriche e dai corsi di formazione, il passo successivo per rafforzare l’Industrial Security è l'applicazione di processi strutturati e orientati alla pratica. La consulenza in ambito Operational Technology (OT) o tecnologia operativa consente di portare a compimento il passaggio dalle basi teoriche alle strategie realizzabili. Utilizzando un approccio graduale, i servizi di Industrial Security identificano le vulnerabilità dei sistemi complessi e

sviluppano misure per ridurre al minimo i rischi. Il risultato è un concept di sicurezza olistico.

Quattro fasi per una maggiore Industrial Security

Le fasi del processo di OT Security sono 4: analisi dei requisiti di protezione, valutazione del rischio di Industrial Security, concept di Industrial Security e verifica del sistema di Industrial Security.

Durante l'analisi dei requisiti di protezione, l'azienda determina le esigenze di protezione dei singoli "asset" della macchina o dell’impianto e i relativi obiettivi di protezione. Nella seconda fase, ossia la valutazione del rischio, vengono considerati tutti i rischi e la loro probabilità di accadimento, per ogni sottoarea per l’intero ciclo di vita del sistema. La fase successiva prevede la creazione di un concept dettagliato di Industrial Security con strategie e misure mirate alla difesa e riduzione di rischi generati da attacchi, manipolazioni, manomissioni e operazioni errate. Vengono inoltre create policy, disposizioni e linee guida per l’ulteriore realizzazione o funzionamento sicuri del sistema. Nell’ultima fase, la verifica del sistema di Industrial Security, viene controllata l’efficacia delle contromisure implementate.

Garantire la disponibilità delle macchine

Il processo dei servizi di Industrial Security supporta nella mitigazione o nella prevenzione dei cyberattacchi. Si riduce anche il numero di incidenti alla sicurezza innescati involontariamente. A sua volta, ciò incrementa la disponibilità delle macchine e, in ultima istanza, consente di risparmiare in termini di costi e mantenere una redditività efficiente.

Questa procedura protegge soprattutto il personale addetto alla macchina con misure di security adeguate. Un incidente di security

può infatti trasformarsi in un ostacolo alle misure di safety. Una barriera fotoelettrica, ad esempio, davanti a una macchina si occupa di evitare che l'operatore entri in una zona pericolosa. Se tuttavia un hacker riesce a introdursi nel relativo sistema di controllo e nel meccanismo, è possibile che la funzione di protezione della barriera fotoelettrica non sia più garantita. La Security protegge la Safety!

Per la concreta implementazione nella macchina è quindi altamente opportuno un approccio comune di safety e security. Perché non c'è safety senza security e senza safety non c'è protezione per l'essere umano.

Regolamentazione chiara: chi può fare cosa sulla macchina?

La sicurezza di una macchina e dei suoi operatori dipende dalla regolamentazione degli accessi, sia che si tratti di persone o di reti. Gli accessi devono essere protetti da interventi non autorizzati: durante il funzionamento della macchina, ad esempio, le persone non possono sostare all'interno della zona pericolosa. Infatti, anche un funzionamento, un service o una manutenzione effettuati con buona intenzione a un impianto, sia in loco che tramite rete, potrebbero avere conseguenze disastrose.

Una componente fondamentale è l'implementazione di un sistema di Identification and Access Management (IAM) che disciplini con chiarezza nelle aziende le autorizzazioni e gli accessi a macchine e impianti. Rientrano in tale ambito misure e disposizioni di tipo organizzativo e anche funzioni di sicurezza adeguate. Un sistema di autorizzazione all'accesso come PITreader di Pilz rappresenta quindi il modulo prodotto adatto. In questo modo, gli utenti sono in grado di far fronte alle sfide poste in materia di tutela della salute e incolumità del personale, responsabilità civile, produttività ai massimi livelli e protezione dei dati.

Solo un approccio olistico a safety e security garantisce una protezione completa per l'uomo e la macchina. Se occuparsi di security e a quale livello occuparsene non è più qualcosa lasciato alla discrezionalità di un’azienda. Nel frattempo questo aspetto è diventato disposizione di legge. Nella costruzione delle macchine, la security intesa come Industrial Security, non è demandata unicamente all’IT ma anche parte integrante del concept e della costruzione. L’implementazione a posteriori della security è onerosa in termini di tempi e costi e implica spesso sacrificare semplicità d’uso per l’utente, funzionalità e produttività.

((Caratteri: 9.784))

((Box:))

La legislazione UE sul tema Industrial Security: una panoramica

In Europa in particolare, il legislatore risponde al panorama delle minacce con una serie di leggi. È per questa ragione che l’Europa vanta le disposizioni più severe in materia al mondo. Sono comunque in corso armonizzazioni con altri Paesi e anche lì arriveranno leggi simili. Si può quindi prospettare un’armonizzazione di portata mondiale per quanto concerne l’Industrial Security.

NIS 2: più obblighi per le aziende

La NIS (Network and Information Security, la Direttiva sulla Sicurezza delle Reti e dei Sistemi Informativi) è una direttiva dell’Unione Europea tesa a rafforzare la sicurezza informatica. Si tratta di una direttiva già in vigore dal 2016 che interessava, finora, i player attivi in infrastrutture critiche, tra cui i settori energia, trasporti, banche e

finanza, sanitario, approvvigionamento e distribuzione di acqua potabile e anche infrastrutture digitali. I fornitori di questi settori erano tenuti, con particolare riferimento alla security, ad adottare “idonee disposizioni e misure di sicurezza” e a notificare incidenti ed eventi gravi in materia di sicurezza informatica. La nuova direttiva NIS 2 ((UE) 2022/2555 ... sulle misure per un livello elevato comune di cybersicurezza in tutta l'Unione) imporrà in futuro a un numero significativamente maggiore di aziende di adottare misure di gestione del rischio in materia di sicurezza informatica. NIS 2 estende, ad esempio, i settori coinvolti aggiungendo l’industria manifatturiera/produttiva, tra cui anche l’automotive e i produttori di apparecchiature elettriche.

Le analisi dei rischi e i concept di sicurezza sono richiesti per i sistemi informatici, la protezione della supply chain e la sicurezza del personale. A tutto questo si aggiungono approcci mirati al controllo degli interventi e alla gestione degli impianti come pure corsi di formazione obbligatori per il management.

La direttiva è stata approvata dal Parlamento e dal Consiglio dell’Unione a fine 2022. Come tutte le direttive UE, anche NIS 2 non entra in vigore subito e in modo vincolante nei singoli Stati membri UE ma deve essere prima recepita come legge nazionale dai singoli Stati membri. Le aziende sono invitate a prendere quanto prima in considerazione NIS 2 e a svolgere un’analisi esaustiva della propria security. In questa analisi rientra, ad esempio, la realizzazione di un sistema di gestione della sicurezza delle informazioni (ISMS - Information Security Management System). Al riguardo può rivelarsi utile una certificazione secondo la norma ISO 27001 sulla sicurezza delle informazioni.

Esempio di applicazione di NIS 2 per turbine eoliche: con l'avvento di NIS 2, anche i fabbricanti di macchine, come del resto chi si occupi di realizzare impianti per la produzione di energia elettrica (ad es. impianti eolici), dovranno soddisfare i requisiti della nuova normativa. Il fabbricante di impianti eolici necessita a sua volta di soluzioni di automazione, sistemi di controllo o sensori. A partire da una determinata dimensione, anche i fabbricanti di componenti elettrici sono soggetti alla NIS 2. NIS 2, inoltre, prescrive la massima attenzione verso i fornitori: un'azienda come Pilz deve dunque occuparsi anche dell'implementazione di una supply chain sicura e stabilire requisiti specifici per i propri fornitori. NIS 2 copre tutti gli aspetti della supply chain.

Il nuovo Regolamento Macchine: nessuna marcatura CE senza security

Nel quadro della sicurezza funzionale delle macchine, la Direttiva Macchine 2006/42/CE riveste un'importanza fondamentale:

per potere introdurre macchine sul mercato europeo, i fabbricanti di macchine sono da sempre tenuti a eseguire una corrispondente procedura di valutazione della conformità al termine della quale si ottiene la Marcatura CE.

Nel giugno 2023, con la nuova denominazione di Regolamento Macchine, è stato pubblicato il documento con le disposizioni allo stato dell'arte della tecnica e tecnologia. Trattandosi di un regolamento non è necessaria la conversione preliminare in legge nazionale. I fabbricanti di macchine avranno tempo fino al 20 gennaio 2027 per adeguarsi ai nuovi requisiti e recepirli entro la scadenza.

Il Regolamento Macchine sostituisce la Direttiva Macchine in vigore, rendendo obbligatoria la cyber security a differenza di quanto stabiliva la normativa precedente. Mentre la Direttiva Macchine si occupava esclusivamente di safety, il Regolamento ha recepito al suo interno l'obiettivo di protezione Security nella sezione "Protezione dall'alterazione" dei "Requisiti essenziali di sicurezza e di tutela della salute": le funzioni di sicurezza della macchina non devono essere compromesse da un'alterazione accidentale o intenzionale.

Questo nuovo percorso verso la marcatura CE solleva tutta una serie di nuovi quesiti e domande per fabbricanti e operatori di macchine: dovranno infatti rivedere e rielaborare i concept di sicurezza finora in uso per safety e security.

Cyber Resilience Act: security per l'intero ciclo di vita del prodotto

Oltre a considerare l'approccio dell'azienda e delle macchine, è imprescindibile implementare anche le misure di security direttamente nei dispositivi (come ad esempio nei sistemi di controllo). Nel settembre 2022, la Commissione Europea ha presentato la bozza di un regolamento il cui obiettivo è l'innalzamento del livello di sicurezza informatica dei prodotti. Il Cyber Resilience Act (CRA) si rivolge ai fabbricanti di prodotti con elementi digitali (hardware e software) che sono in grado di comunicare con altri prodotti. Coinvolti sono i prodotti dell'area B2C, come gli smartphone e i robot aspirapolvere, ma anche dell'area B2B, come i sistemi di controllo e i sensori, oltre ai prodotti software come i sistemi operativi o la macchina stessa.

Gli obblighi di segnalazione delle vulnerabilità attivamente sfruttate per i fabbricanti entreranno in vigore già dall'11 settembre 2026.

Dall’11 dicembre 2027 i prodotti con elementi digitali dovranno soddisfare i requisiti del CRA per poter essere immessi sul mercato nell’Unione Europea. Il CRA è un regolamento dell'UE e potrà quindi essere applicato direttamente negli Stati membri.

Quale sarà di fatto l’entità degli effetti del CRA dipende dai criteri che saranno in ultima istanza stabiliti per la classificazione dei prodotti. Secondo il CRA dovranno essere commercializzati solo i prodotti in grado di assicurare un livello di sicurezza informatica adeguato, più precisamente per l’intero ciclo di vita del prodotto. La security inizia dunque con lo sviluppo del prodotto. Da qualche anno Pilz conforma quindi i propri processi di sviluppo anche alla norma IEC 62443-4-1 “Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements“ e ha sviluppato ad esempio SecurityBridge comprovatamente “secure”.

((Caratteri: 6.062))

Pilz – The spirit of safety

Pilz è fornitore globale di prodotti, sistemi e servizi per la tecnologia di automazione. Azienda “pionieristica” nel settore dell’automazione sicura, Pilz crea sicurezza per l'uomo, le macchine e l'ambiente. Fondata nel 1948 e con sede principale a Ostfildern, vicino a Stoccarda in Germania, Pilz è oggi una realtà diffusa in modo capillare in tutto il mondo grazie a 42 filiali e rappresentanze commerciali ed oltre 2.500 dipendenti.

È leader in ambito tecnologico con soluzioni di automazione olistiche che garantiscono safety e industrial security sulle macchine e che comprendono sensori, sistemi di controllo e azionamento, oltre a sistemi per la comunicazione industriale, la diagnostica e la visualizzazione. L’offerta è integrata da un portafoglio di servizi di livello internazionale che include consulenza, engineering e corsi di formazione. Le soluzioni Pilz trovano applicazione non solo nella costruzione di macchine e impianti ma in numerosi altri settori, come quello dell’intralogistica, dell’imballaggio e packaging e della tecnologia ferroviaria o della robotica.

www.pilz.com

Pilz sui social network:

Sui canali social media Pilz sono disponibili informazioni di carattere generale sull'azienda e le persone; forniscono inoltre informazioni aggiornate su tecnica e tecnologia dell'automazione.

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Contatti per la stampa:

Martin Kurth

Stampa specializzata e aziendale
Tel: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

Stampa specializzata e aziendale
Tel: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

Stampa specializzata

Tel: +49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Rössle

Stampa specializzata

Tel: +49 711 3409-7147
e.roessle@pilz.de