

Informazioni generali

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

Gli approcci alla sicurezza di tipo olistico mettono al centro l'accesso con l'obiettivo di garantire safety e industrial security per la macchina

Pagina 1 di 13

Sicurezza globale grazie alla gestione delle autorizzazioni personalizzata

Ostfildern, Febbraio 2023 – **Ovunque ci sia qualcosa di prezioso da proteggere, mettiamo porte, lucchetti e usiamo chiavi per impedire l'accesso. Lo stesso cosa accade per un altro bene per noi importantissimo: la nostra sicurezza, in ogni forma ed espressione. In ambiente industriale ciò implica, da un lato, proteggere le persone (Safety) e, dall'altro, la macchina e i dati sensibili (Industrial Security). Un gap nella sicurezza può avere svariate conseguenze: funzionamento errato, incidenti, infortuni o un attacco informatico di gravissimo impatto. Un sistema di Identity and Access Management globale, che disciplini in modo chiaro e puntuale le autorizzazioni di accesso e intervento, contribuisce alla realizzazione di un approccio olistico alla sicurezza oltre allo svolgimento di procedure e processi efficienti.**

Nell'ambiente della produzione sono ormai un'immagine consueta: i ripari mobili che indicano chiaramente al personale che dietro quella porta si trova una zona sensibile che richiede di prestare massima attenzione. Mediante un sistema Human Machine Interface (HMI) oppure una chiave, le persone hanno accesso al processo che si svolge oltre il riparo. Ma cosa accade quando una persona non è qualificata, o meglio, non è autorizzata e mette in pericolo se stessa o gli altri? Anche una persona con cattive intenzioni può manipolare/manomettere un processo, direttamente sulla macchina o da accesso remoto. Considerando più da vicino il tema dell'autorizzazione all'accesso, si scopre che i concetti di safety e industrial security si intersecano continuamente e sono strettamente legati tra loro. E ancora: l'industrial security garantisce l'integrità della safety sulla macchina. La "security" riguarda, ad esempio, la protezione di macchine o impianti da accessi non autorizzati dall'esterno, ma anche la protezione di

dati sensibili di processi e macchine da contraffazione, perdita e accesso illecito a livello interno. Ciò include sia attacchi espliciti, sia incidenti involontari alla security.

Safety e Industrial Security sono una cosa sola

Per gli operatori di macchine e impianti è necessario distribuire e attribuire in modo chiaro e preciso, task, attività e autorizzazioni, quindi creare un sistema di Identity and Access Management. Ciò implica la realizzazione di misure organizzative, come stabilire procedure operative o svolgere controlli periodici dei processi, ma anche l'integrazione, nell'ambiente di produzione, di opportune soluzioni di sicurezza. In mancanza di misure di questo tipo, le persone che in azienda si occupano di sicurezza possono essere ritenute personalmente responsabili per perdite di produzione e perseguibili in caso incidenti o infortuni. Fino a oggi, questa tipologia di soluzione di security era qualcosa di facoltativo, in molte situazioni non era assolutamente considerata come una necessità. Nel frattempo, il legislatore ha realizzato che safety e security sono concetti che si intersecano e strettamente legati tra loro. Il nuovo regolamento macchine prevede pertanto l'obbligo di misure di security.

Le modalità operative incrementano la sicurezza

Svariate norme di tipo C prevedono già che a ogni modalità operativa debba corrispondere un'idonea funzione di sicurezza. Come, ad esempio, il funzionamento automatico, interventi manuali limitatamente a certe condizioni o gli interventi di assistenza. La norma EN ISO 16090-1 prescrive che i centri di lavorazione e le macchine speciali dispongano obbligatoriamente di almeno due di queste modalità operative al fine di garantire la sicurezza funzionale. È quindi importante che sia selezionata e attiva sempre

e solo una modalità operativa e che quest'ultima sia visibile in modo chiaro.

Evitare accessi anonimi

Altrettanto importante: come si decide chi deve accedere o intervenire in una determinata procedura o quali persone sono addirittura autorizzate a modificare la procedura stessa? A tale scopo si definiscono gruppi differenti di persone che entrano in contatto con la macchina, come ad esempio il personale addetto al funzionamento, alla pulizia o alla manutenzione. In un secondo momento, le persone vengono assegnate ai gruppi in base alla loro mansione o qualifica. A seconda delle dimensioni dell'azienda, i diritti di accesso o di intervento di un tipo di macchina, utilizzata a livello di intero gruppo aziendale, potranno ad esempio essere assegnati a gruppi di utenti differenti. Nell'ambito di una valutazione del rischio, gli esperti in sicurezza stimano, per ogni pericolo, il rischio derivante da un accesso anonimo e lo analizzano. Ne risultano infine misure allo stato dell'arte della tecnica che vengono specificate tenendo conto delle norme armonizzate, che riducono il rischio.

La semplicità d'uso previene manipolazioni e manomissioni

In fase di implementazione delle misure è importante che all'utente siano assicurate maneggevolezza e usabilità durante il processo allo scopo di escludere manipolazioni e manomissioni. Per i costruttori di macchine, questi aspetti sono già fondamentali a partire dal processo di sviluppo. Sistemi di comando e controllo intuitivi che gli utenti possono gestire con semplicità impediscono di aggirare le misure di sicurezza e di azionare le macchine in modo errato. Inoltre, un sistema di sicurezza ottimamente concepito e sviluppato è fondamentale per processi efficienti senza inutili fermi macchina. Proprio il tema relativo a come utilizzare e maneggiare i ripari mobili è un punto centrale della norma EN ISO 14119 che definisce le linee guida per la configurazione e la scelta di sistemi

per ripari mobili, fornendo in questo modo un'assistenza concreta su come sia possibile ovviare a manipolazioni e manomissioni.

Approccio alla sicurezza personalizzato

Per evitare qualsiasi rischio correlato all'apertura involontaria o non autorizzata, sulle porte di accesso viene installato un sistema di sicurezza per ripari mobili. Dal punto di vista della safety è centrale la protezione dell'operatore da movimenti pericolosi della macchina. A seconda se si tratti di una macchina stand-alone o anche di impianti concatenati complessi, è richiesto allo scopo un approccio alla sicurezza su misura. Se le macchine hanno un movimento per inerzia pericoloso, il sistema di interblocco svolge un ruolo importantissimo: quando i ripari sono accessibili, lo sblocco di fuga diventa imprescindibile.

Messa in sicurezza su misura per i ripari mobili

Un sistema a struttura modulare, come PSEnMlock di Pilz, unisce il controllo sicuro dei ripari mobili e un interblocco di sicurezza in un unico sistema e dispone inoltre di funzioni di sicurezza, quali arresto di emergenza, sblocco di fuga e un blocco di riavvio meccanico. Offre flessibilità e un'intelligenza decentralizzata per proteggere in modo sicuro molteplici applicazioni. Una soluzione personalizzata è composta dalla combinazione di sensori, sblocco di fuga, maniglie e da un'unità pulsanti e un pannello operatore. In base all'applicazione, gli utenti impostano la propria soluzione per ripari mobili. Per soddisfare i requisiti di Industrial Security, si analizzeranno ora gli accessi e le autorizzazioni.

Un sistema per Safety e Industrial Security

La protezione da accesso non autorizzato può essere realizzata, in pratica, con un sistema di selezione della modalità operativa e di

autorizzazione all'accesso. Nel sistema sono riunite insieme safety e industrial security: la selezione della modalità operativa e la gestione dell'autorizzazione all'accesso della macchina. Una soluzione di questo tipo può essere realizzata con i dispositivi della gamma di prodotti PITmode di Pilz che consentono la commutazione tra modalità operative definite e la regolamentazione dell'autorizzazione all'accesso. La gestione è intuitiva: l'utente riceve un proprio transponder con codifica personalizzata che permette l'autenticazione univoca dello user ed evita manipolazioni/manomissioni.

Gestione personalizzata di accessi e modalità operative

Per realizzare un approccio alla sicurezza su misura sono disponibili svariate versioni di PITmode. Come dispositivo compatto "all-in-one", PITmode include i pulsanti per la scelta della modalità operativa e anche un'unità di valutazione che permette di risparmiare spazio in fase di installazione. PITmode fusion è un sistema a struttura modulare, composto dall'unità di lettura PITreader con tecnologia RFID e server web integrato oltre a un'unità di valutazione sicura nota come Safe Evaluation Unit (SEU). Un'ulteriore versione è PITmode flex: in questo caso, PITreader viene installato con un sistema di controllo Pilz e un modulo software per la valutazione di sicurezza. Grazie alla struttura modulare, è possibile integrare l'autorizzazione all'accesso e la selezione della modalità operativa nel design di pannelli di comando esistenti. È quindi possibile utilizzare i pulsanti già presenti per la scelta della modalità operativa, con conseguente maggiore facilità d'uso per l'utente. L'identificazione con il transponder avviene attraverso l'unità di lettura PITreader. PITmode e PITmode fusion offrono una scelta della modalità operativa e

un'autorizzazione all'accesso sicure dal punto di vista funzionale fino a PL d.

Autenticazione semplice, anche da remoto

Per selezionare la modalità operativa, l'utente inserisce il proprio transponder direttamente in PITmode e aziona un pulsante specifico per la modalità operativa oppure l'interfaccia corrispondente di un HMI. Se esiste l'autorizzazione, l'utente ottiene l'accesso al processo. La medesima procedura funziona anche qualora un addetto al service intendesse accedere alla macchina per una manutenzione da remoto: solo se una persona in loco attiva la relativa abilitazione nel sistema, è possibile iniziare con l'intervento di manutenzione da remoto. Una volta completate le attività di service, l'accesso viene nuovamente chiuso prima di far ripartire la macchina. In questo modo si possono escludere manipolazioni/manomissioni da parte di persone non autorizzate o di una porta che dovesse rimanere inavvertitamente aperta. In questo modo si incrementa il livello di Industrial Security perché gli operatori controllano e gestiscono le singole autorizzazioni e quindi l'accesso a un determinato processo.

Soluzione completa di Access Management

Nel caso fosse necessaria la sola regolamentazione degli accessi, PITreader può essere installato anche in versione stand-alone o in combinazione con un sistema di controllo Pilz come sistema di autorizzazione all'accesso. Insieme al modulo compatto di sicurezza configurabile PNOZmulti 2, l'amministratore può configurare le autorizzazioni di accesso per macchine e impianti con un semplice "drag and drop" grazie all'applicativo software PNOZmulti Configurator integrato. Le autorizzazioni vengono quindi trasmesse alle chiavi a transponder RFID attraverso l'unità di lettura PITreader.

Grazie all'integrazione dello standard OPC UA, la versione PITreader S può essere installata indipendentemente dall'uso di un sistema di controllo Pilz. Come già ricordato, i dispositivi PITmode sono facilmente integrabili in pannelli di comando esistenti.

La scelta tra key, card e sticker

Una flessibilità ancora maggiore per operatori e utenti è offerta dalla versione PITreader card unit: le card e gli sticker con RFID possono essere utilizzati insieme o al posto di una chiave a transponder RFID. Qualora in azienda si utilizzino già schede RFID, è possibile impiegarle in combinazione con le PITreader card unit: l'utente necessita in questo caso di una sola card per più funzioni.

Fondamentalmente, il vantaggio dei transponder RFID, siano essi key, card o sticker, è questo: più funzioni vengono raggruppate in un transponder e quindi è possibile riunire insieme un intero mazzo di chiavi meccaniche. Per gli utenti si tratta di una soluzione comoda e semplice perché hanno l'esigenza di avere con sé solo un dispositivo di identificazione. Gli amministratori invece risparmiano tempo e fatica nella gestione e nell'aggiornamento delle chiavi.

Un valore aggiunto in security

Anche gli aspetti legati alla security sono presi in considerazione, con riferimento all'autenticazione degli utenti, alla qualifica e alla protezione di accesso. Nel caso in cui, nonostante tutte le misure di sicurezza, si verificasse un incidente o un evento legato alla "security" della macchina, mediante lettura del transponder RFID è possibile risalire alla modifica effettuata e al suo autore. Si tratta di una funzione opzionale che, se richiesta, consente al sistema di controllo di rilevare, grazie all'autenticazione, data e ora di accesso in un audit trail (registro degli eventi) interno e non modificabile.

La chiave di tutto è un'amministrazione precisa e puntuale

Per potere garantire Safety e Industrial Security lungo l'intero ciclo di vita dell'applicazione, gli amministratori aggiornano con precisione e con la massima cura le autorizzazioni. I tool software Pilz supportano l'organizzazione di utenti e transponder semplificando così la configurazione dell'amministrazione. In una piccola chiave RFID si possono nascondere matrici di autorizzazione complesse o specifiche stabilite per un intero gruppo aziendale. Grazie al server web integrato PITreader, gli amministratori programmano i transponder per PITmode o di PITreader memorizzandovi i dati utente e le autorizzazioni. Tutte le impostazioni importanti vengono eseguite direttamente sull'unità di lettura, accelerando così la messa in servizio, configurazione delle interfacce inclusa.

Delimitazione dell'accesso alle interfacce

Le possibilità offerte da Identity and Access Management includono anche l'abilitazione per porte USB speciali per l'industria, notoriamente una delle "porte di ingresso principali" in eventi legati alla security. A tale scopo, il sistema di autorizzazione all'accesso PITreader viene combinato con un elemento di comando come PIT o USB che dispone di un'interfaccia Host USB 2.0 attivabile. Questa soluzione consente di installare programmi a prova di manomissione o manipolazione, richiamare dati e anche collegare una tastiera o un mouse. L'attivazione dell'interfaccia avviene infatti solo in presenza di relativa autorizzazione e protegge così il flusso di dati di una specifica produzione. Insieme a un firewall industriale, come SecurityBridge di Pilz che controlla la comunicazione dati all'interno di una rete di automazione industriale, è possibile

proteggere le macchine da accessi non autorizzati e da manipolazioni/manomissioni.

Macchine esistenti, “safe & secure”

Qualora fosse necessario portare le macchine esistenti allo stato dell'arte della tecnica o durante una valutazione del rischio fosse necessario un intervento, è possibile adattare con semplicità il sistema di autorizzazione all'accesso PITreader: il dispositivo può essere montato direttamente sulle uscite a norma per interruttori a chiave da 22,5 mm di diametro. Insieme a un sistema di controllo Pilz si può impostare direttamente la funzione di sicurezza richiesta. Se si utilizza un sistema di controllo di terzi, si installa PITmode per integrare la valutazione dell'autorizzazione all'accesso e della selezione della modalità operativa. A seconda del tipo di transponder coinvolto, è possibile utilizzare le keycard RFID presenti in azienda per l'autenticazione.

In conclusione:

Per proteggere un bene importantissimo come la nostra sicurezza, è necessario sviluppare approcci di tipo olistico e analizzarne periodicamente lo stato dell'arte. Una parte costitutiva importante è l'implementazione di un sistema di Identity and Access Management che disciplini in modo chiaro autorizzazioni e accessi all'interno dell'azienda. La soluzione è un concept che include misure organizzative e anche funzioni di sicurezza adeguate. Un sistema di autorizzazione all'accesso come PITreader è quindi il modulo hardware adatto che viene completato con i componenti software integrativi per l'organizzazione degli utenti e dei transponder. Altri componenti, come il sistema per ripari mobili, il sistema di controllo e il software e anche funzioni come la selezione della modalità operativa, ampliano la soluzione trasformandola in un

concept olistico di Safety e Industrial Security. Per l'utente diventa quindi semplice da gestire, avendo appunto tra le mani una chiave personalizzata.

Caratteri: 14.675

Immagini

Fig. 1:

F_Press_IAM_Man_using_PITreader_Key_cold1.jpg (© Pilz GmbH & Co. KG)



Didascalia: Un sistema completo di Identity and Access Management regola l'accesso all'applicazione e garantisce quindi l'integrità delle funzioni e delle misure di sicurezza, Safety e Industrial Security incluse.

Fig.2:

F_Press_PITmode_fusion_402251_PIT_oe_4023311_P1_B_8_2_cold_2020_01 (Pilz GmbH & Co. KG)



Didascalia: PITmode fusion di Pilz è un sistema modulare di scelta della modalità operativa e di autorizzazione all'accesso che unisce Safety e Security in un unico sistema.

Fig. 3:
F_Press_PITreader_S_card_unit_402321_and_PITreader_card_ye_g_402330_P1_B8_2_cold.jpg (Pilz GmbH & Co. KG)



Didascalia: Il sistema di autorizzazione all'accesso PITreader card unit di Pilz offre, con le schede RFID PITreader card e gli sticker PITreader sticker, nuovi formati per l'utilizzo di un sistema di autorizzazione all'accesso efficiente e sicuro.

Fig. 4:
F_Press_PITreader_Webserver.jpg (© Pilz GmbH & Co. KG)



Didascalia: Le chiavi a transponder RFID vengono inserite in memoria e acquisite all'interno dell'unità di lettura PITreader. L'assegnazione delle autorizzazioni all'accesso e di quelle delle modalità operative avviene in modo semplice tramite il relativo server web.

Fig. 5:
F_Press_Group_7_Modular_safety_gate_system_with_diagnostic_and_evaluation_P1_B8_2_cold_v0.jpg (© Pilz GmbH & Co. KG)



Didascalia: La combinazione flessibile di sistema per ripari mobili PSEnmlock con il modulo maniglia specifico (in alto a sinistra), unità pulsanti PITgatebox con sistema di autorizzazione all'accesso PITreader integrato (in alto a destra), modulo compatto di sicurezza configurabile PNOZmulti 2 (in basso a destra) e soluzione di diagnostica Safety Device Diagnostics (in basso a sinistra) offre una soluzione per ripari mobili completa e dotata di autorizzazione di accesso.

Box: Lockout/tagout digitale “key in pocket”

Oltre alla semplice autorizzazione all'accesso, è possibile implementare PITreader con un sistema di controllo come il modulo compatto configurabile PNOZmulti 2 o il sistema di automazione PSS 4000 per un lockout/tagout digitale “key in pocket” efficiente. Questa soluzione impedisce il riavvio della macchina durante le attività di manutenzione e l'accesso alle persone non autorizzate. In pratica funziona così: uno o più utenti autorizzati possono autenticarsi all'impianto per le attività di manutenzione. Dopo l'autenticazione, l'ID di sicurezza personale dell'utente viene memorizzato in un elenco sicuro nel sistema di controllo Pilz. A questo punto è possibile spegnere la macchina, aprire il riparo mobile e accedere alla macchina. Nel frattempo, le chiavi RFID restano “in tasca” ai rispettivi utenti. Al termine della manutenzione, tutto il personale lascia la zona pericolosa ed effettua il logout. Gli ID di sicurezza vengono rimossi dall'elenco di sicurezza del sistema di controllo Pilz ed è possibile riavviare la macchina. A differenza di un sistema di lockout/tagout con chiavi meccaniche, è possibile accedere o abbandonare l'impianto da qualsiasi riparo. “Key in pocket” offre quindi al personale una maggiore flessibilità e consente di risparmiare tempo durante la manutenzione. Il lockout/tagout digitale è stato progettato appositamente per le macchine con zone pericolose protette da recinzioni. L'azienda sa sempre chi accede alla macchina e per quale compito e può anche assegnare autorizzazioni temporanee.

1.578 caratteri

Fig. box “key in pocket”:

F_Press_Group_PIT_Key_in_pocket_solutions_P1_B8_2_cold.jpg (© Pilz GmbH & Co. KG)



Didascalia: Il sistema di lockout/tagout “Key in pocket” è costituito dal sistema di autorizzazione all’accesso PITreader, dall’unità pulsanti PITgatebox e anche da un sistema di controllo Pilz, come il modulo compatto configurabile PNOZmulti 2 o il sistema di automazione PSS 4000.

Box: Assegnazione e aggiornamento di autorizzazioni

Se in azienda viene implementato un sistema di autorizzazione all’accesso, diventa fondamentale gestire e aggiornare periodicamente le autorizzazioni e i dati degli utenti in modo tale che sia garantito un livello di sicurezza elevato. Pilz propone, a questo scopo, l’applicativo software PIT Transponder Manager (PTM): da un’interfaccia grafica, l’amministratore gestisce le proprie impostazioni utente, le liste di blocco e i dati degli utenti. Con i modelli preconfigurati e una funzione di importazione, le singole autorizzazioni utente vengono registrate con immediatezza e seguendo pochi semplici passi sulle chiavi a transponder.

Qualora in azienda siano in uso molteplici unità di lettura PITreader, queste vengono organizzate con il software PIT User Authentication

Service (UAS) di Pilz. Questo consente di connettere i sistemi di gestione come PTM o un altro software di gestione degli utenti con PITreader. PIT UAS è dotato di un database di autorizzazione centrale per gli utenti e consente così l'importazione e l'assegnazione dei dati da PTM a tutti i PITreader. Gli amministratori possono visionare lo stato attuale di tutti i PITreader e visualizzare una lista di diagnostica. In questo modo, è possibile effettuare controlli generali con rapidità anche quando si utilizzano molti dispositivi.

1.218 caratteri

Fig. box Gestione utente:

((Segue immagine)).jpg (© Pilz GmbH & Co. KG)



Didascalia: Qualora in azienda siano in uso molteplici unità di lettura PITreader, questi dispositivi vengono organizzati con lo User Authentication Service (UAS).

Il gruppo Pilz

Il gruppo Pilz è fornitore globale di prodotti, sistemi e servizi per la tecnologia di automazione. È un'impresa familiare con sede a Ostfildern e una forza lavoro di circa 2.500 unità. Grazie a 42 controllate e filiali, Pilz è ambasciatore della sicurezza per l'uomo, le macchine e l'ambiente in tutto il mondo.

In qualità di azienda leader in questo settore, Pilz offre soluzioni di automazione complete per la tecnologia destinata a sensori, sistemi di controllo e azionamento, inclusi i 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 della logistica, della tecnologia ferroviaria o della robotica.

www.pilz.it

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

Sabrina Schilling

Stampa specializzata
Tel: +49 711 3409-7147
s.schilling@pilz.de

**Hansjörg Sperling-
Wohlgemuth**

Gestione Congressi e Conferenze
Tel: +49 711 3409-239
h.sperling@pilz.de