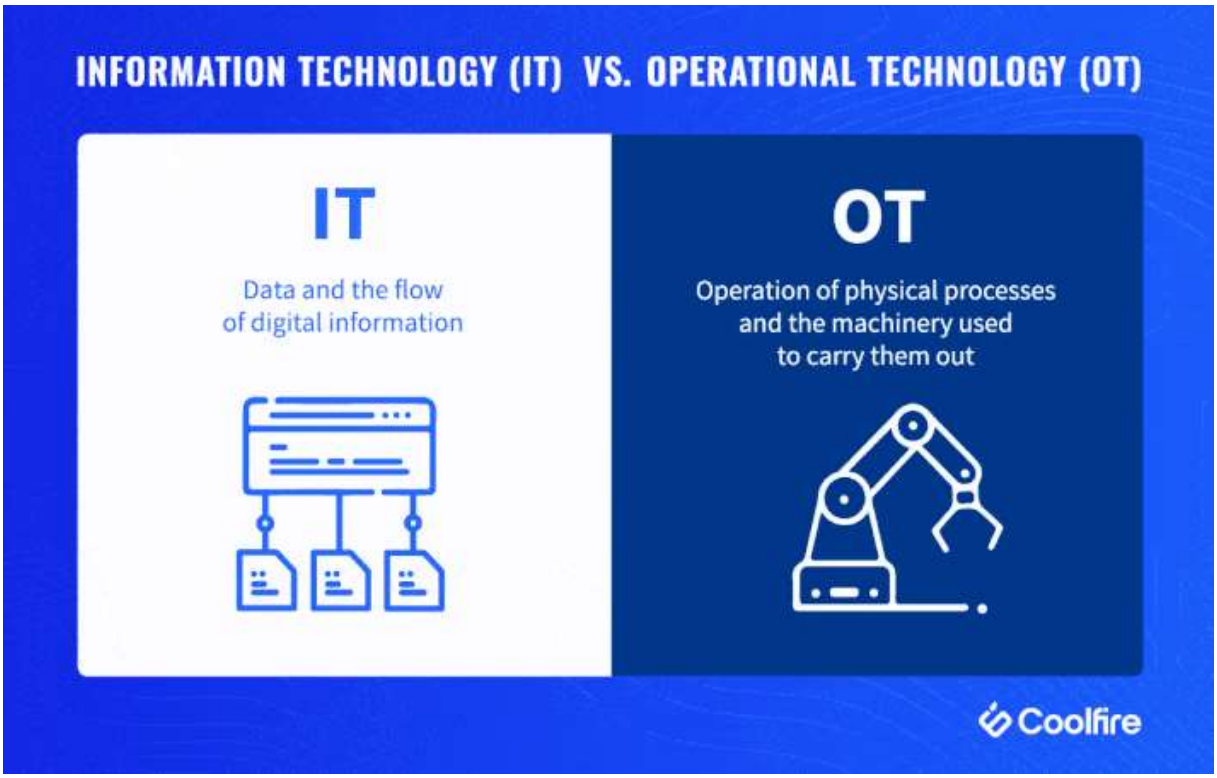
IT ile OT AĞLARI ARASINDAKİ FARKLAR NELERDİR?

Yağmur DELİCE

Karabük Üniversitesi

Bilgisayar Mühendisliği

yagmur.delice@gmail.com



IT (Bilgi Teknolojisi) Hakkında

Bilgi Teknolojisi (IT), genellikle bir işletme veya başka bir girişim bağlamında veri veya bilgi depolamak, almak, iletmek, çalışmak ve işlemek için bilgisayarların kullanılmasıdır.

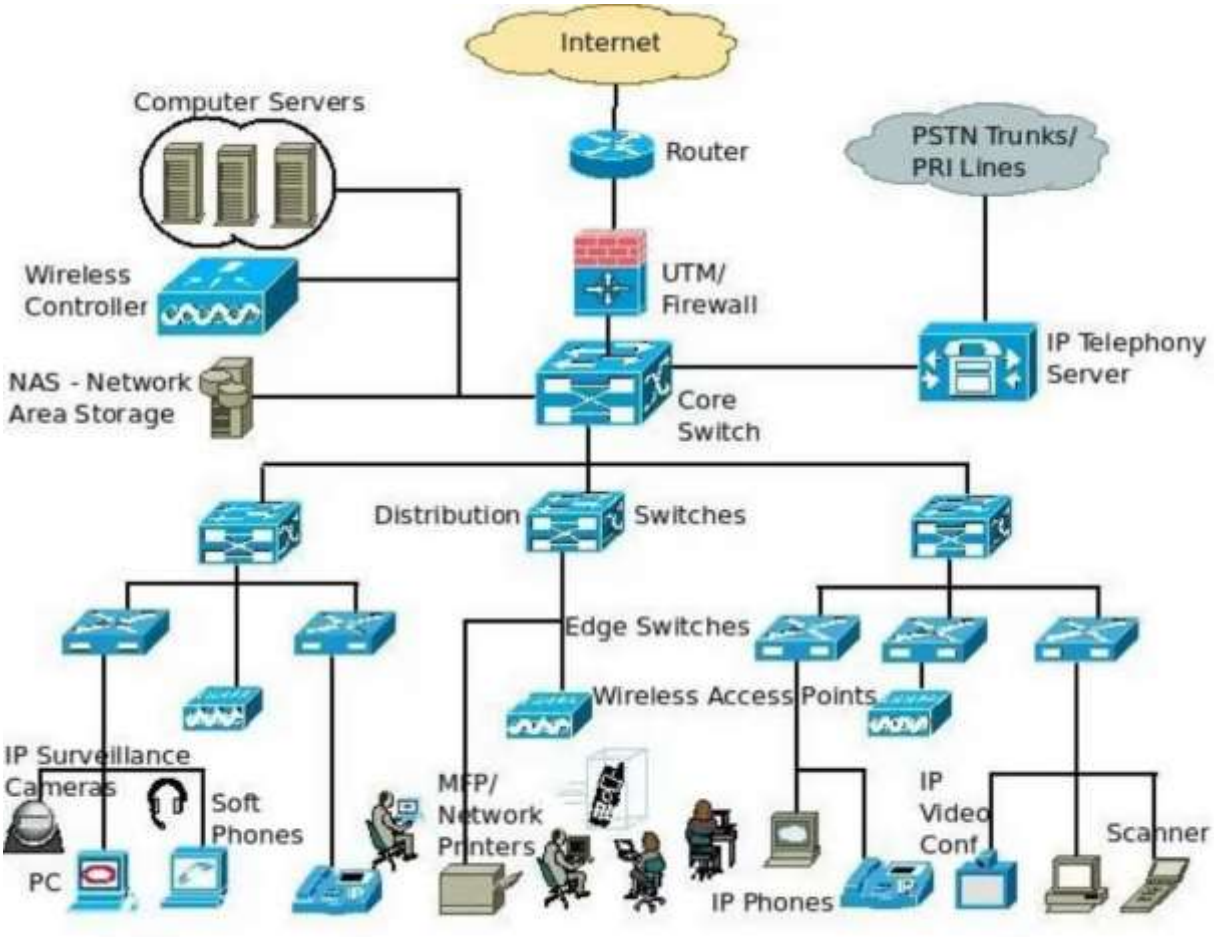
Terim, yaygın olarak bilgisayarların ve bilgisayar ağlarının eş anlamlısı olarak kullanılır, ancak aynı zamanda televizyon ve telefonlar gibi diğer bilgi dağıtım teknolojilerini de kapsar. Bilgisayar donanımı, yazılım elektronik, yarı iletkenler, internet, telekom ekipmanı ve e-ticaret de dahil olmak üzere çeşitli endüstriler bilgi teknolojisi ile ilişkilidir.

OT (Operasyonel Teknoloji) Hakkında

Operasyonel Teknoloji (OT), endüstriyel ekipmanın, varlıkların, süreçlerin ve olayların doğrudan izlenmesi ve / veya kontrolü yoluyla bir değişikliğe ne olan veya algılayan donanım ve yazılımdır.

Gerçek zamanlı işlemleri gerçekleştirmek için tasarlanmış bir yazılım ve donanım kombinasyonunu kullanır (örneğin, sıcaklığı kontrol etme, mekanik performansı izleme, acil durum kapatmalarını başlatma, vb.). OT 'ye bir örnek, su kontrolü, atık kontrolü, petrol ve gaz arıtmada kullanılan SCADA 'dır (Denetleyici Kontrol ve Veri Toplama).

Özetle, OT makinelerle ilgilenirken, BT bilgiyle ilgilenir.



OT neden BT ’den ayrı kaldı?

OT ’nin BT ’den ayrı kalmasının önemli bir nedeni, farklı yollarda başlamış olmalarıdır. Sadece son yıllarda, OT ve BT sistemlerinin birbirleriyle kolayca veri paylaşmasına izin veren daha güçlü bilgi işlem, daha iyi ağ oluşturma, geliştirilmiş depolama ve yeni IoT teknolojileri mevcut hale geldi.

BT önce ana bilgisayarlarla ortaya çıktı, daha sonra kişisel bilgisayarları ve dosya sunucularını içerecek şekilde gelişti. Bilgi işlem, veri depolama ve ağ oluşturmadaki ileri gelişmeler, İnternet ve bulut tabanlı ERP, Müşteri İlişkileri Yönetimi (CRM), İş Zekası (BI) ve bugün aşina olduğumuz diğer BT sistemlerinin yükselişine yol açtı.

OT, doğrudan dijital kontrol teknolojilerini makinelere ve diğer ekipman türlerine entegre eden şirketlerle başladı. Zaman içinde OT, şirketlerin programlanabilir mantıksal denetleyicileri ekipmanlarına entegre etmesi ve robotik devreye sokmasıyla BT ’nin gelişimini ilerleten aynı teknolojik gelişmelerin çoğunu kullandı.

Günümüzde şirketler, SCADA sistemleri, Bilgisayar Sayısal Kontrol (CNC) sistemleri ve Bina Otomasyon Sistemleri (BAS) dahil olmak üzere fiziksel süreçleri yönetmek için birçok farklı OT sistemi kullanıyor.

Ancak bu OT sistemlerinin çoğu, BT sistemleriyle entegre olacak şekilde tasarlanmıştır. Örneğin, birçoğu BT sistemleri tarafından kullanılmayan DNP3 veya Modbus gibi iletişim protokollerini ve standartlarını kullanır. Güvenlik endişeleri, yüksek ön maliyet, yatırım getirisi tahminlerini hesaplanması zor, IIoT bağlantı zorlukları ve diğer zorluklarla birlikte bu entegrasyon zorlukları, BT ve OT sistemlerinin ayrı tutulmasına yardımcı oldu.

IT/OT Amaç ve Hedefleri

	Bilgi Teknolojileri BT (Information Technology IT)	Operasyonel Teknolojiler OT (Operational Technology OT)
Amaç	Aktarım prosesi	Varlık izleme ve kontrol
	Sistem analizi ve uygulamaları	Proses kontrol, ölçüm ve koruma
	Teknik ve iş analizleri	Cihaz – Cihaz haberleşme
	İnsan kararlarına Destek	Sunucu – Cihaz haberleşme
Çalışma Ortamı	Kurumsal veri merkezleri	Alt istasyonlar
	Ofis ve sunucu odaları	Saha ekipmanları
	Kontrol odaları	Kontrol odaları

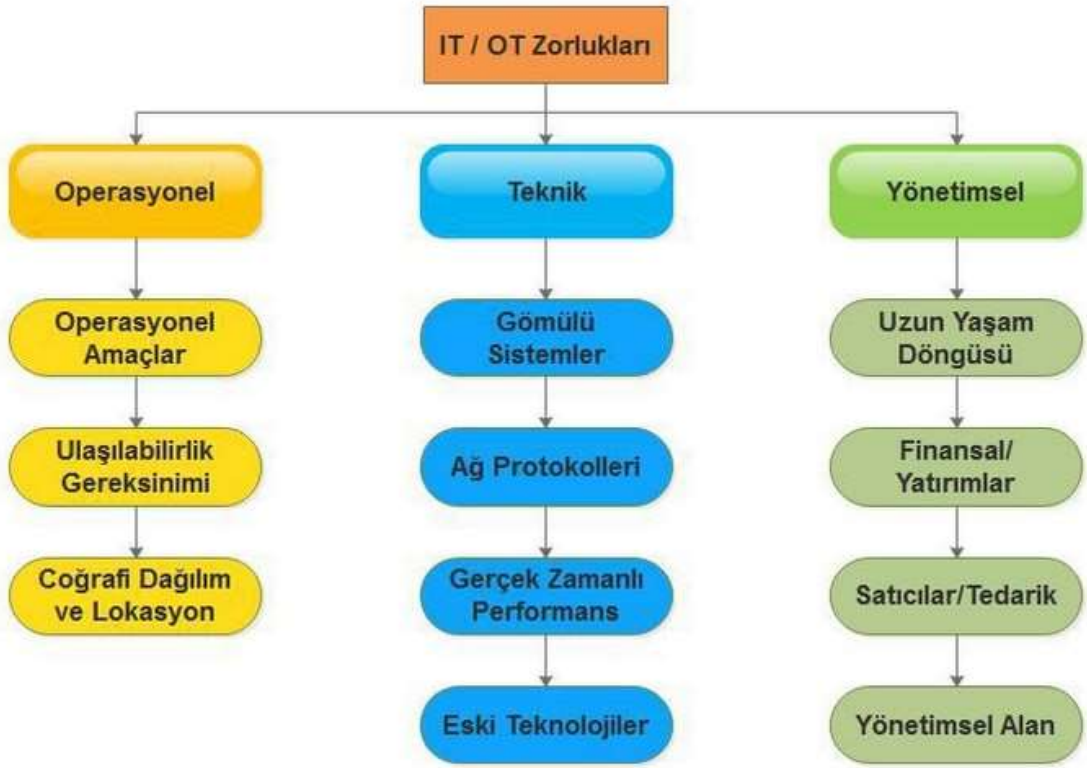
Veri Girişi	Manuel veri girişi	Sensörler, transmitterler, RTU ve PLC'ler
	Diğer IT sistemleri	IED'ler, röleler, ölçüm cihazları
	OT sistemlerinden gelen veri	Operatör girişleri ve diğer OT sistemleri
Çıkış	Veri özetleri	Cihaz kontrol eylemleri
	Analiz ve hesaplamaların sonucu	Durum ve alarm göstergeleri
	Diğer OT sistemlerine gönderilen komutlar	Operasyon kayıtları
Sorumlu	CIO ve IT departmanları	Operasyon ve mühendislik müdürleri
	Finans	İşletme müdürü
	Operasyon (OMS, DMS, EMS)	Bakım departmanları
Bağlantı	Kurumsal ağ	Proses kontrol protokolleri
	Ip tabanlı	IP tabanlı, seri, hardwired analog, dijital

Bilgi Teknolojileri ve Operasyonel Teknolojiler Arasındaki Farklar

1) OT makinelerle etkileşime girer. BT bilgi ile ilgilenir.
2) OT, izleme, kontrol ve denetim verileriyle ilgilenir. BT, işlemsel, ses, video ve büyük verilerle ilgilenir.
3) OT, erişim sınırlaması olmaksızın dış dünyaya bağlanır. BT, erişimi ayrıcalıklara sahip kişilerle sınırlıdır.
4) OT, verileri gerçek zamanlı olarak işler. BT, verilerin işlemsel işlenmesi üzerinde çalışır.
5) OT 'nin bilgi riski sorunları olabilir. BT 'nin otomasyon sorunları olabilir.
6) OT ağ arızası yaralanma veya ölümle sonuçlanabilir. Bir BT arızası ile veriler kaybolur.
7) OT, gereksinimler sık sık değişmediğinden nispeten statik bir ortama sahiptir. BT ortamı sık sık değişir.
8) OT ağları yalnızca belirli operasyonel bakım dönemlerinde yükseltilir. BT ağları sık sık yükseltme gerektirir.

9) OT sistemleri 15 ile 20 yıllık bir yaşam döngüsüne sahiptir. Bir BT sisteminin yaşam döngüsü 3 ile 5 yıldır.
10) OT sistemleri özel olarak geliştirilmiş yazılım gerektirir. BT sistemleri standart işletim sistemlerinde çalışabilir.

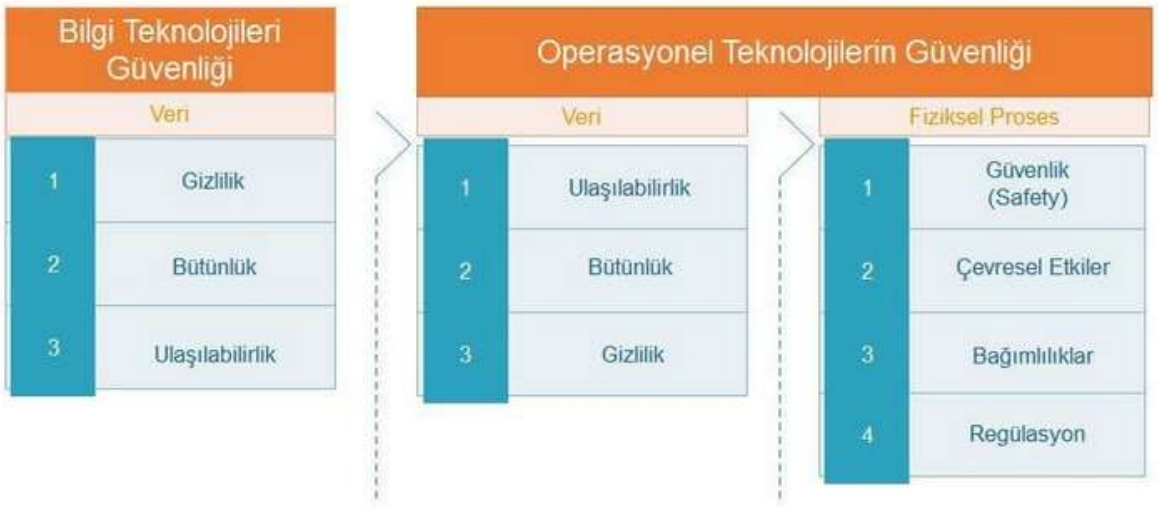
IT ve OT sistemleri arasındaki farklılıklar, ***operasyonel, teknik*** ve ***yönetsel*** alanlarda bulunmaktadır. Her alandaki farklılıklar, Endüstriyel Kontrol Sistemlerinin güvenlik duruşunda benzersiz zorluklar ve kısıtlamalar getirmektedir.



1) Operasyonel Zorluklar

Endüstriyel Kontrol Sistemlerinin amacı, bazı fiziksel süreçleri (su, elektrik şebekesi, doğal gaz/petrol boru hattı, üretim sistemi) kontrol etmek ve izlemektir. Bu tipik olarak bazı sensörler, aktüatörler ve operatörlerin kombinasyonu ile gerçekleştirilir. Bu sayede, geleneksel IT ortamlarından oldukça farklı olan sistem için benzersiz operasyonel gereksinimler yaratır. Bir IT sisteminde, mühendisin ve operatörün öncelikli amacı, sistemindeki verileri kontrol etmek ve yönetmektir. Bu nedenle güvenlik genellikle bu verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sürdürmeye odaklanır.

Ancak, Endüstriyel Kontrol Sistemleri kapsamında güvenlik, fiziksel bir işlemin güvenlik, çevresel faktörler, düzenleme, bağımlılık ce karlılığa da odaklanmalıdır. Endüstriyel Kontrol Sistemleri fiziksel bir süreci izlediğinden, sistem gerçek zamanlı olarak çalışmalı ve genellikle çok yüksek kullanılabilirlik talepleri mevcut olmalıdır.



1.1. Operasyonel Amaçlar

Endüstriyel Kontrol Sistemi genellikle faaliyetleri sırasında dengelenmesi gereken birden fazla hedefe sahiptir. Temel Endüstriyel Kontrol Sistemi hedeflerinin örnekleri arasında şunları sıralayabiliriz: karlılık marjlarının korunması, güvenlik veya çevresel etkileri en aza indirgenmesi, hasarların ve fiziksel varlıklara olan aşınmaların azaltılması, Endüstriyel Kontrol Sistem üzerindeki bağımlılıkların yönetilmesi. Siber güvenlik, bu hedeflerin çoğunu desteklemek için önemli bir özelliktir; fakat, genellikle ana operasyonel amaç değildir. Bu nedenle, kuruluş siber güvenliğin önemini diğer birçok operasyonel zorluklar açısından dengelemelidir.

1.1.1 Güvenlik (Safety)

Endüstriyel Kontrol Sistemi arızası genellikle çalışanların güvenliğini olumsuz yönde etkileme yeteneğine sahiptir. Güvenlik endişeleri, kinetik kuvvetlerden (örneğin, patlamalar, çarpışmalar), elektrik çarpmasından, radyasyondan veya toksik kimyasal salımlarından kaynaklanabilir. Bu nedenle, güvenlik, Endüstriyel Kontrol Sistemi operatörleri için genellikle bir önceliktir. Endüstriyel Kontrol Sistemleri genellikle güvenlik parametrelerini izlemek için özel sistemlere sahiptir. Ayrıca, Endüstriyel Kontrol Sistemi içindeki prosedürlerin ve politikaların çoğu güvenlik odaklı bir ilkeye odaklanmıştır.

1.1.2 Çevresel Etkiler

Endüstriyel Kontrol Sistemi arızası, tehlikeli kimyasallar, radyasyon veya diğer materyallerin salınması nedeniyle çevreyi de olumsuz yönde etkileyebilir. Ekosistemin bitkiler, yaban hayatı, hava kalitesi ve su kaynakları dahil olmak üzere Endüstriyel Kontrol Sistemi tarafından zarar görebilecek birçok yönü vardır.

Endüstriyel Kontrol Sistemi arızasının çevreye nasıl zarar verebileceğine dair bir örnek, 2000 yılında Avustralya'daki Maroochy Shire kanalizasyon tesisinde meydana geldi. Kısa bir süre önce işine son verilen bir çalışan, tesisin kablosuz ağlarına uzaktan erişebildi ve kanalizasyonun yakındaki nehirlere dökülmesi için komut verdi. Bunun sonucunda yerel su kanallarına yüz binlere galon kanalizasyon ile kirlenmesine sebep oldu.

1.1.3 Bağımlılıklar

Çoğu zaman, farklı sistemlerin fiziksel bileşenleri, Ulusal Kritik Altyapılarının birbiriyle olan bağımlılıklarını içerir. Bu nedenle, Endüstriyel Kontrol Sistemlerin 'deki bir başarısızlık ya doğrudan ya da dolaylı olarak birbirine bağlı alt yapıları etkileyebilir.

1.1.4 Fiziksel Altyapı

Endüstriyel Kontrol Sistemi arızaları, Endüstriyel Kontrol Sisteminin pahalı fiziksel sistem bileşenlerine (örneğin, kazanlar, motorlar, transformatörler, depolama tankları, jeneratörler, boru hatları) zarar verme potansiyeline de sahiptir. Bu öğeler aşırı yüksek sermaye maliyetine sahiptir ve kolayca tamir edilemez veya değiştirilemez. Buda genellikle uzun bir sitem kesintisi ve Endüstriyel Kontrol Sistemi için önemli maliyetler gerektirir.

Endüstriyel Kontrol Sistemine karşı bir siber saldırının sisteme fiziksel zarar vermesi durumunda yaşanan birçok örnek mevcuttur. Idaho Ulusal Laboratuvarı (INL) tarafından gerçekleştirilen aşamalı bir saldırı, elektrik şebekesine yapılan bir saldırının, jeneratörlere fiziksel olarak nasıl zarar verebileceğini göstermiştir. Bu saldırıda, bir koruma rölesi saldırıya uğradı ve jeneratörü şebekeye bağlayan bir devre kesiciyi açmak için kullanıldı. Jeneratör şebekeyle senkronize olmadığında kesiciyi sürekli olarak kapatmak istedi ve jeneratörü imha etti. Ek olarak, Stuxnet zararlı yazılımı, fiziksel altyapının siber saldırı ile yok edildiği başka bir örneği göstermektedir.

1.2 Yüksek Derece ’de Ulaşılabilirlik Gereksinimi

Endüstriyel Kontrol Sistemleri sıklıkla siber güvenlik korumalarının uygulanması konusunda birçok kısıtlama sunan çok yüksek kullanılabilirlikle çalışmalıdır. Yüksek kullanılabilirlik gereksinimleri olan Endüstriyel Kontrol Sistem örnekleri arasında elektrik güç şebekesi, su/doğal gaz sistemleri ve üretim sistemleri bulunmaktadır. Bu sistemlerin genellikle çalışma süreleri %99,99, %99,999 oranında olması gerekir; bu da bir yıl boyunca yalnızca 5 ile 50 dakikaya kadar çalışmaması anlamına gelir. Bu arıza süresinin, sistemler için birçok sistem bakım fonksiyonu ile birlikte öngörülemeyen kesintileri de içerecek şekilde programlanması gerekir. Sıklıkla, tüm sistem bakımı yıllık olarak veya altı ayda bir planlanan bir kesinti döneminde gerçekleştirilmelidir.

1.3 Coğrafi Dağılım ve Lokasyon

Endüstriyel Kontrol Sistemleri genellikle coğrafi olarak dağıtılmış konumlarda çalışmaktadır. Örneğin, elektrik güç şebekeleri, petrol/doğal gaz boru hatları ve ulaşım sistemleri yüzlerce hatta binlerce kilometreye yayılabilir. Barajlar ve atık su tesisleri gibi diğer sistemler kara ve su kütleleri arasında faaliyet gösterebilir.

Bu coğrafi dağınıklık, fiziksel sistem korumalarını uygulayarak, sistemi fiziksel olarak kurcalanmasına karşı savunmasız bırakan sorunlar yaratır. Saldırgan uzak noktadaki cihazı kurcalayabilirse, bu cihazın kontrolünün manipüle edebilir, cihazdan kaynaklanan ölçüm verilerini bozabilir veya sistem verilerine erişebilir. Saldırgan fiziksel sistem erişimi kazanabiliyorsa, genellikle şifreler ve şifreleme anahtarları da dahil olmak üzere diğer sistem kaynaklarına erişmek ve Endüstriyel Kontrol Sistemleri içindeki diğer sistemlere daha fazla erişim sağlamak için önemli veriler elde edebilir.

Bunlara ek olarak, dağıtık sistemlerde, sistem yönetimi zordur; çünkü operatörler ve mühendisler her zaman sisteme fiziksel olarak erişemezler. Bu işlevleri merkezi bir konumdan gerçekleştirmek için uzaktan yönetim ara yüzleri uygulamak zorunda kalırlar. Ancak, saldırganlar sistem erişimini kazanmak için bu uzaktan yönetim ara yüzlerini kullanabilirler.

2) Teknik Zorluklar

Endüstriyel Kontrol Sistemleri, operasyonlarını desteklemek amacıyla kullanılan yazılım ve iletişim platformları için birçok benzersiz teknik gereksinime de sahiptir. Endüstriyel Kontrol Sistemlerinin; Eşsiz iletişim protokolleri ve mimarileri, Gerçek zamanlı performans talepleri, Kaynak kısıtlı gömülü cihazlara bağımlılık, Alana özgü cihaz üreticileri ve entegratörleri, Dijital, analog ve mekanik kontrollerin karmaşık entegrasyon sebebiyle farklılık oluşturmaktadır.

2.1 Güvenlik Mekanizmaları için Sınırlı Destek

OT sistemleri genellikle Endüstriyel Kontrol Sistemlerini korumak için gerekli teknik güvenlik mekanizmalarından yoksundur. Kapsamlı bir Endüstriyel Kontrol Sistemleri güvenlik stratejisinin tasarlanması, her sistemin teknik yeteneklerinin güçlü bir şekilde anlaşılmasını gerektirir. NIST 800-82, birçok OT sisteminde desteklenen güvenlik özelliklerinin eksikliği nedeniyle bu kontrolleri uygularken karşılaşılan zorlukların birçoğu ile birlikte, Endüstriyel Kontrol Sistemlerini korumak için gerekli teknik güvenlik kontrollerini gözden geçirmektedir (NIST 2015).

2.2 Gömülü Sistemler

Endüstriyel Kontrol Sistemi ortamları, sınırlı işlem gücü, depolama ve bant genişliği gibi kaynak kısıtlamaları olan gömülü sistemlere büyük ölçüde bağımlıdır. Bu kaynak kısıtlamaları genellikle önemli güvenlik özelliklerini uygulama becerisini doğrudan etkiler. Sınırlı belleğe ve işlem gücüne sahip sistemler, genellikle sistemlerde depolama ve bellekte kullanılan hesaplama pahalı algoritmalara bağlı olduğundan, izinsiz giriş tespiti veya anti-virüs yazılımı gibi belirli güvenlik mekanizmalarını destekleyemez. Ayrıca, gerçek zamanlı sistem işlemlerinin gerçekleştirilmesi, sistem işlemlerinin zamanlamasını zorlaştırır ve güvenlikle ilgili görevleri zamanlamak için çok az zaman bırakır. Güvenlik mekanizmalarının birçoğunu desteklemek için gereken ek hesaplama ve iletişim, güç tüketimini de arttırır, böylece batarya gücüne bağlı olarak cihazların ömrünü doğrudan azaltır.

2.3 Ağ Protokolleri

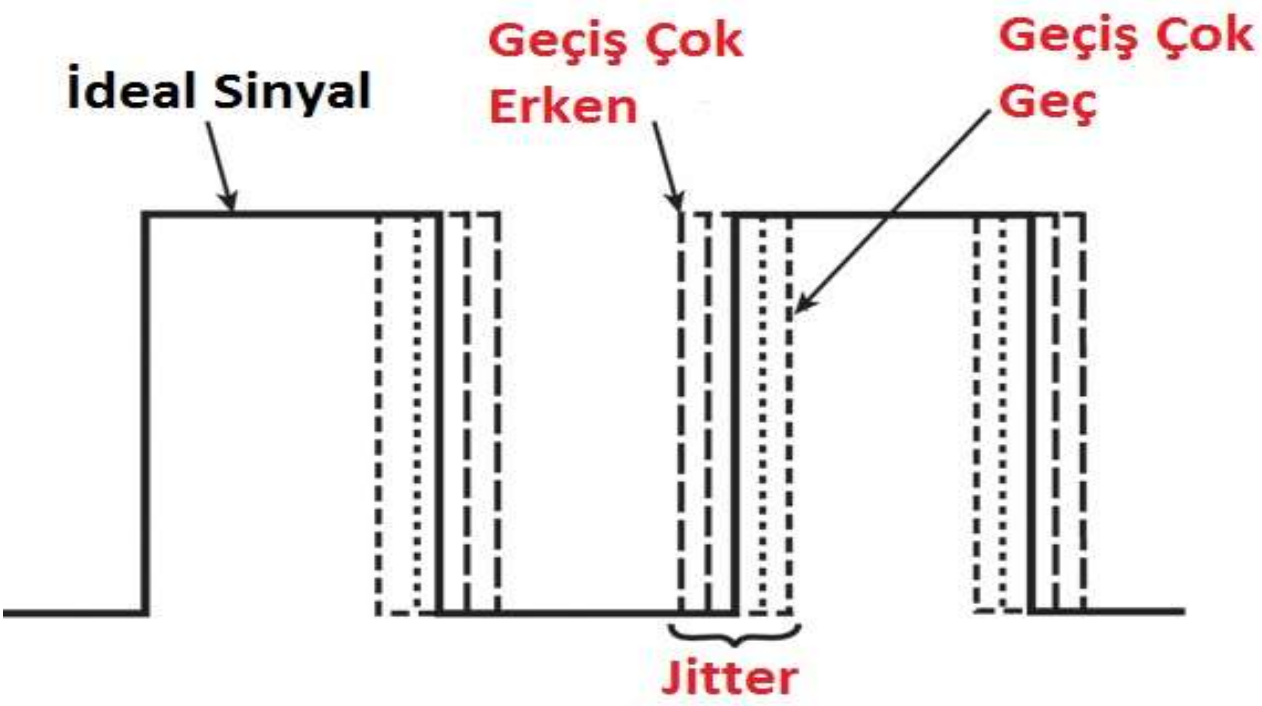
Endüstriyel Kontrol Sistemi, özellikle IT gereksinimlerini desteklemek için özel olarak tasarlanmış, geleneksel IT'de yaygın olarak kullanılanlar da dahil olmak üzere çok geniş bir ağ protokolü setine sahiptir. Aşağıdaki tablo ile OT ve IT'ye özgü bazı protokolleri ve iki alan arasındaki bazı farkları özetleyebiliriz.

	IT	OT
Protokoller	HTTP, DNS, SSH, SMTP, SNMP, NTP	DNP3, Modbus, IEC 61850, IEC 608705,EtherCat, BACnet
Veri	Büyük Yükler (Payloads)	Analog, İkili Değerler
Operasyon	Stokastik	Deterministik

2.4 Gerçek Zamanlı Performans

Bazı fiziksel süreçleri yönetmek için Endüstriyel Kontrol Sistemleri genellikle gerçek zamanlı olarak çalışmalıdır. Bu hem denetleyicilerin tasarımı hem de sistem iletişimleri

üzerinde güçlü bir etkiye sahiptir. İletişim gecikmesi ve eko titreşimi (Jitter), sistemin gerçek zamanlı olarak çalışmasını sağlamak için son derece önemli özellikler haline gelir.
İletişim gecikmesi, bir iletinin yönlendirici sıralarındaki gecikmeler ve fiziksel ağ üzerindeki sinyal yayılma süresi de dahil olmak üzere ağ üzerinden geçmesi için gereken süredir. Gecikme varyansı olan Jitter de sınırlandırılmalıdır. Bu kısıtlamalar, hesaplamaların pahalı kriptografik işlemlerine dayanan mesajların şifrelenmesi ve kimlik doğrulaması gibi birçok güvenlik mekanizmasını uygulanmasında zorluklar yaratmaktadır.



2.5 Eski ve Ezoterik Teknolojiler

Kullanılan teknolojilerin, platformların ve cihazların çoğu genel Endüstriyel Kontrol Sistemine veya belirli Endüstriyel Kontrol Sistemi alanlarına özgü olabilir. Her iki olay da güçlü bir güvenlik uygulaması yapmaya çalışırken zorluklar oluşmaktadır. Eskiyen sistemler geleneksel olarak birçok modern tehdide karşı korunmak için yeterli güvenlik mekanizmasına sahip değildir. Örneğin, eski ağ protokolleri genellikle güvenilir olmayan ağlar üzerinden gönderilen mesajların şifreleme ve kimlik doğrulama için destek yoksundur. Yazılım tarafında, bu sistemler genellikle kullanıcı kimlik doğrulaması, erişim kontrolü ve denetim yeteneklerinden yoksundur. Ek olarak, cihazlar genellikle güvenlik açıkları veya arka kapıları olmadıklarını doğrulamak için tasarımlarında sıkı güvenlik testlerine tabi tutulmamışlardır. Bu eski sistemlerin korunması, Endüstriyel Kontrol Sistemin eski aygıtlarını çevreleyen ve gerekli güvenlik işlevlerini uygulayabilen VPN'ler ve güvenlik duvarları gibi ek teknolojileri kullanmasını gerektirir.

Endüstriyel Kontrol Sistemleri teknolojilerinin eski olmasına ek olarak, birçok teknoloji de ezoteriktir, çünkü bunlar genellikle Endüstriyel Kontrol Sistemlerinin dışında yaygın olarak kullanılmamaktadır. Genel olarak teknolojilerin güvenlik duruşu iyi anlaşılmamıştır. Ayrıca, sistemi yönetmek ve gerekli güvenlik değerlendirmelerini gerçekleştirmek için yetenekli profesyonelleri bulmakta zorluklar yaratmaktadır.

3) Yönetimsel Zorluklar

OT sistemlerinin yönetimi de IT yönetiminden farklıdır. Örneğin, Endüstriyel Kontrol Sistemi sermaye yatırımları genellikle daha büyüktür çünkü karmaşık bir fiziksel altyapıya sahiptirler. Bu nedenle, Endüstriyel Kontrol Sistemleri altyapısının maliyetini iyileştirmek için yıllarca faaliyet göstermelidir. Ek olarak, Endüstriyel Kontrol Sistemi, kurumların siber güvenlik bütçesinden daha kısıtlı gelir akışlarına sahip olabilir.

3.1. Uzun Yaşam Döngüsü

Endüstriyel Kontrol Sistemi, genellikle çeşitli sistemleri temin etmek, dağıtmak ve entegre etmek için daha büyük maliyetlere sahiptir. Sistem, bu yatırımın maliyetini karşılayabilmek için uzun bir süre için üretimde kalmalıdır. Örneğin, güç sistemindeki rölelerin tipik olarak 20 yılı aşkın bir süredir çalışması beklenmektedir, bu geleneksel IT ortamlarındaki sistem yaşam döngüsü tipik olarak 3-5 yıldır.

Bu uzun yaşam döngüsü, özellikle (i) siber tehditleri ve (ii) desteklenmeyen sistemlere bağımlılıkları geliştirmek gibi birçok siber güvenlik sorununu ortaya çıkarmaktadır. Geleneksel IT ortamlarındaki kısa yaşam döngüleri, onları gelişen siber tehditleri ele almak için daha manevra yapabilir. Endüstriyel Kontrol sistemleri uzun ömürlü olduğundan, çoğu zaman birçok yeni tehdide hitap etmekte zorluk çekerler. Örneğin, birçok yaygın kriptografik mekanizma (ör., DES, MD5) artık yeterli güvenlik sağlamazken, yaygın olarak kullanılan birçok şifreleme protokolü (ör. SSLv2) artık güvenli değildir. Ayrıca, Windows XP'nin çoğu sürümü 8 Nisan 2014'te sona erdi ve bu da Microsoft'un bu sistemde bulunan güvenlik açıkları için düzeltme eki içermediği anlamına geliyor. Bu platformların çoğu Endüstriyel Kontrol Sistemi ortamlarında yaygın olarak kullanılsa da yeni güvenlik açıklarından gelen yamaları almayacaklardır.

3.2 Finansal Yatırımlar

Endüstriyel Kontrol sistemlerinin gelir yapısı genellikle, kamu hizmetleri gibi, siber güvenlik için bütçeleri üzerinde sınırlı kontrol sahibi olan sabit hizmet oranlarına dayanmaktadır. Örneğin, Amerika Birleşik Devletleri'ndeki kamu hizmetleri genellikle bir kamu hizmetleri komisyonu (PUC) tarafından yönetilmektedir. PUC, yardımcı programların müşterilere makul bir hizmet oranı sunmasını sağlayarak, şirketin gelirinin işletme maliyetlerine ve sermaye yatırımlarına bağlı olmasını sağlar. Çoğu zaman, programın siber güvenlik yatırımları (ör. Teknoloji, çalışanlar ve süreçler) doğrudan PUC tarafından onaylanmalıdır, bu nedenle hizmet, siber güvenlik yatırımı için bütçelerini doğrudan kontrol etmemektedir.

Kamu hizmetlerinin siber saldırıdan korunma maliyeti, doğrudan işletim maliyetlerini artırır, maalesef çoğu zaman hizmet bedeli bu maliyet artışını içerecek şekilde ayarlanmamıştır. Birçok durumda PUC, siber saldırı riskini yeterli düzeyde değerlendirmek için yeterli faydaya sahip değildir ve bu durum, hizmetlerin yeterli fon toplamasını engeller. Bu, kritik siber güvenlik yatırımı ihtiyaçlarının ne zaman tanımlandığı ve fayda maliyetinin yatırım maliyetini artırabileceği zaman arasında bir boşluk yaratmaktadır.

3.3. Satıcılar ve Tedarikçiler

Endüstriyel Kontrol sistemlerinde, IT ortamlarından farklı ürün satıcıları ve sistem satın alma süreçleri vardır. Bu, sistemin yaşam döngüsü boyunca güvenlik yönetiminde geniş kapsamlı etkileri olabilir. Örneğin, çoğu IT sağlayıcısının, güvenlik açığı açıklamasının nasıl ele alınacağını ve yamalar yayımlandığında nasıl tanımlandığını belirten iyi tanımlanmış politikaları vardır.

Ek olarak, birçok IT platformu yamaları yönetmeye ve takmaya yardımcı olacak araçlar geliştirir (ör. Microsoft Windows Server Update Services). Endüstriyel Kontrol sistemi satıcıları genellikle benzer prosedürlere sahip değildir. Bildirilen güvenlik açıkları çoğu zaman gönderilmez ve bir yamanın mevcut olması durumunda, sistem kullanılabilirliğini etkileyeceğinden endişe duyulduğu için sık sık uygulanamaz. Sistem güncellemeleri genellikle iş güvenilirliğini benzersiz yapılandırılmasına ve diğer OT yazılım platformlarını doğrulamak için ek testlere tabi tutulmalıdır. Ayrıca, Endüstriyel Kontrol sistemi, üretim sistemlerine geçmeden önce yamaların doğrulanabileceği bir test ağına / ortamına sahip olmayabilir.

Genellikle Endüstriyel Kontrol sistemi, sistemleri dağıtmak ve yapılandırmak için üçüncü taraf bir şirket veya entegratörle sözleşme yapar. Endüstriyel Kontrol sistem operatörünün, iletişimi ve kontrolü sağlamak için kullanılan yapılandırma ve teknolojiler hakkında derin teknik bilgiye sahip olamayacağı anlamına gelir. Sistem yaşam döngüsü boyunca çok sayıda güvenlik sorunu sunar. İlk olarak, sistem teknolojileri ve yapılandırmaları hakkında güçlü bir anlayışa sahip olmayan Endüstriyel Kontrol sistem operatörü, sistemlerini saldırı veya saldırılara karşı etkin bir şekilde izleyemez. İkincisi, Endüstriyel Kontrol sistemi, entegratörler doğrudan müdahalede bulunmadıkça, beklenmedik durum planlama ve kurtarma faaliyetlerini yürütme konusunda sınırlı bir kabiliyete sahip olabilir.

Ayrıca, Endüstriyel Kontrol sistemi, güvenlik yamaları ya da bu sistemlerdeki güncellemeler gibi gelecekteki sistem değişikliklerini gerçekleştirmek için sınırlı bir yeteneğe sahip olabilir. Çoğunlukla Endüstriyel Kontrol sistemi, sistemin hem güvenlik açığı süresini artırabilecek yamaların hem test edilmesi hem de yüklenmesi için entegratöre bağlıdır.

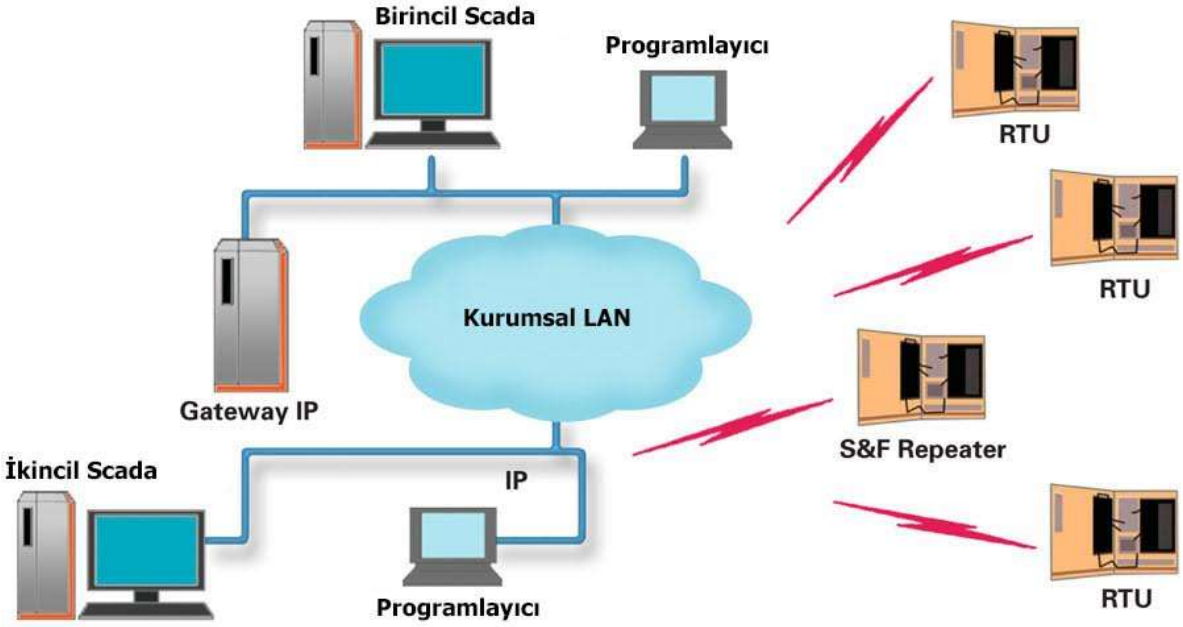
3.4. Yönetimsel

Önceden tanımlanan Endüstriyel Kontrol sistemi operasyonel zorluklarına ek olarak, bu sistemler yönetim ve idaresinde kültürel zorluklarla da karşı karşıyadır. Endüstriyel Kontrol sistemi genel olarak iki farklı alana odaklanan benzersiz personel yerine hem IT hem de OT teknolojileri aynı anda yöneten personellere eğilim içerisindedir. Bu, Endüstriyel Kontrol sistemlerinde farklı sistemler ve yazılımlar üzerinde dağıtılan yöneticilik sorumluluğu bulunanlar arasında çatışma yaratabilir.

Bir yaklaşım, her alanın kendi uzmanlıklarına giren sistemleri yönetmesidir. IT personeli, IT ortamlarında (ör. Microsoft, Cisco, HTTP, IP ağları) yaygın olarak kullanılan teknolojiler / satıcılar konusunda uzmanlığa sahiptir ve bu nedenle bunları yönetmelidir; OT insanlar geleneksel OT teknolojilerinden ve satıcılardan (örneğin Siemens, GE, DNP3, RS-232) cihazları yönetmelidir. Bununla birlikte, OT bileşenleri genellikle bazı meta IT teknolojilerini de içereceğinden, IT personeli, yanlış yapılandırmayı gerçekleştirerek veya potansiyel olarak sorunlu bir yama ekleyerek Endüstriyel Kontrol sisteminin çalışmasını olumsuz yönde etkileyebilir.

Tam tersi yaklaşım, IT personeli sadece operasyonel Endüstriyel Kontrol sistemi verilerini saklamayan veya yönetmeyen ofis otomasyon sistemini ve sunucularını desteklemek için çalışırken, OT personeli tüm SCADA ve kontrol sistemlerini yönetmesidir. Bu yaklaşım, Endüstriyel Kontrol sistemi operasyonlarının daha iyi desteklenmesini sağlamalı, ancak OT personelinin IT teknolojilerine ilişkin derinlemesine bilgiye sahip olamayacağı için, sistemin güvenlik açığını da artırabilir. Ek olarak, bir sistemin OT veya IT olarak kategorileştirilmesiyle ilgili olarak düştüğü belirsiz sınırlar (gri ve açıkta kalan noktalar) olabilir.

Endüstriyel Kontrol sistemi geleneksel olarak OT kontrol sistemidir ve süreç kontrolünün operatörler tarafından kullanılabilirlik ve güvenliğe ilişkin önceliği olduğu için güvenlik endişeleri hakimdir. Öte yandan IT sistemleri, farklı donanım ve ağ altyapısına, insan kullanım politikalarına, performans gereksinimlerine ve güvenlik savunma yöntemlerine sahiptir. IT güvenlik yöntemleri, genellikle çok çeşitli "süreçleri" yürütürken kullanıcı gizliliğini ve bütünlüğünü korumaya odaklanır. IT sistem teknolojileri, Endüstriyel Kontrol sistemlerine yakınlaşmaya başladıkça, gelecekteki Endüstriyel Kontrol sistemlerinin beklentilerini yönetmek için bu farklılıkları anlamak ve analiz etmek daha kritik hale gelir.



KAYNAKÇA

https://tr.esc.wiki/wiki/Operational_Technology

https://tr.wikipedia.org/wiki/Bilgi_teknolojisi

https://ozdenercin.com/2018/10/22/bilgi-teknolojileri-ve-operasyonel-teknolojiler-arasindaki-farklar/

https://www.isssource.com/wp-content/uploads/2015/11/111115statseeker-IT-OT-Convergence-White-Paper.pdf

https://www.coolfiresolutions.com/blog/difference-between-it-ot/

https://planetechusa.com/operational-technology-and-information-technology-networks/

https://fluchsfriction.medium.com/why-ot-has-different-needs-than-it-18ba9baa36e7

https://www.sierrawireless.com/iot-blog/it-ot-convergence/

https://otomasyonadair.com/2016/07/13/it-ot-yakinlasmasi-it-nedir-ot-nedir/

https://haber.sol.org.tr/sites/default/files/images/2016/11/25/5.jpg

https://www.pc-audiophile.com/jitter/

https://teslaakademi.com/scada-nedir

https://www.parsecuremap.com/#2/42.4/-17.6