IEC62433 Standardı ve Operasyonel Teknolojilerde Siber Güvenlik

Hakan Duran

February 15, 2024

1 Giriş

IEC62433 endüstriyel otomasyon ve kontrol sistemlerini (IACS) siber açıdan korumaya yönelik geliştirilmiş holistik bir standartlar serisidir. Bu standart serisi kurum ve kişileri üç ana role ayırır: son kullanıcı (varlık sahibi), entegratör ve üretici. Her rolün standartları sağlaması adına belli sorumluluklar yüklenir.

ISA (The International Society of Automation), 2002 yılında Amerika kritik alyapısını korumaya yönelik çalışmaları düzenlemek adına ISA99 komitesini kurdu. ISA99 komitesinin ortaya koymuş olduğu ISA62433 standartları uluslarası bir kurum olan IEC (International Electrotechnical Commission) tarafından onaylanarak global perspektifte de ISA/IEC62433 adıyla yer buldu. 20 farklı ülkede kullanım haline gelen bu standart, operasyonel teknoloji dışındaki alanlarda da önemi vurgulanır hale geldi.

Sistemlerin siber güvenliğini en verimli ve maksimum düzeyde tutabilmek sadece tek bir kurumun veya rolün elinde olmayan bir durumdur. Standartlar sistemin siber güvenliğini sağlamak için 3 farklı role sorumluluklar yüklemiştir:

- **Varlık sahibi (asset owner)**: Son kullanıcı olarak da bilinen varlık sahibi, endüstriyel otomasyon kontrol sisteminin sahibi/operatörüdür.
- **Sistem entegratörü (system entegrator)**: Entegratörün görevi, sistemin entegrasyonu, konfigürasyonunu ve testidir. Entegratör sistemi ayarladıktan sonra

sistem, varlık sahibine devredilir.

- **Ürün sağlayıcı (product supplier)**: Ürün sağlayıcı, endüstriyel ürünün imalatından sorumludur. Bu ürün PLC ya da RTU gibi gömülü bir donanım, firewall ya da router gibi ağ cihazı, bilgisayar ya da telefon gibi son-cihaz veya bir yazılım ürünü olabilir.

Bu üç ana rol dışında daha az belirtilen; destek, bakım ve onarımdan sorumlu bakım servis sağlayıcı vardır.

2 Standart ailesi

Standartlar 4 mantıksal bölüme ve her mantıksal bölüm kendi içinde bileşenlerine ayrılmıştır.

Figure 1: 4 ana bölüm ve 14 ara bileşene ayrılan IEC62433 standart ailesi

Her mantıksal bölümün özelliği belli bir anahtar kelime üzerinde olmasıdır, ilk bölüm herkese genel terimler hakkında bilgiler verirken diğer 3 bölüm ana rollerin (varlık sahibi, entegratör, ürün sağlayıcı) her birine daha çok ifade etmektedir.

2.1 Bölüm 1

İlk mantıksal bölüm olan "Genel"; standartlar boyunca kullanılacak genel terimlerden ve modellerden bahseder ve temel konulara değinir. İlk bölüm her rol ile bağlantılıdır.

- **Bölüm 1-1: Terminoloji, konsept ve modeller** tanıtılır ve seri boyunca kullanılırlar. Hedef kitleye herkes dahildir. Oluşturan temel kavramlar serinin temelini oluşturuyor.
- **Bölüm 1-2: Temel terimler ve tanımlar sözlüğü** standart boyunca kullanılacak olan tanımlar ve terimlerin bir listesidir.
- **Bölüm 1-3: Sistem güvenliği uygunluk metrikleri** standartlardaki süreçten ve teknik gerekliliklerden elde edilen niceliksel ölçümlerin geliştirilmesine yönelik metodoloji ve ölçümler bütünüdür.
- **Bölüm 1-4: IACS güvenlik yaşam döngüsü ve kullanım senaryoları** IACS güvenliğinin temelini oluşturan yaşam döngüsünün daha ayrıntılı bir açıklamasını ve ayrıca bu döngünün çeşitli uygulamalarını örneklerle açıklayan birçok kullanım senaryolarını sağlar.

2.2 Bölüm 2

İkinci mantıksal bölümün ismi "Politikalar ve Prosedürler"dir. Bu bölüm efektif bir siber güvenlik programının daha çok insan ve süreç yönlerine odaklanır, tesis operasyonlarının nasıl olacağını belirtir. Daha çok varlık sahibini ve biraz da sistem entegratörlerini hedef alır.

- **Bölüm 2-1: Bir IACS güvenlik programının oluşturulması** etkili bir IACS siber güvenlik yönetim sisteminin tanımlanması ve uygulanması için neyin gerekli olduğunu açıklamaktadır. Hedef kitle, böyle bir programın tasarlanması ve uygulanmasından sorumlu varlık sahiplerini içerir.

- **Bölüm 2-2: IACS güvenlik programı derecelendirmeleri**, ISA/IEC 62443 standart serisindeki gereksinimlere göre operasyonel bir IACS tarafından sağlanan koruma düzeyini değerlendirmek için bir metodoloji sağlar.

- **Bölüm 2-3: IACS ortamındaki yama yönetimi** IACS için yama yönetimi konusunda rehberlik sağlar. Hedef kitle, bir yama yönetimi programının tasarlanması ve uygulanmasından sorumlu olan herkesi içerir.

- **Bölüm 2-4: IACS hizmet sağlayıcılarına yönelik güvenlik programı gereksinimleri** sistem entegratörleri veya bakım servis sağlayıcıları gibi IACS hizmet sağlayıcılarına yönelik gereksinimleri belirtir. Bu standart IEC tarafından geliştirilmiştir.

- **Bölüm 2-5: IACS varlık sahipleri için implementasyon kılavuzu** etkili bir IACS siber güvenlik programını yürütmek için nelerin gerekli olduğuna ilişkin rehberlik sağlar. Hedef kitle, böyle bir programın operasyonundan sorumlu olan varlık sahiplerini içerir.

2.3 Bölüm 3

Üçüncü mantıksal bölümün ismi "Sistem"dir, sistemler için güvenliğin teknolojiyle ilgili yönlerine odaklanır. Güvenliği sağlamak için uygulama ve entegrasyonun gerçekleştirilmesine yönelik yol gösterici ilkeleri açıklar. Bölüm 1 gibi her rol ile bağlantılı olmakla birlikte daha çok sistem entegratörlerini hedef alır.

- **Bölüm 3-1: IACS için güvenlik teknolojileri** çeşitli güvenlik teknolojilerinin bir IACS ortamına uygulanmasını açıklar. Hedef kitle, belirli teknolojilerin kontrol sistemleri ortamında uygulanabilirliği hakkında daha fazla bilgi edinmek isteyen herkesi içerir.

- **Bölüm 3-2: Sistem tasarımına yönelik güvenlik riski değerlendirmesi** IACS için siber güvenlik risk değerlendirmesine ve sistem tasarımına yöneliktir. Bu standardın vermek istediği genel kavramlar bölge ve kanal modeli (zone and conduit model) ve modelle ilgili risk değerlendirmeleri ile hedef güvenlik seviyeleridir

(security level, SL). Bunlar siber güvenlik gereksinimleri spesifikasyonunda belgelenmiştir. Bu standart öncelikle varlık sahiplerine ve sistem entegratörlerine yöneliktir.

- **Bölüm 3-3: Sistem güvenlik gereksinimleri ve güvenlik düzeyleri** güvenlik düzeyine dayalı olarak bir IACS sisteminin gerekliliklerini açıklar. Ana hedef kitle kontrol sistemleri tedarikçilerini, sistem entegratörlerini ve varlık sahiplerini içerir.

2.4 Bölüm 4

Dördüncü mantıksal bölümün ismi "Bileşen"dir. Ürünlerin teknik içeriklerini ve bunları yaşam döngüleri boyunca yönetmek için kullanılan süreçleri kapsar. Ürünler ve bileşenler için güvenlikle ilgili belirli gereksinimlere odaklanır. Ürün sağlayıcılarını hedef alır.

- **Bölüm 4-1: Ürün güvenliği geliştirme yaşam döngüsü gereksinimleri** bir ürün geliştiricisinin uyguladığı güvenlik geliştirme yaşam döngüsüne ilişkin gereksinimleri açıklar. Ana hedef kitle, kontrol sistemi ve bileşen ürünlerinin tedarikçilerini (sağlayıcılarını) içerir.

- **Bölüm 4-2: IACS bileşenleri için teknik güvenlik gereksinimleri** güvenlik düzeyine dayalı olarak IACS Bileşenleri için gereksinimleri açıklar. Bileşenler gömülü aygıtları, son kullanıcı aygıtlarını, ağ aygıtlarını ve yazılım uygulamalarını içerir. Ana hedef kitle, kontrol sistemlerinde kullanılan bileşen ürünlerinin tedarikçilerini (sağlayıcılarını) içerir.

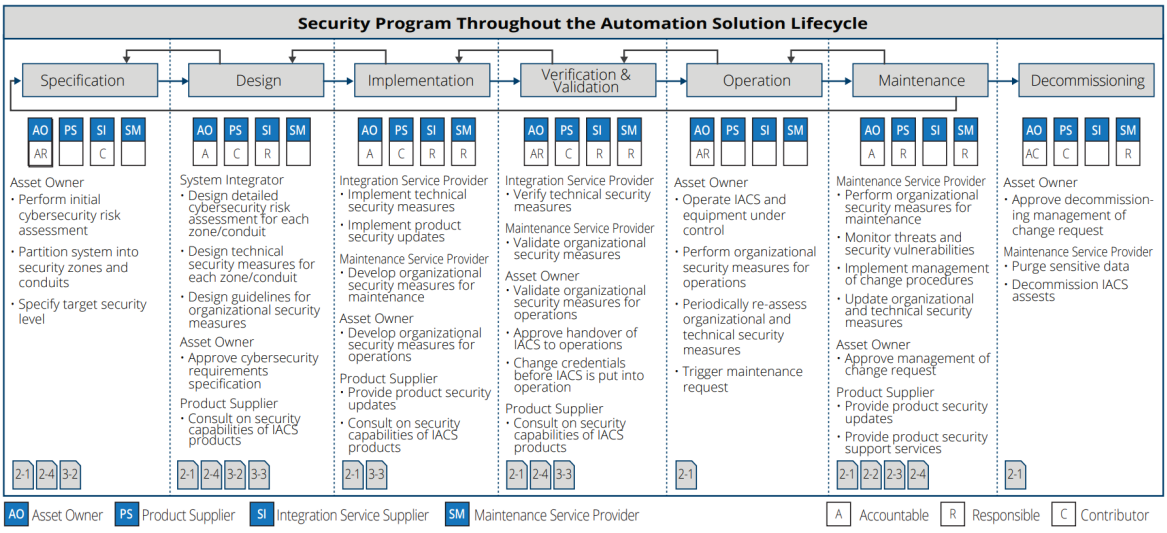

Figure 2: Ana roller ve IACS güvenliği yaşam döngüsü ile olan bağlantısı

3 Siber Güvenlik Yönetim Sistemi

Çoğu şirket için en sıkıntılı durum siber güvenlik süreçlerini ve sistemlerini anlamada veya pratiğe geçirmedeki zorluktur. Bu sıkıntıyı atlatabilmek için IEC 62433 standartları yol göstermektedir. Bu bölüm anahtar kelimeleri ve yol haritasını gösterecektir.

IEC 62433 standartları tarafından önerilen siber güvenlik yönetim sistemi (Cyber security management system (CSMS)) altı elemente sahiptir:

- CSMS programının başlatılması (Yönetimin desteğini almakla ilgilidir).
- Genel risk değerlendirilmesi (Risklerin öneminin değerlendirilmesi).
- Detaylı risk değerlendirilmesi (Güvenlik açıklarının detaylı teknik değerlendirilmesi).
- Güvenlik, organizasyon ve farkındalığı arttırma politikalarını oluşturmak
- Önlemleri seçmek ve implemente etmek.
- CSMS'yi sürdürmek (CSMS'nin efektif kaldığından ve organizasyonun hedeflerini desteklediğinden emin olmak).

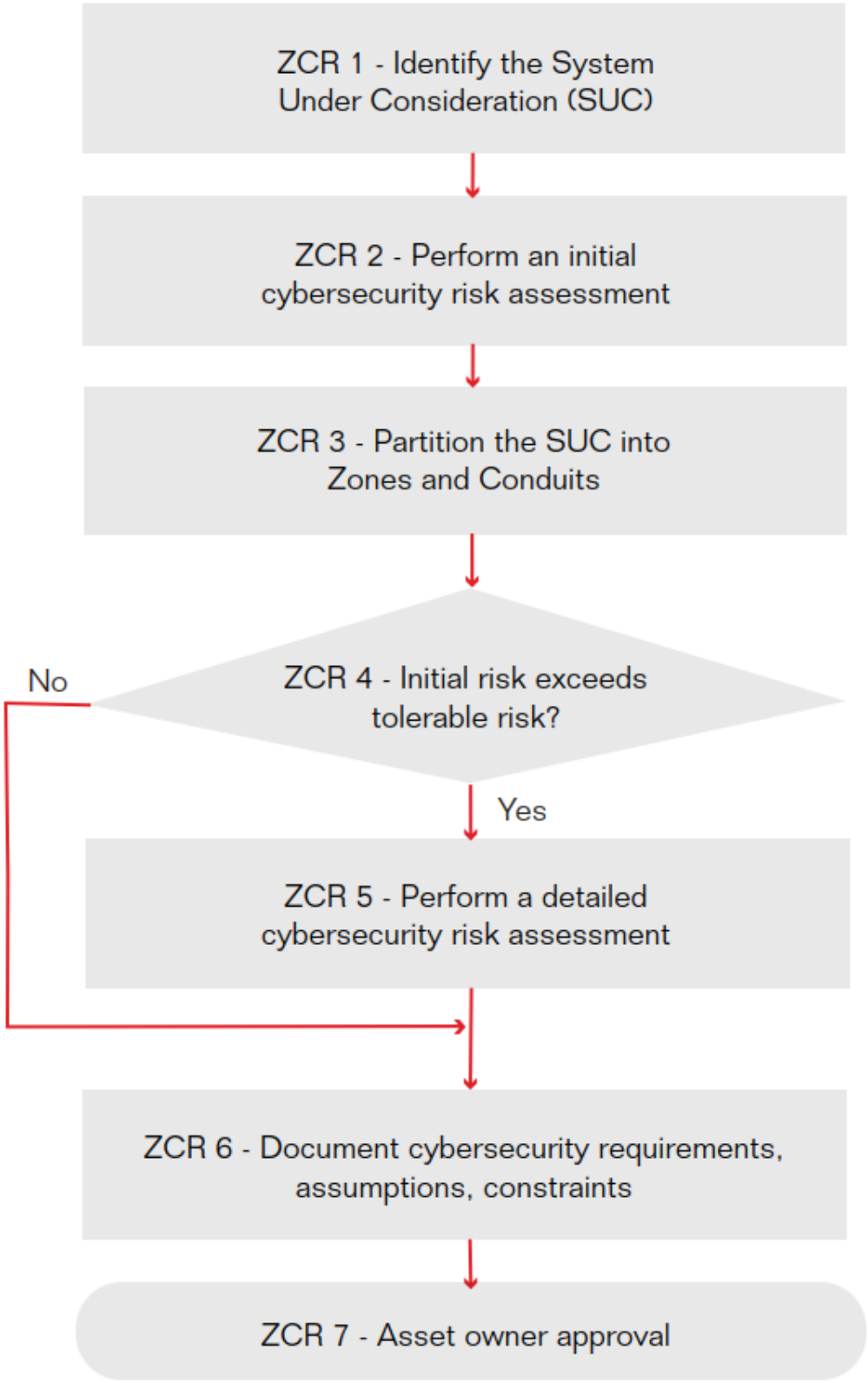

Figure 3: ISA/IEC 62433 genel yaklaşım metadolojisi, CSMS'de güvenlik politikaları oluşturma kısmına kadar olan süreçleri kapsar

3.1 CSMS programının başlatılması

İş gerekçelerini dikkate almak ve yönetimden CSMS programının başlatılabilmesi adına destek almak bir siber güvenlik sisteminin oluşturulmasının ilk adımıdır. Yönetimin neden bu işe girildiğini, nelerin etkileneceğini ve nelerin korunacağını anlaması adına ilk önce kritik varlıklardan (critical assets) bahsedilir. Kritik varlıklar, bir kez tehlikeye atıldığında bir kuruluş için yüksek mali, sağlık, güvenlik veya çevresel etki oluşturabilecek her türlü cihazı içerir. Şirketin kritik varlıklarının listesi risk yönetimi analizinin temelini oluşturur ve daha sonraki kararlara rehberlik etmek için kullanılacaktır. Figür 3'te ZCR 1'e denk gelmektedir.

3.2 Genel seviye risk değerlendirilmesi

Risk değerlendirilmesi (risk assessment), her şirketin genel risk yönetimi stratejisinin bir parçasıdır ve sağlam ve etkili bir siber güvenlik stratejisi oluşturmak için zorunlu bir adımdır. IACS'nin risk değerlendirmesini gerçekleştirmek için, değerlendirilecek olan sistemin -Değerlendirme Altındaki Sistem (System Under Consideration)(SuC) olarak da bilinir- kapsamının ve sınırlarının tanımlanması gerekir. SuC tanımlandıktan sonra tehditleri ve güvenlik açıklarını sistematik olarak belirlemek, analiz etmek ve potansiyel sonuçlarına göre riskleri önceliklendirmek gerekir. Aynı zamanda varlıkların kritikliğini ve operasyona olan bağımlılıklarını tanımlamak da önemlidir. Figür 3'te ZCR 2'ye denk gelmektedir.

$$Olasılık_{Olayın\_Gerceklesmesi} = Olasılık_{Tehditin\_Anlasılması} * Olasılık_{Zaafiyetin\_İstismarı}$$

$$Risk = Olasılık_{Olayın\_Gerceklesmesi} * Netice$$

3.3 Detaylı risk değerlendirmesi

Genel seviye risk değerlendirilmesinin yetersiz olduğu durumlarda detaylı risk değerlendirilmesi gerçekleştirilir. Detaylı risk değerlendirmesi daha teknik bir süreçtir. Detaylı teknik

değerlendirmenin ilk aşaması bölgeler ve iletim hatlarının (zone & conduits) belirlenmesidir. Bazı yeni temel terimleri ve dizayn prensiplerini içerir. Bunlara örnek olarak temel gereksinimler (foundational requirements), güvenlik seviyeleri (security levels), olgunluk seviyeleri (maturity model), tasarımla beraber güvenlik (secure by design), atak yüzeyini azaltma (reduce attack surface), derinlemesine güvenlik (defence-in-depth) verilebilir. Bu terimler rapor boyunca daha sonraki başlıklarda detaylı incelenecektir.

3.4 Politikalar, uygulamalar ve devamlılık

Gerekli riskler değerlendirilip yeni savunma stratejileri belirlendikten sonra risklere bağlı olarak yeni güvenlik, organizasyon ve farkındalığı arttırma politikalarının organizasyon içerisinde yeniden düşünülmesi elzemdir. Varlık sahibinin riskleri onaylayıp güvenliği sağlama projelerine desteğinden sonra riskin azaltılması için önlemler seçilip implemente edilir. Bir diğer önemli husus da CSMS sisteminin devamlılığını, stabil ve efektif işleyişinin devamlılığından emin olmaktır. Bu devamlılığı sağlamak adına sistem güvenliği izlenmeli ve kayıtlar tutulmalıdır. Bu işlem için genelde IDS cihazları kullanılır. Sistem güvenliğini izlemenin yanında gelen saldırılara cevap verebilmek de sistemin güvenliğini arttırmada önemli bir avantaj sağlar. Bunlar için IPS cihazları veya SIEM/SOAR uygulamaları birebirdir.

4 Bölgeler ve iletim hatları

Detaylı risk değerlendirmesinin ilk adımı SuC içini bölgelere ayırarak kontrolü ve belirliliği arttırmaktır. **Bölge (zone)**; risk veya varlıkların kritikliği, operasyonel işlev, fiziksel veya mantıksal konum, gerekli erişim veya sorumlu kuruluş gibi kriterlere dayalı olarak mantıksal veya fiziksel varlıkların gruplandırılması olarak tanımlanır. **İletim kanalı (conduit)**, iki veya daha fazla bölgeyi birbirine bağlayan ortak güvenlik gereksinimlerini paylaşan iletişim kanallarının mantıksal bir gruplaması olarak tanımlanır.

Risk değerlendirme sürecindeki önemli bir adım, incelenen sistemi ayrı bölgelere ve iletim kanallarına bölmektir. Amaç, siber güvenlik riskini azaltan bir dizi ortak güven-

lik gereksinimi oluşturmak amacıyla ortak güvenlik özelliklerini paylaşan varlıkları belirlemektir.

Sistemin bölgelere ve kanallara bölünmesi, bir siber saldırının kapsamını sınırlayarak genel riski de azaltabilir. Bölüm 3-2, bazı varlıkların aşağıdaki şekilde bölümlendirilmesini gerektirir veya tavsiye eder:

- İş ve kontrol sistemi varlıklarını ayırın.
- Emniyetle ilgili varlıkları ayırın.
- Geçici olarak bağlanan cihazları ayırın.
- Kablosuz cihazları ayırın.
- Dış ağdan bağlanan cihazları ayırın.

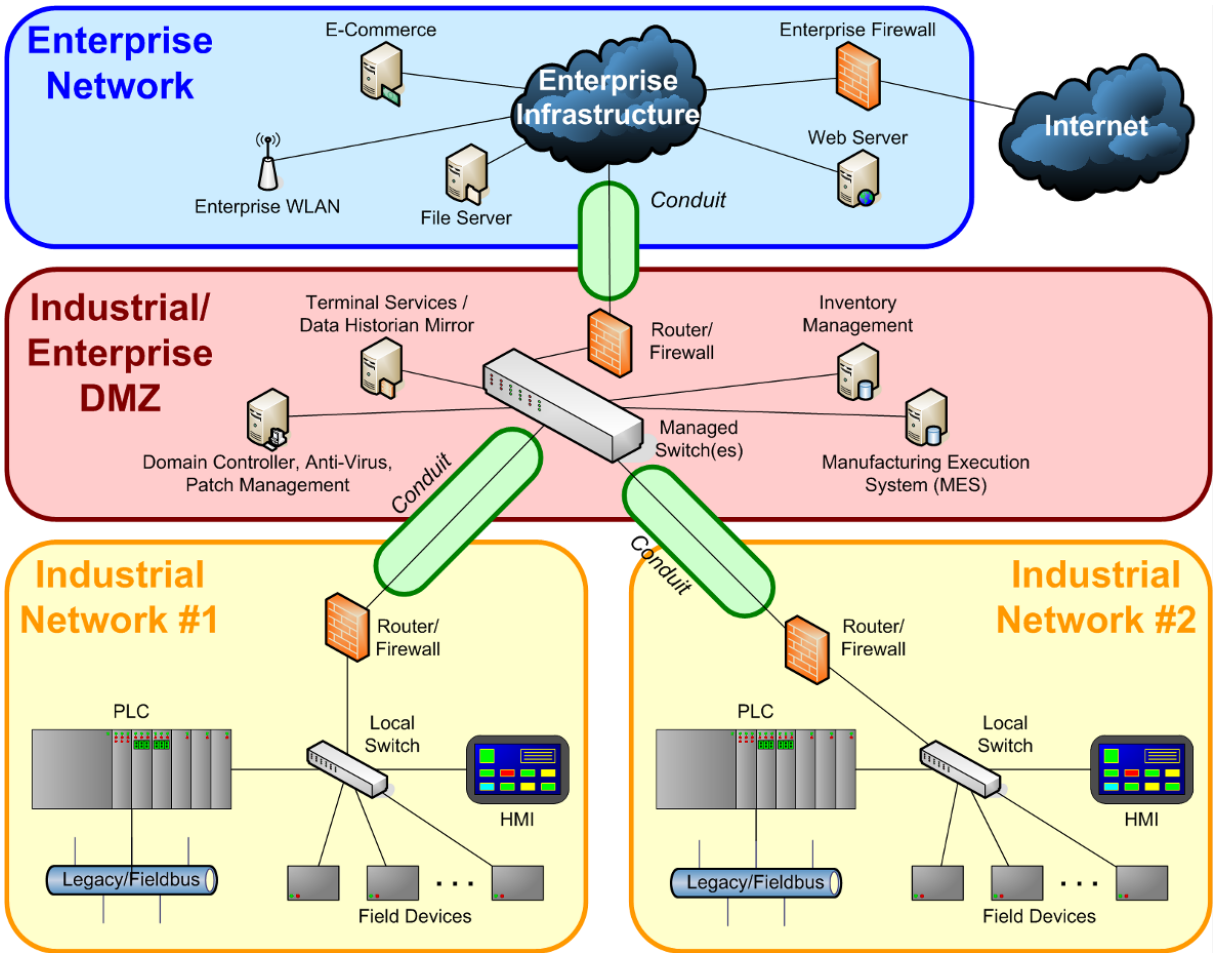

Figure 4: ISA/IEC 62433 bölge ve kanal örneği, SuC kurumsal ve endüstriyel cihazları bir arada içermektedir.

Figür 4'te görülebileceği üzere SuC bölge ve iletim kanallarına ayrılmıştır. Kurum ağından endüstriyel ağa doğru (daha derine doğru) erişim kısıtlıdır. DMZ ise silahsızlaştırılmış bölge (demilitarized zone) anlamına gelir ve hem internete daha yakın bölgelerden ve internetten, hem de daha derin bölgelerden ulaşılabilmesine karşın DMZ'in kendisinin derin bölgelere ulaşımı kısıtlanmıştır. IACS sistemlerinde DMZ'i OT ağını IT ağından ayırmak için kullanmak iyi bir pratiktir.

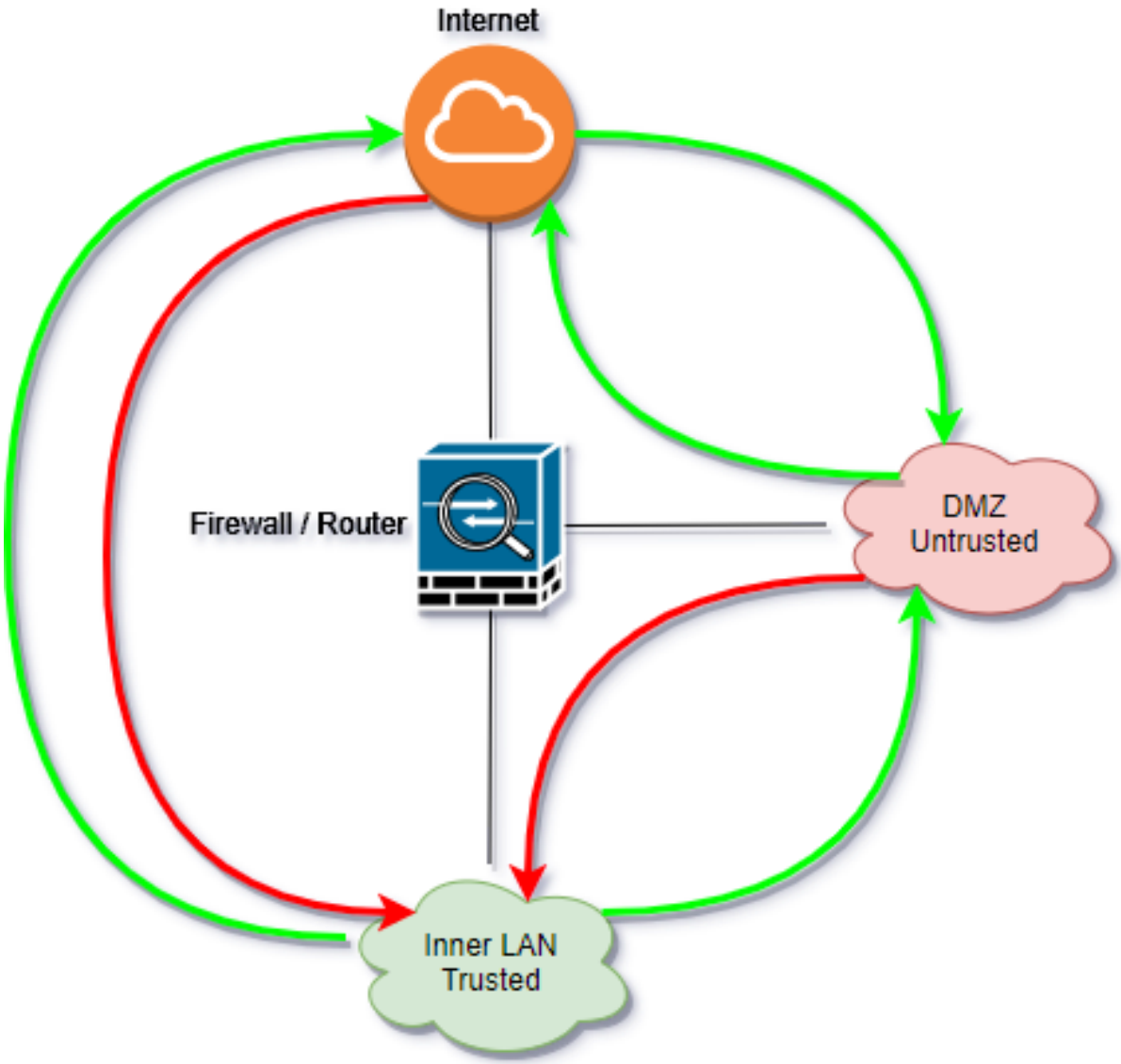

Figure 5: DMZ'de daha hafif kısıtlamaların olduğu trafik yeşil, daha ağır kısıtlamaların olduğu trafik kırmızı ile ifade edilmiştir.

5 Güvenlik düzeyleri (Security Levels)

Güvenlik düzeyi, SuC'un, bölgenin veya iletim kanalının güvenlik açıklarından arınmış olduğuna ve amaçlanan şekilde çalıştığına dair güvenin ölçüsü olarak tanımlanır. 3 farklı güvenlik düzeyi tipi ve dört farklı güvenlik düzeyi vardır.

Hedef Güvenlik Düzeyleri (SL-T), belirli bir otomasyon çözümü için istenen güvenlik düzeyidir. Risk değerlendirme süreci sonucunda belirlenirler. SL-T, IACS yaşam döngüsünün Entegrasyon aşaması sırasında ürünleri seçmek ve ek karşı önlemler tasarlamak için kullanılır.

Varlık Sahibi, bu SL-T'ye dayanarak alt sistemlerin ve bileşenlerin tedarikini gerçekleştirir ve IACS'yi belirli hedef ortamda uygular. Her bileşen ve alt sistem bir "Yetenek Güvenlik Düzeyi" (SL-C) ile karakterize edilir.

Sisteme implementasyonundan sonra, "Ulaşılan Güvenlik Seviyesi"nin (SL-A) daha önce belirtilen gereksinimleri karşılayıp karşılamadığını doğrulamak için varlık sahibi tarafından değerlendirilir (SL-A'nın SL-T'den büyük veya eşit olup olmadığının kontrol edilmesi). Telafi edici karşı önlemler (hem teknik hem de prosedürsel), hedefe tam olarak ulaşılıncaya kadar sistem düzeyinde veya süreç ve prosedürlerde uygulanır.

Güvenlik düzeyi, belirli bir cihazın araştırılması ve ardından sistemdeki yerine bağlı olarak hangi güvenlik düzeyine sahip olması gerektiğinin belirlenmesiyle tanımlanır. Güvenlik seviyeleri 1'den 4'e kadar dört farklı seviyeye ayrılabilir (her ne kadar standartta nadiren kullanılan "açık" seviye 0'dan da bahsedilse de).

Bir bölgenin güvenlik seviyesi hedefi belirlendikten sonra, bölge içindeki cihazların ilgili güvenlik seviyesini karşılayıp karşılamadığının analiz edilmesi gerekir. Aksi takdirde, hangi karşı önlemlerin SL hedefine ulaşmaya yardımcı olabileceğini planlamak gerekir. Bu karşı önlemler teknik (ör. güvenlik duvarı), idari (ör. politikalar ve prosedürler) veya fiziksel (ör. kilitli kapılar) olabilir.

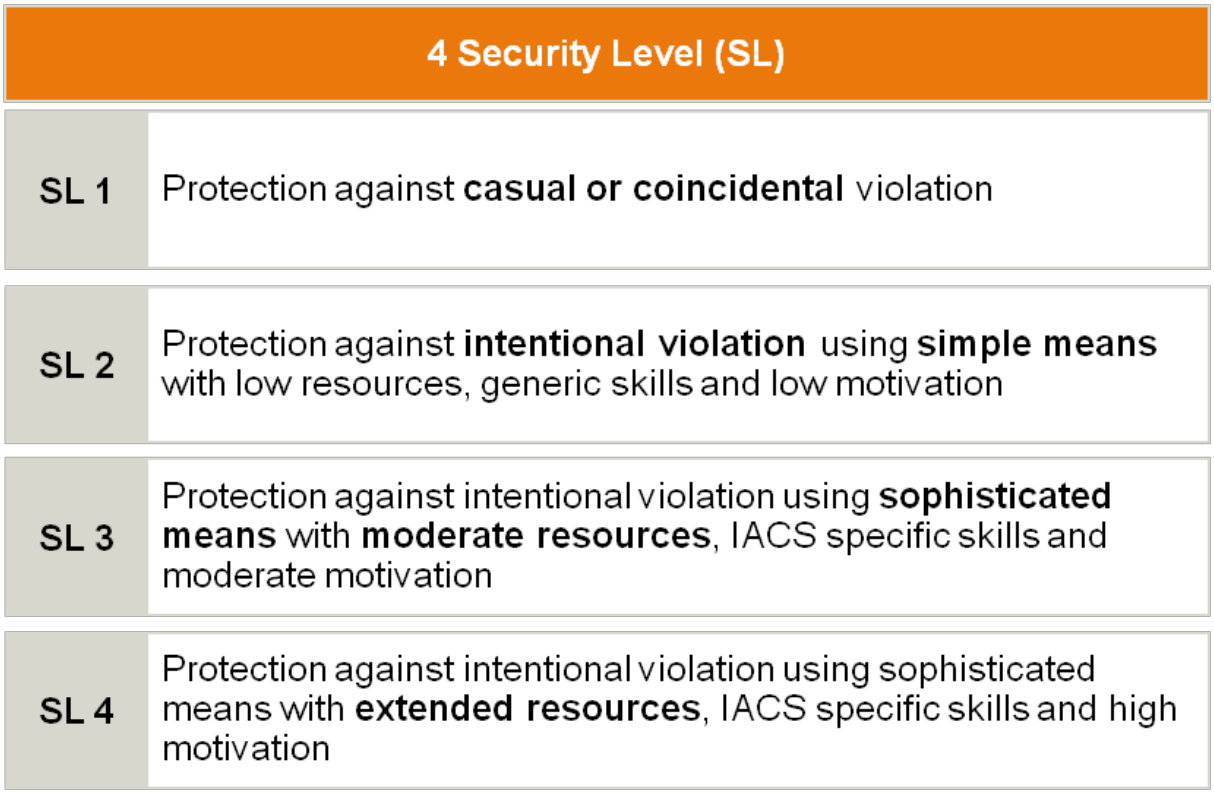

Figure 6: Güvenlik düzeylerinin listesi

6 Olgunluk modeli (Maturity model)

Güvenlik seviyeleri teknik gereksinimlerin gücünün bir ölçüsü iken, olgunluk seviyeleri süreçlerin (kişiler, politikalar ve prosedürler) bir ölçüsüdür. Tabloda gösterildiği gibi olgunluk modeli, seviye 4 ve 5'in seviye 4'te birleştirildiği yetenek olgunluk modeli entegrasyonuna (CMMI) dayanmaktadır.

Level	CMMI	62443	Description
1	Initial	Initial	• Product development is typically ad-hoc and often undocumented • Consistency and repeatability may not be possible
2	Managed	Managed	• Product development managed using written policies • Personnel have expertise and are trained to follow procedures • Processes are defined but some may not be in practice
3	Defined	Defined (Practiced)	• All processes are repeatable across the organization • All processes are in practice with documented evidence
4	Quantitively Managed	Improving	• CMMI Levels 4 and 5 are combined • Process metrics are used control effectiveness and performance
5	Optimizing		• Continuous improvement

Figure 7: Olgunluk seviyeleri

7 Derinlemesine defans (Defence-in-Depth)

ISO/IEC 62433 standartlarında birçok dizayn prensibi belirtilmiştir, bunlar arasından örnekler tasarımla beraber güvenlik (secure by design), atak yüzeyini azaltma (reduce attack surface) ve derinlemesine defans (defence-in-depth)'tır.

Derinlemesine defans (defence-in-depth) (DiD), bir SuC içine çok sayıda güvenlik kontrolü (defans) katmanının yerleştirildiği, IACS'larda kullanılan kritik bir siber savunma yaklaşımıdır. Amacı, bir güvenlik kontrolünün başarısız olması veya sistemin yaşam döngüsü boyunca personel, prosedür, teknik ve fiziksel güvenlik hususlarını kapsayabilecek bir güvenlik açığından yararlanılması durumunda yedeklilik sağlamaktır.

IACS sistemlerindeki en büyük hatalardan birisi SuC içinde herhangi bir katman veya hiyerarşi olmadan tüm cihazların birbirleriyle iletişime geçirtilmesidir. Cihazların bu tarz kullanımı tehditlere daha çok kapı aralamaktadır. Bir diğer hata IT güvenliğinin yeterli olduğunu, IACS elemanlarının komplike olmasından kaynaklı kendiliğinden güvenli olduğu yanılgısıdır. Endüstri 4.0 ve IIOT ile cihazlar daha interaktif hale gelmiştir. IACS sistemlerinde IT ve OT güvenliği bir arada sağlanmalıdır.

Bu, Ulusal Güvenlik Ajansı (NSA) tarafından bilgi ve elektronik güvenliğe kapsamlı bir yaklaşım olarak tasarlanan bir katmanlama taktiğidir. DiD, aynı adı taşıyan bir askeri stratejiden esinlenmiştir, ancak kavram olarak oldukça farklıdır.

DiD tekniğinin ilk aşaması bölgeler ve iletim kanallarının belirlenmiş olmasıdır. Bu bölgeler baz alınarak katmansal bir güvenlik sistemi kurulmaya çalışılır. Her bölgenin yalnızca en zayıf halkası kadar güvenli olduğu unutulmamalıdır, bu nedenle yüksek riskli varlıkların belirli bölgelere izole edilmesi tavsiye edilir. Bölgeleri ayırmada gateway, firewall, VPN, VLAN gibi teknolojiler kullanılabilir.

Genel olarak 6 katmanlı bir yapı söz konusudur; bunlar veri (data), uygulama (application), host, dahili ağ (internal network), çevre (perimeter) ve fiziksel (physical) katmanlardır. Ancak bazı kaynaklar Compute ve Politika katmanlarını da DiD yaklaşımına dahil edebiliyorlar.

7.1 Güvenlik soğanı ve enginarı

Güvenlik soğanı ve enginarı, derinlemesine defans metadolojisini görselleştirmeye yarayan kavramlardır. Güvenlik soğanı, saldırının tüm katmanları aşmaya çalıştığı ideal bir sisteme saldırısını ifade ederken; enginar, ideal olmayan sistemlerde eksik veya hatalı katmanların bulunduğu sistemleri saldırgan bakış açısından görselleştirir.

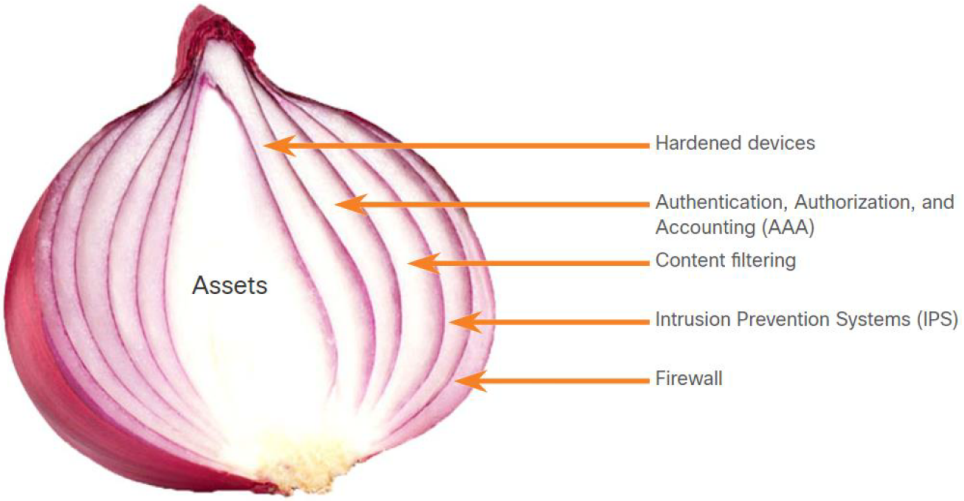

Figure 8: Güvenlik soğanı

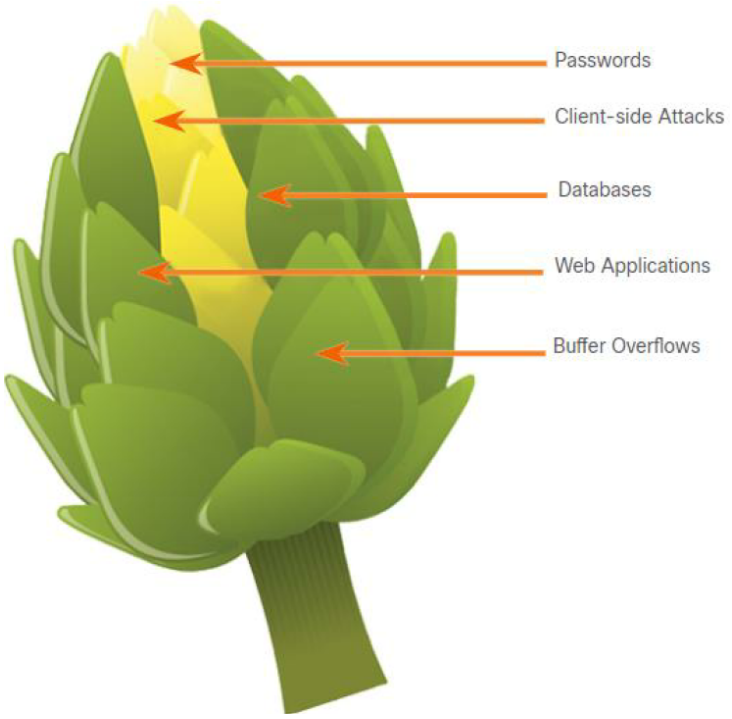

Figure 9: Güvenlik enginarı

7.2 Fiziksel güvenlik katmanı

İlk katman organizasyonun fiziksel güvenliğini sağlamaya yöneliktir. Kritik varlıklara fiziksel erişim organizasyonun politikalarınca kısıtlanmalıdır. Burada AAA metadolojisi ve smart-card veya biometrik sistemler fiziksel erişimi düzenlemek adına kullanılabilecek teknolojilerdendirler. Fiziksel güvenlik, kritik varlık ve bölgelere erişim ile elektronik cihazlara fiziksel erişim yollarını kapsar.

Fiziksel güvenlik katmanının ihmaline örnek olarak alınan stajyerin organizasyon içinden çaldığı harddiskleri dışarıya çıkarması örnek verilebilir, çözüm örneği fiziksel güvenlik katmanını güçlendirmektir. Bunu gerçekleştirmek adına organizasyon metal dedektörlerini arttırabilir veya güvenlik görevlilerine fiziksel güvenlik katmanı hakkında bilgilendirmeler yapılabilir.

7.2.1 AAA

AAA metadolojisinin ingilizce açılımı authentication, authorization, accounting yani kimlik doğrulama, yetkilendirme ve kayıt tutmadır. Bu yöntemde fiziksel erişim sağlamak için önce organizasyon politikalarınca kişinin tanımlanması gereklidir. Tanımdan sonra bilinen kişinin hangi kritik varlıklara veya bölgelere (zone) ne düzeyde erişebileceğinin belirlenmesi gereklidir. Yetkisi daha fazla olan kişinin organizasyonun kritik bölgelerinde yer alması sağlanabilir. Yetkilendirme aşamasında dikkat edilen önemli hususlardan bazıları verilen yetkinin diğer şahıslara ne kadar yetki verilebileceğine dikkat etmektir ve kritik varlıklar üzerindeki yetkisidir. AAA metadolojisinin son kavramı accounting yani kayıt tutmadır. Kimin nerede ne kadar süre hangi yetkiyle bulunduğunu bilmek ileride olacak sızıntının tespitinde işe yarayacaktır.

7.2.2 Smart kart ve biometrik sistemler

Smart-kartlar kişinin tanımlanması ve kimlik doğrulamasında kullanılabilecek bir karttır. NFC protokollerinin kullanıldığı temassız kartlar fiziksel güvenliği daha iyi yapabilmek daha uygundur ve kartın kopyalanması neredeyse imkansızdır. Daha ciddi güvenlik önlemi alınmak isteniliyorsa, yüz ve iris tanımlanmasının yapıldığı biometrik sistemler kullanılabilir.

7.3 Çevre güvenlik katmanı

İngilizce adı "Perimeter" olan bu katmanın amacı sistemi bölgelere ayıran geçiş bölgelerindeki güvenliği ima eder. IACS sistemlerinde özellikle endüstriyel işlemlerin yürütüldüğü OT ve güvensiz ağlara ve internete daha yakın olan IT ağları arasındaki çevre güvenlik katmanına dikkat edilmelidir.

Çevre katmanı, erişim kısıtlama ve yetkilendirilmemiş/istenmeyen içeriği filtreleme işlemlerini uygular. Bunu yapmak adına en önemli işlevi IP ve port erişiminin ayarlanmasıdır. Trafiğin akmaması gereken inbound veya outbound portların kapatılması veya kısıtlandırılması, sadece yetkilendirilmiş ağların IP'lerine izin verilmesi, çevre güvenlik katmanının fonksiyonlarından en önemlileridir. Bu işlem genelde firewall'ler tarafından yürütülür. OT bölgesini IT bölgesinden ve güvensiz internetten korumak için geliştirilen DMZ'ler de firewall ve gateway gibi çevre güvenlik katmanı cihazları ile mümkün olur.

Bir diğer önemli nokta dışarıdan gelecek saldırıların çevre güvenlik cihazlarında tespit edilmesi veya durdurulmasıdır. Bunu yapabilmek için IDS ve IPS cihazları kullanılır. NGFW denilen firewall çeşitleri IDS/IPS özelliğine sahip olabilirler.

Son olarak, uzaktan erişim sağlayan endpoint'lerin içeriye VPN ile girmesi de bu katmanı ilgilendiren bir durumdur.

Çevre güvenlik katmanı elemanları implemente edilmesi yetersizdir, bölgelerin de iyi belirlenmiş olması elzemdir. Firewall'e bağlı olmayıp internete bağlı olan bir IOT cihazı, yüksek bir güvenlik ihlalidir.

7.3.1 Firewall tipleri

En temel firewall tipi stateless firewall'lerdir. Bu firewall'lerde ACL (Access Control List), yani erişim kontrol listesi bulunur. Bu liste firewall'in interface'lerinde inbound (giren) ve outbound (çıkan) iletişimlerde peketlerin network ve transport katmanlarındaki IP ve port bilgilerine bakarak erişim kontrolünü ayarlar. Stateless firewall katı kurallarında esneme yapmaz ve genelde ucuz ve basit yapıları vardır.

Katı kurallara sahip bir firewall'dan ziyade var olan iletişimlerin kayda tutulup erişimin açıldığı tarzdan firewall'lere stateful firewall denir. Bu firewall'ler içeriden dışarıya bir

iletişim oluşup TCP bağlantısı kurulduktan sonra kurallarda olmasa bile geçici bağlantılara izin verip iletişimde esneme oluşturabilir. Bu tarz esnemelerin oluşabilmesi için durumların tutulduğu ACL dışında bir de state table bulunur.

Sadece IP veya port kısıtlaması değil, aynı zamanda paketlerin uygulama katmanlarının incelenmesi de firewall içinde yapılması istenilebilir. Bunun yapılabilmesi Application-level firewall (Uygulama katmanı firewall'leri) sayesinde mümkün olur. Bir diğer ismi proxy firewall'dir.

Çevre birimlerinden olan firewall için manipülasyonu veya iletişim buffer'ına aşırı yüklenilmesi söz konusu olabilir. Bunların gerçekleştirilmemesi adına yapay zekaya sahip NGFW (Next Generation Firewall) kullanılabilir. Bu tarz firewall'ler paketleri derinlemesine inceler, IDS/IPS özelliklerini taşır ve DDOS korumasına sahiptir.

7.3.2 IDS/IPS

IDS, intrusion dedection system (saldırı tespit sistemi), olası saldırıları ağ içinde tespit etmeye yarayan sistemdir. Bu sistem, kendisine gönderilen paketleri inceleyerek saldırı amaçlı paketler olup olmadığını anlamaya çalışır. IDS ağ içinde trafik oluşturmaz ancak saldırı tespiti halinde kendisi saldırıya bir cevap oluşturmaz. Evasion tekniklerine karşı daha savunmasızdır.

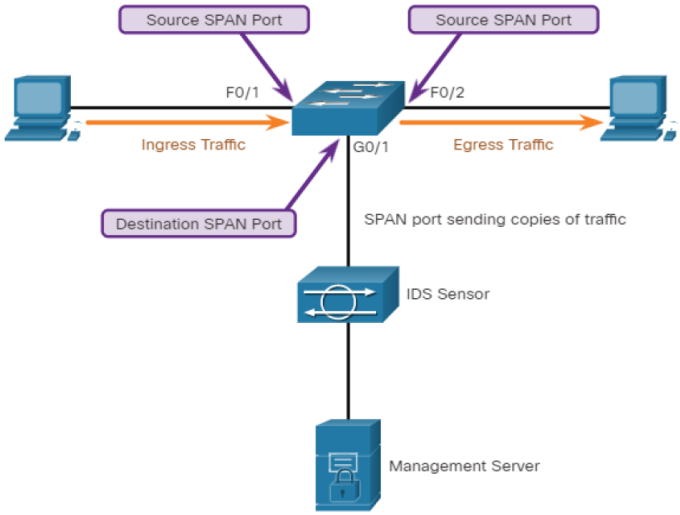

Figure 10: IDS'e kopyalanan trafik

IPS, intrusion prevention system (saldırı önleme sistemi), olası saldırılara cevap üretir. Bazı IPS sistemleri saldırıyı kendisi yakalayıp engellerken, bazı sistemler diğer sistemlerden gelen (IDS gibi) uyarıların gelmesiyle birlikte cevap üretir.

7.4 Ağ güvenlik katmanı

Saldırgan, çevre güvenlik katmanlarını geçip ağ içerisine ulaşması halinde saldırgan kritik varlıklara ulaşmasındaki ilk engel ağ güvenlik katmanıdır. Ağ güvenlik katmanı, oluşturulan paketlerin ağ cihazlarını manipüle etmesini içermesine karşı alınan önlemlerdir. Bu saldırı paketleri TCP/IP internet protokol dizisindeki her türlü katmanda değişiklikleri içerebilir. Ağ cihazlarının manipülasyonundaki amaç host cihazlara ulaşmak veya sistemi etkisiz hale getirmektir.

Network katmanında en çok görülen saldırı biçimleri arasında eavesdropping, reconnaissance, sniffing, snooping, man-in-the-middle yer almaktadır.

7.4.1 Data link katmanı

Data link katmanında görülen en sık saldırılar ARP ve wireless üzerinedir.

Wireless eavesdropping, saldırı cihazı wireless sinyalinin ulaşabileceği bir yerdeyse bu çok kolaydır. Önlem olarak wireless cihazlarının sinyalinin nereye kadar ulaştığını tespit edip topolojiyi bu bilgilere göre ayarlamaktır. En yeni wireless teknolojilerini kullanmak ve sahte wireless isimlerine karşı tetikte olmak önemlidir.

ARP kullanılarak yapılan saldırılara en önemli örnek ARP cache poisoning'tir. Ağdaki cihazların arp cache'lerindeki bilgileri değiştirerek kendisini default gateway yapmaya yarayan bu saldırı biçimi man-in-the-middle örneğidir. Ağdaki switch ve benzeri cihazların konfigürasyonu default gateway'in mac adresine ayrı bir şekilde dikkat edilerek yapılmalıdır.

7.4.2 Network katmanı

Network katmanı IP bilgisinin yer aldığı katmandır. Bu katmanda IP/ICMP gibi temel network protokolleri üzerinden veya dinamik routing/gateway protokolleri (OSPF, BGP,

FHRP) üzerinden yapılan saldırıları görürüz.

Temel network protokolü üzerinden yapılan saldırılara örnek amplification ve reflection saldırılarıdır. Bu saldırının amacı DoS yaratmaktır. Saldırgan sahte bir kaynak IP ile ağdaki cihazları tek bir cihaza doğru echo reply oluşturmaya zorlar.

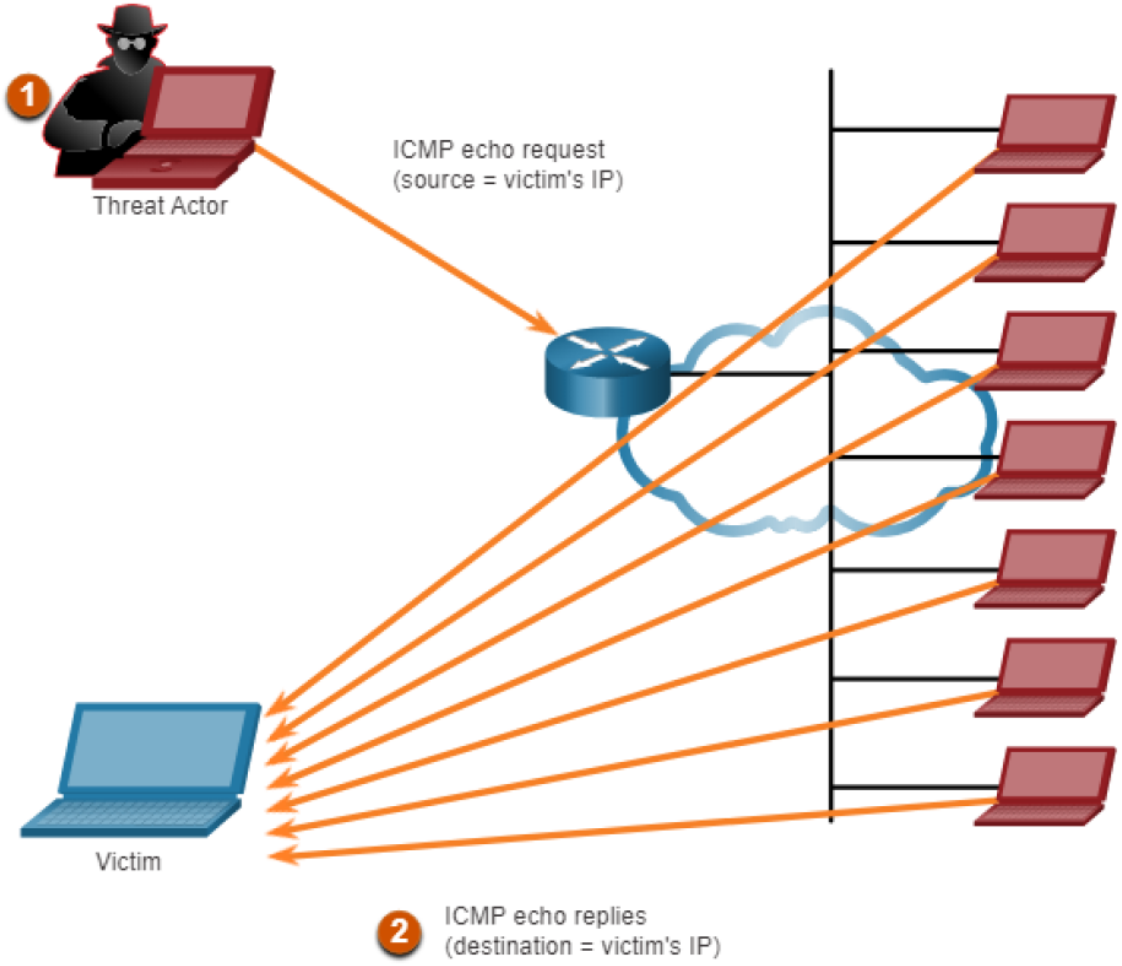

Figure 11: ICMP amplification ve reflection

Dinamik routing ve gateway protokollerinde saldırgan kendisini default gateway olarak ayarlayarak man-in-the-middle atağı gerçekleştirebilir. Bunu önlemek için router'ların konfigürasyonu üreticinin önerilen yoluyla yapmak en iyi pratiktir.

7.4.3 Transport katmanı

Transport katmanlarındaki ataklar genellikle TCP session'larını bozmaya yöneliktir. Bu ataklar arasında TCP SYN Flood attack, TCP Reset Attack, TCP Session hijacking,

UDP flooding örnek verilebilir.

SYN Flood attack, server ile birçok TCP bağlantısı oluşturarak diğer kullanıcıların server'ı kullanmasını zorlaştırır. Reset, network paketinin TCP bölümündeki FIN bitini ve diğer kimlik bilgilerini değiştirip daha önce oluşmuş bir bağı kesmeye yöneliktir. Session hijacking daha önce oluşmuş TCP bağlantısını TCP sıra sayısını tahmin ederek kendi üzerine alması saldırısıdır. UDP flooding bir tür DoS saldırısıdır.

7.4.4 Uygulama katmanı

Bu katmandaki saldırılar birincil olarak ağ güvenlik katmanını ilgilendirmekle beraber host, uygulama ve veri güvenlik katmanlarını da ilgilendirir ancak saldırı hala ağ içerisinde gerçekleştirilir, endpoint içerisine sızılmamıştır.

Network üzerinde dolaşan DNS, DHCP, NTP, HTTP gibi protokollerin zaafiyetlerinden yararlanılarak yapılan saldırılar ifade edilir. Kimi saldırılar sahte DHCP paketleriyle sistemin IP konfigürasyonunu bozarken, kimisi oluşmuş HTTP trafiğini değiştirerek sahte veri iletmeyi amaçlar. Paketlerin anlamlı bir şekilde değiştirilmeye uğratılamaması için şifrelenmesi önerilir.

7.4.5 Önlemler

Ağ güvenlik katmanında alınabilecek önemli önlemler arasında router ve switch gibi cihazların doğru konfigürasyonu; ağ cihazlarına erişimin prosedür ve poliçelerle belirlenmiş olması; AAA server'larının kullanımı; ACL, SNMP, NetFlow, NTP, Syslog gibi protokollerin kullanımı; SIEM/SOAR yazılımlarının kullanılması örnek verilebilir.

7.5 Host güvenlik katmanı

Host veya end-point cihazları program çalıştırabilen ve ağ içinde verinin gelebileceği en uç nokta olarak tanımlanır. Bu cihazlar bilgisayar veya telefon gibi üzerinde işletim sistemi çalıştırabilen cihazlar olabilir. Veya dış bilgisayara seri veya paralel iletişim protokkolü ile bağlanmış, özel olarak tasarlanmış programlanabilir bir cihaz da olabilir.

Bu güvenlik katmanı IACS'i en ilgilendiren taraflardan biridir çünkü SCADA ve DCS

gibi sistemlerdeki PLC'lerde genelde işletim sistemi bulunmaz, onun yerine PLC için tasarlanmış özel bir firmware bulunur.

Bu tarz cihazların güvenliğini sağlamak host güvenlik katmanının işlevidir. Bir endpoint cihazının güvenliğini sağlamak sezgisel olarak üç bölüme ayrılabilir: Gömülü taraf, işletim sistemi tarafı, erişim kontrolü tarafı.

7.5.1 Gömülü taraf

Host cihazının gömülü tarafı bootloader, firmware, kernel veya işletim sisteminin kendisine yönelik saldırıları içerir. Sahte firmware update'i veya cihaz tasarımının manipülasyonu gömülü tarafa olan saldırılara örnektir.

7.5.2 İşletim sistemi tarafı

İşletim sistemine sahip olan cihazlara host'un güvenliğini sağlamak adına bazı yazılımlar kullanılabilir. Bunlara ilk örnek antivirus/antimalware uygulamalarıdır. Bu uygulamalar host'a sızmış olan virüs ve malware'leri tespit edip gerekli karantinayı sağlamaya çalışır. Host-based firewall'ler ağdaki firewall cihazı ile aynı işlevi görür, buna en iyi örnek Windows Defender Firewall with Advanced Security'dir.

Daha gelişmiş savunma için HIDS ve HIPS kullanılabilir. HIDS, antimalware ve firewall özelliklerini içinde kapsayan hostlar için gelişmiş bir güvenlik ürünüdür. Anomalilere veya önceden oluşturulmuş politikalara bakarak sisteme uyarı verebilirler. HIPS, host içine kurulan ve host'a saldıran atakları engellemeye çalışır.

7.5.3 Erişim kontrolü

IACS sistemlerinde HMI'a olacak erişimin düzenlenmesi operasyonal sistemin işlevselliğini devam ettirmek için gereklidir. Host'lara erişimin düzenlenmesi ve AAA'ye dikkat edilmesi, atak yüzeyini azaltacak önemli bir faktördür. Bunu sağlayabilmek adına Active Directory gibi AAA server'lar kullanılabilir. Erişim kontrolünü sağlamanın altı örnek yolu aşağıda gösterilmiştir:

- İsteğe bağlı erişim kontrolü (Discretionary Access Control)(DAC): Bu, en az kısıtlayıcı

modeldir ve kullanıcıların, verilerin sahibi olarak verilere erişimi kontrol etmesine olanak tanır. Hangi kullanıcıların veya kullanıcı gruplarının bilgiye erişim sahibi olduğunu belirlemek için ACL'leri veya başka yöntemleri kullanabilir.

- Zorunlu erişim kontrolü (Mandatory Access Control)(MAC): Bu, en katı erişim kontrolünü uygular ve askeri veya kritik görev uygulamalarında kullanılır. Bilgilere güvenlik seviyesi etiketleri atar ve kullanıcıların güvenlik seviyesi yetkilerine göre erişime sahip olmalarını sağlar.

- Rol tabanlı erişim kontrolü (Role-based Access Control)(RBAC): Erişim kararları, bireyin kuruluş içindeki rollerine ve sorumluluklarına dayanır. Farklı rollere güvenlik ayrıcalıkları atanır ve kişiler, rol için RBAC profiline atanır.

- Nitelik tabanlı erişim kontrolü (Attribute-based Access Control)(ABAC): Erişilecek nesnenin niteliklerine, kaynağa erişen özneye ve nesneye nasıl erişileceğine ilişkin çevresel faktörlere bağlı olarak erişime izin verir.

- Kural tabanlı erişim kontrolü (Rule-based Access Control)(RBAC): Ağ güvenlik personeli, verilere veya sistemlere erişimle ilişkili kural dizisini belirler. Bu kurallar, izin verilen veya reddedilen IP adreslerini veya belirli protokolleri ve diğer koşulları belirtebilir. Kural Tabanlı RBAC olarak da bilinir.

- Zamana dayalı erişim kontrolü (time-based Access Control)(TAC): Ağ kaynaklarına zamana ve güne bağlı olarak erişim sağlar.

7.6 Uygulama güvenlik katmanı

Uygulama güvenlik katmanı, hedefin ulaşabileceği son katmanlardan biridir ve host içindeki uygulamaları hedef alır. Uygulamaların sahip olduğu güvenlik zaafiyetlerini kullanarak yetki yükseltme veya kritik verilere/varlıklara ulaşmaya çalışmak söz konusudur. Bu atak yüzeyini en aza indirmek adına yazılımcılar; uygulamaları güvenli yazmalı ve varlık sahipleri uygulamaları güncel tutarak güvenlik önlemi almalıdırlar. IACS içinde

SCADA/DCS sistemlerine input oluşturan veya düzenleyen yazılımlara (CAD, CAM, CNC gibi) dikkat edilmesi gerekir.

Uygulamaları bir ağ sistemi içinde güncel tutmanın yolu patch managament server'larından kullanmak olabilir. Bu server'lar host'tan gelen patch istekleri üzerine güncellemeler yapabilir veya ağı tarayıp uygulamalarının güncellenmesi gereken host'lara gerekli yamayı gönderebilir.

Bir diğer önemli husus hangi uygulamaların ve ne kadar çalıştırılabileceğinin izlenmesidir. Bunun için işletim sisteminde kullanıcılar için hangi uygulamaların çalıştırılabileceğine dair whitelisting-blacklisting yöntemi izlenebilir.

7.6.1 Stuxnet örneği

Stuxnet, ABD ve İsrail'in geliştirdiği İran'ın nükleer santrallerini hedef alan solucan yazılımdır. Bu solucan yazılımının hedefi SCADA ve PLC sistemleriydi. Stuxnet solucanı, girdiği sistemde PLC'yi kontrol eden Siemens Step7 yazılımını tarar ve kodu bozarak PLC'yi anormal komutlar gönderir. Siemens Step7 yazılımının kullanımının erişimini kısıtlamak ve güncel tutmak bu zaafiyete karşı iyi bir önlem olabilir.

7.7 Veri güvenlik katmanı

Veri, saldırganın nihai hedefidir. Verinin nasıl tutulması gerektiği CIA Triad ile belirlenmiştir. CIA Triad, bilgi güvenliği alanında temel bir kavramı temsil eder ve bilginin ve bilgi sistemlerinin güvenliğini sağlamak için temel prensipleri veya hedefleri temsil eder. CIA Triad'in üç bileşeni şunlardır:

- Gizlilik (Confidentiality): Gizlilik, hassas bilgilerin yetkisiz erişim veya ifşadan korunması anlamına gelir. Bu, yalnızca yetkili kişilerin veya kurumların bilgiye erişimine izin verilmesini ve yetkisiz ifşayı önlemek için şifreleme, erişim denetimleri ve diğer güvenlik önlemlerinin alınmasını içerir.

- Bütünlük (Integrity): Bütünlük, bilginin ve verilerin güvenilirliği ve güvenilirliğini ifade eder. Bu, bilginin depolanması, iletilmesi veya işlenmesi sırasında doğru, eksiksiz ve değişmeden kalmasını sağlamayı içerir. Bütünlüğü korumak için alınacak

önlemler arasında veri doğrulama, kontrol toplamları, dijital imzalar ve yetkisiz değişiklikleri önlemek için erişim denetimleri bulunur.

- Erişilebilirlik (Availability): Erişilebilirlik, bilginin ve bilgi sistemlerinin yetkili kullanıcılar tarafından ihtiyaç duyulduğunda erişilebilir ve kullanılabilir olmasını sağlama anlamına gelir. Bu, erişimi engelleyebilecek kesintilere, aksaklıklara veya hizmet reddi saldırılarına karşı korunmayı içerir. Erişilebilirliği sağlamak için alınacak önlemler arasında yedekleme ve kurtarma süreçleri, felaket kurtarma planlaması, yedeklilik, hata tolere edicilik ve yedekleme bulunur.

8 Sonuç

IEC62433'ün belli kavramları bu yazıda incelenmiş ve derinlemesine defans yöntemi detaylı incelenmiştir. Organizasyonların en iyi güvenliği sağlamak adına bu standartları takip etmesi kişi ve kurumların güvenliğini sağlamak için bir temel taşı görevi görmektedir.

9 Kaynakça

- Mosteiro-Sanchez, A., Barcelo, M., Astorga, J., & Urbieta, A. (2020). Securing IIoT using defence-in-depth: towards an end-to-end secure industry 4.0. Journal of Manufacturing Systems, 57, 367-378.
- Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X., & Terpenny, J. (2018). Cybersecurity for digital manufacturing. Journal of manufacturing systems, 48, 3-12.
- Gouda, M. G., & Liu, A. X. (2005, June). A model of stateful firewalls and its properties. In 2005 International Conference on Dependable Systems and Networks (DSN'05) (pp. 128-137). IEEE.
- Endüstriyel Otomasyon ve Kontrol Sistemleri için Güvenlik
- Defence-in-Depth for Azure

- ISA/IEC 62443 Series of Standards
- A practical approach to adopting the IEC62433 standards
- IEC: "IEC Cyber security Brochure overview," 2018.
- SH Piggin: "Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security," 2013.
- M Portella, M Hoeve, F Hwa, et al: "Implementing An Isa/Iec-62443 And ISO/IEC-27001 OT Cyber Security Management System At Dutch DSO Enexis," 2019.
- ANSI/ISA-62443-2-1: "Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program," 2009.
- Doan: "Companies Need to Rethink What Cybersecurity Leadership Is" Accessed May 17, 2019.
- J Parenty, JJ Dome: "Sizing Up Your Cyberrisks" Accessed May 17, 2019.
- Elkhannoubi, M Belaissaoui: "Fundamental pillars for an effective cybersecurity strategy," 2015.
- Winkler I: "7 elements of a successful security awareness program," CSO Accessed July 26, 2021.
- ISA/IEC-62443-3-2: "Security for Industrial Automation and Control Systems: Security Risk Assessment and System Design," 2015.
- Homeland Security: "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," 2016.
- NIST SP 800-82 Rev. 2: "Guide to Industrial Control Systems (ICS) Security."
- FIPS PUB 200: "Minimum Security Requirements for Federal Information and Information Systems."

- NIST SP 800-39: "Managing Information Security Risk Organization, Mission, and Information System View," 2011.
- Ganin P, Quach M, Panwar Z, et al: "Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management," 2017.
- Office of the Secretary of Defense: "Handbook for Self-Assessing Security Vulnerabilities and Risk of Industrial Control Systems on DOD Installations," 2014.
- NISTIR 8179: "Criticality Analysis Process Model," 2018.
- "IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models," 2009.
- Papakonstantinou J, Linnosmaa A, Z Bashir, et al: "Early Combined Safety - Security Defense in Depth Assessment of Complex Systems," 2020.
- Idaho National Laboratory: "Control Systems Cyber Security: Defense in Depth Strategies," 2006.
- Creation of ISA/IEC 62443-compliant products Matteo Giaconia, Security Pattern and Xavier Bignalet, Microchip Technology Inc.
- Quick Start Guide: An Overview of ISASecure® Certification
- Quick Start Guide: An Overview of ISA/IEC 62443 Standards
- Roles and Responsibilities in the Security Lifecycle
- Cisco CyberOps slides