25.05.2023

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

Mesaja týkla

Thomas Pilz: Emniyet ve Güvenlik dijital otomasyon için

Ostfildern, 25.05.2023 - **(Teslimatı kontrol ediniz)**

Thomas Pilz

Güvenlik: Mevzuat endüstri ve mühendislik için geçerli olacak

Endüstriyel bir ortamda emniyet standartları ve yasaları şu anda kargaşayla karşı karşıya. Bu durum, güvenlik ve Yapay Zeka (AI) konularından kaynaklanıyor. Genel olarak endüstri ve makine mühendisliğinde, güvenlikle ilgili üç yeni veya gelecek yasal gereklilik vardır: AB Direktifi NIS 2, yeni Makine Yönetmeliği ve Siber Dayanıklılık Yasası. Geçen Yıllık Basın Toplantısında olduğu gibi, güvenlik konusuna odaklanacağım ve bugün size etkilerin tüm endüstri için ne kadar geniş kapsamlı olacağını göstermek istiyorum.

NIS 2: Daha fazla şirket için daha fazla yükümlülük ve daha fazla yaptırım

NIS (Ağ ve Bilgi Güvenliği), siber güvenliği güçlendirmeyi amaçlayan bir Avrupa Birliği Direktifidir. Bu direktif 2016 yılından beri yürürlüktedir ve şimdiye kadar enerji, trafik, bankalar ve finans, sağlık, içme suyu temini ve dağıtımı ve dijital altyapı dahil olmak üzere kritik altyapı sağlayıcılarına uygulanmıştır. Bu sektörlerdeki sağlayıcılar "uygun güvenlik önlemleri" uygulamak ve ciddi siber güvenlik olaylarını bildirmek zorunda kaldılar. Halefi, 2023'ün başında yürürlüğe giren ve 2024 sonbaharına kadar AB üye devletleri tarafından ulusal yasalara uyarlanması gereken NIS 2'dir. Direktif artık mühendislik ve otomotiv sektörlerinde, diğerlerinin yanı sıra, 50 çalışandan fazlası veya yıllık cirosu 10 milyon Euro'dan fazla olan şirketler için de geçerlidir. Alman Makine Mühendisliği Endüstrisi Birliği VDMA'ya göre, bu durum Avrupa genelinde yaklaşık 9.000 şirketi etkileyecek. Gelecekte bu şirketlerin güvenlik olaylarına karşı korunmak için teknik, operasyonel ve organizasyonel önlemler aldıklarını kanıtlamaları gerekecektir. İlk olarak bu, üretim ortamları, başka bir deyişle OT (Operasyon Teknolojisi) dahil olmak üzere mevcut sistemlerin risk analizini içerecektir. Bunu, parola koruması veya şifreleme gibi belirli süreçlerin ve önlemlerin geliştirilmesi ve uygulanmasının yanı sıra çalışanlar için sürekli eğitim ve öğretim izleyecektir. Siber güvenlik olayları 24 saat içinde ilgili makamlara bildirilmelidir. Tedarik zincirlerinin açıkça dahil edilmesi de yenidir. Özetlemek gerekirse NIS 2 artık daha fazla şirketi etkiliyor, yükümlülükleri genişletiyor ve daha katı yaptırımlar getiriyor. Önlem almayan şirketler ağır cezalarla tehdit ediliyor.

Siber Dayanıklılık Yasası - Tüm ürün yaşam döngüsü için güvenlik

Eylül 2022'de Avrupa Komisyonu, ürünlerin siber güvenliğini artırmayı amaçlayan bir düzenleme taslağı sundu. Bu Siber Dayanıklılık Yasası, dijital unsurlara sahip ürün üreticilerine yöneliktir. Bu, yazılımın (örneğin ürün yazılımı) yanı sıra donanım anlamına gelir. Yönetmelikte, hem tüketici ürünleri hem de örneğin makine kontrolörleri gibi endüstriyel uygulamalara yönelik ürünlerden bahsedilmektedir. Siber Dayanıklılık Yasası uyarınca, yalnızca uygun bir siber güvenlik seviyesini garanti eden ürünler piyasaya sürülebilir. Üreticiler ayrıca müşterileri güvenlik açıkları hakkında bilgi vermek ve bunları mümkün olduğunca çabuk kapatmakla yükümlüdür. Bu nedenle yönetmelik, bir ürünün yaşam döngüsünün tamamı için geçerlidir. Bu, üreticilerin artık normal garanti süresinin ötesinde yazılım güncellemeleri sunmaları gerektiği anlamına gelir, böylece gelecekteki tehditler de engellenir. Yönetmeliğin 2024 yılı sonunda kabul edileceğini varsayıyoruz.

Yeni Makine Yönetmeliği - Zorunlu siber güvenlik

Üçüncü yeni yasal güvenlik gereksinimi AB Makine Yönetmeliğidir. Yayınlanması yakındır. Bir yönetmelik olduğu için öncelikle ulusal hukuka dönüştürülmesi gerekmez. Makine üreticilerinin yeni gereksinimleri karşılamak için 42 ayları vardır. Makine Yönetmeliği, mevcut Makine Direktifi'nin yerini alıyor ve selefinin aksine, siber güvenliği zorunlu kılmaktadır. Makine Direktifi tamamen emniyeti incelediyse Yönetmelik, güvenlik koruma hedefini "Yolsuzluğa karşı koruma" altındaki "Temel sağlık ve emniyet gereksinimlerini EHSR" de içerir: Makinenin emniyet fonksiyonları, kasıtlı veya kasıtsız bozulma nedeniyle tehlikeye atılmamalıdır. Şimdiye kadar Siber dayanıklılık Yasası gereksinimlerinin karşılanmasının Makine Yönetmeliğine uygunluk varsayımına yol açtığı bilinmektedir.

Ancak şimdi: Kimin neyle ilgilenmesi gerekiyor?
Yasal gereksinimler ne anlama geliyor? Korelasyonları göstermek için enerji üretim sektörünü kullanmak istiyorum:
Şimdiye kadar, NIS Direktifinden sadece enerji tedarikçileri etkileniyordu. NIS 2 ile, enerji üretim santralleri üreticileri (örneğin rüzgar türbinleri) gibi makine üreticilerinin de gelecekte gereksinimleri karşılaması gerekecektir. Buna karşılık, rüzgar türbini üreticilerinin Pilz'in otomasyon çözümlerine, kontrolörlerine veya sensörlerine ihtiyacı vardır. Belirli bir boyuttan itibaren, elektrikli bileşen üreticileri de NIS 2 kapsamına girer. NIS 2 de tedarikçilerin dikkate alınmasını şart koştuğundan, Pilz gibi bir şirket emniyetli tedarik zincirleriyle de ilgilenmeli ve tedarikçilerinden taleplerde bulunmalıdır. Böylece NIS 2 tüm tedarik zincirini kapsar.

Avrupa'ya makine ithal etmek için makine imalatçıları her zaman CE işareti ile biten uygunluk değerlendirme prosedüründen geçmek zorunda kalmıştır.
Şimdi, yeni Makine Yönetmeliği ile makine üreticileri, makinelerinin manipülasyona karşı da korunduğunu kanıtlamak zorundadır. Son olarak, elektrikli bileşen üreticileri, planlanan Siber Dayanıklılık Yasasının gelecekteki gereksinimlerine tabidir.

Özetlemek gerekirse: Artık güvenlikle uğraşmak isteyip istemediği ve ne ölçüde uğraşmak istediği şirketin takdirine bağlı değildir. Hayır, bu yasal bir gerekliliktir! Şirketlerin NIS 2 ile mümkün olan en kısa sürede ilgilenmeleri ve şirket için bütünsel bir güvenlik değerlendirmesi yapmaları akıllıca olacaktır. Örneğin, ISO 27001 bilgi güvenliği standardına göre sertifikalandırılmış bir Bilgi Güvenliği Yönetim Sisteminin (ISMS) geliştirilmesi buna dahildir.

Mühendislikte, endüstriyel koruma biçimindeki güvenlik yalnızca BT için bir görev değil, aynı zamanda tasarım ve yapımın ayrılmaz bir parçasıdır. Güvenliği geriye dönük olarak uygulamak her zaman karmaşıktır ve genellikle kullanıcı dostu, fonksiyonellik ve üretkenlikte azalma anlamına gelir. Risk değerlendirmesi artık emniyetin yanı sıra güvenliği de içermektedir. Güvenlik yoksa CE işareti de yok!

Ayrıca dijital elemanların olduğu ürün üreticileri için IEC 62443 serisi standartlar iyi bir yönlendirme sağlar. Örneğin, IEC 62443-4-1 alt standardında, "Güvenli geliştirme yaşam döngüsü sürecinin" gereksinimleri açıklanmaktadır.

AB, güvenlik mevzuatı ile hızlı şekilde harekete geçti; Avrupa'da dünyanın en katı gereksinimleri geçerli olacak. Ancak diğer ülkelerle anlaşmalar zaten yürürlükte ve bu tür yasalar oralarda da uygulanacak. Örneğin, Avustralya şu anda AB ile görüşmelerde bulunuyor ve muhtemelen Avrupa standartlarını uygulayacak. Bu nedenle, endüstriyel korumanın küresel olarak uyumlu hale getirilmesi beklenmektedir.

Thomas Pilz

Tarihi misyon olarak açık iletişim standartları

Pilz'de açıklık ve kullanım kolaylığı, portföyün temel özellikleridir. Müşterilerimize her zaman son teknoloji ürünü olan, kullanımı kolay ve herhangi bir otomasyon mimarisine eklenebilen ürünler sunmak istiyoruz.

İlk emniyetli endüstriyel haberleşme sistemi olan SafetyBUS p ve emniyetli gerçek zamanlı Ethernet SafetyNET p ile emniyetli endüstriyel iletişimin gelişimini şekillendirdik. Ancak şirkete özgü iş çözümlerinin günleri geride kaldı. Endüstri standartları oluşturmaya tamamen kararlıyız. Bu tarihi bir görevdir!

OPC UA

Endüstri, endüstriyel tesisler için emniyetli, satıcılar arası ağ iletişimine yönelik için OPC UA (Açık Platform İletişimi Birleşik Mimarisi) üzerinde anlaştı. Bu iletişim protokolü, endüstrideki farklı veri kaynakları arasındaki iletişim için standartlaştırılmış (IEC 62541) bir arayüz sağlar. OPC Vakfı'nın bir üyesi olarak Pilz çalışanları hem yönlendirme komitesinde hem de Saha Seviyesi İletişimi (FLC) grubunun teknik çalışma gruplarında aktiftir. Pilz'in odak noktası, emniyet (OPC UA üzerinden emniyet) ile ilgilenen çalışma grubundadır.

İşlevsel olarak emniyetli endüstriyel haberleşme protokollerinin gerekliliklerileyle bağlantılı olarak Yayıncı/Abone teknolojisi (Pub/Sub) kullanımındaki uzmanlığımız özellikle önemlidir. Klasik Ana/Yardımcı mimarisine kıyasla, Pub/Sub ile veri alışverişi doğrudan aboneler arasında yapılabilir. Bu, OPC UA'nın zorlu, dağıtılmış otomasyon görevleri için de kullanılmasını sağlar. SafetyNET p'miz Pub/Sub'u en başından beri destekleyen tek emniyetli, Ethernet tabanlı endüstriyel haberleşme sistemi olduğundan Pilz, bu alanda özel bir uzmanlığa sahiptir.

Fonksiyonel emniyet konularında çalışmalarımız iyi ilerliyor. Grup, test spesifikasyonu ve test sistemlerinin yanı sıra OPC UA Safety için iletişim yığınlarının sertifikalandırılması konusunda denetim makamlarıyla el ele çalışmaktadır. Sürüm 1.05 zaten yayınlandı.

IO-Link Safety
Sensör düzeyinde otomasyon, açıklık açısından şimdiden büyük bir adım attı. IO-Link Safety iletişim protokolü ticari olarak kullanılabilir olmak üzeredir. Noktadan noktaya iletişim, daha basit kurulum (örneğin standartlaştırılmış kablolama ve paralel kablolamanın olmaması), otomatik, alet destekli parametrelendirme ve gelişmiş arıza teşhisi seçenekleri gibi birçok avantaj sunar.

IO-Link'in emniyetle ilgili otomasyon görevlerine yönelik de kullanılabilmesi için Pilz, IO-Link topluluğunun bir parçası olarak, ilgili testler ve sertifikalarla ilgili eklenti üzerinde yoğun şekilde çalışmaktadır. Pilz'den uzmanlar, ilgili testler ve sertifikalarla birlikte IO-Link Safety çalışma gruplarına (pazarlama ve teknoloji için) liderlik etmektedir.

Pazara hazır ilk sensörleri Kasım ayında SPS'de tanıtacağız. Pilz'in yaklaşımı, sensörler, aktüatörler ve Ana modüller gibi eksiksiz bir sistem sunmaktır. Bu, müşterinin uygulamasını basitleştirir ve performansı artırır.

Gelecekteki otomasyon çözümlerinin fonksiyonlarıyla daha da farklılaşacağına inanıyoruz: Kullanıcı arayüzleri ne kadar iyi, kullanımı ne kadar basit, ne gibi ek avantajlar sunuyorlar? Bunun arkasında, yeni uygulamalar için büyük bir potansiyelle sonuçlanan muhteşem bir yenilik gücü vardır.

Thomas Pilz

Emniyetin geleceği dinamiktir

İnsan ve makinelerin korunması için daha fazla dijitalleşme ne anlama geliyor? Hangi teknolojiler emniyet gereksinimlerini karşılamaktadır? İnsanların rolü nedir? Bugün geleceğe de göz atmak istiyoruz. Öncelikle iyi haber: Odak noktası, rolü daha da güçlenecek olan insandır.

Aktif bir şekillendirici olarak insan

Örneğin, Arena 2036'daki "Sıvı Üretimi" projesinde olduğu gibi. Pilz, özellikle otomotiv üretimi için insan merkezli, siber-fiziksel bir üretim konsepti geliştirmek ve uygulamak için iş ortaklarıyla birlikte çalışmaktadır. Projenin arkasındaki fikir, üretim tesislerini tamamen ihtiyaca göre dinamik birimler oluşturmak ve daha sonra dağıtmak için konum açısından esnek modüllere ayırmaktır. Modüller, insanın üretim ortamlarının aktif şekillendiricisi rolüne odaklanarak tasarlanmıştır.

Bu gereksinimlerden, dinamik emniyet için artan bir istek vardır, örn. emniyet fonksiyonlarını değişen üretim süreçlerine ve ilgili koruma gereksinimlerine daha fazla esneklikle uyarlama yeteneği. Örneğin, bir kişi çalışma alanına girdiğinde hemen durmak zorunda kalmak yerine, robotların veya mobil platformların daha düşük (ve dolayısıyla daha emniyetli) bir hızda çalışmaya devam etmesine veya daha da iyisi, emniyetli kaçınma stratejilerinin dahil edilmesine olanak tanırlar. Dağıtılmış sistemlerdeki akıllı sensörler ve aktüatörler, kontrolörlerden giderek daha fazla fonksiyonu devralacak ve bireysel makine modülleri arasında ve insan ile makine arasında daha iyi etkileşime neden olacaktır.

Gerçek zamanlı emniyet
Emniyetle ilgili olarak, gelecekteki üretim ortamlarındaki dinamik durumlar gerçek zamanlı olarak kontrol edilmeli ve etkinleştirilmelidir, böylece insan ve makinenin korunması her zaman garanti edilir. Buradaki anahtar kelime "Gerçek zamanlı emniyet"tir. Gelecekte, çeşitli makinelerin (veya genel varlıkların) emniyet cihazlarını paylaşması düşünülebilir. SmartFactory KL'de test ettiğimiz "Paylaşılan Emniyet" budur. Emniyet bu şekilde anlaşıldığında, analog uygunluk değerlendirme prosedürünün sonucu olarak klasik CE işareti göz ardı edilir. İlgili tüm varlıklarla ilgili bilgiler şu anda çalışma zamanında mevcut olmalıdır; burada anahtar kelimeler dijital tip plakası ve yönetim kabuğudur.

Daha önce bahsettiğim "Sıvı Üretimi" projesinde, insanların ve nesnelerin tanımlanması (ve dolayısıyla farklılaşması) gibi gelecekteki diğer konular üzerinde çalışıyoruz. Bu, yapay zekanın kullanımına uygundur. Riskler daha sonra uyarlanabilir AI algoritmaları ile tanımlanabilir ve değerlendirilebilir Bu durumda "analog" CE işareti temel koruma sağlar. Ancak, emniyeti daha da esnek hale getiren ve daha fazla üretkenliğe katkıda bulunan ek risk azaltma önlemleri getirilebilir.

Baþlýk:

You can find texts and images at www.pilz.com also for downloading. To go directly to the relevant internet pages in the press centre, enter the following Web code in the search of the home page.: **237512**

Pilz Grubu

Pilz Grubu, otomasyon teknolojileri için ürün, system ve hizmet sağlayan küresel bir sağlayıcıdır. Stuttgart yakınlarında Ostfildern'de yer alan aile şirketi yaklaşık 2.500 çalışana sahiptir. Dünyanın dört bir yanında 42 iştirak ve şubesiyle Pilz insan, makine ve çevre için emniyetli çözümler sunar. Teknoloji lideri, endüstriyel iletişim, teşhis ve görselleştirme dahil olmak üzere sensörler ile kontrol ve sürücü teknolojilerinden oluşan eksiksiz çözümler sunar. Uluslararası hizmetleri arasında danışmanlık, mühendislik ve eğitim yer alır. Mekanik ve tesis mühendisliğine ek olarak Pilz'in çözümleri rüzgar enerjisi, demiryolu teknolojileri ve robot bilimi gibi farklı sektörlerde kullanılır.

www.pilz.com

Sosyal ağlarda Pilz

Sosyal medya kannalarýmýzda sizlere þirketimiz ve Pilz çalýþanlarý hakkýnda bilgiler veriyor ve otomasyon teknolojisindeki güncel geliþmeleri rapor ediyoruz.

https://www.facebook.com/pilzINT

https://twitter.com/Pilz_INT

https://www.youtube.com/user/PilzINT

https://www.xing.com/companies/pilzgmbh%26co.kg

https://www.linkedin.com/company/pilz

Gazeteciler için irtibat

Martin Kurth
Kurumsal ve Teknik Basın
+49 711 3409 - 158
publicrelations@pilz.com

Sabine Skaletz-Karrer
Teknik Basın
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de