Geçmiş bilgiler

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

Bütünsel emniyet konseptleri, makinede emniyet ve endüstriyel korumayı sağlamak için erişime odaklanır

Kişiselleştirilmiş izin yönetimi ile bütünsel emniyet

Ostfildern, Şubat 2023 – **Önemli bir şeyleri korumak istediğimiz her yerde erişimi sınırlamak için kapılar, kilitler ve anahtarlar kullanıyoruz. Bu aynı zamanda nihai varlık için de geçerlidir: Her türlü emniyet. Endüstriyel ortamda, amaç bir yandan insanları koruyarak emniyetini sağlamak, diğer yandan makineleri ve hassas verileri koruyarak endüstriyel korumayı sağlamaktır. Emniyet ve güvenlik eksikliğinin çeşitli sonuçları olabilir: Yanlış çalışmadan kazaya ve ciddi bir siber saldırıya kadar. Erişim ve giriş izinlerini açıkça tanımlayan Kapsamlı Yetkilendirme ve Erişim Yönetimi, bütünsel bir emniyet ve endüstriyel koruma konseptine ve verimli prosedürlere katkıda bulunur.**

Üretim ortamında bunlar tanıdık bir manzaradır: Emniyet kapısının arkasında tehlikeli bir alan olduğuna ve dikkat edilmesi gerektiğine dair insanlara net bir sinyal veren korumalar. İnsanlar, emniyet çitinin arkasındaki sürece bir insan makine arayüzü (HMI) veya bir anahtar aracılığıyla erişebilir. Peki ya kişi bunun için hiç nitelikli veya yetkili değilse ve kendisini veya diğer insanları tehlikeye atarsa? Kötü niyetli bir kişi, doğrudan makinede veya uzaktan erişim yoluyla bu sürece müdahale edebilir. Erişim izni konusu, emniyet ve endüstriyel korumanın yakından bağlantılı olduğunu göstermektedir. Veya bir adım daha ileri giderek: Endüstriyel koruma, makinedeki emniyetin bütünlüğünü sağlar. Örneğin, üretimdeki tesis veya makinelerin dışarıdan yetkisiz erişime karşı korunmasını sağlar ve hassas proses ve makine verilerini içeride tahrifat, kayıp ve yetkisiz erişime karşı korur. Bu, açık saldırıların yanı sıra kasıtsız güvenlik olaylarını da içerir.

Emniyet ve endüstriyel koruma birlikte yürür

Tesis ve makine operatörleri, Yetkilendirme ve Erişim Yönetimini kurarak, görevleri ve izinleri açıkça düzenleyebilmeli ve atayabilmelidir. Bu, yalnızca iş talimatları veya prosedürlerin düzenli kontrolleri gibi organizasyonel önlemler değil, aynı zamanda üretim ortamına uygun güvenlik çözümlerinin entegrasyonu anlamına da gelir. Bu önlemler ihmal edilirse bir şirketteki sorumlu taraflar kaza veya durma süreleri durumunda kişisel olarak sorumlu tutulabilir. Bu tür güvenlik çözümleri daha önce gönüllülük esasına dayanıyordu; birçok yerde eyleme gerek olmadığı tespit edildi. Bununla birlikte, emniyet ve güvenlik arasındaki bu bağlantı o zamandan beri kanun koyucular tarafından kabul edilmiştir. Bu nedenle yeni Makine Yönetmeliği zorunlu güvenlik önlemlerini öngörmektedir.

Çalışma modları emniyeti artırır

Çeşitli C standartları, farklı çalışma modlarının da ilgili emniyet fonksiyonlarını içermesi gerektiğini öngörmektedir. Çalışma modları, örneğin otomatik mod, kısıtlı koşullar altında manuel müdahale veya servis modu olabilir. EN ISO 16090-1, fonksiyonel emniyeti garanti altına almak için bu çalışma modlarından en az ikisini işleme merkezleri ve özel amaçlı makineler için zorunlu olarak şart koşar. Her seferde yalnızca bir çalışma modunun seçilmesi ve etkin olması ve bunun açıkça görüntülenmesi çok önemlidir.

Bilinmeyen erişimi engelleme

Ancak, hangi kişilerin hangi çalışma modunda erişime sahip olacağına veya hatta çalışma modunu değiştirebileceğine nasıl karar veriyorsunuz? Bu amaçla, makine ile temas halinde olan, örneğin çalıştırma, temizleme veya bakım personeli gibi farklı çalışan grupları tanımlanır. Çalışanlar daha sonra görevlerine veya

niteliklerine göre gruplara atanır. Şirketin büyüklüğüne bağlı olarak, farklı kullanıcı grupları veya örneğin şirket genelinde kullanılan bir makine türü için etkinleştirmeler veya erişim hakları da verilebilir. Risk değerlendirmesi sırasında, emniyet uzmanları her tehlike için bilinmeyen erişim riskini değerlendirir ve derecelendirir. Riski azaltmaya yönelik önlemler, son olarak, en son teknolojiye göre ve uyumlaştırılmış standartlar dikkate alınarak tanımlanır.

Kullanıcı dostu olması manipülasyonu önler

Önlemleri uygularken, manipülasyonu önlemek amacıyla şirketteki kullanıcılar için kullanım kolaylığı ve kullanılabilirlik sağlamak önemlidir. Bu, makine üreticileri için geliştirme sürecinde zaten geçerlidir. Kullanıcıların kullanımı kolay olan sezgisel işletim sistemleri, çalışanların emniyet önlemlerini atlamasını veya makineleri yanlış çalıştırmasını önler. İyi düşünülmüş bir emniyet sistemi, gereksiz durma süreleri olmadan verimli prosedürlere de katkıda bulunur. Bu "Korumaların engellenmesi" sorunu, EN ISO 14119'un önemli bir yönüdür. Standart, emniyetli kapı sistemlerinin tasarımı ve seçimi için yol gösterici ilkeleri tanımlar ve bu nedenle manipülasyonun nasıl önleneceği konusunda pratik rehberlik sunar.

Bireysel emniyet konsepti

Erişim kapılarının kasıtlı olarak veya kazara açılması durumunda herhangi bir tehlikenin ortaya çıkmamasını sağlamak için bunlar bir emniyet kapısı sistemi kullanılarak korunur. Emniyet açısından, buradaki odak noktası, çalışanın tehlikeli makine hareketlerine karşı korunmasıdır. Bağımsız bir makine mi yoksa birbirine bağlı karmaşık tesisler mi olduğuna bağlı olarak, uygun şekilde uyarlanmış bir emniyet konsepti gereklidir. Makinelerde tehlikeli bir

aşırı çalışma varsa, koruma kilidi önemli olacaktır. Kapılara erişilebiliyorsa, bir kaçış kilidi şarttır.

Emniyet kapılarının özel olarak korunması

Pilz'in PSENmlock gibi modüler emniyetli kapı sistemi, emniyet kapısı izlemeyi emniyetli koruma kilidi ile tek bir sistemde birleştirir ve ayrıca acil durdurma, kapı koruma kilidi ve mekanik yeniden başlatma kilidi gibi emniyet fonksiyonları sağlar. Çok çeşitli uygulamaları korumak için esneklik ve merkezi olmayan akıllı çözüm sunar. Bireysel bir çözüm, sensörler, kapı kilidi koruma, kapı kolları ile bir kontrol ve buton ünitesi kombinasyonundan oluşur. Uygulamaya bağlı olarak, kullanıcılar kendi özelleştirilmiş emniyet kapısı çözümlerini tasarlarlar. Endüstriyel koruma taleplerini karşılamak için artık erişim ve izinlere odaklanılmaktadır.

Emniyet ve endüstriyel koruma için tek bir sistem

Yetkisiz erişime karşı koruma, çalışma modu seçimi ve erişim izni sistemi ile pratik olarak uygulanabilir. Emniyet ve endüstriyel korumayı birleştirir: Çalışma modunun seçimi ve makine erişimi için izin kontrolü. Bu tür bir çözüm, Pilz'in PITmode ürün grubundaki cihazlarla sağlanmaktadır. Bunlar, tanımlanmış çalışma modları arasında geçiş yapılmasına ve erişim izninin denetlenmesine olanak tanır. Her kullanıcı net kullanıcı kimlik doğrulaması sağlayan ve manipülasyonu önleyen ayrı bir transponder aldığından, işlem sezgiseldir.

Erişim ve çalışma modlarının bireysel yönetimi

PITmode, emniyet konseptinin bireysel tasarımına izin vermek için çeşitli sürümlerde mevcuttur. Kompakt bir hepsi bir arada cihaz olan PITmode, çalışma modu seçimine yönelik butonların yanı sıra bir değerlendirme ünitesi içerir, böylece kurulumda yerden tasarruf

sağlar. Öte yandan modüler sistem PITmode fusion, RFID teknolojisine sahip PITreader okuma ünitesi ve entegre web sunucusunun yanı sıra emniyetli bir değerlendirme ünitesinden (SEU) oluşur. Başka bir versiyon PITmode flex'tir: PITreader, burada emniyetli değerlendirme için bir Pilz kontrolörü ve bir yazılım bloğu ile birlikte kullanılmaktadır. Modüler kurulum, erişim izninin ve çalışma modu seçiminin mevcut kontrol konsollarının tasarımına entegre edilmesini sağlar. Mevcut butonlar, kullanıcı için kolay kullanım sağlayan çalışma modunun seçimi için kullanılabilir. Transponder ile tanımlama, okuma ünitesi PITreader ile gerçekleştirilir. PITmode ve PITmode fusion, PLd'ye kadar fonksiyonel olarak emniyetli çalışma modu seçimi ve erişim izni sağlar.

Uzaktan bile basit kimlik doğrulama

Çalışma modunu seçmek için kullanıcı transponderini doğrudan PITmode'a bağlar ve çalışma modu için tanımlanan bir butona veya bir HMI'daki ilgili butona basar. Kullanıcının izni varsa sürece erişim sağlar. Aynı durum, bir servis çalışanı uzaktan bakım yoluyla bir makineye erişmek istediğinde de geçerlidir: uzaktan bakım, yalnızca sahadaki bir kişi sistemde ilgili izni verirse başlatılabilir. Bakım çalışmasından sonra, makine yeniden çalışmaya başlamadan önce bu erişim tekrar kapatılır. Yetkisiz kişiler tarafından manipüle edilmesi veya bakım çalışmasının ardından yanlışlıkla açık kalan bir bağlantı noktası böylece engellenebilir. İşletmeci şirketler, kimin hangi izne sahip olduğunu ve dolayısıyla kime sürece erişim izni verildiğini kontrol ettiklerinden endüstriyel korumayı artırır.

Erişim yönetimi için eksiksiz çözüm

Yalnızca erişim kontrolü gerçekleştirilecekse PITreader bağımsız bir cihaz olarak veya Pilz'in bir kontrolörü ile birlikte bir erişim izin

sistemi olarak da kullanılabilir. PNOZmulti 2 konfigüre edilebilir küçük kontrolör ile birlikte yönetici, ilgili konfigürasyon aracı PNOZmulti Configurator ile "sürükle ve bırak" özelliğini kullanarak tesis ve makineler için erişim izinlerini kolayca konfigüre eder. Bunlar daha sonra PITreader okuma ünitesi aracılığıyla RFID transponder anahtarına aktarılır. PITreader S sürümü, Pilz kontrolöründen bağımsız olarak OPC UA standardının entegrasyonu yoluyla diğer üreticilerin cihazlarıyla da kullanılabilir. Daha önce de belirtildiği gibi, PITmode cihazları mevcut kontrol panellerine kolayca entegre edilebilir.

Anahtar, kart veya etiket arasında seçim

PITreader kart ünitesi sürümü, operatörler ve kullanıcılar için ek esneklik sunar: RFID özellikli kartlar ve etiketler, RFID transponder anahtarıyla birlikte veya yerine kullanılabilir. Şirket zaten RFID özellikli kartlar kullanıyorsa bunlar PITreader kart ünitesi ile birlikte de kullanılabilir: Bu durumda, kullanıcıların birden fazla fonksiyon için yalnızca bir karta ihtiyacı vardır. Genel olarak, RFID transponderlerinin avantajı (anahtar, kart veya etiket), birkaç fonksiyonun bir transponder üzerinde paketlenebilmesi ve böylece tüm mekanik anahtarlığın birleştirilebilmesi gerçeğinde yatmaktadır. Bu durum, yalnızca bir yetkilendirme ortamı taşımaları gerektiğinden, kullanıcı için uygundur. Yöneticiler ayrıca anahtarları yönetirken ve bakımını yaparken zaman ve emek tasarrufu sağlar.

Güvenlik için bir artı

Güvenlik hususları da kullanıcı kimlik doğrulaması, kalifikasyonu ve erişim koruması açısından ele alınır. Tüm emniyet ve güvenlik önlemlerine rağmen, makinede bir kaza veya güvenlik olayı meydana gelirse RFID transponder hangi değişikliği kimin yaptığını belirlemek için okunabilir. Bu isteğe bağlı fonksiyon istenirse kontrol

sistemi erişim süresini dahili, değiştirilemeyen denetim izine (olay günlüğü) kaydetmek için kimlik doğrulamasını kullanır.

Dikkatli yönetim esastır

Emniyet ve endüstriyel korumanın uygulamanın tüm yaşam döngüsü boyunca garanti edilmesini sağlamak amacıyla yöneticiler izinleri korumak için çok çaba sarf eder. Basit bir yönetim sağlamak için Pilz'in uygun yazılım araçları, kullanıcıların ve transponderlerin organizasyonunu destekler. Bu, karmaşık izin matrislerinin veya grup genelindeki teknik özelliklerin küçük bir RFID anahtarında gizlenebileceği anlamına gelir. Entegre PITreader web sunucusu ile yöneticiler, PITmode veya PITreader'a ait RFID transponderlerini programlar ve kullanıcı verilerini ile izinlerini bunlara kaydeder. Tüm önemli ayarlar doğrudan okuma ünitesinde yapılır ve bu da arayüzlerin konfigürasyonu da dahil olmak üzere devreye almayı hızlandırır.

Arayüzlere erişimi sınırlama

Yetkilendirme ve Erişim Yönetiminin olanakları, güvenlik olaylarında ana ağ geçitlerinden biri olan özel endüstriyel USB bağlantı noktalarını etkinleştirmeye kadar uzanır. Erişim izni sistemi PITreader, etkinleştirilebilir bir USB 2.0 ana bilgisayar arayüzüne sahip PIT oe USB gibi bir işlem öğesiyle birleştirilir. Bu çözüm, programların manipülasyona dayanıklı olarak içe aktarılmasını, verilerin dışa aktarılmasını ve bir klavye veya farenin bağlanmasını sağlar. Arayüzün etkinleştirilmesi yalnızca ilgili izinle gerçekleştirildiğinden, böylece bir üretim tesisinin veri akışı korunur. Endüstriyel otomasyon ağı içindeki veri iletişimini kontrol eden Pilz'in SecurityBridge gibi endüstriyel bir güvenlik duvarı ile birlikte, makineler yetkisiz erişim ve manipülasyona karşı korunabilir.

Mevcut makineler - emniyetli ve güvenli

Mevcut makineler son teknolojiye göre güncellenirse veya risk değerlendirmesinin bir parçası olarak bir eylem ihtiyacı tespit edilirse erişim izni sistemi PITreader kolayca uyarlanabilir: Cihaz, 22,5 mm çaplı anahtar şalterleri için standartlaştırılmış kesiciler kullanılarak doğrudan monte edilebilir. Pilz kontrolörü ile birlikte, istenen emniyet fonksiyonu doğrudan ayarlanabilir. Üçüncü taraf bir kontrolör kullanılıyorsa erişim izninin ve çalışma modunun değerlendirilmesini entegre etmek için PITmode fusion kullanılır. Değerlendirilen transponder ortamına bağlı olarak, şirketteki mevcut RFID anahtar kartları kimlik doğrulama için kullanılabilir.

Sonuç

Nihai varlığımızı, yani emniyetimizi korumak için bütünsel emniyet konseptleri tasarlamak ve güncel olup olmadıklarını düzenli olarak incelemek gerekir. Önemli bir unsur, bir şirketteki izinleri ve erişimi açıkça düzenleyen Yetkilendirme ve Erişim yönetimidir. Çözüm, önlemleri ve teknik özellikleri içeren ve aynı zamanda uygun emniyet ve güvenlik fonksiyonlarını içeren bir konsepttir. PITreader gibi bir erişim izni sistemi, kullanıcıları ve transponderleri organize etmek için ek yazılım bileşenleriyle birlikte tamamlandığında bunun için uygun donanım bloğudur. Emniyetli kapı sistemleri, kontrolör ve yazılım gibi ek bileşenler ve çalışma modu seçimi gibi fonksiyonlar, çözümü bütünsel bir emniyet ve endüstriyel koruma konsepti oluşturmak için geliştirir. Kullanıcının elindeki bireysel anahtar ile sistem kullanımı kolaydır.

Karakter sayısı: 14.675

Şekiller

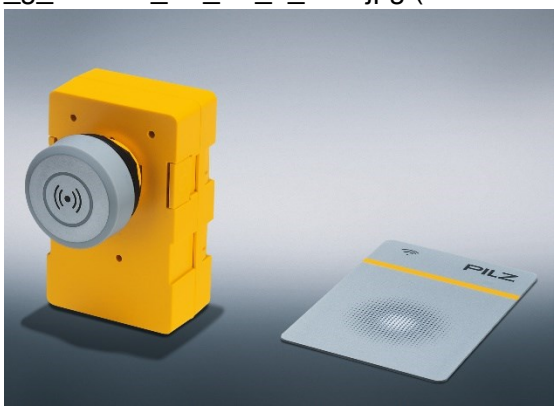
Şekil 1:
F_Press_IAM_Man_using_PITreader_Key_cold1.jpg (© Pilz GmbH & Co. KG)

RESİM YAZISI: Kapsamlı bir Yetkilendirme ve Erişim Yönetimi, uygulamaya erişimi kontrol eder, böylece emniyet ve endüstriyel koruma da dahil olmak üzere emniyet fonksiyonlarının ve önlemlerinin bütünlüğünü sağlar.

Şekil 2:
F_Press_PITmode_fusion_402251_PIT_oe_4023311_P1_B_8_2_cold_2020_01.jpg (Pilz GmbH & Co. KG)

RESİM YAZISI: Pilz PITmode fusion, emniyet ve endüstriyel korumayı tek bir sistemde birleştiren modüler bir çalışma modu seçimi ve erişim izni sistemidir.

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



RESİM YAZISI: Pilz'in erişim izni sistemi PITreader kart ünitesi, RFID özellikli kartlar PITreader kart ve etiketler, PITreader etiketi ile birlikte verimli bir erişim izni sisteminin uygulanması için ek formatlar sunar.

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

RESİM YAZISI: RFID transponder anahtarları PITreader'da okunur ve öğretilir. Erişim izinlerinin ve çalışma modlarının atanması, ilişkili web sunucusu kullanılarak kolayca gerçekleştirilir.

Şekil 5:
F_Press_Group_7_Modular_safety_gate_system_with_diagnostic_and_evaluation_P1_B8_2_cold.jpg (© Pilz GmbH & Co. KG)

RESİM YAZISI: PSENmlock emniyet kapısı sisteminin uygun kol modülü (sol üstte), entegre erişim izin sistemi PITreader (sağ üstte) ve konfigüre edilebilir emniyetli küçük kontrolör PNOZmulti 2 (sağ altta) ile PITgatebox buton ünitesinin ve ayrıca arıza teşhisi çözümü

Emniyet Cihazı Arıza Teşhisinin (sol altta) esnek kombinasyonu, erişim iznine sahip eksiksiz bir emniyet kapısı çözümü sunar.

Kutu: Anahtar Cepte dijital bakım koruma sistemi

Tamamen erişim izninin ötesinde, konfigüre edilebilir emniyetli küçük kontrolör PNOZmulti 2 veya PSS 4000 otomasyon sistemi gibi bir Pilz kontrolörü ile birleştirildiğinde, PITreader verimli dijital "Anahtar Cepte" bakım koruması için kullanılabilir. Bu, bakım çalışmaları yapılırken makinenin yeniden çalışmamasını ve yetkisiz kişilerin erişiminin engellenmesini sağlar. Bu, pratikte şu şekilde gerçekleştirilir: Bakım çalışması için yetkilendirilmiş bir veya daha fazla kullanıcı, tesiste kendilerini doğrular. Başarılı kimlik doğrulamasından sonra, kullanıcı için kişiselleştirilmiş bir güvenlik kimliği Pilz kontrolöründe, emniyetli bir listede saklanır. Makine artık kapatılabilir, emniyet kapısı açılabilir ve makineye erişilebilir. Bu süre zarfında, RFID anahtarları ilgili kullanıcıların "cebinde" kalır. Bakım tamamlandıktan ve insanlar tehlike bölgesinden ayrıldıktan sonra, herkes oturumu kapatır. Güvenlik kimlikleri Pilz kontrolöründeki emniyet listesinden kaldırılır ve makine yeniden başlatılabilir. Mekanik anahtarlarla bakım korumasının aksine, tesise herhangi bir emniyet kapısından girmek veya tesisten çıkmak mümkündür. Bu şekilde, "anahtar cepte" personele bakım sırasında daha fazla esneklik ve zaman tasarrufu sağlar. Dijital bakım koruması, emniyet çitleriyle korunan tehlikeli bölgeleri olan makineler için özel olarak tasarlanmıştır. Operatör her zaman kimin hangi göreve erişimi olduğunu bilir; geçici izinler de atanabilir.

1.578 karakter

Anahtar cepte kutusu için şekil:
F_Press_Group_PIT_Key_in_pocket_solutions_P1_B8_2_cold.jpg (© Pilz GmbH & Co. KG)

RESİM YAZISI: Bakım koruma sistemi "anahtar cepte", erişim izni sistemi PITreader, buton ünitesi PITgatebox ve konfigüre edilebilir küçük kontrolör PNOZmulti 2 veya otomasyon sistemi PSS 4000 gibi bir Pilz kontrolöründen oluşur.

Kutu: İzinleri atama ve koruma

Şirkette bir erişim izni sistemi kullanılıyorsa izinlerin ve kullanıcı verilerinin düzenli olarak bakımı ve yönetimi, yüksek derecede emniyet ve güvenlik sağlamak için hayati önem taşır. Pilz, bu amaç için yazılım aracı PIT Transponder Manager'ı (PTM) sağlar: Bir grafik arayüzde yönetici, kullanıcı ayarlarını, engelleme listelerini ve kullanıcı verilerini yönetir. Önceden konfigüre edilmiş şablonlarda ve içe aktarma fonksiyonunda, bireysel kullanıcı izinleri yalnızca birkaç adımda transponder anahtarına yazılır.

Bir şirkette birden fazla PITmode veya PITreader cihazı kullanılıyorsa bunlar Pilz'in PIT Kullanıcı Kimlik Doğrulama Hizmeti (UAS) yazılımı kullanılarak düzenlenir. PTM gibi yönetim sistemlerinin veya farklı bir kullanıcı yönetim yazılımının PITreader ile bağlanmasını sağlar. PIT UAS, kullanıcılar için merkezi bir

yetkilendirme veritabanına sahiptir, böylece PTM'den tüm PITreader cihazlarına veri aktarımı ve atanması sağlanır. Yöneticiler tüm PITreader'ların mevcut durumunu görüntüleyebilir ve bir arıza teşhisi listesi görüntüleyebilir. Bu şekilde, birkaç cihazın kullanımıyla hızlı bir genel bakış da mümkündür.

1.218 karakter

Kullanıcı yönetimi kutusu için şekil:
((Image to follow)).jpg (© Pilz GmbH & Co. KG)

RESİM YAZISI: Bir şirket birkaç PITreader okuma ünitesi kullanıyorsa
bunlar Kullanıcı Kimlik Doğrulama Hizmeti (UAS)
yazılım aracı kullanılarak düzenlenir.

Pilz Grubu

Pilz Grubu, otomasyon teknolojisine yönelik ürünler, sistemler ve hizmetler sunan küresel bir tedarikçidir. Aile işletmesi Ostfildern'de faaliyet gösterir ve yaklaşık 2.500 personel istihdam eder. Dünya çapında 42 iştiraki ve şubesi ile Pilz, insan, makine ve çevre için emniyetli çözümler sunmaktadır.
Teknoloji lideri, endüstriyel iletişim, teşhis ve görselleştirme sistemleri dahil olmak üzere sensör, kontrol ve sürücü teknolojisinden oluşan eksiksiz otomasyon çözümleri sunar. Danışmanlık, mühendislik ve eğitimden oluşan uluslararası bir hizmet yelpazesi de bu portföyü tamamlar. Pilz çözümleri, örneğin intralojistik, demiryolu teknolojisi veya robotik sektörü gibi makine mühendisliğinin ötesinde birçok endüstride kullanılmaktadır.

www.pilz.com

Basın iletişimi:

Martin Kurth

Kurumsal ve Teknik Basın
Tel: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

Teknik ve Kurumsal Basın
Tel: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

Teknik Basın

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

Sabrina Schilling

Teknik Basın

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

Hansjörg Sperling-Wohlgemuth

Konferans ve Sunum Yönetimi
Tel: +49 711 3409-239
h.sperling@pilz.de