Achtergrondinformatie

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Duitsland/Germany
www.pilz.com

Veiligheidstotaalconcepten concentreren zich op de toegang, om safety en industrial security op de machine te garanderen

Totale veiligheid door individueel autorisatiebeheer

Ostfildern, februari 2023 – **Overal waar we iets waardevols willen beschermen, gebruiken we deuren, sloten en sleutels om de toegang te beperken. Datzelfde geldt voor het hoogste goed: onze veiligheid in al haar verschijningsvormen. In een industriële omgeving moeten enerzijds de mensen beschermd (safety) en anderzijds de machines en gevoelige gegevens beveiligd (industrial security) worden. Een veiligheidslacune kan verschillende gevolgen hebben: Van verkeerde bediening en een ongeval tot een ernstige cyberaanval. Een uitgebreid Identification and Access Management, dat toegangsrechten duidelijk regelt, draagt bij aan een veiligheidstotaalconcept en aan efficiënte processen.**

In de productieomgeving zijn ze een vertrouwd beeld: scheidende veiligheidsvoorzieningen, die aan de mens een duidelijk signaal geven dat er een risicogebied is achter het veiligheidshek en dat voorzichtigheid geboden is. Via een Human Machine Interface (HMI) of een sleutel krijgen personen toegang tot het proces achter het veiligheidshek. Maar wat als de persoon niet gekwalificeerd of bevoegd is en zichzelf of anderen in gevaar brengt? Ook een persoon met kwade bedoelingen kan het proces manipuleren - rechtstreeks op de machine of via toegang op afstand. Bij het onderwerp “toegangsautorisatie” blijkt dat safety en industrial security nauw met elkaar verweven zijn. Sterker nog: industrial security zorgt op de machine voor de integriteit van de safety. Het biedt bijvoorbeeld machines of installaties in de productie bescherming tegen ongeoorloofde toegang van buitenaf en beschermt gevoelige proces- en machinegegevens intern tegen vervalsing, verlies en ongeoorloofde toegang. Dit omvat zowel expliciete aanvallen als onopzettelijke security-incidenten.

Safety en industrial security horen bij elkaar

Voor exploitanten van machines en systemen is het noodzakelijk dat ze taken en bevoegdheden duidelijk toewijzen, d.w.z. dat ze Identification and Access Management instellen. Dit betekent enerzijds organisatorische maatregelen zoals werkinstructies of regelmatige controles van processen, en anderzijds de integratie van passende beveiligingsoplossingen in de productieomgeving. Als dergelijke maatregelen achterwege blijven, kunnen de verantwoordelijken in een bedrijf persoonlijk aansprakelijk worden gesteld bij ongevallen of productieverlies. Tot nu toe zijn dergelijke security-oplossingen gebaseerd op vrijwilligheid, en werd op veel plaatsen nog geen noodzaak gezien om in te grijpen. De wetgever heeft nu echter erkend dat safety en security met elkaar verweven zijn. De nieuwe machineverordening stelt daarom beveiligingsmaatregelen verplicht.

Bedrijfsmodi verhogen de veiligheid

Bovendien is in diverse C-normen reeds bepaald dat verschillende bedrijfsmodi ook overeenkomstige veiligheidsfuncties moeten bevatten. Bedrijfsmodi kunnen bijvoorbeeld automatisch bedrijf, handmatig ingrijpen onder beperkte voorwaarden of servicebedrijf zijn. De norm EN ISO 16090-1 voor bewerkingscentra en speciale machines stelt ten minste twee van deze bedrijfsmodi verplicht om de functionele veiligheid te waarborgen. Het is belangrijk dat altijd slechts één bedrijfsmodus tegelijk geselecteerd en actief is en dat deze duidelijk wordt weergegeven.

Anonieme toegang voorkomen

Maar hoe wordt bepaald welke personen toegang hebben tot welke bedrijfsmodus of zelfs de bedrijfsmodus mogen wijzigen? Daarvoor worden verschillende groepen personen gedefinieerd, zoals bedienings-, schoonmaak- of onderhoudspersoneel dat in contact komt met de

machine. De werknemers worden vervolgens in deze groepen ingedeeld op basis van hun taak of kwalificatie. Afhankelijk van de omvang van het bedrijf kunnen ook vrijgaven of toegangsrechten worden toegewezen voor verschillende gebruikersgroepen of bijvoorbeeld voor een machinetype dat in het hele bedrijf wordt gebruikt. In het kader van een risicobeoordeling schatten beveiligingsdeskundigen het risico van anonieme toegang voor elk gevaar in en beoordelen dit. Vervolgens worden volgens de stand van de techniek en in overeenstemming met de geharmoniseerde normen maatregelen vastgesteld die het risico verminderen.

Gebruiksvriendelijkheid voorkomt manipulatie

Bij de uitvoering van de maatregelen is het van belang de hanteerbaarheid en bruikbaarheid voor de gebruikers tijdens het bedrijf te waarborgen, teneinde manipulatie uit te sluiten. Voor constructeurs van machines geldt dit al voor het ontwikkelingsproces. Intuïtieve bedieningssystemen die gebruikers gemakkelijk kunnen hanteren, voorkomen dat veiligheidsmaatregelen worden ondermijnd of dat machines verkeerd worden bediend. Bovendien draagt een doordacht veiligheidssysteem bij tot efficiënte processen zonder onnodige stilstand. Het thema “negeren van veiligheidsvoorzieningen” staat centraal in EN ISO 14119. De norm definieert principes voor het ontwerp en de selectie van heksystemen en biedt zo concrete hulp bij de manier waarop manipulatie kan worden vermeden.

Individueel veiligheidsconcept

Om er zeker van te zijn dat het opzettelijk of onbedoeld openen van toegangsdeuren niet tot gevaren leidt, zijn deze beveiligd met een veilig heksysteem. Wat de safety betreft, ligt de nadruk daarbij op de bescherming van de werknemer tegen gevaarlijke machinebewegingen. Afhankelijk van de vraag of het gaat om een

op zichzelf staande machine of complexe, onderling verbonden installaties, is een veiligheidsconcept op maat vereist. Als machines een gevaarlijke naloop hebben, speelt dichthouding een belangrijke rol; als deuren betreedbaar zijn, is een noodontgrendeling een must.

Veiligheidshekken op maat beveiligen

Een modulair veiligheidsheksysteem zoals PSENmlock van Pilz combineert veilige hekbewaking met veilige dichthouding in één systeem en beschikt bovendien over veiligheidsfuncties zoals noodstop, noodontgrendeling en een mechanische herstartblokkering. Het biedt de flexibiliteit en decentrale intelligentie om de meest uiteenlopende toepassingen te beveiligen. Een individuele oplossing bestaat uit een combinatie van sensoren, noodontgrendeling, deurgrepen en een bedienings- en knoppenunit. Afhankelijk van de toepassing stellen gebruikers zo hun eigen individuele veiligheidshekoplossing samen. Om te voldoen aan de eisen van industrial security, wordt vervolgens gekeken naar de toegangen en machtigingen.

Eén systeem voor safety en industrial security

Beveiliging tegen ongeoorloofde toegang kan in de praktijk worden gerealiseerd met één systeem voor bedrijfsmoduskeuze en toegangsautorisatie. Dit systeem combineert safety en industrial security: de keuze van de bedrijfsmodus en de regeling van de toegangsrechten voor de machine. een dergelijke oplossing wordt geboden door de apparaten van de productgroep PITmode van Pilz, waarmee tussen gedefinieerde bedrijfsmodi kan worden geschakeld en de toegangsautorisatie kan worden geregeld. De bediening is intuïtief, omdat elke gebruiker zijn of haar individueel gecodeerde transponder krijgt, wat een unieke gebruikersauthenticatie mogelijk maakt en manipulatie voorkomt.

Toegangen en bedrijfsmodi individueel beheren

Om het beveiligingsconcept individueel vorm te geven, is PITmode er in verschillende versies. Als compact all-in-one apparaat bevat PITmode de knoppen voor de bedrijfsmoduskeuze en een verwerkingseenheid, wat een ruimtebesparende installatie mogelijk maakt. Het modulair opgebouwde systeem PITmode fusion daarentegen bestaat uit de uitleeseenheid PITreader met RFID-technologie en geïntegreerde webserver, en een veilige verwerkingseenheid (Safe Evaluation Unit, SEU). Een andere variant is PITmode flex: hierbij wordt PITreader gebruikt in combinatie met een Pilz-besturing en een softwaremodule voor veilige verwerking. De modulaire opbouw maakt het mogelijk toegangsautorisatie en bedrijfsmoduskeuze te integreren in het ontwerp van bestaande bedieningspanelen. Daar kunnen aanwezige knoppen voor de keuze van de bedrijfsmodus worden gebruikt, wat voor de gebruiker een eenvoudigere bediening mogelijk maakt. De identificatie met de transponder wordt uitgevoerd door de uitleesunit PITreader. PITmode en PITmode fusion bieden functioneel veilige bedrijfsmoduskeuze en toegangsautorisatie tot PL d.

Eenvoudige authenticatie – ook op afstand

Om de bedrijfsmodus te kiezen, sluit de gebruiker zijn transponder rechtstreeks aan op de PITmode en drukt hij op een toets die voor de bedrijfsmodus is gedefinieerd of op de overeenkomstige toets op een HMI. Als er autorisatie is, krijgt de gebruiker toegang tot het proces. Hetzelfde werkt ook wanneer een servicemedewerker voor onderhoud op afstand toegang wil tot een machine: pas wanneer een persoon ter plaatse de betreffende vrijgave in het systeem geeft, kan het onderhoud op afstand beginnen. Na de

onderhoudswerkzaamheden wordt deze toegang weer gesloten, voordat de machine weer wordt opgestart. Manipulatie door onbevoegden of een poort die per ongeluk is opengelaten na onderhoudswerkzaamheden, kan zo worden uitgesloten. Exploitanten verhogen de industrial security, omdat ze bepalen wie welke rechten en dus toegang tot het proces krijgt.

Totaaloplossing voor toegangsbeheer

Als uitsluitend de regeling van de toegangen moet worden uitgevoerd, kan PITreader ook alleen of in combinatie met een besturing van Pilz als toegangsautorisatiesysteem worden gebruikt. In combinatie met de configureerbare kleine besturing PNOZmulti 2 configureert de beheerder de toegangsrechten voor machines en installaties eenvoudig door middel van “drag and drop” met de bijbehorende configuratietool PNOZmulti Configurator. Deze worden vervolgens via de uitleesunit PITreader doorgegeven aan de RFID-transpondersleutels. Dankzij de integratie van de OPC UA-standaard is de variant PITreader S onafhankelijk van een Pilz-besturing ook fabrikantoverkoepelend inzetbaar. Zoals al vermeld kunnen PITmode-apparaten eenvoudig in bestaande bedieningspanelen worden geïntegreerd.

De keuze tussen sleutel, kaart of sticker

Nog meer flexibiliteit voor exploitanten en gebruikers biedt de variant PITreader card unit: hiermee kunnen RFID-compatibele kaarten en stickers samen met of in plaats van een RFID-transpondersleutel worden gebruikt. Als er al RFID-compatibele kaarten in een bedrijf worden gebruikt, kunnen deze ook in combinatie met de PITreader card unit worden gebruikt: de gebruiker heeft dan slechts één kaart voor meerdere functies nodig. Het principiële voordeel van RFID-transponders – of het nu gaat om

een sleutel, kaart of sticker – is dat verschillende functies op één transponder worden gebundeld en dat zo een hele mechanische sleutelbos kan worden gecombineerd. Dit is comfortabel voor gebruikers, omdat ze slechts één identificatiemedium hoeven mee te nemen. Beheerders daarentegen besparen tijd en moeite bij het beheer en onderhoud van de sleutels.

Een plus aan security

En er wordt ook rekening gehouden met security-aspecten met het oog op authenticatie, kwalificatie en toegangsbeveiliging van gebruikers. Als er ondanks alle veiligheidsmaatregelen toch een ongeval of security-incident bij een machine voordoet, kan via het uitlezen van de RFID-transponder worden achterhaald wie welke wijziging heeft uitgevoerd. Als deze optionele functie gewenst is, registreert het besturingssysteem op basis van de authenticatie ook het tijdstip van toegang in de interne, onveranderlijke audit trail (gebeurtenissenlogboek).

Zorgvuldig beheer is de sleutel

Om safety en industrial security gedurende de hele levenscyclus van de toepassing te garanderen, besteden beheerders veel zorg aan het onderhoud van autorisaties. Voor een eenvoudig beheer ondersteunen passende softwaretools van Pilz de organisatie van gebruikers en transponders. Achter een kleine RFID-sleutel kunnen bijvoorbeeld complexe autorisatiematrices of bedrijfsbrede voorschriften verborgen gaan. Met de geïntegreerde PITreader webserver programmeren beheerders de bij PITmode of PITreader horende RFID-transponders en slaan daarop de gebruikersgegevens en autorisaties op. Alle belangrijke instellingen vinden rechtstreeks op de uitleeseenheid plaats, wat zorgt voor een snellere inbedrijfstelling, inclusief de configuratie van interfaces.

Toegang tot interfaces beperken

De mogelijkheden van het Identification and Access Management strekken zich uit tot het vrijgeven van speciale industriële USB-poorten, een van de belangrijkste inbraakpoorten bij security-incidenten. Daarvoor wordt het toegangsautorisatiesysteem PITreader gecombineerd met een bedieningselement zoals PIT oe USB, dat over een activeerbare USB 2.0 host-interface beschikt. Deze oplossing maakt het tegen manipulatie beveiligde laden van programma's, het downloaden van gegevens en het aansluiten van een toetsenbord of muis mogelijk. De interface wordt namelijk alleen geactiveerd met de juiste autorisatie, zodat de gegevensstroom van een productie beveiligd is. Samen met een industriële firewall zoals SecurityBridge van Pilz, die de datacommunicatie binnen een industrieel automatiseringsnetwerk regelt, kunnen machines zo worden beschermd tegen onbevoegde toegang en manipulatie.

Bestaande machines – safe en secure

Als bestaande machines aan de stand van de techniek moeten worden aangepast of als in het kader van een risicobeoordeling is vastgesteld dat maatregelen nodig zijn, kan het toegangsautorisatiesysteem PITreader eenvoudig achteraf worden ingebouwd: het apparaat kan rechtstreeks worden gemonteerd op de gestandaardiseerde uitgangen voor sleutelschakelaars met een diameter van 22,5 millimeter. Samen met een Pilz-besturing kan de gewenste veiligheidsfunctie direct worden ingesteld. Bij gebruik van een externe besturing wordt PITmode fusion gebruikt om de beoordeling van de toegangsautorisatie en de bedrijfsmoduskeuze te integreren. Afhankelijk van het transpondermedium kunnen bestaande RFID-keycards in het bedrijf worden gebruikt voor de authenticatie.

Samenvatting

Om het hoogste goed, namelijk onze veiligheid, te beschermen, moeten veiligheidsconcepten als totaaloplossing worden ontworpen en regelmatig op hun actualiteit worden getoetst. Een belangrijk onderdeel is het Identification and Access Management, dat autorisaties en toegang in een bedrijf duidelijk regelt. De oplossing is een concept dat zowel organisatorische maatregelen en specificaties als passende veiligheidsfuncties omvat. Een toegangsautorisatiesysteem zoals PITreader is hiervoor de geschikte hardwarecomponent, die wordt gecompleteerd door de aanvullende softwarecomponenten voor de organisatie van de gebruikers en transponders. Verdere componenten, zoals veiligheidsheksysteem, besturing en software, alsmede functies zoals de bedrijfsmoduskeuze, breiden de oplossing uit tot een safety- en industrial security-totaalconcept. Voor de gebruiker is het bovendien gemakkelijk te hanteren, namelijk met de individuele sleutel in de hand.

Kenmerk: 14.675

Afbeeldingen

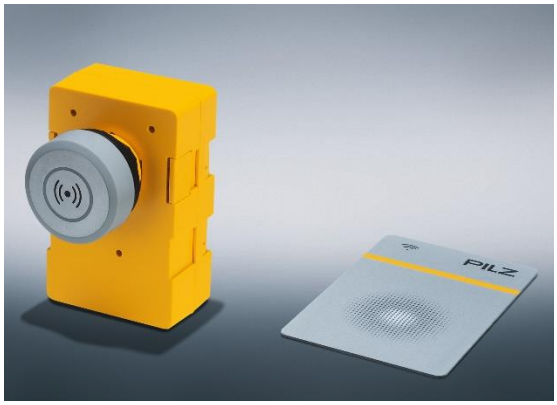
Afb. 1:
F_Press_IAM_Man_using_PITreader_Key_cold1.jpg (© Pilz GmbH & Co. KG)

Onderschrift: Een uitgebreid Identification and Access Management regelt de toegang tot de toepassing en garandeert zo de integriteit van veiligheidsfuncties en -maatregelen – inclusief safety en industrial security.

Afb. 2:
F_Press_PITmode_fusion_402251_PIT_oe_4023311_P1_B_8_2_cold_2020_01 (Pilz GmbH & Co. KG)

Onderschrift: PITmode fusion van Pilz is een modulair opgebouwd bedrijfsmoduskeuze- en toegangsautorisatiesysteem, dat safety en industrial security in één systeem verenigt.

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



Onderschrift: Het toegangsautorisatiesysteem PITreader card unit van Pilz biedt met de RFID-compatibele kaarten PITreader card en stickers PITreader sticker nog meer formaten voor de implementatie van een efficiënt toegangsautorisatiesysteem.

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

Onderschrift: De RFID-transpondersleutels worden in de PITreader ingelezen en ingeleerd. De toewijzing van toegangsrechten en bedrijfsmodi vindt eenvoudig via de bijbehorende webserver plaats.

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

Onderschrift: De flexibele combinatie van het heksysteem PSENmlock, de passende deurgreepmodule (linksboven), de knoppenunit PITgatebox met het geïntegreerde toegangsautorisatiesysteem PITreader (rechtsboven) en de configureerbare kleine besturing PNOZmulti 2 (rechtsonder) en de diagnoseoplossing Safety Device Diagnostics (linksonder) biedt een complete hekoplossing met toegangsrechten:

Kader: Digitale onderhoudsbeveiliging Key-in-pocket

Naast pure toegangsautorisatie kan PITreader samen met een Pilz-besturing zoals de configureerbare kleine besturing PNOZmulti 2 of het automatiseringssysteem PSS 4000 worden gebruikt voor efficiënte digitale onderhoudsbeveiliging “Key-in-pocket”. “Key-in-pocket” zorgt ervoor dat de machine tijdens onderhoudswerkzaamheden niet opnieuw opstart en dat onbevoegden geen toegang krijgen. In de praktijk werkt dat als volgt: Een of meer voor onderhoudswerkzaamheden bevoegde gebruikers authenticeren zich bij de installatie. Na succesvolle authenticatie wordt in de Pilz-besturing voor de gebruiker een gepersonaliseerde security-ID opgeslagen in een veilige lijst. Nu kan de machine worden uitgeschakeld, het veiligheidshek worden

geopend en de machine worden betreden. Ondertussen blijven de RFID-sleutels “in de zak” van de betreffende gebruikers. Nadat het onderhoud is uitgevoerd en de gevarenzone is verlaten, meldt al het personeel zich af, worden de security-ID's uit de veilige lijst van de Pilz-besturing verwijderd en kan de machine opnieuw worden gestart. In tegenstelling tot een onderhoudsbeveiliging met mechanische sleutels kan de installatie bij elke veiligheidsdeur worden betreden of verlaten. “Key-in-pocket” biedt dus voor het personeel meer flexibiliteit en tijdwinst bij het onderhoud. De digitale onderhoudsbeveiliging is speciaal ontworpen voor machines met gevarenzones die door veiligheidshekken worden beschermd. De exploitant weet te allen tijde wie toegang krijgt voor welke taak en kan ook tijdelijke machtigingen toewijzen.

1.578 tekens

Afb. Kader Key-in-pocket:
F_Press_Group_PIT_Key_in_pocket_solutions_P1_B8_2_cold.jpg (© Pilz GmbH & Co. KG)

Onderschrift: De onderhoudsbeveiliging “Key-in-pocket” bestaat uit het toegangsautorisatiesysteem PITreader, de knoppenunit PITgatebox en een Pilz-besturing zoals de configureerbare kleine besturing PNOZmulti 2 of het automatiseringssysteem PSS 4000.

Kader: Autorisaties verlenen en onderhouden

Als in het bedrijf een toegangsautorisatiesysteem wordt ingezet, is het regelmatig onderhouden en beheren van autorisaties en gebruikersgegevens van cruciaal belang om een hoog veiligheidsniveau te waarborgen. Pilz stelt daarvoor de softwaretool PIT Transponder Manager (PTM) beschikbaar: Via een grafische interface beheert de beheerder zijn gebruikersinstellingen, blokkadelijsten en gebruikersgegevens. Met voorgeconfigureerde sjablonen en een importfunctie worden individuele gebruikersrechten in enkele stappen op de transpondersleutel geschreven.

Als er meerdere PITmode of PITreader in een bedrijf worden ingezet, worden deze apparaten met de software PIT User Authentication Service (UAS) van Pilz georganiseerd. Hierdoor kunnen managementsystemen zoals PTM of andere software voor gebruikersbeheer worden gecombineerd met PITreader. PIT UAS heeft een centrale autorisatiedatabase voor de gebruikers en maakt zo het importeren en toewijzen van gegevens uit de PTM naar alle PITreader mogelijk. Beheerders kunnen de huidige status van alle PITreader bekijken en een diagnoselijst weergeven. Dit zorgt voor een snel overzicht, ook bij gebruik van meerdere apparaten.

1.218 tekens

Afb. kader gebruikersbeheer:
((Afbeelding volgt)).jpg (© Pilz GmbH & Co. KG)

Onderschrift: Als er meerdere uitleesunits PITreader in een bedrijf worden ingezet, worden deze apparaten met de User Authentication Service (UAS) georganiseerd.

Pilz Groep

De Pilz-groep is een wereldwijde leverancier van producten, systemen en diensten voor de automatiseringstechniek. Het familiebedrijf met de hoofdvestiging in Ostfildern heeft ongeveer 2500 medewerkers in dienst. Met 42 dochterondernemingen en vestigingen zorgt Pilz wereldwijd voor veiligheid voor mens, machine en milieu.
De technologieleider biedt complete automatiseringsoplossingen die sensoren, besturings- en aandrijftechniek omvatten – inclusief systemen voor de industriële communicatie, diagnose en visualisering. Een internationaal dienstenaanbod met advies, engineering en trainingen completeert het portfolio. Oplossingen van Pilz worden niet alleen gebruikt in de machine- en installatiebouw, maar ook in tal van andere sectoren, zoals intralogistiek, spoorwegtechniek en robotica.

www.pilz.com

Contact voor journalisten:

Martin Kurth

Bedrijfs- en vakpers
Tel: +49 711 3409-158
m.kurth@pilz.de

Sabina Schilling

Sabine Karrer

Vak- en bedrijfspers
Tel: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Hansjörg Sperling-Wohlgemuth

Jenny Skarman

Vakpers

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

Vakpers

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

Congres- en presentatiemanagement
Tel: +49 711 3409-239
h.sperling@pilz.de