



Hassas ölçüm sonuçları mı? Evet, kesinlikle!

Dünyadaki ağlar giderek çoğalıyor, dijitalleşme sürekli ilerliyor. Süreç otomasyonu alanı da bu bağlamda aynı şekilde devamlı ileri gidiyor. Ancak ilerlemenin olduğu yerlerde, yeni tehlikeler de yabana atılmamalı, çünkü siber saldırılar da daha büyük bir tehdit haline geliyor. VEGA, bu nedenle yeni radar sensör VEGAPULS 6X'i kapsamlı güvenlik önlemleri ile donattı.

VEGA seviye sensörleri, on yıllardan beridir endüstriyel proseslerin izlenmesini kolaylaştırmıştır. Bluetooth ile sağlanan kablosuz iletişim sayesinde, farklı endüstriyel alanların proses verilerinin, ölçüm değerlerinin ve durum göstergelerinin gerekli oldukları yerlerde –örneğin, tesisten uzaktaki ofislerde– kullanılması hızlanmıştır.

Siber saldırı: Tehlike nerede yatıyor?

Endüstri kollarında bilgisayar ve makinelerin birbirine olan ağ bağlantılarının gittikçe artması, sadece BT güvenliğine değil, aynı zamanda OT güvenliğine de, yani üretimde kullanılan kontrol teknolojilerinin güvenliğine de odaklanmayı gerektirmektedir. Çünkü bir sensörün verileri şirket ağına ulaşmadan önce, birkaç seviyeden geçmek zorundadır:

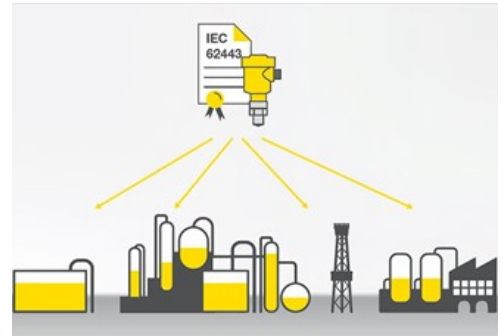
- Sensörler ölçülen değerleri önce ağ geçitlerine ve kontrol sistemlerine iletir.
- Sonra veriler buradan, kontrol odaları gibi kumanda edilebilen makine arayüzlerine gönderilir.
- Tüm bu veriler daha sonra üretim ve bakım sistemlerinde toplanarak BT tarafından işlenir.

Bu işlem aşamalarının her birinin, siber saldırılara karşı emniyet altına alınması gereken kendi arayüzleri vardır. Bütünsel bir güvenlik konsepti bu şekilde oluşturulur.

VEGAPULS 6X'in güvenlik konsepti nasıl işler?

Radar sensör VEGAPULS 6X, IEC 62443-4-2 güvenlik standardına uygun olarak sertifikalandırılmıştır. Bu şekilde, siber güvenlik bağlamında uluslararası standart donanım ve yazılımlarda uyulması zorunlu olan güvenlik koşullarının tanımladığı en yüksek güvenlik standartlarını yerine getirir. **VEGAPULS 6X**, derinlemesine bir savunma stratejisi, yani çeşitli BT güvenlik seviyelerini kapsayan kademeli bir güvenlik konsepti ile emniyet altına alınmıştır. Radar sensör, şu tehlikelere karşı korunmaktadır:

- Veri manipülasyonu
- Denial of Service (DoS: host hizmetlerinin aksatılması)
- Casusluk



Ölçüm cihazında ayrıca şu güvenlik fonksiyonları da mevcuttur:

- Kullanıcının kimlik doğrulaması: : VEGAPULS 6X, bireysel bir cihaz kodu ve Bluetooth erişim kodu ile birlikte teslim edilir.
- Olay günlüğü: Sensör, tüm kilitleme ve kilit açma işlemlerini kaydeder, saldırılar ve manipülasyon girişimleri bellekte bulunabilir.
- Bellek bütünlük kontrolü: Yazılım güncelleme paketi şifreli ve imzalıdır. Dolayısıyla, izin verilmemiş yazılımlar VEGAPULS 6X'e yüklenemez.
- Restorasyon amaçlı veri yedekleme: VEGAPULS 6X'in parametreleri, yedekleme yapılarak koruma altına alınır.

Radar sensör VEGAPULS 6X, ihtiyaca göre farklı güvenlik seviyeleriyle teslim edilir; en yüksek seviyelerde 2 faktörlü kimlik doğrulama gereklidir.

VEGA'nın BT bölümünde çalışan Jürgen ve Stefan, ortaya güvenilir bir sensör çıkarmak için sensörün geliştirilmesi esnasında nelerin dikkate alındığını aşağıdaki videoda anlatıyorlar.

PSIRT ne ifade etmektedir?

PSIRT, Ürün Güvenliği Olaylarına Müdahale Ekibi anlamına gelir. Bu ekip VEGA'da, **VEGAPULS 6X**'in devreye alınmasından sonra da siber güvenliğini takip eder. Ekip, sistemin potansiyel açıklarını bulur ve kapatır, bildirilen sorunları kontrol eder, çözümler geliştirir, yeni tehditleri değerlendirir, müşteriler için güncellemeleri ve diğer gerekli bilgileri sağlar. Radar sensörün, daima siber saldırılardan korunmasını sağlar.



VEGAPULS 6X

