Endüstriyel Güvenlik

PILZ
THE SPIRIT OF SAFETY

Makine üreticileri ve operatörleri için güncel
AB mevzuatını uygulamaya yönelik bir kılavuz

Tanıtım belgesi
Sürüm: Nisan 2025

Sorumluluk Reddi

Tanıtım belgemiz büyük bir özenle derlenmiştir. Yeni AB Makine Regülasyonu, NIS 2 Direktifi ve Siber Dayanıklılık Yasası hakkında Pilz'in mevcutta yorumladığı şekilde bilgiler içerir. Tüm ayrıntılar, mevcut bilgi ve yorumlama durumunun yanı sıra bildiklerimize ve inandıklarımıza en uygun şekilde sunulmaktadır. Verilen bilgilerin doğruluğunu sağlamak için gerekli tüm eforun gösterilmesine karşılık, ağır ihmal durumu haricinde, verilen bilgilerin doğruluğu ve bütünlüğü için sorumluluk kabul etmemekteyiz. Özellikle beyanların yasal güvence veya teminatlı mal niteliğine sahip olmadığı belirtilmelidir. İçerik hakkında verilecek geri bildirimler için teşekkür ederiz.

Telif Hakkı

Bu yayının tüm hakları Pilz GmbH & Co. KG'de saklıdır. Teknik değişiklikler yapma hakkımız saklıdır. Kullanıcının dahili kullanımları için kopyalanabilir. Kullanılan ürün, mal ve teknoloji isimleri, ilgili şirketlerin ticari markalarıdır.

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern, Almanya

© 2025 Pilz GmbH & Co. KG, Ostfildern
Revize edilmiş 2. sürüm

Bir bakışta

Endüstriyel Güvenlik kavramı pek çok farklı boyut içerir. Bu kılavuzda, makine üreticileri ve operatörleri açısından en önemli noktalar ele alınmaktadır. Yeni gereklilikleri anlayıp yönetebilmeleri için hem üreticilerin hem de operatörlerin konuya kolay bir giriş yapabilmeleri önemlidir.

Kılavuz, Avrupa'daki yasal durumu açıklamakta, teknik temellere genel bir bakış sunmakta, makine üreticileri ve operatörleri için en önemli noktaları ortaya koymakta ve müşterilerimiz için izlenebilecek seçeneklere değinmektedir.

Geçtiğimiz aylarda, Avrupa'da, makine mühendisliği üzerinde doğrudan etkisi olan çok sayıda kapsamlı yasal metin yayınlandı.

- **Makine Regülasyonu** (AB) 2023/1230, makinelerle ilgili yolsuzluğa karşı koruma gibi yeni gereklilikler ortaya koyar.
- Avrupa Birliği genelinde yüksek düzeyde ortak bir siber güvenlik sağlanmasına yönelik önlemleri içeren **AB Direktifi (NIS 2) 2022/2555, birçok şirket için bir Bilgi Güvenliği Yönetim Sistemini şart koşar**.
- **Siber Dayanıklılık Yasası** (AB) 2024/2847, makineler dâhil olmak üzere dijital unsurlar içeren ürünlere yönelik gereklilikleri tanımlar.

Mevzuatın uygulanmasında bazı standartlar ve terimler kilit rol oynar:

- **IEC 62443** standartları ailesi, endüstriyel ortamlarda Bilgi Güvenliği için oluşturulmuştur.
- 0'dan 4'e kadar olan **Güvenlik Seviyesi**, saldırganın yeteneklerini tanımlar.
- Endüstriyel Güvenlik, sürekli bir çaba gerektirir; bu nedenle, teknik önlemlerin yanı sıra organizasyonel önlemler de büyük önem taşır. **Bilgi Güvenliği Yönetim Sistemi** (ISMS), bu süreçte önemli bir rol oynar ve pek çok şirket için zorunludur.

Makine üreticileri, bir dizi yasal gerekliliğe uymak zorundadır ve operatörlerin spesifikasyonları ile bileşen üreticileri tarafından sunulan ürünler arasında yolunu çizmek durumundadır. Makine üreticisinin, uyumlu ve yüksek kaliteli ürünler sunmaya devam edebilmesi için burada ara bulucu bir rol üstlenmesi gerekecektir.

Makine operatörleri de gelecekte makinelerinin güvenliğini en iyi şekilde nasıl sağlayacaklarını düşünmek zorunda kalacaklardır. Genel bir bakış elde etmek için önerilen eylem, sistemli bir risk analizi yapmak ve güvenlik açıklarını etkin bir şekilde gidermektir.

Pilz GmbH & Co. KG bu konuda ileri seviyede eğitim ve hizmetler sunmaktadır.

Yazar

Matthias Kuczera, Makine Mühendisliği alanında eğitimini tamamladıktan sonra çeşitli endüstriyel sektörlerde Makine Emniyeti konusunda derinlemesine bilgi ve deneyim kazandı.

Sensör alanında geliştirme mühendisi olarak, fonksiyonel emniyet gerekliliklerinin uygulanmasına yönelik farklı seçenekler hakkında kapsamlı bilgiye sahiptir.

Malzeme taşıma alanında teknik uzman olarak çalıştığı süre boyunca, onaylanmış bir kuruluşta emniyet bileşenlerinin tip incelemelerinin yapılmasından sorumlu olmuştur.

Pilz'de "Fonksiyonel Emniyet – Standartlar" alanında teknik uzman olarak mevcut görevinde, standart komitelerinde aktif olarak yer almakta ve standart yönetimini denetlemektedir.

Görevleri arasında şunlar yer alır:

- Makine Emniyeti konusunda standart komitelerinde işbirliği
- Yeni yasal gerekliliklerin değerlendirilmesi
- Şirket içi eğitimlerin gerçekleştirilmesi

Pilz – Dijital Otomasyonda Emniyet Ruhu

Yaptığımız her şeyde dünyayı daha emniyetli bir yer haline getiriyoruz. Otomasyon teknolojisinde küresel bir ürün, sistem ve hizmet tedarikçisi olan Pilz, 75 yıldan uzun bir zamanı kapsayan bir başarı öyküsüne sahip: 1948'de kurulan Pilz Grubu, bugün 42 iştirak ve şubede yaklaşık 2 500 personel istihdam ediyor. Merkezi Ostfildern'de bulunan bu Makine Emniyeti uzmanı, eksiksiz otomasyon çözümleriyle dünya çapında insan, makine ve çevre için emniyet sağlıyor. Teknoloji liderinin portföyünde sensör, kontrol ve sürücü teknolojisinin yanı sıra endüstriyel iletişim, arıza teşhisi ve görselleştirme sistemleri bulunmaktadır. Danışmanlık, mühendislik ve eğitimden oluşan uluslararası bir hizmet yelpazesi de bu portföyü tamamlamaktadır. Emniyet ve Güvenlik çözümleri, makine mühendisliğinin ötesinde, intralojistik, demiryolu teknolojisi veya robotik sektörü gibi birçok endüstride kullanılmaktadır.

İçerik

1. Avrupa'daki yasal durum

Yeni teknolojiler beraberinde yeni fırsatlar ve riskler getirir. Şu anda sektörümüzdeki en önemli yenilikler, Nesnelerin İnterneti, Yapay Zeka ve robot teknolojisi yoluyla makinelerin yoğun bir şekilde ağ bağlantılı olmasıdır.

Şirketlerin ve makinelerin birbirine bağlanması, bilişim sistemlerindeki güvenlik açıklarının suistimal edilmesi ile ekonomik kayıp ve fiziksel zarar riskini artırır. Örneğin, son yıllarda, şirketlere yönelik başarılı siber saldırı vakalarında bir artış görülmüş ve bu saldırılar milyarlarca dolarlık zararlara yol açmıştır. Statista.com'a göre, 2023 yılında siber saldırıların küresel çapta yaklaşık 8,15 trilyon dolar zarara yol açtığı tahmin edilmektedir. Sadece Almanya'da bu rakam, 2023 yılında yaklaşık 206 milyar Euro ya da gayrisafi yurtiçi hasılanın yaklaşık yüzde 5'ine denk gelmektedir.

Riskleri azaltmak için Avrupalı kanun yapıcılar yeni kurallar belirlemiştir. Makine üretimi için bunlar öncelikle Makine Regülasyonu, NIS 2 Direktifi (NIS 2) ve Siber Dayanıklılık Yasası'dır (CRA). Bunlar sayesinde Endüstriyel Güvenlik zorunlu tutulur. Mevcut tesis ve makinelerin nasıl kullanılacağı, iş ekipmanlarının kullanımına yönelik emniyet ve sağlık gereklilikleri, 2009/104/AT sayılı Direktifte açıklanmaktadır.

Şekil 1: Endüstriyel Güvenlik için gereklilikleri tanımlayan yeni temel mevzuattan bir alıntının görseli.

	Makine Regülasyonu (AB) 2023/1230	NIS 2 Direktifi (AB) 2022/2555	Siber Dayanıklılık Yasası (AB) 2024/2847
Şunlara yöneliktir:	Makineler	Şirketler	Bileşenler
Kabul edildiği tarih:	29.6.2023	27.12.2022	20.11.2024
Şu tarihten itibaren bağlayıcı-dır:	20.1.2027	18.10.2024	11.12.2027
Yükümlülükler	▸ Yolsuzluğa karşı koruma (fonksiyonel emniyet fonksiyonlarına odaklı) ▸ Üçüncü tarafların kötü amaçlı girişimlerine karşı dikkatli olma	▸ Siber güvenlik risklerini yönetmeye yönelik önlemler ▸ Teknik ve organizasyonel önlemlerle uyumluluk ▸ Önemli güvenlik olaylarının bildirilmesi	▸ 11.9.2026 itibarıyla üretici raporlama yükümlülükleri ▸ Güvenli Geliştirme Yaşam Döngüsü Süreci ▸ Kritik ürünler için AB tip incelemesi ▸ Güvenlik açıklarının bildirilmesi ▸ Güvenlik güncellemelerinin sağlanması

Tablo 1: Makine Regülasyonu, NIS 2 Direktifi ve Siber Dayanıklılık Yasası için karşılaştırmalı genel bakış

1.1. Makine Regülasyonu (AB) 2023/1230

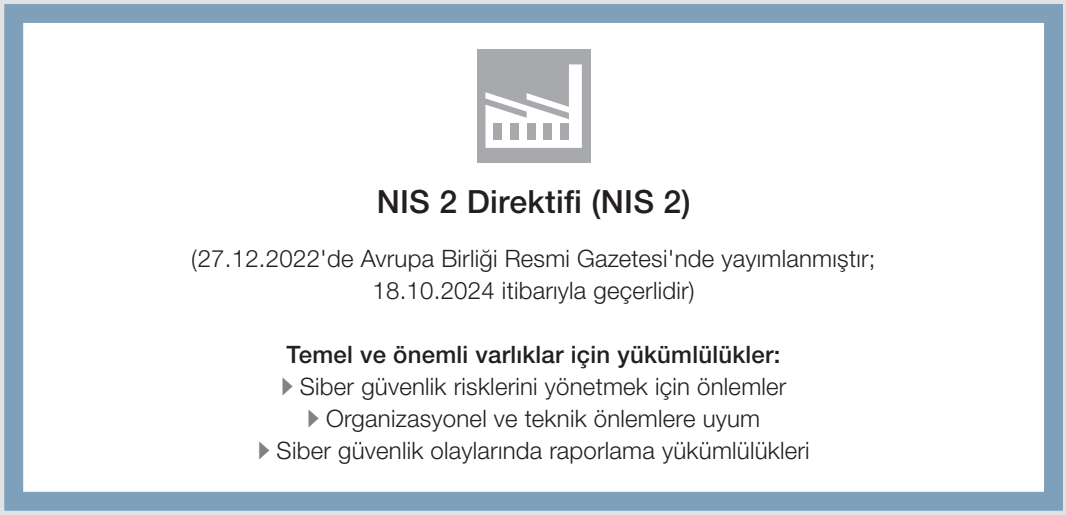
Şekil 2: Makine Regülasyonuna Genel Bakış

Makine Regülasyonu (AB) 2023/1230, Haziran 2023'te kabul edilmiştir ve 42 aylık bir geçiş döneminin ardından tüm AB ülkelerinde bağlayıcı olacaktır. 20 Ocak 2027 itibarıyla 2006/42/AT sayılı Makine Direktifinin yerini alacaktır.

Makine Regülasyonu, makine veya ilgili ürünlerin üreticilerini, ithalatçılarını, bayilerini ve yetkili temsilcilerini etkilemektedir. Gelecekte, makinelerin güvenlik hususları dahil olmak üzere Makine Regülasyonuna uygun olduğunu onaylamaları gerekecektir. Bu aynı zamanda emniyetle ilgili kontrol fonksiyonlarının yolsuzluğa karşı korunmasını da içerir. Makine üreticileri, üçüncü tarafların kötü amaçlı eylemlerinden kaynaklanabilecek ve Makine Emniyetini etkileyebilecek risklere karşı önlem almalıdır. Makine Regülasyonu ile uyumluluk, Uygunluk Beyanında resmi olarak onaylanır ve makine üzerinde CE işareti ile belirtilir. Yeni Makine Regülasyonunun gerekliliklerini karşılamayan makineler artık AB'de piyasaya sürülemez.

Pratik ipucu:
Makine Direktifi ile karşılaştırıldığında, Makine Regülasyonundaki tek değişiklik güvenlik konusu değildir. Yapay Zeka ile çalışma gibi diğer gereklilikler de eklenmiştir. Pilz, şu adresten indirebileceğiniz bir Makine Regülasyonu kılavuzu sunmaktadır: **www.pilz.com/mr**

1.2. NIS 2 Direktifi (AB) 2022/2555



Şekil 3: NIS 2 Direktifine genel bakış

NIS 2 Direktifi AB Resmi Gazetesi'nde şu isim altında bulunabilir: “ Avrupa Birliği genelinde yüksek düzeyde ortak bir siber güvenlik sağlanmasına yönelik önlemler hakkında direktif (AB) 2022/2555 (NIS 2 Direktifi)”. "NIS" kısaltmasının tarihsel bir temeli vardır ve genel olarak "Ağ ve Bilgi Güvenliği" anlamına gelir. NIS 1 Direktifi, esasen kritik altyapılar ve ilgili dijital hizmetlerin sağlayıcıları için geçerli olmuştur. NIS 2 Direktifi, sektör yelpazesini diğerlerinin yanı sıra üretim ticaretini de kapsayacak şekilde genişletmektedir: Mühendislik, bilgi işlem cihazları, elektronik ve optik ürünler, elektrikli ekipman, motorlu taşıtlar ve motorlu taşıt parçaları üreticileri ile diğer tüm araç üretim faaliyetleri. **Bu sektörlerde, 50'den fazla çalışana sahip veya yıllık cirosu ya da yıllık bilançosu 10 milyon Euro üzerinde olan şirketler için bu direktif geçerlidir.**

Bu şirketler, gelecekte siber güvenlik için risk yönetimi önlemleri uygulamakla yükümlü olacaklardır. Buna, aşağıdakiler dahildir:

- Bilgi sistemleri, tedarik zincirinin korunması ve personel emniyetine yönelik risk analizleri ve emniyet konseptleri.
- **Erişim kontrolü** ve tesislerin yönetimine **yönelik konseptler**
- **Yönetim için zorunlu eğitim**
- Ciddi güvenlik olaylarında, 24 saat içinde **erken uyarı** ve 72 saat içinde **sorumlu makamın bilgilendirilmesi**

NIS 2, 2022'nin sonunda Avrupa Parlamentosu ve AB Konseyi tarafından kabul edildi. AB üye devletlerinin bu Direktifi iç hukuka uyarlamak için 18.10.2024 tarihine kadar süreleri vardı.

Pratik ipucu:
Avrupa Birliği Siber Güvenlik Ajansı (ENISA), şirketlerin siber güvenlik stratejilerini kontrol edebilecekleri bir öz değerlendirme aracının yanı sıra siber güvenlik konusunda pek çok yararlı bilgi sunmaktadır: **www.enisa.europa.eu**

Pratik ipucu:
OpenVAS gibi yazılım araçları, şirketlerin güvenlik açıklarını tespit etmelerine ve karşı önlemleri kontrol etmelerine yardımcı olabilir.

1.3. Siber Dayanıklılık Yasası (AB) 2024/2847

Siber Dayanıklılık Yasası (CRA)

(20.11.2024'de Avrupa Birliği Resmi Gazetesi'nde yayımlanmıştır;
11.09.2026 itibarıyla üreticiler için raporlama yükümlülükleri;
11.12.2027 itibarıyla tam olarak uygulanacaktır)

Dijital unsurları olan ürünler için üretici yükümlülükleri:
- Güvenli Geliştirme Yaşam Döngüsü Süreci
- Güvenlik açıklarının bildirilmesi
- Güvenlik güncellemelerinin sağlanması

Şekil 4: Siber Dayanıklılık Yasasına genel bakış

Avrupa Komisyonu, sadece Avrupa Birliği ekonomisi için değil, aynı zamanda demokrasi, tüketicilerin emniyeti ve sağlığı için de kritik sonuçlar doğurabileceği için siber saldırıların kamu yararını ilgilendiren bir konu olduğu görüşünde.

Bu nedenle, Avrupa Komisyonu, Eylül 2022'de ürünlerin siber güvenliğini artırmayı amaçlayan bir Regülasyon taslağı sundu.

Bu Siber Dayanıklılık Yasası (CRA), diğer ürünlerle iletişim kurabilen **dijital unsurları (donanım ve yazılım) olan ürün üreticilerine** yöneliktir.

Diğer bir deyişle, akıllı telefonlar veya robot süpürgeler gibi B2C segmentindeki ürünler, **kontrol sistemleri ve sensörler** gibi B2B segmentindeki ürünlerin yanı sıra işletim sistemleri gibi saf yazılım ürünleri de bundan etkilenir.

CRA uyarınca, gelecekte yalnızca ürünün tüm yaşam döngüsü boyunca yeterli düzeyde siber güvenlik sağlayan ürünler piyasaya sürülebilecektir. Regülasyon, Avrupa Birliği Resmi Gazetesi'nde 20.11.2024'te yayınlandı. Üreticiler için suistimal edilen güvenlik açıklarına ilişkin raporlama yükümlülükleri 11.09.2026 itibarıyla geçerlidir. Dijital unsurlar içeren ürünlerin AB ülkelerinde piyasaya sunulabilmesi için 11.12.2027'den itibaren CRA gerekliliklerini karşılaması gerekir. CRA bir AB Regülasyonudur ve bu nedenle AB üye ülkelerinde hemen geçerli olacaktır.

CRA, Makine Regülasyonu ile paralel olarak uygulanacaktır. Bu, bir makinenin aynı zamanda dijital unsurları olan bir ürün olarak görüldüğü anlamına gelir. Bu da, Makine Regülasyonu gerekliliklerinin yanı sıra CRA'nın da gereklilikleri olduğunu gösterir.

Makine Regülasyonu, makinenin yakın çevresindeki kişileri korumayı hedeflerken, CRA ayrıca gerçek ve tüzel kişileri ekonomik kayıplara karşı koruduğu için gereklidir.

Uygulamada, bir siber güvenlik önlemi hem CRA hem de Makine Regülasyonu gerekliliklerini karşıladığında potansiyel olarak sinerji etkileri ortaya çıkabilir. Bu sinerji etkileri, örneğin uyumlaştırılmış standartların uygulanması yoluyla, üretici tarafından doğrulanmalıdır.

Pratik ipucu:
AB düzeyindeki mevzuat değişikliklerinden her zaman haberdar olmak için **https://eur-lex.europa.eu** adresindeki haber bültenine ve RSS akışlarına abone olun.

1.4. İş ekipmanlarının kullanımı için emniyet ve sağlık gerekliliklerine ilişkin direktif 2009/104/AT

Tesis ve makineleri işleten şirketler, artık hangi yükümlülüklere uymaları gerektiği sorusunu kendilerine sormalıdır. İş ekipmanlarının iş yerinde çalışanlar tarafından kullanımına ilişkin asgari emniyet ve sağlık gerekliliklerini belirleyen Direktif, bu konudaki spesifikasyonları sunmaktadır. Direktif,
3 Ekim 2009 tarihinde Avrupa Birliği Resmi Gazetesi'nde yayınlandı ve ardından tüm üye devletler tarafından ulusal mevzuatlarına dahil edildi. Burada "iş ekipmanı", iş yerinde kullanılan herhangi bir araç, gereç, makine veya düzenek olarak tanımlanır.

Bu Direktif uyarınca, işverenin yükümlülüklerinden biri de çalışanlara uygun iş ekipmanı sağlamak ve böylece ekipman kullanımdayken çalışanın emniyetini ve sağlığını korumaktır.

İş ekipmanı, tüm kullanım süresi boyunca, uygun bakım prosedürleri gibi yollarla, yürürlükteki t üm ilgili AB Topluluk Direktiflerinin hükümlerine uygun şekilde muhafaza edilmelidir.

Makine Regülasyonu, resmi olarak bir Direktif değil Regülasyon olsa da, yasal açıdan ilgili bir Topluluk Direktifi olarak değerlendirildiği varsayılmalıdır. Bu nedenle, Makine Regülasyonundaki yeni gereklilikler, Makine Regülasyonu yürürlüğe girdiği andan itibaren mevcut makineler için de geçerli olacaktır.

Şekil 5: Makine Emniyeti için yasal gerekliliklere dikkat edilmesi ve uyulması gerekir

2. Makine üreticileri için güvenlik

Makineler için güvenlik gerekliliklerinin artmasının iki ana nedeni vardır: Bir yandan, talepkar müşterilerin makinelerin güvenlik özellikleri hakkında sorular sorması, diğer yandan 2027 itibarıyla kanun yapıcıların, makinelerin Avrupa'da piyasaya sürülebilmesi veya tedarik edilebilmesi için belirli temel özellikleri zorunlu hale getirmesidir.

Ayrıca, çoğu makine üreticisinin kanun yapıcılar tarafından önemli kuruluşlar olarak kabul edildiğini ve dolayısıyla NIS 2 Direktifi'ne tabi olduklarını unutmamak önemlidir. Bu da, bir **Bilgi Güvenliği Yönetim Sistemi (ISMS)** kullanmaya başlamalarının önerildiği anlamına gelir.

Kısaca:
Yeni Makine Regülasyonunun gerekliliklerini karşılamayan makineler, 20.01.2027 itibarıyla artık AB'de piyasaya sürülemez. Önlem alınıp alınmaması gerektiği ve alınması gereken önlemler, yapılandırılmış bir risk analiziyle belirlenebilir.

Siber Dayanıklılık Yasası (CRA), kapsamlı bilgi ve dokümantasyon yükümlülükleri de gerektirecektir.
Üreticiler için raporlama yükümlülükleri 11.09.2026 itibarıyla, CRA ise bütünüyle 11.12.2027 itibarıyla geçerli olacaktır.

2.1. Makine Regülasyonu kapsamında güvenlik

Makine Regülasyonu, Bölüm 1.1.9'da belirtilen temel emniyet ve sağlık gerekliliklerinde yolsuzluğa karşı koruma gerektirir. Bu durum şu şekilde açıklanır:

> "[…] Makine veya ilgili ürün, **başka bir cihazın**, **bağlı cihazın herhangi bir özelliği** veya makine ya da ilgili ürünle iletişim kuran herhangi bir uzak cihaz aracılığıyla kendisine bağlanmasının **tehlikeli bir duruma yol açmayacağı** şekilde tasarlanmalı ve üretilmelidir.
>
> **Makinenin veya ilgili ürünün**, temel emniyet ve sağlık gerekliliklerine **uygunluğunu sağlamak için kritik öneme sahip yazılıma bağlantı veya erişim sağlayan sinyal ya da veri ileten donanım bileşenleri, kazara veya kasıtlı bozulmalara karşı yeterli şekilde korunacak şekilde tasarlanmalıdır. Makine** veya ilgili ürün, uyumluluğu açısından **kritik** olan bir yazılıma bağlantı veya erişim sağladığında, söz konusu donanım bileşenine meşru veya gayrimeşru bir müdahalede bulunulduğuna dair kanıt toplamalıdır.
>
> Makine veya ilgili ürün için, ilgili temel emniyet ve sağlık gerekliliklerine uyum açısından kritik öneme sahip **yazılım ve veriler**, **açıkça tanımlanmalı ve kazara veya kasıtlı bozulmalara karşı yeterli düzeyde korunmalıdır.**
>
> Makine veya ilgili ürün, emniyetli çalışması için gerekli olan yüklü yazılımı belirtmeli ve bu bilgileri her zaman kolayca erişilebilecek şekilde sunmalıdır.
>
> Makine veya ilgili ürün, yazılıma meşru veya gayrimeşru bir müdahalede bulunulduğuna veya makine veya ilgili ürüne ya da konfigürasyonuna yüklenen yazılımdabir değişiklik yapıldığına dair kanıt toplamalıdır. […]"

Bölüm 1.2.1 Kontrol sistemlerinin emniyeti ve güvenilirliği şu gerekliliği de içerir:

> “[...] Kontrol sistemleri, şunları sağlayacak şekilde tasarlanmalı ve tesis edilmelidir:
>
> a) Koşullar ve riskler dikkate alındığında, amaçlanan çalışma gerilimlerine, amaçlanan ve amaçlanmayan dış etkilere, üçüncü taraflardan gelebilecek ve tehlikeli bir duruma yol açabilecek, **makul ölçüde öngörülebilir kötü amaçlı girişimlere karşı dayanıklı olmalı;** [...]

"Yolsuzluğa karşı koruma" koruma hedefinin daha ayrıntılı tanımı ve teknik uygulaması, yeni bir Avrupa standardı olan EN 50742'de belirtilecektir. Bu, şu anda geliştirme aşamasındadır. Bu standardın Makine Regülasyonu için geçiş dönemi sona ermeden önce yayınlanıp yayınlanmayacağı ve uyumlaştırılıp uyumlaştırılmayacağı henüz kesin olmadığından, mevcut durum hakkında şimdiden bilgi alınması tavsiye edilir. Burada başvurabileceğiniz bir kaynak, örneğin IEC TS 63074'tür. Bu spesifikasyon, emniyetle ilgili kontrol sistemlerinin fonksiyonel emniyetiyle ilişkili güvenlik hususlarını açıklar. IEC 62443-3-3, endüstriyel otomasyon sistemlerine yönelik güvenlik gerekliliklerini de belirler. Bu kılavuzun ekinde, standartlar ailesine ilişkin temel bilgiler sunulur.

Bazı Makine Regülasyonu gereklilikleri, doğru bileşenlerin seçilmesiyle sağlanabilirken, diğerleri için ek dokümantasyon sunulması gerekir. Pragmatik bir yaklaşım benimsemek amacıyla, makine geliştirme sürecinin tasarım aşamasında sistemli bir risk analizi yapmaya başlanması tavsiye edilir. Bu süreç daha sonra da yapılabilir, ancak deneyimler, geliştirme süreci ne kadar ilerlerse o kadar çok çaba harcandığını göstermektedir.

Şekil 6: AB Makine Regülasyonu, uygunluk değerlendirme sürecinde Endüstriyel Güvenliği zorunlu kılmaktadır

2.2. Bileşen üreticileri ve müşteriler arasında

Makinenin emniyetli ve yasalara uygun şekilde çalıştırılması, makine operatörlerinin görevidir. Uygulama sırasında, makine üreticileri ve entegratörler, müşterilerin gerekliliklerini ve bileşen üreticileri tarafından sunulan ürünleri dengelemelidir.

C Tipi standartlar destek sağlar. Belirli uygulama alanları için son teknolojiyi tanımlar ve bir makinenin sağlaması gereken asgari emniyet seviyelerini belirler. Şu anda güvenlik boyutunu göz önünde bulunduran uyumlaştırılmış bir C standardı bulunmadığından, atılabilecek en iyi adım, mevcut uluslararası standartları mümkün olduğunca uygulayarak bir risk analizi gerçekleştirmek ve bu analizden elde edilen verilerle riskleri azaltmaya yönelik önlemler almaktır.

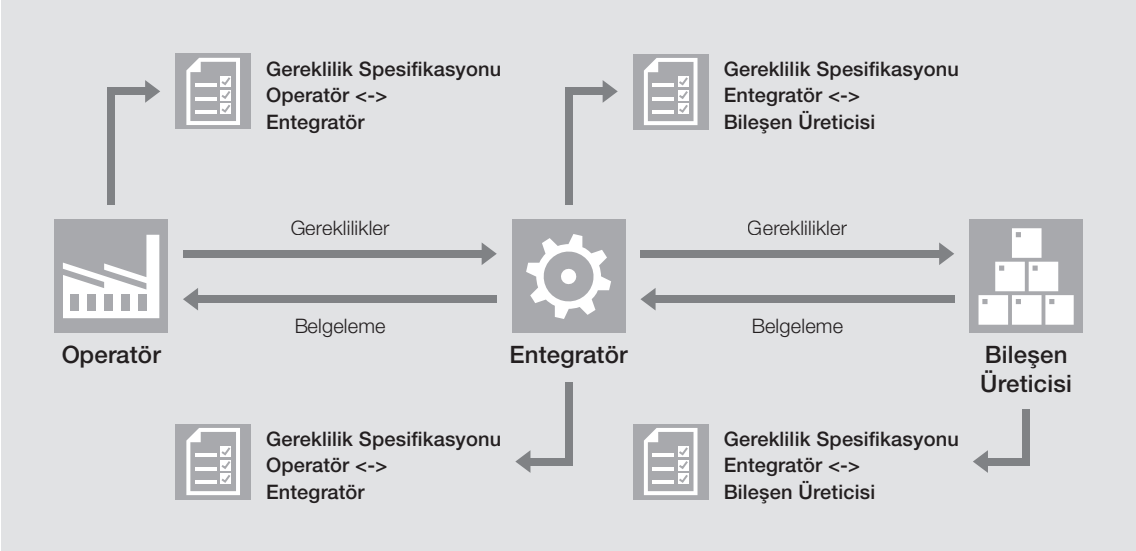
Risk analizini doğru bir şekilde yapabilmek için, makinedeki ortam koşulları ve güvenlik gereklilikleri hakkında detaylı bilgi sahibi olmak büyük önem taşır. Burada iki faktör önemlidir: bir yanda zararın potansiyel boyutu, yani saldırganın zarar verme motivasyonunun ne kadar yüksek olduğu, diğer yanda ise saldırı olasılığı, yani bu tür bir saldırının gerçekleşme ihtimali. Serbestçe erişilebilen bir makinenin saldırıya uğrama olasılığı, yalnızca sınırlı bir grup insanın erişebildiği bir makineden daha yüksektir.

Akıllı telefonlar ve bilgisayarlar gibi günlük ürünlerdeki güvenlik güncellemeleri herkes tarafından bilinir. Makine kontrolörleri ve diğer makine bileşenleri de güvenlik açığı tespit edilmesi durumunda güncellenmelidir. Mevcut durumda, çoğu bileşen otomatik güncelleme gerçekleştirmez ve bileşen üreticileri genellikle operatörlerle doğrudan iletişimde değildir. Bu durum, operatörlerin makinelerinin gerekli güncellemeleri zamanında alıp almadığından nasıl emin olabilecekleri sorusunu gündeme getiriyor.

Makine üreticisi veya sistem entegratörü anlamına gelen entegratör, burada önemli bir role sahiptir ve operatör ile bileşen üreticisi arasında iletişim kurmak için konumunu kullanabilir. Bileşen üreticisine operatörün güvenlik gereklilikleriyle yaklaşabilir ve doğru bileşenleri seçebilirler. Bununla birlikte, yeni güvenlik güncellemeleri gibi bileşenler hakkındaki bilgileri operatörle paylaşabilirler.

Pratik ipucu:
Alman Mühendislik Derneği VDMA e. V., Endüstriyel Güvenlik çalışma grubunda operatörler, entegratörler ve bileşen üreticileri arasındaki iletişimi kolaylaştırmayı amaçlayarak tek tip bir yaklaşımı desteklemek için "Tedarik Zinciri Güvenliği" belge serisini oluşturdu:
www.vdma.org

Aşağıdaki resimde operatörler, entegratörler ve bileşen üreticileri arasındaki arayüzler gösterilmiştir.



Şekil 7: VDMA'dan tedarik zinciri için öneriler (kaynak: https://www.vdma.org/cybersecurity)

2.3. Makine üreticileri için Siber Dayanıklılık Yasası

Siber Dayanıklılık Yasası (CRA), 20.11.2024 tarihinde Avrupa Birliği Resmi Gazetesi'nde yayınlanan bir regülasyondur. Dijital unsurlar içeren ürünleri ifade eder. Dijital unsurlar içeren tüm ürünler, 11.12.2027 tarihinden itibaren CRA gerekliliklerini karşılamalıdır. Dijital unsurlar içeren ürünlerin üreticileri, bunun öncesinde, 11.09.2026 tarihinden itibaren raporlama yükümlülüklerine uymalıdır. Bir makine CRA kapsamındaysa, üreticinin de CRA'ya uygunluğunu belgelemekle yükümlü olduğu varsayılabilir. Bu, bir dizi gerekliliğin karşılanması gerektiği anlamına gelir.

Diğer gereklilikler de geçerli olmakla birlikte, aşağıdakiler özellikle vurgulanmaya değerdir.

- Üreticilerin, suistimal edilen güvenlik açıklarını 24 saat içinde yetkililere **raporlama yükümlülüğü**.
- Dijital unsurlar içeren ürünler, **tespit edilen riske karşılık gelen uygun bir siber güvenlik derecesi sağlayacak** şekilde tasarlanır, geliştirilir ve üretilir.
- Risk analizi doğrultusunda, ürünler yalnızca **tespit edilen istismar edilebilir**güvenlik açıkları olmadan piyasaya sunulabilir.
- Güvenlik açıklarının **güvenlik güncellemeleri** aracılığıyla giderilebileceğinin garanti edilmesi
- Hizmet reddi saldırılarına karşı arıza emniyeti ve iyileştirici önlemler de dahil olmak üzere, bir olaydan sonra bile **kritik ve temel fonksiyonların kullanılabilirliğinin korunması**
- **Dijital unsurlar içeren ürünlerin güvenlik açıklarının ve bileşenlerinin** üreticiler tarafından belirlenmesi ve belgelenmesi. En azından ürünlerin en önemli bağımlılıklarını kapsayan makine tarafından okunabilir formatta bir Yazılım Malzeme Listesi oluşturmak da bu sürece dahildir.
- Ayrıca, üreticinin ürün için güvenlik güncellemeleri sağladığı süre gibi, **güvenlik açıklarının ele alınmasına ilişkin ek belgeler**.
- AB Uygunluk Beyanının Oluşturulması

CRA'dan alınan bu (tam kapsamlı olmayan) gereklilikler listesi, ilgili tüm ekonomik operatörler açısından ciddi bir çaba gerektireceğini açıkça ortaya koymaktadır. Bu spesifikasyonların ürün çeşitliliği üzerindeki etkisi ve öngörülen üç yıllık geçiş süresinin yeterli olup olmayacağı henüz netlik kazanmamıştır.

Pilz, tüm makine üreticilerinin bu konuyu en kısa sürede ele almasını ve CRA gerekliliklerini karşılayacak konseptler geliştirmek üzere bileşen üreticileri ve operatörlerle iş birliği içinde çalışmasını önermektedir.

Pratik ipucu:
Ortak Güvenlik Danışmanlığı Çerçevesi (CSAF), Güvenlik Danışmanları olarak adlandırılan makine tarafından işlenebilir güvenlik açığı ve hafifletme bilgilerinin iletişimi ve otomatik dağıtımı için standartlaştırılmış, açık kaynaklı bir çerçevedir:
https://oasis-open.github.io/csaf-documentation

Pratik ipucu:
Yazılım Malzeme Listesi (SBOM) sayesinde, kullanılan tüm yazılım sürümlerine dair kapsamlı bir genel bakış elde etmek mümkündür.

3. Makine operatörleri için güvenlik

Makine operatörleri de yeni yasal düzenlemelerden etkilenmektedir: yeni makinelerin tedariki, mevcut makinelerde yapılan değişiklikler ve teknolojinin güncel durumunun korunup korunmadığının sürekli denetlenmesi.

Makineler genellikle üretim sektöründe kullanıldığından, makine operatörlerinin de NIS 2 Direktifi'ni izlemesi gerekir.

Kısaca:
Mevcut tesislerin operatörleri de yeni Makine Regülasyonundan etkilenmektedir. Ağ segmentasyonu ve erişim olanaklarının kısıtlanması yoluyla, gerekli koruma genellikle sonradan da sağlanabilir. Önceden gerçekleştirilen yapılandırılmış bir risk analiziyle gerekli eylemler belirlenir.

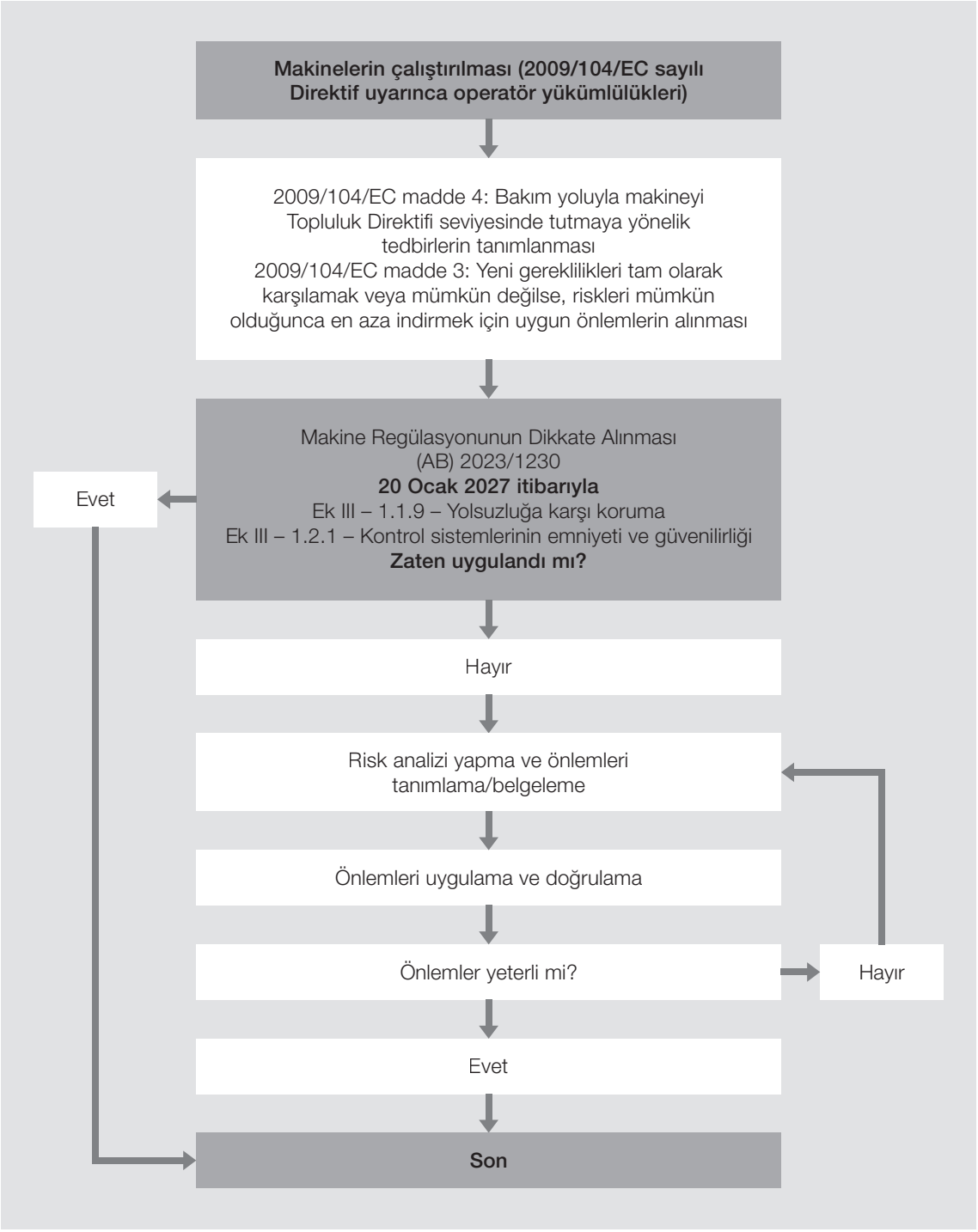
NIS 2 Direktifi, büyük bir grup üretim şirketinden kapsamlı güvenlik konseptleri talep etmektedir.
Ağa bağlı makineler bu değerlendirmelere dahil edilmelidir.

3.1. Mevcut kurulumların yönetimi

Genellikle iş ekipmanı olarak kullanılan makinelerin operatörleri, çalışanlar için iş emniyetinin yeterli olduğundan ve kimsenin yaralanmadığından emin olmalıdır. Bu, yukarıda açıklanan ve tüm üye devletler tarafından iç hukukta uygulanan 2009 tarihli **İş ekipmanlarının kullanımı için emniyet ve sağlık gerekliliklerine ilişkin AB Direktifi**'nde belirtilmektedir.

Bu Direktif, operatörün, iş ekipmanının ilgili bakım süreçleriyle tüm kullanım süresi boyunca yürürlükteki tüm ilgili AB Topluluk Direktiflerinin hükümlerine uygun bir seviyede tutulmasını sağlamak için düzenli kontroller yapmasını gerektirir.

Aksine, bu şu anlama gelir: Makine Regülasyonunun yürürlüğe girdiği günden, yani 20 Ocak 2027 tarihinden itibaren, tüm aktif makinelerin Makine Regülasyonuna uygun olup olmadıkları kontrol edilmiş olmalıdır. İşverenin gereklilikleri tam olarak karşılayamadığı durumlar ortaya çıkabilir. Bu gibi durumlarda, riskleri mümkün olan en üst düzeyde azaltmak için gerekli önlemleri alma yükümlülüğü devam eder.



Şekil 8: Süreç iş akışı – Mevcut kurulumların yönetimi

Bu konuyu henüz değerlendirmemiş operatörler, siber güvenlikle ilgili yeni gereklilikleri karşılamak amacıyla önlemler almalıdır.

İlk adım risk analizi gerçekleştirmektir. Uygulanacak önlemler, bu risk analizine göre belirlenir. Çoğu durumda bu, ağın segmentasyonunu ve erişim fırsatlarının kısıtlanmasını içerir.

3.2. IT Güvenliğinden şirket genelinde Güvenliğe

Genel olarak, bir şirketteki bilgi ve iletişim teknolojilerinden, IT Güvenliği de dahil olmak üzere, Bilgi Teknolojileri (IT) departmanı sorumludur.

Şirketlerde güvenlik konusu, örneğin bir personel fonksiyonu olarak yapılandırılır. Örneğin Baş Bilgi Güvenliği Görevlisi (CISO), NIS 2 Direktifi'nin gerekliliklerine hakim olmalı ve bu gerekliliklerin şirket genelinde nasıl uygulanacağına dair bir konsepte sahip olmalıdır.

Deneyimlerimiz, şirketteki üretim alanının IT Güvenliği ile ilgili sorularda şirketin IT departmanına güvendiğini ve konuyla yalnızca yüzeysel şekilde ilgilendiğini göstermektedir.

Üretim alanındaki makineler şirketin güvenlik konseptinin bir parçası olduğundan, bu alanda kesinlikle yeni bir düşünce tarzı gereklidir. Genel konseptin doğru bir şekilde uygulanabilmesi için şirket, emniyet bölgelerine ayrılmalı; her bir bölge için arayüzler ve gereklilikler tanımlanmalı ve bu yapı, şirkette makine seviyesine kadar uygulanmalıdır.

Şekil 9: Endüstriyel Güvenlik, IT Güvenliği ve OT Güvenliği arasındaki korelasyonu da etkiler.

Pratik ipucu:
https://www.shodan.io/ arama motoru kullanılarak, ağa bağlı cihazlar ve genellikle ağ segmentasyonu nedeniyle artık erişilebilir olmaması gereken cihazlar tespit edilebilir. Cihazlarınız orada da listeleniyor mu?

Pratik ipucu:
En yaygın saldırı türlerinden biri, kimlik avı e-postaları gibi yollarla şirket çalışanları üzerinden gerçekleştirilen saldırılardır. Personelin düzenli olarak eğitilmesi bu riski azaltır.

4. Emniyetli makinelere giden yol – Emniyetli ve Güvenli

Kısaca:
Yapılandırılmış bir risk analiziyle, karşı önlemlerin ve analiz sürecinin maliyetleri büyük ölçüde azaltılabilir. Burada, olası saldırı yollarının sayısı, tanımlanan koruma hedeflerini gerçekten tehdit edenlerle sınırlanmıştır. Olası hasar düzeyinin ve meydana gelme olasılığının değerlendirilmesi, riskleri en aza indirmek için yapılacak uygun çalışmalara dair ek göstergeler sağlar.

Makinelerdeki güvenlik riskleri, hem veri ağları üzerinden hem de fiziksel olarak makineye doğrudan erişim yoluyla farklı şekillerde ortaya çıkabilir. Bir makineye mümkün olan en uygun maliyetli korumayı sağlamak için aşağıda açıklanan şekilde yapılandırılmış bir yaklaşım tavsiye edilir.

- **Varlıkları tanımlayın** İlk adımda, korunacak varlıklar belirlenir ve birbirinden ayrılır. Sonuçta, korunacak tesislere ve tesis bölümlerine ilişkin eksiksiz ve tutarlı bir görünüm elde edilir. Bu önlem, hiçbir parçanın gözden kaçmamasını ve aynı zamanda tehdit vektörlerinin gereksiz yere birden fazla kez dikkate alınmamasını sağlar.
- **Tehditleri analiz edin** Bir sonraki adımda, bir tehlike durumunda olası zararın miktarı belirlenmelidir. Bilgi Güvenliğinin üç koruma hedefi ayrı olarak değerlendirildiğinde, bu soruya cevap vermek daha kolaydır. Bunlar Gizlilik, Bütünlük ve Kullanılabilirliktir ve genellikle CIA olarak kısaltılır.
  - **Gizlilik** Makine, açıklanması durumunda şirkete zarar verebilecek bilgiler içeriyor mu? Bu, şirkete rekabet avantajı sağlayan üretim süreçleri, tarifler veya diğer ticari sırlarla ilgili bilgiler olabilir. Potansiyel hasar ne kadar ciddi olabilir?
  - **Bütünlük** Verilerde istenmeyen bir değişiklik yapılmasının ne gibi etkileri olabilir? Verilerdeki değişiklik, makinenin zarar görmesi gibi ekonomik kayıplara yol açabilir mi veya örneğin emniyet fonksiyonlarını etkileyerek insanları tehlikeye atabilir mi? Potansiyel hasar ne kadar ciddi olabilir?
  - **Kullanılabilirlik** Bir makinenin arızalanması, örneğin üretim kesintileri nedeniyle ne gibi ekonomik kayıplara yol açar?
- **Koruma hedeflerini belirleyin** Koruma hedefleri, bu ön çalışmanın ardından belirlenebilir. Bu hedeflerin daha somut bir şekilde tanımlanması, tehdit vektörlerinin daha spesifik bir şekilde belirlenmesine olanak tanır. Böylece, makinelerin güvenliğini artırabilecek ancak belirlenen koruma hedeflerine ulaşmaya yardımcı olmayan gereksiz önlemler engellenir.
- **Riskleri değerlendirin** Koruma hedefleri belirlendikten sonra, belirlenen risklerin gerçekten gerçekleşme olasılığı tahmin edilir. Sonuçta, ilave önlemlerin mantıklı kapsamına dair bir gösterge elde edilir.
- **Tehdit vektörlerini analiz edin** Bu adımda, bir saldırının gerçekten hangi yollarla gerçekleşebileceği ve örneğin kullanılan makine bileşenlerindeki dahili koruyucu önlemler aracılığıyla halihazırda hangi koruyucu önlemlerin mevcut olduğu sistemli olarak belirlenir. Bu şekilde, kalan tehdit nedenlerinin bir listesi elde edilir.

- **Güvenlik konsepti oluşturun ve uygulayın** Güvenlik konsepti, söz konusu makine için tanımlanan koruma hedeflerine ulaşmak için gereken tüm önlemlerin somut bir açıklamasını sunar. Bu önlemler, makine üzerinde tasarım önlemleri olabileceği gibi, süreçlere ilişkin organizasyonel düzeltmeler de olabilir.
- **Uygulamayı kontrol edin** Alınan önlemlerin gerçek etkinliği, ancak uzman sağlayıcılar tarafından korsan saldırılarının simüle edildiği çok karmaşık sızma testleri ile kontrol edilebilir. Alternatif olarak, güvenlik konseptinin doğru şekilde uygulanıp uygulanmadığı kontrol edilebilir.
- **Düzenli yeniden değerlendirmeler yapın** Emniyet ile karşılaştırıldığında, güvenlik için alınan koruyucu önlemler tek seferlik değildir. Karmaşık sistemlerde sürekli olarak yeni güvenlik açıkları ortaya çıktığı için, analiz düzenli aralıklarla veya tehditlerin ortaya çıkması durumunda tekrarlanmalıdır. Yeni güvenlik açıkları, tedarik piramidinin tüm seviyelerinde ortaya çıkabilir; örneğin, donanım bileşenleri, cihazlardaki açık kaynak kodu veya belirli bir cihazın ürün yazılımı gibi alanlarda. Bir güvenlik açığı tespit edilir edilmez, sorumlu üreticiler, tehdit hakkında bilgi ve uygun karşı önlemlerle ilgili notlar içeren ilgili Güvenlik Tavsiyelerini yayınlar. Tedarikçilerden gelen yeni Güvenlik Tavsiyelerini düzenli olarak kontrol etmeniz önerilir.

Şekil 10: Bileşenler, tesis ve makineler ancak bir güvenlik denetimi yoluyla gerçek anlamda güvenilir bir şekilde güvence altına alınır ve bozulmaya karşı korunur.

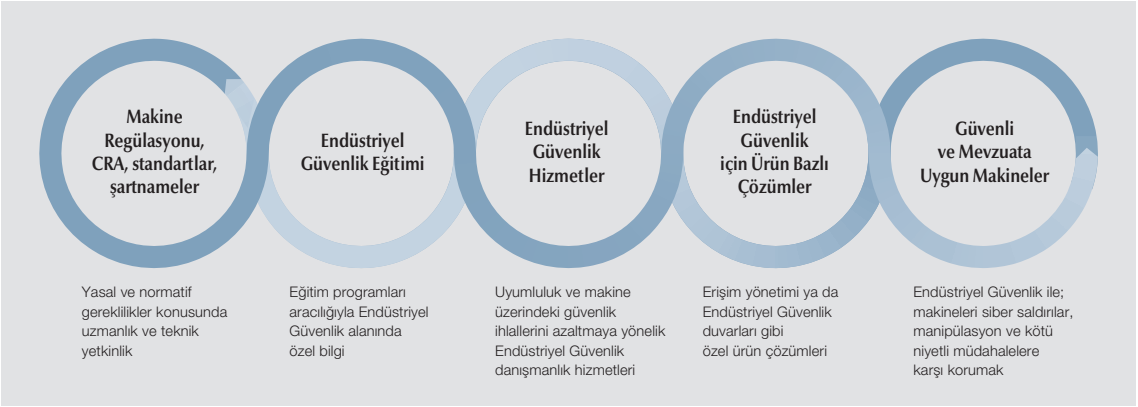
Pratik ipucu:
Pilz Güvenlik Tavsiyelerine **www.pilz.com/advisories adresinden ulaşabilirsiniz.**

5. Tek noktadan Emniyet ve Güvenlik

Güvenlik konusundaki yeni yasal spesifikasyonlar, makine üreticileri ve operatörleri için yeni zorluklar yaratmaktadır. Makinelere yönelik saldırılar için risk azaltma süreçleri (Güvenlik), makinelerden kaynaklanabilecek risklerin azaltılmasına yönelik prosedürler (Emniyet) ile oldukça benzerlik göstermektedir. Pilz, Makine Emniyeti alanında uzmandır ve şirkete özel çözümler ve emniyetli (Emniyetli ve Güvenli) makineler elde etmek için adım adım yardımcı olur.

Şekil 11: Emniyet ve Güvenlik, Makine Emniyetinde bütünsel bir konseptin parçasıdır

- Standart komitelerine katılım yoluyla uzman bilgisi ve uzmanlık
- Mevcut standartların ve yasal uygulamaların araştırılması ve takibi
- Makine odaklı Endüstriyel Güvenlik için temel ve uzmanlık seviyesinde eğitimler
- Makine odaklı Endüstriyel Güvenliğin bir parçası olarak sunulan hizmetler
  - Koruma gereklilikleri analizi
  - Risk analizleri
  - Bütünsel güvenlik konseptleri
  - Doğrulama/onaylama
  - Süreç optimizasyonu
- Ürünler ve çözümler makinede fiziksel erişim kontrolü ve siber güvenlik için



Şekil 12: Makineleri Endüstriyel Güvenlik çözümleriyle adım adım koruyun

Pratik ipucu:
Pilz'in Endüstriyel Güvenlik çözümleriyle ilgili daha fazla bilgiye **www.pilz.com/security adresinden ulaşabilirsiniz.**

6. Özet ve genel bakış

Siber saldırılar ve yolsuzluk gibi tehditlerin artışı, Avrupa'daki yasal durumu doğrudan etkileyerek kanun yapıcıların Endüstriyel Güvenlik konusunda daha net bir yaklaşım benimsemelerine yol açmaktadır. Gelecekte, kanun yapıcılar özellikle Makine Regülasyonu, NIS 2 Direktifi ve CRA aracılığıyla Endüstriyel Güvenlik için yeni gereklilikler getireceklerdir. Makine üreticileri ve operatörler için bu, şirketler, makineler ve bileşenler için yeni gereklilikleri karşılamak üzere kurumsal ve teknik önlemler geliştirilip uygulanarak aktif bir katılım sağlanması anlamına gelmektedir. Yukarıdaki kılavuzda, bu görevler ve bunların nasıl yönetileceği incelenmiştir.

NIS 2 Direktifi, makine üreticileri ve operatörlerinin büyük bir kısmı için halihazırda bağlayıcıdır. Yeni Makine Regülasyonu ve CRA ise 2027 yılında yürürlüğe girecektir. Proaktif bir yaklaşım, gerekli projelerin zamanında planlanmasını ve hayata geçirilmesini sağlayacaktır.

Standart komiteleri, makine üreticilerine yeni gerekliliklerin nasıl uygulanacağı konusunda rehberlik eder. IEC 62443 standart serisinde açıklandığı gibi, yapılandırılmış bir yaklaşım büyük önem taşır.

Deneyimli ve nitelikli hizmet sağlayıcılar, genellikle yeni hedef spesifikasyonları karşılamak için gereken önlemlerin adım adım analiz edilmesine makul bir çabayla yardımcı olurlar.

Makine Emniyeti, gelecekte hem insanları hem de makineleri korumak için Emniyet ve Güvenlik anlamına gelecek. Bütünsel ve koordine bir konsept sayesinde, Makine Emniyeti kapsamındaki karmaşık sorunlar verimli ve düzenli bir şekilde bölümlere ayrılabilir. Risk analizi, Endüstriyel Güvenlik için ilk adımdır ve şirketinizdeki gereklilikleri parçalara ayırmak için yapılandırılmış bir yönlendirme ve metodoloji sağlar.

Bu yaklaşım, şirketlere Endüstriyel Güvenlik alanındaki artan zorlukların üstesinden gelmek için gerekli araçları sunar.


Pilz'den Endüstriyel Güvenlik ile ilgili daha fazla bilgi – hemen keşfedin
PILZ
Buradan daha fazla bilgi alın:
www.pilz.com/security

7. Ek

7.1. Endüstriyel Güvenlik alanından terimler

AB Komisyonu'na göre, **siber güvenlik**, ağ ve bilgi sistemlerini, bu sistemlerin kullanıcılarını ve siber tehditlerden etkilenen diğer bireyleri korumak için gereken tüm görevleri kapsar.

Siber tehdit, ağ ve bilgi sistemlerine, bu sistemlerin kullanıcılarına ve diğer kişilere zarar verebilecek, aksamalara neden olabilecek veya başka bir şekilde olumsuz etki yaratabilecek potansiyel bir durum, olay veya eylemi ifade eder.

Endüstriyel Güvenliğin hedefi, tesis ve makinelerin kullanılabilirliğinin yanı sıra makine verilerinin ve süreçlerinin bütünlüğünü ve gizliliğini garanti etmektir.

IT Güvenliği (Bilgi Teknolojisi), fiziksel süreçlerle ilişkilendirilmeyen verilerin korunmasını sağlar.

OT Güvenliği (Operasyonel Teknoloji), fiziksel süreçlerde yer alan tesis ve makinelerin korunmasını sağlar.

IACS IEC 62443'ün kısaltmasıdır ve Endüstriyel Otomasyon ve Kontrol Sistemleri anlamına gelir.

IEC 62443 standart serisinde, **Güvenlik Seviyesi**, bir bölge veya kanal için yapılan risk değerlendirmesine dayalı olarak belirlenen, gerekli önlemler ve cihaz ve sistemlerin dahili güvenlik özelliklerine karşılık gelen seviyedir.

Bölge, denetlenen bir sistemin fonksiyonel, mantıksal veya fiziksel ilişkilerine (konum dahil) göre bölünmesini yansıtan birimlerden oluşan bir topluluktur.

Kanal, ortak IT güvenlik gerekliliklerinin geçerli olduğu iki veya daha fazla bölgeyi bağlayan iletişim kanallarının mantıksal bir gruplandırmasıdır.

7.2. IEC 62443 – Endüstriyel Güvenlik temel standardı

IEC 62443, "Endüstriyel iletişim ağları – Ağ ve sistem güvenliği" alanında bir dizi uluslararası standarttır.

7.2.1 Genel Bakış

IEC 62443 standartları ailesi, çeşitli bölümlerden oluşur ve bu bölümlerden aşağıda belirtilen standartlar halihazırda yayımlanmıştır.

Bölüm 1, genel ilkelerle ilgilidir:
- IEC TS 62443-1-1: Bölüm 1: Terminoloji, konseptler ve modeller
- IEC TS 62443-1-5: Bölüm 1-5: IEC 62443 güvenlik profilleri şeması

Bölüm 2, operatörler ve hizmet sağlayıcılar için geçerli olan güvenlik gerekliliklerini ifade eder:
- IEC 62443-2-1: IACS varlık sahipleri için güvenlik programı gereklilikleri
- IEC 62443-2-2: IACS Güvenlik Programı Derecelendirmeleri
- IEC TR 62443-2-3: IACS ortamında yama yönetimi
- IEC 62443-2-4: IACS hizmet sağlayıcıları için güvenlik programı gereklilikleri

Bölüm 3, otomasyon sistemleri için güvenlik gerekliliklerini ifade eder:
- IEC TR 62443-3-1: Endüstriyel Otomasyon ve Kontrol Sistemleri için güvenlik teknolojileri
- IEC TR 62443-3-2: Sistem tasarımı için güvenlik riski değerlendirmesi
- IEC 62443-3-3: Sistem güvenlik gereklilikleri ve güvenlik seviyeleri

Bölüm 4'te otomasyon bileşenleri için güvenlik gereklilikleri belirtilmektedir:
- IEC 62443-4-1: Güvenli ürün geliştirme yaşam döngüsü gereklilikleri
- IEC 62443-4-2: IACS bileşenleri için teknik güvenlik gereklilikleri

Bölüm 5'te IEC 62443 profilleri tanımlanmaktadır:
- IEC TS 62443-1-5: IEC 62443 güvenlik profilleri şeması

Bölüm 6'da değerlendirme metodolojisi açıklanmaktadır:
- IEC 62443-6-1: IEC 62443-2-4 için güvenlik değerlendirme metodolojisi

7.2.2 Güvenlik Seviyesi (SL)

Sistem ve bileşenlere yönelik gereklilikler Güvenlik Seviyeleri ile tanımlanır.
Bunlar aşağıdaki gibi tanımlanır:

- Güvenlik Seviyesi 0: Özel bir gereklilik veya koruma gerekmez
- Güvenlik Seviyesi 1: Kazara veya kasıtsız kötüye kullanıma karşı koruma
- Güvenlik Seviyesi 2: Az kaynak, genel beceriler ve düşük motivasyonla basit yollarla kasıtlı kötüye kullanıma karşı koruma
- Güvenlik Seviyesi 3: Orta seviye kaynaklar, IACS'ye özgü beceriler ve orta düzeyde motivasyon ile gelişmiş yollarla kasıtlı kötüye kullanıma karşı koruma
- Güvenlik Seviyesi 4: Genişletilmiş kaynaklar, IACS'ye özgü beceriler ve yüksek motivasyon ile gelişmiş yollarla kasıtlı kötüye kullanıma karşı koruma

Bu, gerekli Güvenlik Seviyesi arttıkça, uygulanan önlemlerin sağlaması gereken etkinliğin de arttığı anlamına gelir.

Yedi Temel Gereklilik (FR olarak kısaltılır) vardır:

- FR 1 – Yetkilendirme ve kimlik doğrulama kontrolü
- FR 2 – Kullanım kontrolü
- FR 3 – Sistem bütünlüğü
- FR 4 – Veri gizliliği
- FR 5 – Kısıtlı veri akışı
- FR 6 – Olaylara zamanında müdahale etme
- FR 7 – Kaynak kullanılabilirliği

Temel Gerekliliklerin her birinin arkasında, gerekli seviyeye ulaşmak için uygulanabilecek farklı kalitede önlemler bulunur. Tipik önlemler arasında çok faktörlü kimlik doğrulama veya şifreleme mekanizmaları vardır.

Ulaşılması gereken Güvenlik Seviyesi, söz konusu siber riske dayalıdır. Avrupa kanun yapıcıları önemli ve temel varlıklar arasında ayrım yapmaktadır. Bu nedenle kabul edilmesi gereken siber risk, şirketin türüne, büyüklüğüne ve potansiyel etkilere bağlıdır. Çeşitli standart kuruluşları şu anda bu konuyu ele almakta ve sektörler ve makine türleri için evrensel gereklilikleri tanımlamaktadır.

7.2.3 Bilgi Güvenliği Yönetim Sistemi (ISMS)

Bileşenler ve sistemler için teknik gerekliliklere ek olarak, başarılı bir saldırı riskini azaltmak için uygulanması gereken organizasyonel önlemler de vardır. Her şirket, Bilgi Güvenliği Yönetim Sistemini (ISMS) nasıl kurmak istediğine kendisi karar vermelidir. ISO/IEC 27000 standart serisi oluşturulmuştur ve yaygın olarak bilinmektedir. IEC 62443-2-1, ISO/IEC 27001'in endüstriyel otomasyon sistemlerine uygulanması için bir kılavuz olarak kabul edilebilir. Ayrıca, diğer şeylerin yanı sıra, endüstrisinde kendini kanıtlamış TISAX sertifikasyon programı da mevcuttur.

ISMS'de riskler adlandırılır, sınıflandırılır, değerlendirilir ve bunların nasıl yönetileceğine dair bir açıklama bulunur. Tipik olarak uygulama alanı ve diğer alanlara yönelik arayüzler öncelikle tanımlanmalıdır. Aşağıdakiler de oldukça önemlidir:
- Yönetimin güvenlik sorumluluğunu üstlenmesi
- Sorumlulukların netleştirilmesi
- İleri seviyede eğitim faaliyetlerinin tanımlanması
- Şirkette güvenlik kılavuzlarının oluşturulması

ISMS, risklerin sistemli bir şekilde değerlendirilmesine ve ilgili önlemlerin alınmasına yardımcı olur.

Şirket riskleri şunları içerebilir:
- Üretim kesintilerinden kaynaklanan ekonomik kayıplar
- Çalışanların yaralanması
- Veri koruma ihlalleri
- Çevresel hasar
- Müşteri güveni kaybı

Tipik önlemler şunları içermekle birlikte bunlarla sınırlı değildir:
- Uygulanacak acil durum planlarının geliştirilmesi
- Yetkili kullanıcıların tanımlanması
- Fiziksel ve sanal erişim kontrolü
- Ağ segmentasyonu

Önlemlerin nasıl uygulanacağı da ISMS tarafından belirlenir. Şunları içerir:
- Sistem geliştirme
- Sistem bakımı
- Veri yedekleme
- Olayların planlanması ve yönetilmesi

7.3. Makine üreticileri ve operatörleri için diğer faydalı belgeler

IEC 62443 standartlar ailesinin yanı sıra, makine üretimini etkileyen ve gereklilikleri tanımlayan başka güvenlik standartları da vardır.

IEC TS 63074, emniyetle ilgili kontrol sistemlerinin fonksiyonel emniyetiyle ilişkili güvenlik hususlarını açıklar. Bu teknik spesifikasyonda, bir makinenin güvenli ve emniyetli bir şekilde çalışması için dikkate alınması gereken IEC 62443 standartlar ailesinin ilgili unsurları tanımlanmıştır.

Makine Regülasyonunun "yolsuzluğa karşı koruma" gerekliliği için, yeni bir Avrupa standardı olan EN 50742 şu anda geliştirme aşamasındadır. Pilz, standartlar komitesinin aktif bir üyesidir.

2014/53/AB sayılı Radyo Ekipmanı Direktifi ve buna bağlı (AB) 2022/30 sayılı Regülasyon, güvenlik gereklilikleri doğurmaktadır. EN 18031 standart serisi, bu gereklilikler için geliştirilmiştir.

7.4. Purdue modelini kullanarak ağ segmentasyonu

Ağ segmentasyonu konusunu görselleştirmek için Purdue modeli kullanılabilir. Bu model, Mühendislik Profesörü Theodore Joseph Williams tarafından, 1990 yılında ABD'deki Purdue Üniversitesi'nde yayınlanmıştır. Aşağıdaki görselde, Purdue modeli, amaçlarımıza uygun önlem örneklerini içerecek şekilde genişletilmiştir.

Şekil 13: Purdue modelini kullanarak ağ segmentasyonu

Seviye 0, tipik olarak üretim ticaretindeki gerçek fiziksel süreçtir. Bu, genellikle sensör ve aktüatör teknolojisiyle izlenir ve devreye alınır. Bu cihazlar Seviye 1'de yer almaktadır. Süreç, genellikle Seviye 2'de bulunan bir programlanabilir lojik kontrolör (PLC) tarafından yönetilir. PLC programlaması, Seviye 3'teki üretim süreçleri sistemleri yoluyla gerçekleştirilir. Gerçek işler, Seviye 4'teki lojistik sisteminden alınır.

Seviye 0 ile 3 arası Operasyonel Teknoloji (OT), Seviye 4 ve üzeri ise Bilgi Teknolojisi (IT) kapsamına girer.

Şekilde, olası bir saldırıda hedef alınabilecek alanı en aza indirmek amacıyla, Seviye 4 ile 3 ya da Seviye 3 ile 2 arasındaki veri aktarımını sınırlayan güvenlik duvarlarıyla sağlanan bir segmentasyon türü gösterilmektedir.

Amaç, saldırı fırsatlarını etkili bir şekilde azaltırken sistem performansını da kısıtlamayan başarılı bir segmentasyon uygulamaktır. Bu noktada arayüzlerin açık şekilde tanımlanması gereklidir; böylece, örneğin bir güvenlik duvarı yapılandırılırken tüm gerekli bağlantı noktaları ve protokol türleri göz önünde bulundurulabilir.

Doğru bileşenlerin doğru şekilde seçilmesi, emniyetli ve güvenli çalışma için büyük önem taşır. Sonuçta, alt seviyelerde bileşenlerden kaynaklanan ek güvenlik açıkları varsa, en iyi güvenlik duvarı bile etkili olamaz. Gerekli Güvenlik Seviyesine bağlı olarak, sistemdeki bileşenlerin birbirlerinin kimliklerini doğrulamaları ve böylece sistemdeki değişiklikleri izlemeleri gerekebilir. Bileşenler ve konfigürasyonları seçilirken bu da dikkate alınmalıdır.

Bu örnekte, Seviye 3'teki tüm bileşenler birbirlerine kalıcı olarak bağlanmıştır ve bilgi akışı iki güvenlik duvarı ile güvence altına alınmıştır. Endüstriyel ortamda, sistemlerin kablosuz arayüzlere de sahip olması oldukça yaygındır (ör. otomatik yönlendirmeli araç sistemlerinde). Burada, güvenlik önlemlerinin nasıl etkili bir şekilde uygulanabileceğini belirlemek için kontroller yapılmalıdır.

Pratik ipucu:
Cihazlarınızın konfigürasyonuna yönelik pratik örnekleri **www.pilz.com** adresinde bulabilirsiniz.
"Uygulama notları" anahtar kelimesiyle arama yapabilirsiniz.

8. Literatür

- 1. Bilgisayarla Bütünleşik Üretim (CIM) için referans modeli: endüstriyel otomasyon perspektifinden bir açıklama. Düzenleyen: Theodore J. Williams, 1989
- 2. Endüstriyel iletişim ağları – Ağ ve sistem güvenliği – Bölüm 3-3: Sistem güvenlik gereklilikleri ve güvenlik seviyeleri IEC 62443-3-3:2013
- 3. Endüstriyel otomasyon ve kontrol sistemleri için güvenlik – Bölüm 4-2: IACS bileşenleri için teknik güvenlik gereklilikleri IEC 62443-4-2:2019
- 4. AB Makine Regülasyonu 2023/1230 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1230)
- 5. Avrupa Birliği genelinde yüksek düzeyde ortak bir siber güvenlik sağlanmasına yönelik önlemler hakkında Direktif (AB) 2022/2555 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555)
- 6. Siber Dayanıklılık Yasası P9_TA(2024)0130 (https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.pdf)
- 7. Direktif 2009/104/AT (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0104)
- 8. Avrupa Birliği Siber Güvenlik Ajansı (https://www.enisa.europa.eu/)
- 9. Pilz GmbH & Co. KG (https://www.pilz.com/en-INT/products/industrial-security/security-incident-management)
- 10. VDMA e. V. (https://www.vdma.org/cybersecurity)
- 11. Bilgi Güvenliği, siber güvenlik ve gizliliğin korunması – Bilgi Güvenliği Yönetim Sistemleri – Gereklilikler ISO/IEC 27001
- 12. Endüstriyel Güvenlik tanıtım belgesi (Pilz 2018) (www.pilz.com/security)
- 13. Makine Regülasyonu Kılavuzu tanıtım belgesi (Pilz 2023) (www.pilz.com/mr)
- 14. https://de.statista.com/statistik/kategorien/kategorie/21/themen/896/branche/cyberkriminalitaet/#overview (viewed 20/01/2025)
- 15. Siber Güvenlik Yasası AB 2019/881, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1728407971719

Destek

Teknik destek hizmeti Pilz tarafından günün her saati mevcuttur.

Amerika
ABD
+1 877-PILZUSA (745-9872)
Brezilya
+55 11 97569-2804
Kanada
+1 888 315 7459
Meksika
+52 55 5572 1300

Asya
Çin
+86 400-088-3566
Güney Kore
+82 31 778 3390
Japonya
+81 45 471-2281

Avustralya ve Okyanusya
Avustralya
+61 3 95600621
Yeni Zelanda
+64 9 6345350

Avrupa
Almanya
+49 711 3409-444
Avusturya
+43 1 7986263-444
Belçika, Lüksemburg
+32 9 3217570
Fransa
+33 3 88104003
Hollanda
+31 347 320477
İngiltere
+44 1536 460866
İrlanda
+353 21 4804983
İskandinavya
+45 74436332
İspanya
+34 938497433
İsviçre
+41 62 88979-32
İtalya, Malta
+39 0362 1826711
Türkiye
+90 216 5775552

Uluslararası teknik destek hattımıza aşağıdaki numaradan ulaşabilirsiniz:
+49 711 3409-222
support@pilz.com

Pilz ekolojik materyaller ve enerji verimliliği sağlayan teknolojiler kullanarak çevre-dostu ürünler üretir. Ofisler ve üretim alanları, enerji verimliliği ve çevre duyarlılığı dikkate alınarak ekolojik olarak tasarlanmıştır. Böylelikle Pilz önerdiği sürdürülebilirliğe ek olarak enerji verimliliğine sahip ürünlerin ve çevre-dostu çözümlerin güvenilirliğini de sunuyor.

BLUECOMPETENCE Alliance Member
Partner of the Engineering Industry Sustainability Initiative

German Standards
BRAND OF THE CENTURY 2022

Quality Management ISO 9001:2015 REG. NO. 2462
Environmental Management ISO 14001 REG. NO. 2462
Energy Management ISO 50001 REG. NO. 2462

Yetkili kişi:

Uluslararası temsil edilmekteyiz. Lütfen merkez ofisimizle veya www.pilz.com.tr internet sayfamızdan bizimle irtibata geçerek detaylı bilgi alın.

Merkez: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Almanya
Telefon: +49 711 3409-0, E-Mail: info@pilz.com, Internet: www.pilz.com

Çevreyi korumak için %100 geri dönüşümlü kağıt üzerine basılmıştır.

PILZ
THE SPIRIT OF SAFETY

8-4-tr-3-023, 2025-05 Printed in Germany
© Pilz GmbH & Co. KG, 2025

CECE, CHRE, CMSE®, INDUSTRIAL PI®, Leansafe®, Myzel®, PAS4000®, PAScal®, PASconfig®, Pilz®, PIT®, PMCprimo®, PMCprotego®, PMCtendo®, PMD®, PMI®, PNOZ®, Primo®, PSEN®, PSS®, PVIS®, SafetyBUS p®, SafetyEYE®, SafetyNET p®, THE SPIRIT OF SAFETY® are registered and protected trademarks of Pilz GmbH & Co. KG in some countries. We would point out that product features may vary from the details stated in this document, depending on the status at the time of publication and the scope of the equipment. We accept no responsibility for the validity, accuracy and entirety of the text and graphics presented in this information. Please contact our Technical Support if you have any questions.