25.05.2023

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Germania
http://www.pilz.com

Premi Messaggio

Thomas Pilz: Safety e Security per l’automazione digitale

Ostfildern, 25.05.2023 - **(In caso di discrepanze, fa fede il discorso effettivamente pronunciato)**

Thomas Pilz

Security: una sfida “giuridica” per il settore industriale e della costruzione delle macchine

Per quanto riguarda norme e leggi sulla sicurezza in ambiente industriale è in atto una rivoluzione, determinata e trainata da temi quali Security e Intelligenza Artificiale (IA). Per l’industria in generale e per il settore della costruzione di macchine e impianti sono rilevanti, per la Security, tre nuove e/o imminenti disposizioni di legge: la direttiva UE NIS 2, il nuovo Regolamento Macchine e il Cyber Resilience Act.

Come durante la scorsa conferenza stampa annuale, la mia analisi sarà incentrata sul tema della security e oggi intendo illustrarvi come e quanto vasti saranno effetti e conseguenze per l’intero settore industriale.

NIS 2: più obblighi e sanzioni per un numero maggiore di aziende

La NIS (Network and Information Security) 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 direttiva è stata sostituita dalla NIS 2, entrata in vigore a inizio 2023, che dovrà essere recepita e convertita in normativa nazionale dai singoli Stati membri dell'UE entro l'autunno del 2024. Questa normativa si applica ora anche ai settori della costruzione di macchine e Automotive e, nello specifico, coinvolge le imprese con oltre 50 dipendenti o con un fatturato annuo superiore ai 10 milioni di Euro. Secondo stime del VDMA (Verband Deutscher Maschinen- und Anlagenbau e.V.), questo provvedimento dovrebbe interessare circa 9.000 aziende in tutta Europa. In futuro, le imprese dovranno dimostrare di essere in grado di adottare misure di carattere tecnico, operativo e organizzativo per proteggersi da incidenti di sicurezza. In queste misure rientra, in prima istanza, l'analisi del rischio di sistemi esistenti anche negli ambienti di produzione, quindi l'OT (Operations Technology). Successivamente, sono da prendere in considerazione la definizione e l'implementazione di misure e processi specifici, quali la protezione delle password o la codifica, ma anche la formazione continua e il training del personale. Gli incidenti alla sicurezza informatica devono essere comunicati alle autorità competenti entro 24 ore dal loro verificarsi. Una novità è anche l'inclusione esplicita delle supply chain. Riassumendo, la NIS 2 interessa ora un numero maggiore di imprese, espandendone gli obblighi e prevedendo sanzioni più severe. Alle aziende che non adotteranno le misure previste, saranno inflitte sanzioni importanti.

Cyber Resilience Act – Security per l’intero ciclo di vista del prodotto

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 si rivolge ai fabbricanti di prodotti con elementi digitali. Sono contemplati sia hardware che software (come ad esempio i firmware). Il regolamento fa riferimento a prodotti consumer ma anche a quelli per le applicazioni industriali, come i sistemi di controllo delle macchine. Secondo quanto stabilito dal Cyber Resilience Act dovranno essere commercializzati solo i prodotti in grado di assicurare un livello di sicurezza informatica adeguato. I fabbricanti saranno inoltre tenuti a informare il più tempestivamente possibile i clienti di eventuali gap di sicurezza e quindi a colmarli. Il regolamento si occupa anche dell’intero ciclo di vita di un prodotto. Ciò implica che i produttori dovranno ora offrire gli update di un software oltre il periodo di garanzia solitamente previsto, anche per evitare rischi e attacchi in futuro. Ci aspettiamo che il regolamento sarà varato a fine 2024.

Il nuovo Regolamento Macchine – La sicurezza informatica come dovere

La terza, nuova prescrizione di legge sulla security è il Regolamento Macchine della UE. La pubblicazione è imminente. Trattandosi di un regolamento non è necessaria la conversione preliminare in legge nazionale. I costruttori di macchine hanno 42 mesi di tempo per ottemperare ai nuovi requisiti. Il Regolamento Macchine sostituisce la Direttiva Macchine in vigore, rendendo obbligatoria la cyber security a differenza di quanto stabiliva la normativa precedente. Se la Direttiva Macchine era una semplice riflessione sulla safety, nel Regolamento l’obiettivo di protezione Security è stato recepito alla voce “Protection against corruption” all’interno della sezione “Essential health and safety requirements EHSR”: le funzioni di sicurezza della macchina non devono essere pregiudicate da un’alterazione involontaria o intenzionale. Allo stato attuale è noto che, ottemperando alle prescrizioni del Cyber Resilience Act, si consegue la presunzione di conformità per il Regolamento Macchine.

E adesso: chi si occupa di cosa?
Qual è l'importanza e il senso delle prescrizioni di legge? Mi baserò sul settore della produzione di energia elettrica per illustrare implicazioni e correlazioni:
Finora, solo il fornitore di energia elettrica era tenuto a rispettare la Direttiva NIS. Con l'avvento di NIS 2, anche i costruttori di macchine, come del resto quelli di 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, ad esempio di Pilz. 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 e quindi un'azienda come Pilz deve 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.

Per potere introdurre macchine sul mercato europeo, i costruttori di macchine sono da sempre tenuti a eseguire una procedura di valutazione della conformità al termine della quale si ottiene la Marcatura CE.
Ora, con il nuovo Regolamento Macchine, i costruttori di macchine devono dimostrare che le loro macchine sono protette anche da manipolazioni e manomissioni. Il produttore di componenti elettrici è poi soggetto alla future prescrizioni del previsto Cyber Resilience Act.

In breve: se occuparsi di security e a quale livello occuparsene non è più qualcosa lasciato alla discrezionalità di un'azienda. È un requisito di legge! Le aziende farebbero meglio a prendere quanto prima in considerazione NIS 2 e a svolgere un'analisi olistica 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) con certificazione secondo la norma per la sicurezza delle informazioni ISO 27001.

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 sempre onerosa in termini di tempi e costi e implica spesso sacrificare semplicità d'uso per l'utente, funzionalità e produttività. In fase di valutazione del rischio, oltre alla safety entra ora in gioco anche la security. Niente marcatura CE senza security!

E per i costruttori di prodotti con elementi digitali è possibile orientarsi in modo ottimale con la serie di norme IEC 62443. La norma IEC 62443-4-1 subordinata illustra ad esempio i requisiti del cosiddetto processo di "Security Development Lifecycle" (processo SDL - Ciclo di vita di sviluppo della sicurezza).

L'Unione Europea ha giocato d'anticipo per quanto riguarda la legislazione sulla security e in Europa entreranno in vigore le prescrizioni più stringenti e severe al mondo. Sono comunque in corso armonizzazioni con altri Paesi e anche lì arriveranno leggi simili. Allo stato attuale, ad esempio, l'Australia sta interagendo con l'UE e si ispirerà probabilmente alle normative europee. Si può quindi prospettare un'armonizzazione di portata mondiale per quanto concerne l'Industrial Security.

Thomas Pilz

Standard di comunicazione aperti sono un must. Da sempre

Per Pilz, apertura e orientamento all'utente sono caratteristiche essenziali e distintive della sua gamma di prodotti. Il nostro impegno è quindi orientato a offrire ai clienti prodotti costantemente all'avanguardia della tecnica e della tecnologia, semplici da utilizzare e integrabili in qualsiasi architettura di automazione.

Con SafetyBUS p, il primo sistema fieldbus sicuro, e con l'Ethernet real-time SafetyNET p di sicurezza, abbiamo plasmato lo sviluppo della comunicazione industriale sicura. E tuttavia, il tempo delle soluzioni proprietarie è ormai definitivamente trascorso. Ci stiamo impegnando con tutte le nostre forze per creare standard industriali: significa rendere un servizio di portata storica!

OPC UA

Per la connessione in rete sicura e cross-vendor degli impianti industriali, il settore si è accordato per l’impiego dello standard OPC UA (Open Platform Communications Unified Architecture). Questo protocollo di comunicazione offre un'interfaccia standard (IEC 62541) per la comunicazione tra diverse sorgenti dati in ambito industriale. Pilz è membro di OPC Foundation: i suoi dipendenti partecipano attivamente sia allo Steering Committee o Comitato di Coordinamento, sia ai gruppi di lavoro tecnici del Gruppo Field Level Communication (FLC). L'attenzione di Pilz si rivolge in modo particolare al gruppo di lavoro che si occupa del tema Safety (Safety over OPC UA).

Particolarmente utile e apprezzato è il know-how di Pilz in materia di impiego della tecnologia Publisher/Subscriber (Pub/Sub) in combinazione ai requisiti dei protocolli fieldbus sicuri dal punto di vista funzionale: contrariamente alla classica architettura master/slave, nel caso dei dati Pub/Sub è possibile passare direttamente tra nodi. Ciò consente di implementare OPC UA anche per task di automazione distribuiti con requisiti impegnativi. Pilz dispone di una specifica competenza in questo campo: SafetyNET p è l'unico sistema fieldbus sicuro che si basa su Ethernet e che fin dall'inizio ha supportato Pub/Sub.

Stiamo procedendo bene anche per quanto riguarda il lavoro sulle tematiche inerenti la sicurezza funzionale. In stretta collaborazione con le autorità di controllo competenti, il Gruppo sta sviluppando specifiche e sistemi di test nonché la certificazione di stack di comunicazione per OPC UA Safety. La versione 1.05 è già stata rilasciata.

IO-Link Safety

Per quel che concerne i sensori, l’automazione è decisamente un passo avanti in tema di protocolli aperti. Nello specifico, è imminente la disponibilità in commercio del protocollo di comunicazione IO-Link Safety. La comunicazione punto-punto offre numerosi vantaggi: la semplicità di installazione (ad es. tramite cablaggio standard e l'omissione di cablaggi in parallelo), una parametrizzazione automatizzata e supportata da tool come pure opzioni di diagnostica ampliate.

Per potere utilizzare IO-Link anche per task di automazione rilevanti in tema sicurezza, Pilz ha collaborato intensamente, con la community IO-Link, alla sua estensione con test, certificazioni e omologazioni corrispondenti. Gli esperti Pilz sono a capo dei due gruppi di lavoro IO-Link Safety (per marketing e tecnica).

I primi sensori, pronti per essere immessi sul mercato, saranno presentati a novembre, in occasione di SPS. La strategia di Pilz è offrire un sistema completo, che includa quindi sensori e attuatori più moduli master, semplificando così l'applicazione per i clienti e incrementando la performance.

Siamo certi che, in futuro, le soluzioni di automazione si differenzieranno sempre più facendo leva sulle loro funzionalità: le interfacce utente sono valide per la mia attività? Il funzionamento è semplice? Quale valore aggiunto offrono? È qui che risiede la notevole forza innovativa e si rivela l'enorme potenziale per le nuove applicazioni.

Thomas Pilz

Il futuro della sicurezza è dinamico

Cosa implica l'ulteriore digitalizzazione per la protezione di persone e macchine? Quali tecnologie tengono testa ai requisiti di sicurezza? Qual è il ruolo dell'essere umano? Oggi vogliamo rivolgere il nostro sguardo anche al futuro. Prima la buona notizia: la persona è al centro della nostra attenzione. Il suo ruolo è addirittura rafforzato.

L'essere umano è protagonista attivo

Ad esempio nel progetto "Produzione fluida" di Arena 2036. Pilz sta collaborando con alcuni partner allo sviluppo e all'implementazione di un concept di produzione cyber-fisico e incentrato sulla persona, in particolare per il settore Automotive. L'idea alla base di questo progetto è 'scomporre' gli impianti produttivi in moduli a installazione flessibile per potere realizzare unità dinamiche e, a seconda delle esigenze, smontarle nuovamente. I moduli sono concepiti con particolare attenzione al ruolo della persona che è protagonista attiva del suo ambiente di produzione.

È proprio in considerazione di queste esigenze che aumenta la richiesta di sicurezza dinamica, ovvero di un adeguamento flessibile delle funzioni di sicurezza ai processi produttivi in continuo cambiamento e, di conseguenza, ai nuovi requisiti di protezione, grazie ai quali non è più necessario, ad esempio, arrestare immediatamente i robot o le piattaforme mobili se una persona si muove nella stessa zona di lavoro, ma possono continuare a funzionare a velocità ridotta (e quindi meno pericolosa) e gestire strategie alternative ancora più sicure. Attuatori e sensori intelligenti dei sistemi distribuiti rileveranno sempre più le funzioni dei sistemi di comando e controllo e porteranno ad una migliore interazione tra i moduli stessi della macchina oppure tra uomo e macchina.

Safety in real-time

Le situazioni dinamiche che si prospettano per gli ambienti di produzione devono essere testate per la sicurezza in tempo reale e omologate affinché la protezione di essere umano e macchina sia costantemente garantita. Qui, la parola chiave è “Safety in real-time”. Si può ipotizzare che molteplici macchine, o più in generale asset, condividano in futuro i dispositivi di sicurezza. Si tratta della cosiddetta “Shared Safety” che sperimentiamo nella SmartFactory KL. Una marcatura CE standard, quale esito di un’analoga procedura di valutazione della conformità, è da escludere da una concezione di sicurezza di questo tipo. Le informazioni su tutti gli asset coinvolti devono essere effettivamente disponibili per il run-time; le parole chiave sono qui Targhetta digitale e Administration Shell.

Nel già citato progetto “Produzione fluida”, stiamo lavorando ad altri temi del futuro come l’identificazione (e quindi la distinzione/differenziazione) di persone e oggetti. In questo caso, è opportuno l’uso dell’intelligenza artificiale. I rischi possono quindi essere riconosciuti e valutati dagli algoritmi di apprendimento dell’IA. La marcatura CE “analogica” è la protezione di base. Sarà tuttavia possibile introdurre ulteriori misure di riduzione del rischio che rendano la sicurezza ancora più flessibile contribuendo all’incremento della produttività.

Didascalia:

Immagini e testi sono disponibili, anche per il download, sul sito di Pilz all’indirizzo www.pilz.com. Per consultare direttamente le relative pagine Internet nella sezione Ufficio Stampa, inserire il seguente Web code nel campo Ricerca della Home page Pilz.: **237512**

Il gruppo Pilz

Il gruppo Pilz è fornitore completo di prodotti, sistemi e servizi per l’automazione. Questa azienda familiare con sede principale a Ostfildern conta ca. 2.500 dipendenti. Con 42 filiali e rappresentanze commerciali in tutto il mondo Pilz sviluppa soluzioni per tutelare persone, macchine e ambiente. Questo leader tecnologico offre soluzioni di automazione complete che includono sensori, sistemi di controllo e azionamenti così come i sistemi integrati per la visualizzazione, la diagnostica e la comunicazione industriale. L’ampia offerta è completata da servizi internazionali quali consulenza, engineering e corsi di formazione. Le soluzioni Pilz trovano applicazione nella costruzione di macchine e impianti e in numerosi altri settori, come quello del trasporto ferroviario, della robotica e dell’energia eolica.

www.pilz.com

Pilz sui social network

Sui canali dei social media forniamo informazioni generali sull'azienda, sui collaboratori Pilz e sui continui sviluppi nelle tecnologie di automazione.

https://www.facebook.com/pilzINT

https://twitter.com/Pilz_INT

https://www.youtube.com/user/PilzINT

https://www.xing.com/companies/pilzgmbh%26co.kg

https://www.linkedin.com/company/pilz

Contatto per la stampa

Martin Kurth
Stampa settoriale e specializzata
+49 711 3409 - 158
publicrelations@pilz.com

Sabine Skaletz-Karrer
Stampa specializzata
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de