IV. Güç ve Enerji Sistemleri Sempozyumu

Akıllı Şebekelerde Siber Güvenlik

Çağrı POLAT | 18.10.2019 |14:00

Çağrı POLAT

Siber Güvenlik Uzmanı / Eğitmeni
Endüstri 4.0 Güvenlik Uzmanı
ISO 27001 Baş Denetçi & Danışman

Facebook.com/cagripolatmsc
Twitter.com/cagripolatmsc
Instagram.com/cagripolatmsc
Linkedin.com/in/cagripolat

Firma:
Maxion İnci Jant Grubu - Türkiye IT Operasyonları Md.

Eğitim:
Yüksek Lisans: Bilgisayar Mühendisliği (DEU)
Lisans: Elektrik-Elektronik Mühendisliği (Anadolu Üni.)
Lisans: İşletme Fakültesi (Anadolu Üni.)

Sertifikalar:
MCSE+S & CEH (Eğitmen)
ISO 27001 Baş Denetçi
Bilirkişi

Çalışma Alanları:
#Siber Güvenlik, #Endüstri 4.0, #Kritik Altyapı Güvenliği
#ISO27001, #Sızma Testi, #KVKK Güvenlik, #Blockchain

Mail / Telefon:
cagripolat@gmail.com , 0 553 337 48 11

Web Sitesi:
https://www.cagripolat.com

0 İçerik

- **Kritik Altyapı/Akıllı Şebekeler/Aktörleri**
- **ISA 99**
- **IEC 62443**
- **Purdue Modeli/Şeması**
- **Akıllı Şebekelerde Siber Güvenlik(NIST-Guidelines for Smart Grid Cybersecurity)**
- **Sorular**

1 Kritik Altyapı/Akıllı Şebekeler

- “Kritik altyapı” terimi ilk defa Ekim 1997 tarihli “Amerika Birleşik Devletleri Başkanlık Komisyonu’nun Kritik Altyapıların Korunması Hakkında Raporunda kullanılmıştır.

- Siber Güvenlik Kurulu 2013-2014 Eylem planının 5 numaralı maddesinde ülkemizin kritik altyapıları bilgi güvenliği kapsamında ilk etapta "Ulaşım, Enerji, Elektronik Haberleşme, Finans, Su Yönetimi" Kritik Kamu Hizmetleri olarak belirlenmiştir. [1]

- Akıllı şebeke(Smart Grid) mevcut elektrik altyapısını günümüz otomasyon, gömülü sistemler ve bilişim teknolojileri ile harmanlayıp enerji ihtiyacını karşılayacak sisteme denir[2].

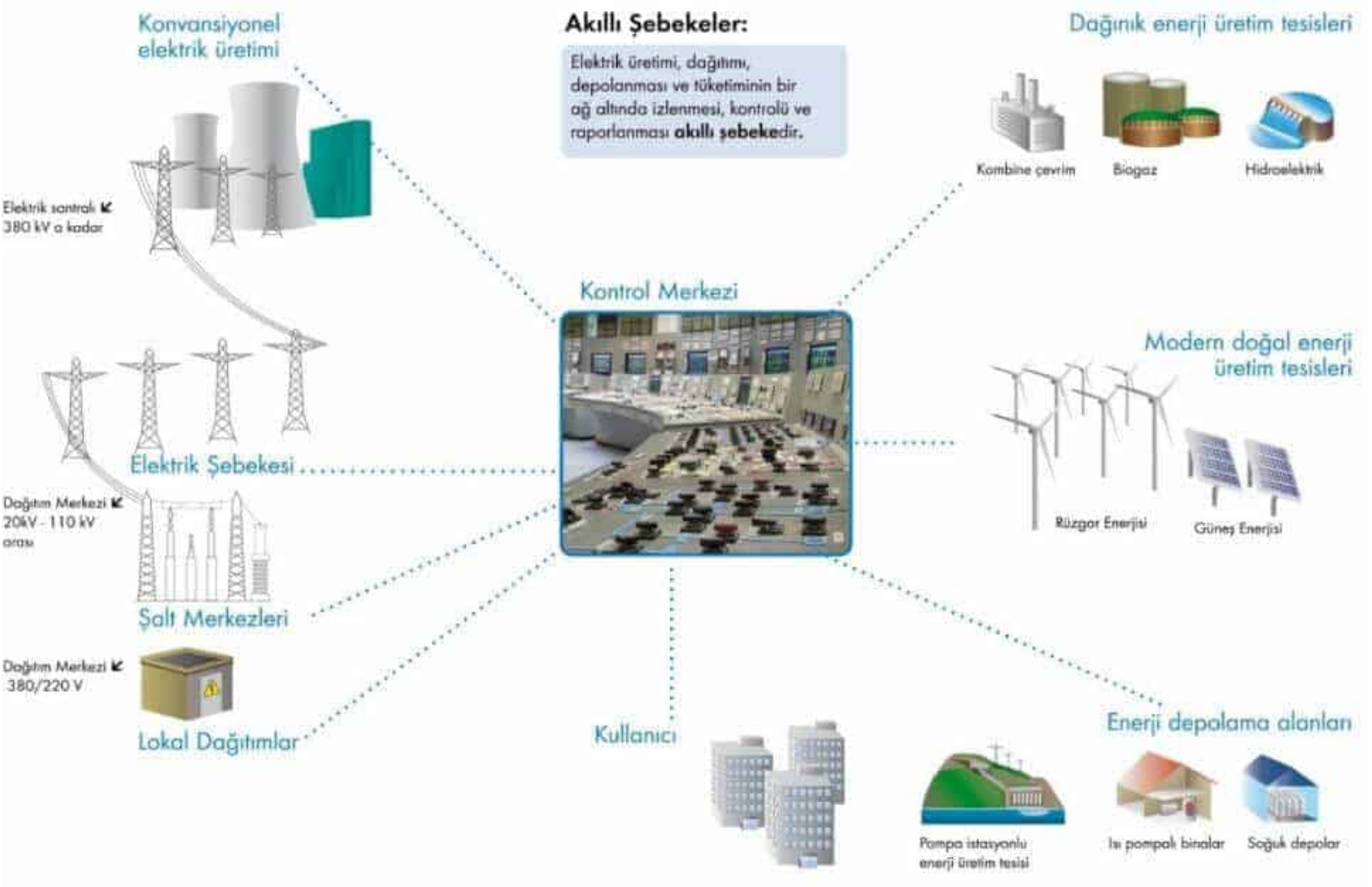
- Akıllı Şebeke Bileşenleri ve Teknolojisi şunlardır [3];
  1) Akıllı Üretim
  2) Akıllı İstasyonlar
  3) Akıllı Dağıtım
  4) Akıllı Sayaçlar
  5) Bütünleştirilmiş Haberleşme
  6) İleri Kontrol Metotları

Akıllı şebekelerin yazılım ve donanım bileşenleri vardır:

Yazılım: Veri altyapısı, internet tabanlı sistemler, sezgisel çalışan yazılımları

Donanım: Akıllı sayaçlar ve akıllı ev aletleri vb.

Akıllı Şebekeler



https://www.muhendisbeyinler.net/akilli-sebekeler-smart-grid

2 ISA 99 (Industrial Automation and Control Systems Security)

- ISA 99(Industry Standards on Automation) Endüstriyel Otomasyon ve Kontrol Sistemleri Güvenlik Standardıdır. Ağ üzerinde *etkin ve güvenli üretim uygulamalarının* tasarlanması için politikaları ve yapıları tanımlar. [4]

- ISA99 standartları geliştirme komitesi, endüstriyel otomasyon ve kontrol sistemleri güvenliği konusunda ISA standartlarını geliştirmek için dünya genelindeki endüstriyel siber güvenlik uzmanlarını bir araya getirir.

- Üretim ve kontrol sistemleri elektronik güvenliği kavramı, *tüm endüstrilerdeki her tür tesisi ve sistemi kapsayan* mümkün olan en geniş anlamda uygulanır. Üretim ve kontrol sistemleri şunları içerir, ancak bunlarla sınırlı değildir: [5]

    - DCS, PLC, SCADA, ağ bağlantılı elektronik algılama, izleme ve tanılama sistemleri gibi donanım ve yazılım sistemleri

    - Sürekli, toplu, ayrık ve diğer işlemlerde kontrol, güvenlik ve üretim işlemlerinin işlevselliğini sağlamak için kullanılan insan, ağ veya makine ara yüzleri

3 ISA/IEC 62443

- ISA99 komitesi tarafından geliştirilmiş standartlar serisidir. [6]
  (IEC: International Electrotechnical Commission)

- Bu standart ile ***şirketlerin kritik altyapı ve kontrol sistemlerindeki olası açıkları*** incelenmesi ve etkin koruma önlemleri geliştirilmesi için temel oluşturulması hedeflenmektedir.

- Endüstriyel otomasyon ve kontrol sistemlerine yönelik IT güvenliği, bu standardın odak noktasıdır. [7]

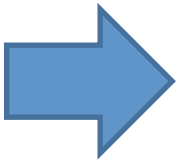
- IEC 62443 standardı, dört temel üzerinde şekillendirilmiştir.
  1. Standart fonksiyonları içerir.
  2. Zorunlu şartları karşılayan endüstriyel otomasyon ve kontrol sistemleri için IT güvenlik yönetimi sisteminin çerçevesini belirlemektedir.
  3. Endüstriyel otomasyon ve kontrol sistemleri (IACS) için tasarı kılavuzu olarak kullanılabilecek teknik özelliklerdir.
  4. Kontrol sistemi bileşenlerine ilişkin tasarım ve geliştirme şartlarından oluşmaktadır.

4 Purdue (PERA) Modeli

- ISA 99 komitesi, Purdue Enterprise Reference Architecture (PERA) modeli ve ICS ağ bölümlemesi için bu modeli kullanmıştır. [8]

- Purdue çok katmanlı mimari, **her katmanın gereksinimlerini dikkate alarak BT ve endüstri ağlarını alt ağlara ayırma ilkesine dayanır.**

- Purdue modeli 6 katmandan oluşur:
  - Seviye 5: Kurumsal ağ
  - Seviye 4: Yerel ağ
  - Seviye 3: Saha işlemleri
  - Seviye 2: Saha kontrolü
  - Seviye 1: Mantık kontrol
  - Seviye 0: Sensör, sürücü vb.

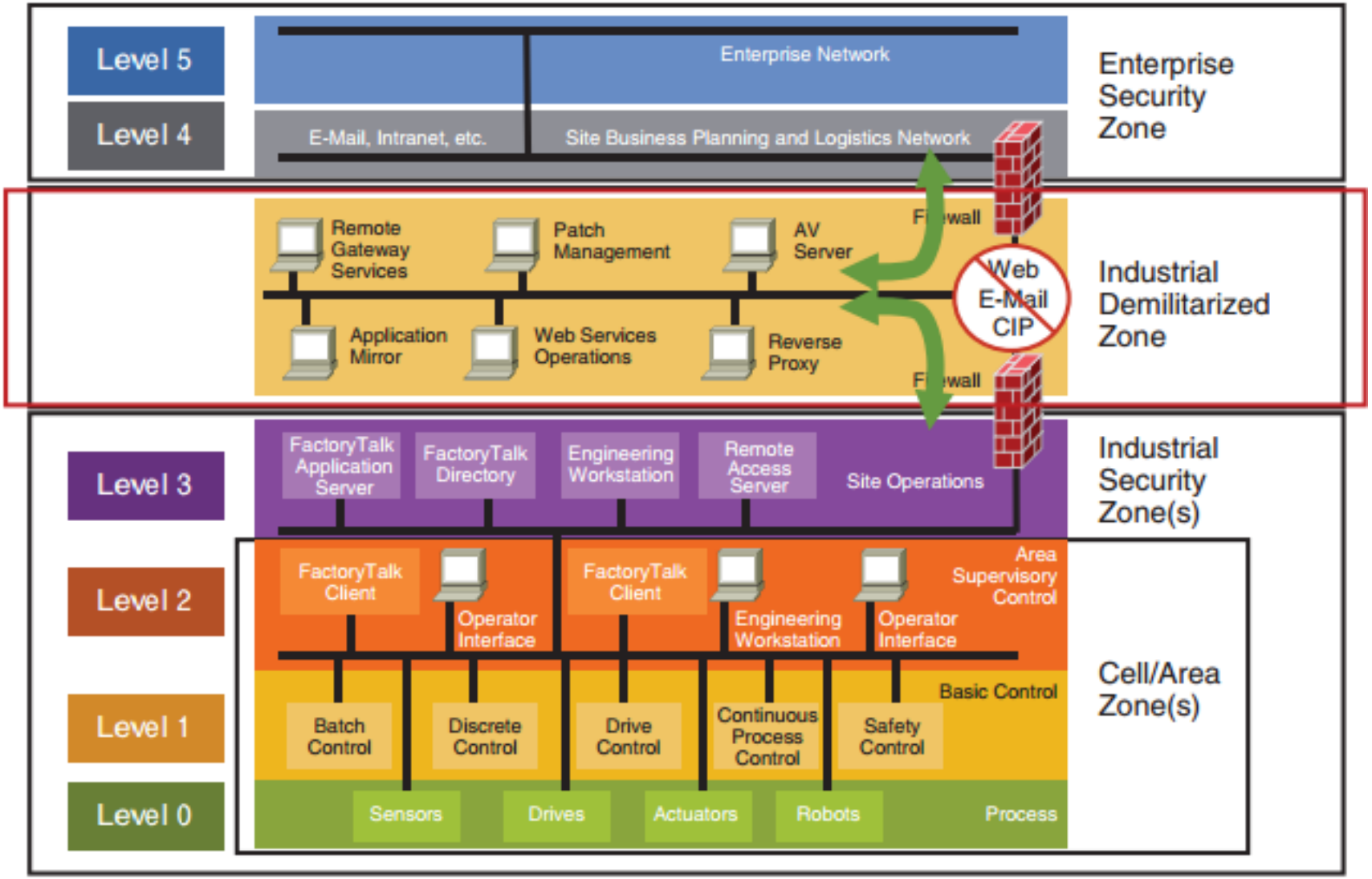


Yanda belirtilen 6 katmanın her biri için, aşağıdaki dört ana odak alanı tartışılmalıdır:

1.Giriş kontrolü
2.Log Yönetimi
3.Ağ güvenliği
4.Uzaktan erişim

Çok katmanlı Güvenlik Mimarisi!

Purdue Şeması



https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems

Akıllı Şebeke Aktörleri

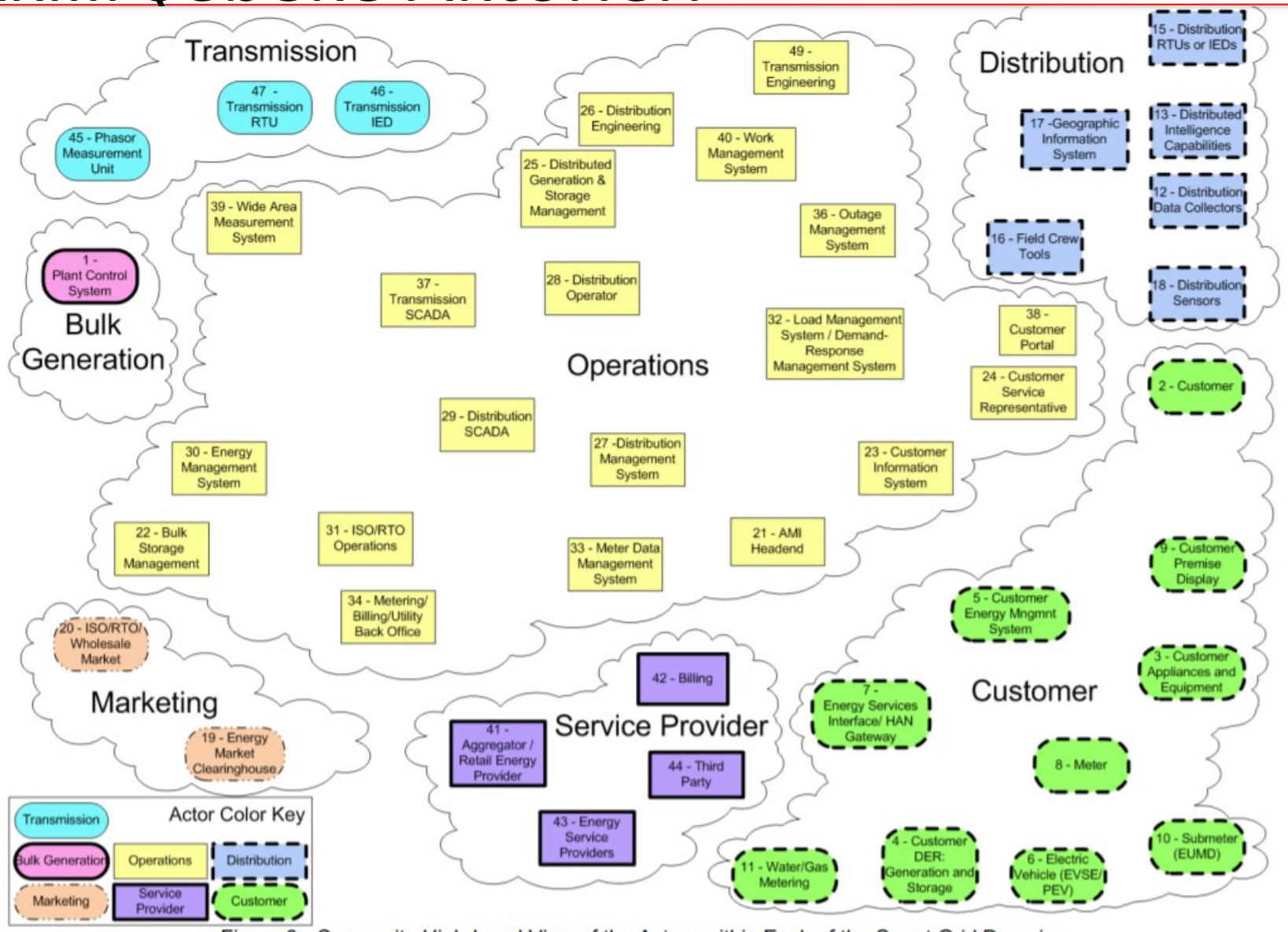


Figure 3 - Composite High-Level View of the Actors within Each of the Smart Grid Domains

Akıllı Şebeke Mantıksal Referans Modeli

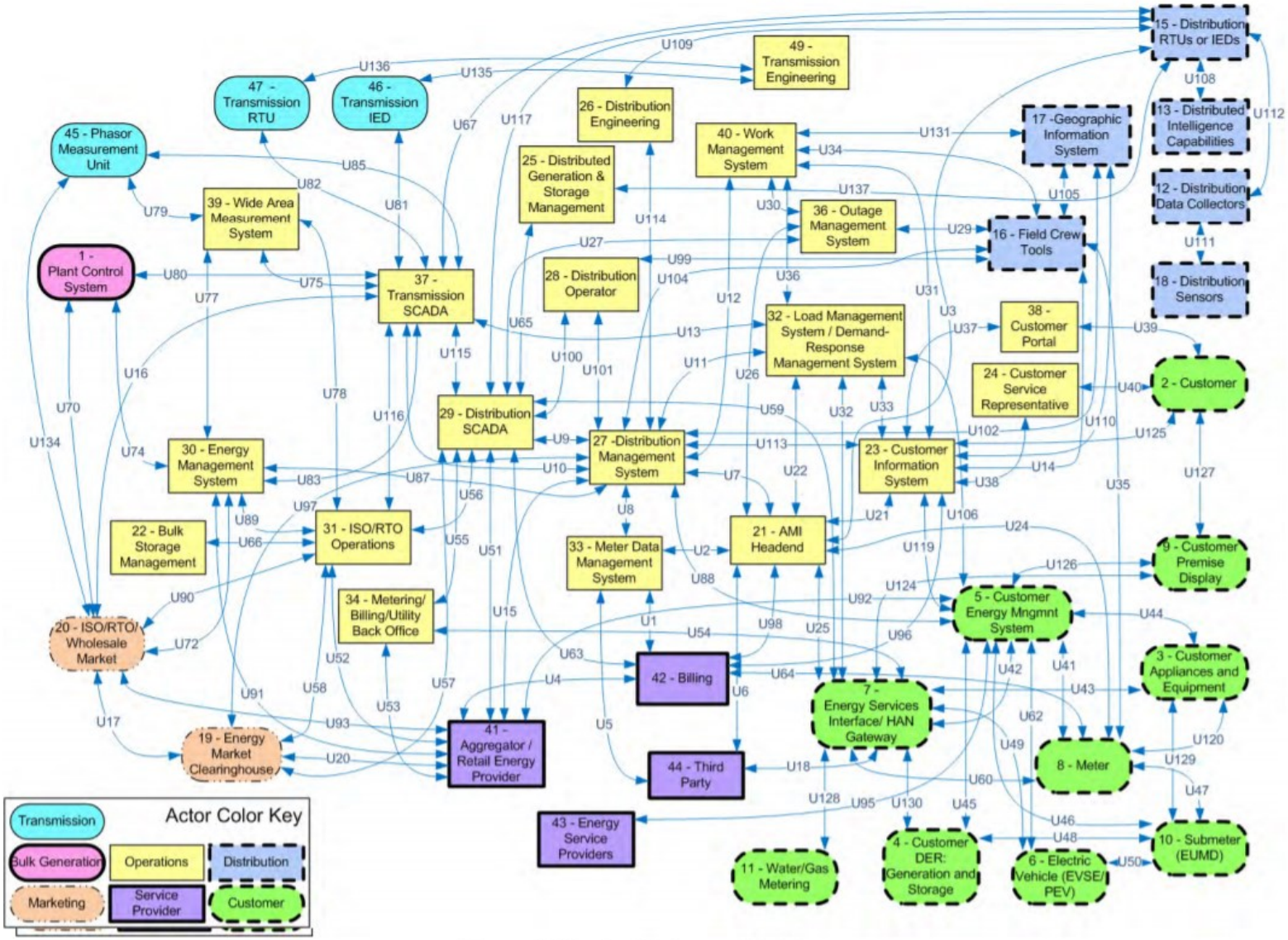


Figure 2-3 Logical Reference Model

5 Akıllı Şebekelerde Siber Güvenlik

Gizlilik, güç sistemi güvenilirliği için en az kritik olandır.
- Müşteri bilgilerinin gizliliği;
- Elektrik piyasası bilgisi;
- Bordro, iç stratejik planlama, genel kurumsal bilgiler vb. [9]

Erişilebilirlik, güç sistemi güvenilirliği için en önemli güvenlik hedefidir. Kullanılabilirlikle ilişkili zaman gecikmesi değişebilir -
- Koruyucu röle için 4 ms;
- Trafo merkezi ve besleyici SCADA verileri için saniye;
- Sayaç okuma ve uzun vadeli piyasa fiyat bilgisi için saatler; ve
- Güç kalitesi bilgisi gibi uzun vadeli veri toplamak için günler / haftalar / aylar.

Bütünlük, Güç sistemi operasyonlarının bütünlüğü, aşağıdakileri garanti eder:
- Veriler izinsiz olarak değiştirilmedi;
- Veri kaynağı doğrulandı;
- Verilerle ilişkili zaman damgası bilinir ve doğrulanır;
- Veri kalitesi bilinir ve doğrulanır.

Akıllı Şebekelerde Siber Güvenlik Gereksinimleri

- **Erişim Kontrol** (Erişim Kontrol Politika, Uzaktan Erişim Politikası ve Prosedürleri, Hesap Yönetimi, Erişim Uygulaması, Bilgi Akışı Uygulaması, Görevlerin Ayrılığı, En Düşük Ayrıcalık, Başarısız Giriş Denemeleri, Akıllı Şebeke Bilgi Sistemi Kullanım Bildirimi, Önceki Oturum Açma Bildirimi, Eşzamanlı Oturum Kontrolü, Oturum Kilitlenmesi, Uzak Oturum Sonlandırma, Kimlik Tespiti veya Kimlik Doğrulaması Olmadan İzin Verilen Faaliyetler, Uzaktan Erişim, Kablosuz Erişim Kısıtlamaları, Taşınabilir ve Mobil Cihazlar için Erişim Kontrolü, Dış Bilgi Kontrol Sistemlerinin Kullanımı, Kontrol Sistemi Erişim Kısıtlamaları, Genel Olarak Erişilebilir İçerik, Şifre)

- **Farkındalık ve Eğitim** (Farkındalık ve Eğitim Politikası ve Prosedürleri, Güvenlik farkındalığı, Güvenlik Eğitimleri, Güvenlik Farkındalığı ve Eğitim Kayıtları, Güvenlik Grupları ve Birlikleri ile İletişim, Güvenlik Sorumluluk Eğitimi, Süreç Eğitimi Planlaması)

- **Denetim ve Hesap Verebilirlik** (Denetim ve Hesap Verebilirlik Politikası ve Prosedürleri, Denetlenebilir Etkinlikleri, Denetim Kayıtlarının İçeriği, Denetim Depolama Kapasitesi, Denetim İşleme Hatalarına Yanıt, Denetim İzleme, Analiz ve Raporlama, Denetim Analiz Araçları ve Rapor Üretimi, Zaman Damgası, Denetim Bilgilerinin Korunması, Denetim Kayıtları Muhafaza, Denetimlerin Yapılması ve Sıklığı, Denetçi Yeterliliği, Denetim Araçları, Güvenlik Politikası Uyumluluğu, Denetim Üretimi, İnkar edilemezlik)

Akıllı Şebekelerde Siber Güvenlik Gereksinimleri

- **Güvenlik Değerlendirmesi ve Yetkilendirme** (Güvenlik Değerlendirme ve Yetkilendirme Politikası ve Prosedürleri, Güvenlik Değerlendirmeleri, Sürekli gelişme, Akıllı Şebeke Bilgi Sistemi Bağlantıları, Güvenlik Yetkilendirmesi, Sürekli izleme)

- **Yapılandırma Yönetimi** (Yapılandırma Yönetimi Politikası ve Prosedürleri, Temel Yapılandırma, Yapılandırma Değişikliği için Erişim Kısıtlamaları, Fabrika Varsayılan Ayarları Yönetimi, Yapılandırma Yönetim Planı, …)

- **Operasyonların Sürekliliği** (Operasyon Politikasının Sürekliliği ve Prosedürleri, Operasyon Planının Sürekliliği, Operasyon Rollerinin Sürekliliği ve Sorumlulukları, Alternatif Telekomünikasyon Hizmetleri, …)

- **Tanımlama ve Kimlik Doğrulama** (Kimlik ve Kimlik Doğrulama Politikası ve Prosedürleri, Kullanıcı Kimliği ve Kimlik Doğrulama, …)

- **Bilgi ve Belge Yönetimi** (Bilgi ve Belge Yönetimi Politikası ve Prosedürleri, Bilgi Değişimi, …)

- **Olay Müdahalesi** (Olay Müdahale Politikası ve Prosedürleri, Olay Müdahale Rolleri ve Sorumlulukları, Eğitim, İzleme, Raporlama, …)

Akıllı Şebekelerde Siber Güvenlik Gereksinimleri

- **Akıllı Şebeke Bilgi Sistemi Geliştirme ve Bakım** (Akıllı Şebeke Bilgi Sistemi Bakım Politikası ve Prosedürleri, Uzaktan Bakım, …)
- **Ortam Koruması** (Ortam Koruma Politikası ve Prosedürleri, Ortam Hassaslık Seviyesi, Ortam Temizlik ve Bertarafı, Ortam Taşınması, …)
- **Fiziksel ve Çevre Güvenliği** (Fiziksel ve Çevre Güvenliği Politikası ve Prosedürleri, Fiziksel Erişim Yetkileri, Fiziksel Erişimi İzleme, Ziyaretçi Katıları, Ziyaretçi Kontrol, Fiziksel Erişim Günlüğü Tutma, …)
- **Planlama** (Stratejik Planlama Politikası ve Prosedürleri, Akıllı Şebeke Bilgi Sistemi Güvenlik Planı, Güvenlikle İlgili Aktivite Planlama, …)
- **Güvenlik Programı Yönetimi** (Güvenlik Politikası ve Prosedürleri, Güvenlik Program Planı, Üst Yönetim Otoritesi, Güvenlik Mimarisi, Risk Yönetim Stratejisi, …)
- **Personel Güvenliği** (Personel Güvenlik Politikası ve Prosedürleri, Personel Kategorisi, Transferi, Görevleri, Sorumluluk Sonlandırma, …)

Akıllı Şebekelerde Siber Güvenlik Gereksinimleri

- **Risk Yönetimi ve Değerlendirmesi** (Risk Değerlendirme Politikası ve Prosedürleri, Risk Yönetim Planı, Güvenlik Etki Seviyesi, Güvenlik Açığı Değerlendirmesi ve Farkındalık, Risk Değerlendirmesi, …)

- **Akıllı Şebeke Bilgi Sistemi ve Servis Satın Alma** (Akıllı Şebeke Bilgi Sistemi ve Hizmetleri Satın Alma Politikası ve Prosedürleri, Yaşam Döngüsü Desteği, Yazılım Lisansı Kullanım Sınırlamaları, Güvenlik Mühendisliği İlkeleri, Geliştirici Güvenlik Testi, …)

- **Akıllı Şebeke Bilgi Sistemi ve İletişim Koruması** (Akıllı Şebeke Sistemi ve İletişim Koruma Politikası ve Prosedürleri, Güvenlik Fonksiyonu İzolasyonu, Hizmet Reddi Koruması(DoS), İletişim Bütünlüğü, İşletim Sisteminden Bağımsız Uygulamalar, Genel Anahtar Altyapı Sertifikaları, Güvenlik Rolleri, heterojenite, VoIP, Balküpleri, İletişim Gizliliği, …)

- **Akıllı Şebeke Bilgi Sistemi ve Bilgi Bütünlüğü** (Akıllı Şebeke Sistemi ve Bilgi Bütünlüğü Politikası ve Prosedürleri, Kusur Düzeltme, Kötü Amaçlı Kod ve Spam Koruması, Akıllı Şebeke Bilgi Sistemi İzleme Araçları ve Teknikleri, Güvenlik Uyarıları ve Tavsiyeler, Bilgi Girişi Doğrulama, Hata işleme, Yazılım ve Bilgi Bütünlüğü, …)

Kaynaklar

[1] https://www.slideshare.net/ZhreAydn/kritik-enerji-altyapilarinin-korunmasi-ve-siber-gvenlik
[2] https://www.muhendisbeyinler.net/akilli-sebekeler-smart-grid-nedir/
[3] http://www.emo.org.tr/ekler/e8fff8ce0a6ccb5_ek.pdf?dergi=1101 (Mehmet Oktay ELDEM)
[4] https://otomasyonadair.com/2014/11/07/bilinmesi-gereken-4-it-standardi/
[5] https://www.isa.org/isa99/
[6] https://www.isa.org/intech/201810standards/
[7] https://www.tuv-sud.com.tr/tr-tr/merkez/kaynak-merkezi/yayimlar/e-ssentials-haber-buelteni/demiryolu-hizmetleri-ile-ilgili-e-ssentials/e-ssentials-3-2015/certification-according-to-iec-62443-boosting-security-against-cyber-attacks
[8]https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems
[9] https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf


SORULAR
TEŞEKKÜRLER