Baggrundsinformation

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



# Helhedsorienterede sikkerhedskoncepter fokuserer på adgang for at sikre Safety og Industrial Security ved maskinen

**Helhedsorienteret sikkerhed ved hjælp af individuel autorisationsstyring**

Ostfildern, februar 2023 – **Overalt, hvor vi ønsker at beskytte noget værdifuldt, bruger vi døre, låse og nøgler til at begrænse adgangen**. **Det samme gælder for det allervigtigste: Vores sikkerhed i alle dens afskygninger. I industrimiljøet er det vigtigt på den ene side at beskytte mennesker (Safety) og på den anden side maskinen og følsomme data (Industrial Security). Manglende sikkerhed kan have forskellige konsekvenser: Lige fra forkert betjening over en ulykke til et alvorligt cyberangreb. Omfattende Identification and Access Management, som klart regulerer adgangsautorisationer, bidrager til et helhedsorienteret sikkerhedskoncept og effektive processer.**

I produktionsmiljøet er de et velkendt syn: Afskærmninger, der giver et klart signal til personalet om, at der befinder sig et følsomt område bag beskyttelsesdøren, og at man skal være forsigtig. Personalet får adgang til processen bag beskyttelsesbarrieren via et Human Machine Interface (HMI) eller en nøgle. Men hvad nu, hvis personen ikke er kvalificeret eller autoriseret til at gøre det og bringer sig selv eller andre personer i fare? Også en person med ulovlige hensigter kan manipulere processen – enten direkte på maskinen eller via fjernadgang. Når det drejer sig om adgangsautorisation, viser det sig, at Safety og Industrial Security er tæt forbundet. Ja, endda mere end det: Industrial Security sørger for integriteten af Safety på maskinen. Den giver f.eks. maskiner eller anlæg beskyttelse under produktionen mod uvedkommende adgang udefra og beskytter følsomme proces- og maskindata mod forfalskning, mistede data og uvedkommende adgang til de indvendige dele. Dette omfatter både eksplicitte angreb og utilsigtede Security-hændelser.

## Safety og Industrial Security hører sammen

Det er nødvendigt, at de driftsansvarlige for maskiner og anlæg klart tildeler og tilknytter opgaver og autorisationer, dvs. at de etablerer Identification and Access Management. Det betyder på den ene side organisatoriske foranstaltninger som f.eks. arbejdsanvisninger eller regelmæssige kontroller af processer og på den anden side integration af passende sikkerhedsløsninger i produktionsmiljøet. Hvis sådanne foranstaltninger undlades, kan de ansvarlige personer i en virksomhed gøres personligt ansvarlige i tilfælde af ulykker eller produktionsudfald. Tidligere var sådanne Security-løsninger baseret på frivillighed, og mange steder så man endnu ikke noget behov for handling. Lovgiveren har imidlertid nu erkendt, at Safety og Security hænger sammen. Den nye maskinforordning foreskriver derfor obligatoriske Security-foranstaltninger.

**Driftstyper øger sikkerheden**

Derudover foreskriver forskellige C-standarder allerede nu, at forskellige driftstyper også skal indeholde de passende sikkerhedsfunktioner. Driftstyper kan f.eks. være automatisk drift, manuel indgriben under begrænsede forhold eller servicedrift. EN ISO 16090-1 for værktøjsmaskiner og specialmaskiner foreskriver mindst to af disse driftstyper som obligatoriske for at sikre Functional Safety. Det er vigtigt, at der altid kun er valgt én driftstype, som er aktiv, og at dette er tydeligt angivet.

**Forhindring af anonym adgang**

Men hvordan afgøres det, hvilke personer der har adgang til hvilken driftstype eller i det hele taget har lov til at ændre driftstypen? Til dette formål defineres forskellige persongrupper, som f.eks. betjenings-, rengørings- eller vedligeholdelsespersonale, der kommer i kontakt med maskinen. Derefter knyttes medarbejderne til grupperne ud fra deres opgave eller kvalifikation. Afhængigt af virksomhedens størrelse kan der

også tildeles frigivelser eller adgangsrettigheder til forskellige brugergrupper eller f.eks. til en maskintype, der anvendes i hele koncernen. I forbindelse med en risikovurdering vurderer sikkerhedseksperter risikoen for anonym adgang for hver enkelt risiko. Derefter fastlægges der foranstaltninger, som reducerer risikoen, i overensstemmelse med det aktuelle tekniske niveau og med overholdelse af de harmoniserede standarder.

**Brugervenlighed forebygger manipulation**

Ved implementeringen af foranstaltningerne er det vigtigt at sikre håndtering og brugervenlighed for brugerne under driften, således at manipulation udelukkes. For maskinproducenter gælder dette allerede fra udviklingsprocessen. Intuitive betjeningssystemer, der er lette at håndtere for brugerne, forhindrer, at sikkerhedsforanstaltninger omgås, eller maskiner betjenes forkert. Derudover bidrager et gennemtænkt sikkerhedssystem til effektive processer uden unødvendige stilstandsperioder. Emnet "omgåelse af beskyttelsesanordninger" er et centralt punkt i EN ISO 14119. Denne standard definerer principper for udformning og valg af beskyttelsesdørssystemer og giver således konkret hjælp til, hvordan manipulation kan undgås.

**Individuelt sikkerhedskoncept**

For at undgå, at forsætlig eller utilsigtet åbning af adgangsdøre medfører farer, er disse sikret med et sikkert beskyttelsesdørssystem. Når det gælder Safety, fokuseres der på at beskytte arbejdstageren mod farlige maskinbevægelser. Det er nødvendigt at have et skræddersyet sikkerhedskoncept, afhængigt af om der er tale om en stand-alone-maskine eller komplekse, kombinerede anlæg. Hvis maskinerne har et farligt efterløb, spiller

tvangskobling en vigtig rolle, og hvis dørene kan passeres, er det absolut nødvendigt med flugtfrigørelse.

**Skræddersyet sikring af beskyttelsesdøre**

Et modulopbygget beskyttelsesdørssystem som PSENmlock fra Pilz kombinerer sikker overvågning af beskyttelsesdøre med sikker tvangskobling i ét system og har også sikkerhedsfunktioner som nødstop, flugtfrigørelse og en mekanisk genstartsspærre. Det giver fleksibilitet og en decentral intelligens med mulighed for at sikre mange forskellige applikationer. En individuel løsning består af en kombination af sensorer, flugtfrigørelse, dørgreb samt en betjenings- og trykknap-enhed. Afhængigt af applikationen kan brugerne således skabe deres egen individuelle beskyttelsesdørsløsning. For at opfylde kravene til Industrial Security ser man nu på adgangene og autorisationerne.

**Ét system til Safety og Industrial Security**

Beskyttelse mod uautoriseret adgang kan i praksis implementeres med ét system til både driftstypevalg og adgangsautorisation. Det kombinerer Safety og Industrial Security: Valg af driftstype og regulering af adgangsautorisationen til maskinen. Enhederne i produktgruppen PITmode fra Pilz er en sådan løsning, der gør det muligt at skifte mellem definerede driftstyper og regulere adgangsautorisationen. Betjeningen er intuitiv, fordi hver bruger modtager sin egen individuelt kodede transponder, hvilket muliggør entydig brugerautentificering og forhindrer manipulation.

**Individuel administration af adgange og driftstyper**

For at udforme sikkerhedskonceptet individuelt fås PITmode i forskellige udførelser. Som kompakt all-in-one-enhed indeholder PITmode knapperne til driftstypevalg samt en analyseenhed, der

muliggør pladsbesparende installation. Det modulopbyggede system PITmode fusion består derimod af udlæsningsenheden PITreader med RFID-teknologi og integreret webserver samt en sikker evalueringsenhed, der kaldes Safe Evaluation Unit (SEU). En yderligere variant er PITmode flex: Her anvendes PITreader sammen med en Pilz-styring og et softwaremodul til den sikre evaluering. Modulopbygningen gør det muligt at integrere adgangsautorisation og driftstypevalg i designet af eksisterende betjeningspulte. Her kan eksisterende taster bruges til at vælge driftstype, hvilket giver brugeren mulighed for enkel betjening. Identifikationen med transponderen udføres ved hjælp af udlæsningsenheden PITreader. PITmode og PITmode fusion har funktionsmæssigt sikkert driftstypevalg og adgangsautorisation op til PL d.

**Enkel autentificering – også med fjernbetjening**

For at vælge driftstype tilslutter brugeren sin transponder direkte til PITmode og trykker på en knap, der er defineret for driftstypen, eller på den passende knap på et HMI. Hvis autorisationen er til rådighed, får brugeren adgang til processen. Det fungerer på samme måde, når en servicemedarbejder ønsker at få adgang til fjernservice på en maskine: Først når en person på stedet giver den passende frigivelse i systemet, kan fjernservicen begynde. Efter vedligeholdelsesarbejdet lukkes denne adgang igen, før maskinen genstarter. På denne måde kan man udelukke manipulation fra uautoriserede eller en port, der utilsigtet er blevet efterladt åben efter vedligeholdelsesarbejdet. De driftsansvarlige øger Industrial Security, fordi de styrer, hvem der får autorisation og dermed adgang til processen.

**Komplet løsning til adgangsstyring**

Hvis der kun skal gennemføres adgangskontrol, kan PITreader også anvendes alene eller i kombination med en styring fra Pilz som adgangsautorisationssystem. I kombination med den konfigurerbare lille styring PNOZmulti 2 konfigurerer administratoren nemt adgangsautorisationerne til maskiner og anlæg med det tilhørende konfigurationsværktøj PNOZmulti Configurator ved hjælp af "drag and drop". Disse overføres derefter til RFID-transpondernøglerne via udlæsningsenheden PITreader. Varianten PITreader S kan ved hjælp af integrationen af OPC UA-standarden også anvendes på tværs af producenter uafhængigt af en Pilz-styring. Som allerede nævnt kan PITmode-enheder nemt integreres i eksisterende betjeningspaneler.

**Valget mellem nøgle, kort eller sticker**

Varianten PITreader card unit giver yderligere fleksibilitet for driftsansvarlige og brugere: Med denne kan RFID-kompatible kort og stickers anvendes sammen med eller i stedet for en RFID-transpondernøgle. Hvis virksomheden allerede bruger RFID-kompatible kort, kan disse også bruges sammen med PITreader card unit: Brugeren behøver derefter kun ét kort til flere funktioner. Grundlæggende er fordelen ved RFID-transponderne – uanset om det er nøgle, kort eller sticker – at flere funktioner er samlet på én transponder, og at det således er muligt at samle et komplet mekanisk nøglebundt. Det er komfortabelt for brugeren, fordi han kun skal have ét identifikationsmedie på sig. Administratorer sparer til gengæld tid og kræfter i forbindelse med administration og vedligeholdelse af nøglerne.

**Ekstra Security**

Der tages også hensyn til Security-aspekter med hensyn til brugerautentificering, kvalificering og adgangsbeskyttelse. Hvis der

trods alle sikkerhedsforanstaltninger sker en ulykke eller en Security-hændelse på maskinen, kan man ved at udlæse RFID-transponderen spore, hvem der har foretaget hvilken ændring. Hvis denne valgfrie funktion ønskes, registrerer styringssystemet ud fra autentificeringen også tidspunktet for adgangen i den interne, skrivebeskyttede Audit Trail (hændelseslog).

**Den omhyggelige administration er nøglen**

For at sikre Safety og Industrial Security i hele applikationens livscyklus er administratorer meget omhyggelige med at vedligeholde autorisationerne. For at gøre administrationen enkel understøttes bruger- og transponderorganisationen af passende softwareværktøjer fra Pilz. Således kan der bag en lille RFID-nøgle f.eks. skjule sig komplekse autorisationsmatricer eller retningslinjer, der er reguleret i hele koncernen. Med den integrerede PITreader-webserver programmerer administratorer de RFID-transpondere, der hører til PITmode eller PITreader, og gemmer brugerdataene og autorisationerne på dem. Alle vigtige indstillinger foretages direkte på udlæsningsenheden, hvilket fremskynder idrifttagningen, inklusive konfigurationen af interfaces.

**Begrænsning af adgangen til interfaces**

Mulighederne med Identification and Access Management rækker helt til frigivelse af særlige industrielle USB-porte, som er en af de vigtigste indgange i forbindelse med Security-hændelser. Til dette formål kombineres adgangsautorisationssystemet PITreader med et betjeningselement som f.eks. PIT oe USB, der har et aktiverbart USB 2.0-host-interface. Denne løsning gør det muligt manipulationssikkert at indlæse programmer, udlæse data og tilslutte et tastatur eller en mus. Dette skyldes, at interfacet kun aktiveres med den passende autorisation og dermed beskytter

dataflowet i en produktion. Sammen med en industriel firewall som f.eks. SecurityBridge fra Pilz, der kontrollerer datakommunikationen i et industrielt automatiseringsnetværk, kan maskiner på denne måde beskyttes mod uautoriseret adgang og manipulation.

**Eksisterende maskiner – safe og secure**

Hvis eksisterende maskiner skal opgraderes til det aktuelle tekniske niveau, eller hvis der i forbindelse med en risikovurdering er blevet konstateret et behov for handling, er det enkelt at eftermontere adgangsautorisationssystemet PITreader: Enheden kan monteres direkte på de standardiserede udgange til nøgleafbrydere med en diameter på 22,5 millimeter. Sammen med en Pilz-styring kan den ønskede sikkerhedsfunktion konfigureres direkte. Hvis der anvendes en styring fra en tredjepart, anvendes PITmode fusion til at integrere evalueringen af adgangsautorisation og driftsvalg. Afhængigt af hvilket transpondermedie der er tale om, kan eksisterende RFID-Keycards i virksomheden anvendes til autentificeringen.

**Facit**

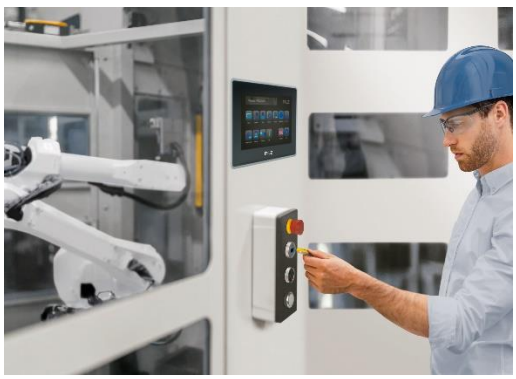
For at beskytte det allervigtigste, nemlig vores sikkerhed, er det nødvendigt at udforme helhedsorienterede sikkerhedskoncepter og regelmæssigt undersøge, om de er tidssvarende. En vigtig komponent er et Identification and Access Management, som tydeligt regulerer autorisationer og adgang i en virksomhed. Løsningen er et koncept, der omfatter organisatoriske foranstaltninger og specifikationer samt passende sikkerhedsfunktioner. Et adgangsautorisationssystem som PITreader er det passende hardwaremodul til dette, som kompletteres med de supplerende softwarekomponenter til organisation af brugerne og transponderne. Yderligere komponenter

fra beskyttelsesdørssystem, styring og software samt funktioner som driftstypevalg udvider løsningen, så den bliver til et helhedsorienteret Safety- og Industrial Security-koncept. For brugeren er det nemt at håndtere, nemlig med den enkelte nøgle i hånden.

Tegn: 14.675

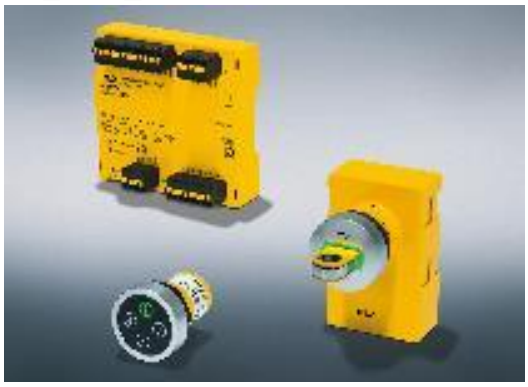
## Billeder

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



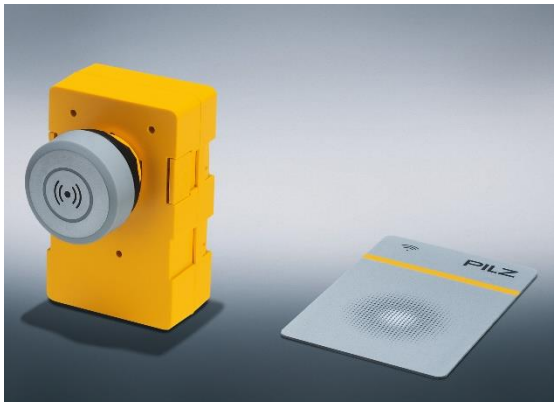
Billedtekst: Omfattende Identification and Access Management regulerer adgangen til applikationen og sørger dermed for sikkerhedsfunktioners og -foranstaltningers integritet – inklusive Safety og Industrial Security.

**Billede 2:**
F_Press_PITmode_fusion_402251_PIT_oe_4023311_P1_B_8_2_cold_2020_01 (Pilz GmbH & Co. KG)



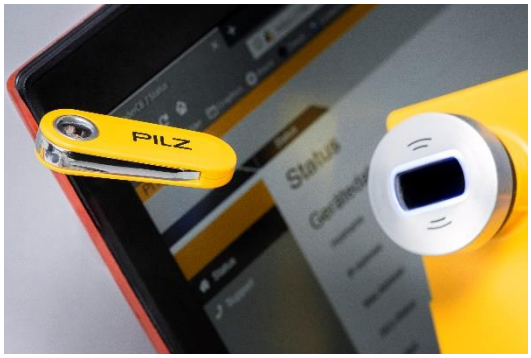
Billedtekst: PITmode fusion fra Pilz er et modulopbygget driftstypevælger- og adgangsautorisationssystem, som kombinerer Safety og Industrial Security i ét system.

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



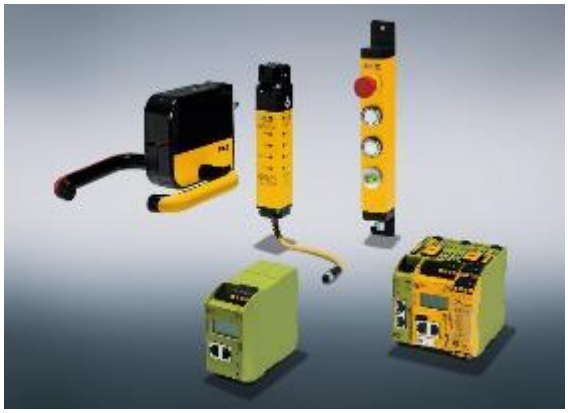

Billedtekst: Adgangsautorisationssystemet PITreader card unit fra Pilz tilbyder med de RFID-kompatible kort PITreader card og PITreader sticker flere formater til implementering af et effektivt adgangsautorisationssystem.

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




Billedtekst: RFID-transpondernøglerne indlæses og initialiseres i PITreader. Tildelingen af adgangsautorisationer og driftstyper foretages nemt via den tilhørende webserver.

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



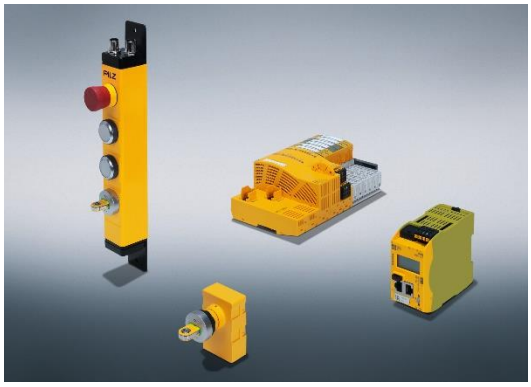
Billedtekst: Den fleksible kombination af beskyttelsesdørssystemet PSENmlock med det passende dørgrebsmodul (øverst til venstre), knapenheden PITgatebox med integreret adgangsautorisationssystem PITreader (øverst til højre) samt den konfigurerbare, lille styring PNOZmulti 2 (nederst til højre) og diagnoseløsningen Safety Device Diagnostics (nederst til venstre) giver en komplet beskyttelsesdørsløsning med adgangsautorisation.

**Boks: Den digitale vedligeholdelsessikring Key-in-pocket**

Ud over ren adgangsautorisation kan PITreader anvendes sammen med en Pilz-styring som f.eks. den konfigurerbare, lille styring PNOZmulti 2 eller automatiseringssystemet PSS 4000 til den effektive, digitale vedligeholdelsessikring "Key-in-pocket". Den sørger for, at maskinen ikke genstarter under vedligeholdelsesarbejde, og at uautoriserede personer ikke får adgang. I praksis fungerer det på følgende måde: En eller flere brugere, som er autoriseret til vedligeholdelsesarbejde, autentificerer sig ved anlægget. Efter gennemført autentificering gemmes der i Pilz-styringen et personligt Security-ID for brugeren på en sikker liste. Nu kan maskinen slukkes, beskyttelsesdøren åbnes og maskinen betrædes. Imens bliver RFID-nøglerne "i bukselommen" hos de forskellige brugere. Når vedligeholdelsen er gennemført og farezonen forladt, logger alle personer ud, Security-ID'erne fjernes fra Pilz-styringens sikre liste, og maskinen kan startes igen. I modsætning til en vedligeholdelsessikring med mekaniske nøgler kan anlægget betrædes eller forlades gennem en vilkårlig beskyttelsesdør. På denne måde giver "Key-in-pocket" personalet større fleksibilitet og tidsbesparelse i forbindelse med vedligeholdelse. Den digitale vedligeholdelsessikring er specielt konstrueret til maskiner med farlige områder, som er sikret med beskyttelsesbarrierer. Den driftsansvarlige ved altid, hvem der får adgang til hvilken opgave, og kan også tildele midlertidige autorisationer.

1.578 tegn

**Billede af boks med Key-in-pocket:**
F_Press_Group_PIT_Key_in_pocket_solutions_P1_B8_2_cold.jpg (© Pilz GmbH & Co. KG)



Billedtekst: Vedligeholdelsessikringen "Key-in-pocket" består af adgangsautorisationssystemet PITreader, knapenheden PITgatebox samt en Pilz-styring som f.eks. den konfigurerbare, lille styring PNOZmulti 2 eller automatiseringssystemet PSS 4000.

**Boks: Tildeling og vedligeholdelse af autorisationer**

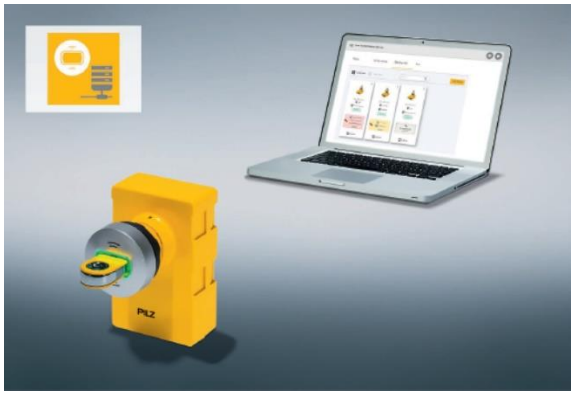
Hvis der anvendes et adgangsautorisationssystem i virksomheden, er regelmæssig vedligeholdelse og administration af autorisationerne og brugerdataene afgørende for at give et højt sikkerhedsniveau. Derfor stiller Pilz softwareværktøjet PIT Transponder Manager (PTM) til rådighed: Administratoren administrerer sine brugerindstillinger, blokeringslister og brugerdata på en grafisk brugerflade. De individuelle brugerautorisationer overføres i få trin til transpondernøglen med forkonfigurerede skabeloner og en importfunktion.

Hvis der anvendes flere PITmode eller PITreader i en virksomhed, organiseres disse enheder med softwaren PIT User Authentication Service (UAS) fra Pilz. Den gør det muligt at forbinde managementsystemer som PTM eller en anden

brugeradministrationssoftware til PITreader. PIT UAS har en central autorisationsdatabase for brugerne, som gør det muligt at importere og tildele data fra PTM til alle PITreader. Administratorer kan få vist den aktuelle status for alle PITreader og en diagnoseliste. Dette giver et hurtigt overblik, også når der anvendes flere enheder.

1.218 tegn

**Billede af boks med brugeradministration:**
((Billede følger)).jpg (© Pilz GmbH & Co. KG)



Billedtekst: Hvis der anvendes flere udlæsningsenheder af typen PITreader i en virksomhed, organiseres disse enheder
med User Authentication Service (UAS).

**Pilz-gruppen**

Pilz-gruppen er en global udbyder af produkter, systemer og serviceydelser til automatiseringsteknik. Familievirksomheden med hovedafdeling i Ostfildern beskæftiger ca. 2.500 medarbejdere. Pilz skaber verdensomspændende sikkerhed for mennesker, maskiner og miljø med 42 datterselskaber og filialer. Den teknologisk førende virksomhed tilbyder komplette automatiseringsløsninger, der omfatter sensorteknologi, styringsteknik og drevteknik – inklusive systemer til industriel kommunikation, diagnose og visualisering. Et internationalt program af serviceydelser med rådgivning, udvikling og kurser afrunder porteføljen. Løsninger fra Pilz anvendes ikke kun inden for maskin- og anlægsproduktion, men også i forbindelse med intralogistik, jernbaneteknik og robotteknologi.

www.pilz.com

**Kontaktpersoner for pressen:**

**Martin Kurth**

Erhvervs- og fagpresse
Tlf.: +49 711 3409-158
m.kurth@pilz.de

**Sabrina Schilling**

Fagpresse

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

**Sabine Karrer**

Fag- og erhvervspresse
Tlf.: +49 711 3409-7009
s.skaletz-karrer@pilz.de

**Hansjörg Sperling-Wohlgemuth**
Kongres- og foredragsadministration
Tlf.: +49 711 3409-239
h.sperling@pilz.de

**Jenny Skarman**

Fagpresse

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