Taustatietoa

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

Kokonaisvaltaisissa turvallisuuskonsepteissa keskitytään kulunhallintaan koneen Safetyn ja Industrial Securityn varmistamiseksi

Kokonaisvaltainen turvallisuus yksilöllisten valtuutusten hallinnan avulla

Ostfildern, helmikuu 2023 - **Aina kun haluamme suojella jotain arvokasta, käytämme ovia, lukkoja ja avaimia rajoittaaksemme pääsyä. Sama pätee kaikkein tärkeimpään: Omaan turvallisuutemme kaikissa ilmenemismuodoissaan. Teollisuusympäristössä on tärkeää suojella toisaalta ihmisiä (Safety) ja toisaalta koneita ja arkaluonteisia tietoja (Industrial Security). Turvallisuuden puutteella voi olla erilaisia seurauksia: Käyttövirheistä onnettomuuteen tai vakavaan kyberhyökkäykseen. Kokonaisvaltainen tunnistus- ja käyttöoikeuksien hallinta, jolla säännellään selkeästi käyttöoikeuksia ja -valtuuksia, edistää kokonaisvaltaista turvallisuuskäsitystä ja tehokkaita prosesseja.**

Tuotantoympäristössä ne ovat tuttu näky: Erottavat suojavarusteet, jotka antavat ihmisille selkeän signaalin siitä, että turvaportin takana on herkkä alue ja että varovaisuus on tarpeen. Ihmiset pääsevät käsiksi aidan takana olevaan prosessiin käyttöliittymän (HMI) tai avaimen avulla. Mutta entä jos henkilöllä ei ole siihen pätevyyttä tai lupaa ja hän saattaa itsensä tai muut vaaraan? Myös pahantahtoinen henkilö voi manipuloida prosessia - joko suoraan koneella tai etäyhteyden kautta. Kulkuoikeuksien hallinta osoittaa, että Safety ja Industrial Security liittyvät läheisesti toisiinsa. Lisäksi Industrial Security varmistaa koneen turvallisuuden eheyden. Se tarjoaa esimerkiksi tuotannossa oleville koneille tai järjestelmille suojaa ulkopuolelta tulevaa luvatonta pääsyä vastaan ja suojaa arkaluonteisia prosessi- ja konetietoja väärentämiseltä, häviämiseltä ja sisäiseltä luvattomalta käytöltä. Niihin sisältyvät sekä tahalliset hyökkäykset että tahattomat Security-vahingot.

Safety ja Industrial Security kuuluvat yhteen

Koneiden ja laitosten operaattoreiden on tarpeen määrittää ja jakaa selkeästi tehtävät ja valtuudet eli luoda tunnistaminen ja käyttöoikeuksien hallinta. Tämä tarkoittaa toisaalta organisatorisia toimenpiteitä, kuten työohjeita tai prosessien säännöllistä tarkastamista, ja toisaalta sopivien turvallisuusratkaisujen sisällyttämistä tuotantoympäristöön. Jos tällaiset toimenpiteet lyödään laimin, yrityksen vastuuhenkilöt voidaan saattaa henkilökohtaiseen vastuuseen onnettomuuksien tai tuotannonmenetysten yhteydessä. Toistaiseksi tällaiset turvallisuusratkaisut ovat perustuneet vapaaehtoisuuteen, eikä monissa paikoissa ole nähty tarvetta toimenpiteisiin. Lainsäätäjä on kuitenkin nyt tunnustanut, että Safety ja Security liittyvät toisiinsa. Uudessa koneasetuksessa turvatoimenpiteet ovat sen vuoksi pakollisia.

Toimintatilat lisäävät turvallisuutta

Lisäksi useissa C-standardeissa on jo määritelty, että eri toimintatilojen on sisällettävä myös vastaavat turvatoiminnot. Toimintatilat voivat olla esimerkiksi automaattikäyttö, manuaalinen käyttö rajoitetuissa olosuhteissa tai huoltotila. Työstökeskuksia ja erikoiskoneita koskevan standardin EN ISO 16090-1 mukaan vähintään kaksi näistä toimintatiloista on pakollisia toiminnallisen turvallisuuden varmistamiseksi. On tärkeää, että vain yksi toimintatila on valittu ja aktiivinen kerrallaan ja että se näkyy selvästi.

Estää anonyymin käytön

Mutta miten päätetään, ketkä henkilöt pääsevät käyttämään mitä toimintatilaa tai saavat edes muuttaa toimintatilaa? Tätä varten määritellään erilaisia henkilöryhmiä, kuten koneen kanssa kosketuksiin joutuva käyttö-, puhdistus- tai huoltohenkilöstö. Tämän jälkeen työntekijät

jaetaan ryhmiin heidän tehtävänsä tai pätevyytensä mukaan. Yrityksen koosta riippuen valtuuksia tai käyttöoikeuksia voidaan antaa myös eri käyttäjäryhmille tai esimerkiksi konetyypille, jota käytetään koko konsernissa. Riskinarvioinnin aikana turvallisuusasiantuntijat arvioivat ja arvioivat analysoivat nimettömän hyökkäyksen riskin kunkin vaaran osalta. Tämän jälkeen määritellään tekniikan tason mukaiset ja yhdenmukaistettujen standardien mukaiset toimenpiteet, jotka vähentävät riskiä.

Käyttäjäystävällisyys estää manipuloinnin

Toimenpiteitä toteutettaessa on tärkeää varmistaa, että ne ovat käyttäjille käyttökelpoisia, jotta manipulointi voidaan sulkea pois. Koneenrakentajien kohdalla tämä koskee jo kehitysprosessia. Intuitiiviset käyttöjärjestelmät, joita käyttäjien on helppo käsitellä, estävät turvatoimien laiminlyönnin tai koneiden virheellisen käytön. Lisäksi hyvin suunniteltu turvajärjestelmä edistää tehokasta toimintaa ilman tarpeettomia seisokkeja. ”Suojalaitteiden ohittaminen" on EN ISO 14119 -standardin keskeinen kohta. Standardissa määritellään turvaporttijärjestelmien suunnittelua ja valintaa ohjaavat periaatteet ja tarjotaan siten konkreettista apua manipuloinnin välttämiseksi.

Yksilöllinen turvallisuuskonsepti

Jotta varmistetaan, että kulkuovien tahallinen tai vahingossa tapahtuva avaaminen ei aiheuta vaaratilanteita, ne on suojattu turvajärjestelmällä. Turvallisuuden osalta pääpaino on työntekijän suojaamisessa vaarallisilta koneen liikkeiltä. Tarvitaan räätälöity turvallisuuskonsepti riippuen siitä, onko kyseessä itsenäinen kone vai monimutkainen, ketjutettu laitos. Jos koneissa on vaarallista jälkikäyntiä, suojalukituksella on tärkeä merkitys; jos ovista voidaan kulkea, evakuointiavaus on välttämätön.

Räätälöity suojaus turvaoville

Modulaarisessa turvaporttijärjestelmässä, kuten Pilzin PSENmlockissa, yhdistyvät turvallinen turvaportin valvonta ja turvalukitus samaan järjestelmään, ja siinä on myös turvatoimintoja, kuten hätäpysäytys, evakuointiavaus ja mekaaninen uudelleenkäynnistyslukitus. Se tarjoaa joustavuutta ja hajautettua älykkyyttä monien erilaisten sovellusten suojaamiseen. Yksilöllinen ratkaisu koostuu antureiden, evakuointiavauksen, ovenkahvojen sekä käyttö- ja painikeyksikön yhdistelmästä. Käyttäjät voivat sovelluksesta riippuen luoda oman yksilöllisen turvaporttiratkaisunsa. Industrial Securityn vaatimusten täyttämiseksi tarkastellaan nyt käyttöoikeuksia ja valtuutuksia.

Safety ja Industrial Security -järjestelmä

Suojaus luvattomalta käytöltä voidaan käytännössä toteuttaa toimintatilan valinta- ja kulunhallintajärjestelmällä. Siinä yhdistyvät Safety ja Industrial Security: Käyttötavan valinta ja koneen kulkuoikeuksien valvonta. Yhden tällaisen ratkaisun tarjoavat Pilz PITmode -tuoteryhmän laitteet, jotka mahdollistavat vaihtamisen määriteltyjen toimintatilojen välillä ja kulkuoikeuksien hallinnan. Käyttö on intuitiivista, koska jokainen käyttäjä saa yksilöllisesti koodatun transponderin, joka mahdollistaa käyttäjän yksilöllisen tunnistautumisen ja estää peukaloinnin.

Hallitse käyttöoikeuksia ja toimintatiloja yksilöllisesti

Turvallisuuskonseptin mukauttamiseksi PITmode on saatavana eri versioina. PITmode on kompakti all-in-one-yksikkö, joka sisältää painikkeet toimintatilan valintaa varten sekä arviointiyksikön, joka mahdollistaa tilaa säästävän asennuksen. Modulaarinen PITmode fusion -järjestelmä puolestaan koostuu RFID-tekniikalla varustetusta lukuyksiköstä PITreader ja integroidusta verkkopalvelimesta sekä

turvallisesta arviointiyksiköstä Safe Evaluation Unit (SEU). Kolmas vaihtoehto on PITmode flex: Tässä tapauksessa PITreader käytetään yhdessä Pilz-ohjausjärjestelmän ja ohjelmistomoduulin kanssa turvallista arviointia varten. Modulaarisen rakenteen ansiosta kulkuoikeuksien hallinta a toimintatilan valinta voidaan integroida olemassa olevien ohjauspaneelien suunnitteluun. Olemassa olevia painikkeita voidaan käyttää toimintatilan valitsemiseen, minkä ansiosta käyttäjä voi käyttää laitetta helposti. Tunnistaminen transponderin avulla tapahtuu lukuyksikössä PITreader. PITmode ja PITmode fusion tarjoavat toiminnallisesti turvallisen toimintatilan valinnan ja kulkuoikeuksien hallinnan luokkaan PL d:hen asti.

Yksinkertainen todennus - myös etänä

Toimintatilan valitsemiseksi käyttäjä kytkee transponderinsa suoraan PITmode-tilaan ja painaa toimintatilaa varten määriteltyä painiketta tai käyttöliittymän vastaavaa painiketta. Jos valtuutus on olemassa, käyttäjä pääsee prosessiin. Sama pätee, kun huoltotyöntekijä haluaa käyttää konetta etänä: Etähuolto voi alkaa vasta, kun paikalla oleva henkilö antaa järjestelmään vastaavan vapautuksen. Huoltotöiden jälkeen tämä käyttö estetään uudelleen ennen koneen käynnistämistä uudelleen. Näin voidaan sulkea pois luvattomien henkilöiden suorittama manipulointi tai portti, joka on vahingossa jätetty auki huoltotöiden jälkeen. Operaattorit lisäävät Industrial Securityä, koska he valvovat, kuka saa minkä valtuutuksen ja siten pääsyn prosessiin.

Kokonaisratkaisu kulkuoikeuksien hallinnalla

Jos halutaan toteuttaa vain kulunvalvonta, PITreader voidaan käyttää myös yksinään tai yhdessä Pilz-ohjauksen kanssa kulunvalvontajärjestelmänä. Yhdessä konfiguroitavan PNOZmulti 2 -

pienohjauksen kanssa järjestelmänvalvoja konfiguroi koneiden ja laitosten käyttöoikeudet yksinkertaisesti "raahaamalla ja pudottamalla" siihen liittyvää konfigurointityökalua PNOZmulti Configurator käyttäen. Ne siirretään sitten RFID-transponderiavaimella lukuyksikköön PITreader. OPC UA -standardin integroinnin ansiosta PITreader S-versiota voidaan käyttää itsenäisesti Pilz-ohjausjärjestelmästä valmistajista riippumatta. Kuten jo mainittiin, PITmode-yksiköt voidaan helposti integroida olemassa oleviin ohjauspaneeleihin.

Valinta avaimen, kortin tai tarran välillä

PITreader card unit -vaihtoehto tarjoaa lisää joustavuutta operaattoreille ja käyttäjille: RFID-kortteja ja -tarroja voidaan käyttää yhdessä RFID-transponderiavaimen kanssa tai sen sijaan. Jos yrityksessä on jo käytössä RFID-kortteja, niitä voidaan käyttää myös yhdessä PITreader card unitin kanssa: Käyttäjä tarvitsee tällöin vain yhden kortin useita toimintoja varten. RFID-transpondereiden - olipa kyseessä avain, kortti tai tarra - etuna on periaatteessa se, että yhteen transponderiin on yhdistetty useita toimintoja, ja näin voidaan yhdistää kokonainen mekaaninen avainnippu. Tämä on kätevää käyttäjälle, koska hänen tarvitsee kantaa mukanaan vain yhtä tunnistusvälinettä. Järjestelmänvalvojat puolestaan säästävät aikaa ja vaivaa avainten hallinnoinnissa ja ylläpidossa.

Plussaa Securitylle

Myös Security näkökohdat otetaan huomioon käyttäjän todennuksen, pätevöitymisen ja suojauksen osalta. Jos kaikista turvatoimista huolimatta koneessa tapahtuu onnettomuus tai turvallisuusvälikohtaus, RFID-transponderi voidaan lukea, jotta voidaan jäljittää, kuka on tehnyt minkä muutoksen. Jos tämä valinnainen toiminto halutaan, valvontajärjestelmä tallentaa myös

käytön ajankohdan sisäiseen, muuttumattomaan kirjausketjuun (tapahtumalokiin), joka perustuu todennukseen.

Huolellinen hallinto on avainasemassa

Varmistaakseen Safetyn ja Industrial Securityn koko sovelluksen elinkaaren ajan järjestelmänvalvojat kiinnittävät paljon huomiota valtuutusten ylläpitoon. Jotta hallinnointi olisi yksinkertaista, Pilzin sopivat ohjelmistotyökalut tukevat käyttäjien ja transponderien organisointia. Esimerkiksi pieni RFID-avain voi kätkeä sisäänsä monimutkaisia valtuutusmatriiseja tai konsernin laajuisia määräyksiä. Integroidun PITreader -verkkopalvelimen avulla ylläpitäjät ohjelmoivat PITmode- tai PITreader -järjestelmiin kuuluvat RFID-tunnistimet ja tallentavat niihin käyttäjätiedot ja valtuutukset. Kaikki tärkeät asetukset tehdään suoraan näyttölaitteessa, mikä nopeuttaa käyttöönottoa, mukaan lukien rajapintojen konfigurointi.

Rajoita pääsyä rajapintoihin

Tunnistus- ja kulunhallintamahdollisuudet ulottuvat myös erityisten teollisten USB-porttien vapautukseen, jotka ovat yksi tärkeimmistä tietoturvaloukkausten väylistä. Tätä tarkoitusta varten kulunhallintajärjestelmä PITreader yhdistetään esimerkiksi PIT oe USB:n kaltaiseen ohjauselementtiin, jossa on aktivoitava USB 2.0 -isäntäliitäntä. Tämä ratkaisu mahdollistaa manipulaatiosuojatun ohjelmien asennuksen, tietojen poimimisen ja näppäimistön tai tietokonehiiren liittämisen. Tämä johtuu siitä, että rajapinta aktivoidaan vain asianmukaisella valtuutuksella, mikä suojaa tuotannon tietovirtaa. Yhdessä Pilzin SecurityBridgen kaltaisen teollisen palomuurin kanssa, joka valvoo tietoliikennettä teollisuusautomaatioverkossa, koneet voidaan näin suojata luvattomalta käytöltä ja manipuloinnilta.

Olemassa olevat koneet – safe ja secure

Jos olemassa olevat koneet on saatettava ajan tasalle tai jos riskinarvioinnin yhteydessä on havaittu tarvetta toimenpiteisiin, kulunhallintajärjestelmä PITreader voidaan helposti asentaa jälkiasennuksena: Laite voidaan asentaa suoraan avainkytkimille tarkoitettuihin standardoituihin ulostuloihin, joiden halkaisija on 22,5 millimetriä. Tarvittava turvatoiminto voidaan määrittää suoraan Pilz-ohjauksen avulla. Jos käytössä on kolmannen osapuolen valvontajärjestelmä, PITmode fusionia käytetään kulunhallinnan ja toimintatilan valinnan analysointiin. Riippuen siitä, mikä transponderiväline on kyseessä, tunnistautumiseen voidaan käyttää yrityksen nykyisiä RFID-avainkortteja.

Loppupäätelmä

Turvallisuuden suojaamiseksi on tarpeen suunnitella turvallisuuskäsitteet kokonaisvaltaisesti ja tarkastella niitä säännöllisesti niiden ajantasaisuuden varmistamiseksi. Tärkeä osatekijä on tunnistaminen ja käyttöoikeuksien hallinta, jolla säännellään selkeästi valtuutuksia ja käyttöoikeuksia yrityksessä. Ratkaisu on konsepti, joka sisältää organisatorisia toimenpiteitä ja eritelmiä sekä asianmukaisia turvatoimintoja. Se voidaan toteuttaa PITreader kulunhallintajärjestelmällä ja täydentävillä ohjelmistokomponenteilla käyttäjien ja transpondereiden organisoimiseksi. Muut turvaporttijärjestelmän, ohjausjärjestelmän ja ohjelmiston komponentit sekä toiminnot, kuten toimintatilan valinta, laajentavat ratkaisua kokonaisvaltaiseksi turvallisuus- ja teollisuusturvakonseptiksi. Käyttäjän on helppo käsitellä sitä yksilöllisen avaimen avulla.

Zeichen: 14.675

Abbildungen

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

BU: Kokonaisvaltainen tunnistus ja kulunhallinta sääntelee selkeästi käyttöoikeuksia ja -valtuuksia ja varmistaa siten turvallisuustoimintojen ja -toimenpiteiden eheyden - mukaan lukien Safety ja Industrial Security.

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

BU: Pilzin PITmode fusion on modulaarinen toimintatilan valinta- ja kulkulupajärjestelmä, jossa yhdistyvät turvallisuus ja teollinen turvallisuus yhdessä järjestelmässä.

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

BU: Pilzin kulunhallintajärjestelmä PITreader card unit tarjoaa uusia muotoja tehokkaan hallintajärjestelmän toteuttamiseen RFID-korttien PITreader card ja PITreader sticker avulla.

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

BU: PITreader lukee ja oppii transponderiavaimen. Kulkuoikeuksien ja toimintatilojen määrittäminen onnistuu helposti liitetyn verkkopalvelimen kautta.

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

BU: PSENmlock-turvaporttijärjestelmän, siihen sopivan ovenkahvamoduulin (vasemmalla ylhäällä), PITgatebox-painikeyksikön (alhaalla oikealla), integroidun PITreader kulunhallintajärjestelmän ja konfiguroitavan PNOZmulti 2 -pienohjausjärjestelmän sekä Safety Device Diagnostics -diagnostiikkaratkaisun joustava yhdistelmä (alhaalla vasemmalla) tarjoaa täydellisen turvaporttiratkaisun kulkuoikeuksien hallinnalla.

Kasten: Digitaalinen huoltovarmistus Key-in-pocket

Pelkkien kulkulupien lisäksi PITreader voidaan käyttää Pilz-ohjausjärjestelmän, kuten konfiguroitavan PNOZmulti 2 -pienohjauksen tai PSS 4000 -automaatiojärjestelmän kanssa tehokkaaseen digitaaliseen "avain taskussa" -huoltosuojaukseen. Se varmistaa, että kone ei käynnisty uudelleen huoltotöiden aikana ja että asiattomat henkilöt eivät pääse koneeseen käsiksi. Käytännössä se toimii näin: Yksi tai useampi huoltotyöhön valtuutettu käyttäjä todentaa itsensä yksikössä. Onnistuneen todennuksen jälkeen käyttäjän henkilökohtainen turvatunnus tallennetaan ohjausyksikön turvaluetteloon. Kone voidaan nyt kytkeä pois päältä, turvaluukku avata ja koneeseen voidaan mennä sisään. Samalla RFID-avaimet pysyvät käyttäjien taskussa - "avain taskussa". Huoltotöiden suorittamisen ja vaaravyöhykkeeltä poistumisen jälkeen kaikki työntekijät kirjautuvat ulos, turvatunnukset poistetaan Pilz-ohjausjärjestelmän turvaluettelosta ja kone voidaan käynnistää uudelleen. Toisin kuin mekaanisilla avaimilla toteutetussa huoltovarmistuksessa, järjestelmään voidaan mennä sisään tai sieltä poistua mistä tahansa turvaovesta. ”Key-in-pocket" tarjoaa siten henkilöstölle enemmän joustavuutta ja ajansäästöä huollossa. Digitaalinen huoltovarmistus on suunniteltu erityisesti koneisiin, joissa on suoja-aidoilla suojattuja vaarallisia alueita. Operaattori tietää aina, kenellä on pääsy mihinkin tehtävään, ja hän voi myös antaa tilapäisiä käyttöoikeuksia.

1 578 merkkiä

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

BU: Key-in-pocket-huoltovarmistus koostuu PITreader kulunhallintajärjestelmästä, PITgatebox-painikeyksiköstä ja Pilz-ohjausjärjestelmästä, kuten konfiguroitavasta PNOZmulti 2 -pienohjauksesta tai PSS 4000 -automaatiojärjestelmästä.

Kasten: Valtuuksien myöntäminen ja ylläpito

Jos yrityksessä käytetään kulunhallintajärjestelmää, valtuuksien ja käyttäjätietojen säännöllinen ylläpito ja hallinnointi on keskeistä korkean turvallisuustason varmistamiseksi. Pilz tarjoaa tähän tarkoitukseen PIT Transponder Manager (PTM) -ohjelmiston: Ylläpitäjä hallinnoi käyttäjäasetuksia, estolistoja ja käyttäjätietoja graafisessa käyttöliittymässä. Ennalta määritettyjen mallien ja tuontitoiminnon avulla yksittäisten käyttäjien valtuutukset kirjoitetaan transponderiavaimeen muutamassa vaiheessa.

Jos yrityksessä on käytössä useita PITmode tai PITreader -laitteita, ne organisoidaan PIT User Authentication Service (UAS) -ohjelmistotyökalulla. Sen avulla hallintajärjestelmät, kuten PTM tai muut käyttäjähallintaohjelmistot, voidaan liittää PITreader:n kanssa. PIT UAS:ssa on keskitetty valtuutustietokanta käyttäjiä varten, minkä ansiosta PTM:stä voidaan tuoda ja määrittää tietoja kaikille PITreader:lle. Ylläpitäjät voivat tarkastella kaikkien PITreader

nykytilaa ja näyttää diagnoosiluettelon. Tämä takaa nopean yleiskatsauksen, vaikka käytössä olisi useita yksiköitä.

1 218 merkkiä

Abb. Kasten Benutzerverwaltung:
((Bild folgt)).jpg (© Pilz GmbH & Co. KG)

BU: Jos yrityksessä on useita PITreader lukulaitteita,
nämä laitteet
järjestetään User Authentication Service (UAS) -palvelun avulla.

Pilz-konserni

Pilz-konserni on automaatiotekniikan tuotteiden, järjestelmien ja palvelujen globaali toimittaja. Pilz-konsernin pääkonttori sijaitsee Ostfildernissa ja se työllistää noin 2500 ihmistä. Pilz varmistaa ihmisten, koneiden ja ympäristön turvallisuuden kaikkialla maailmassa 42 tytäryhtiön voimin. Teknologiajohtaja tarjoaa kokonaisvaltaisia automaatioratkaisuja, jotka sisältävät anturi, ohjaus- ja käyttötekniikkaa sekä teollisuusviestintä-, diagnostiikka- ja visualisointijärjestelmiä. Salkun täydentää kansainvälinen palvelutarjonta, johon sisältyy neuvonta, suunnittelu ja koulutus. Pilzin ratkaisuja käytetään lukuisilla muilla aloilla kuin kone- ja laitostekniikassa, kuten intralogistiikassa, rautatietekniikassa ja robotiikassa.

www.pilz.com

Yhteystiedot lehdistölle:

Martin Kurth

Yritys- ja ammattilehdistö
Puh: +49 711 3409-158
m.kurth@pilz.de

Sabrina Schilling

Ammattilehdistö

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

Sabine Karrer

Yritys- ja ammattilehdistö
Puh: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Hansjörg Sperling-Wohlgemuth
Kongressi- ja luentohallinto
Puh: +49 711 3409-239
h.sperling@pilz.de

Jenny Skarman

Ammattilehdistö

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