Journal of the Faculty of Engineering and Architecture of Gazi University 41:1 (2026) 211-227

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University
Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

A new model approach for security rule recommendation based on Purdue architecture-aware topology inference and asset communication for ICS

Firdevs Sevde Toker*, İbrahim Özçelik
Department of Cyber Security Engineering, Faculty of Computer and Information Science, 54187, Sakarya, Türkiye

Highlights:

- Purdue-compatible architectural inference of complex ICS structure
- Inference network access rules using access analysis
- Topology inference with NIST 800-82, IEC 62443, Defense in Depth compliance

Keywords:

- ICS Purdue architecture
- Topology inference
- Secure architecture
- ICS modelling

Article Info:

Research Article
Received: 14.01.2025
Accepted: 29.10.2025

DOI:

10.17341/gazimmfd.1619701

Correspondence:

Author: Firdevs Sevde Toker
e-mail: firdevstoker@sakarya.edu.tr
phone: +90 264 295 5897

Graphical/Tabular Abstract

In this study, different architectures resulting from different interpretations of ICS architectures called PERA architecture were modeled and security rules were derived. Our ICS architectural modeling (topology and firewall rule inference) consists of two main parts in Figure A: (i) Asset Layer and (ii) Network Layer. In asset layer, ICS assets were analyzed according to their functions and features. According to the communication between the assets, Purdue levels of the assets were determined. In network layer, locations of the assets (VLAN, zone, and level) are defined. According to the Purdue model, the location makes network topology inferences of the assets in different network segmentations. An architectural inference model is developed by considering the compliance of ICS network security issues such as network segmentation, restricted data flow with the IEC 62443, NIST 800-82 standards, and security recommendations suggested in the Defense in Depth approach.

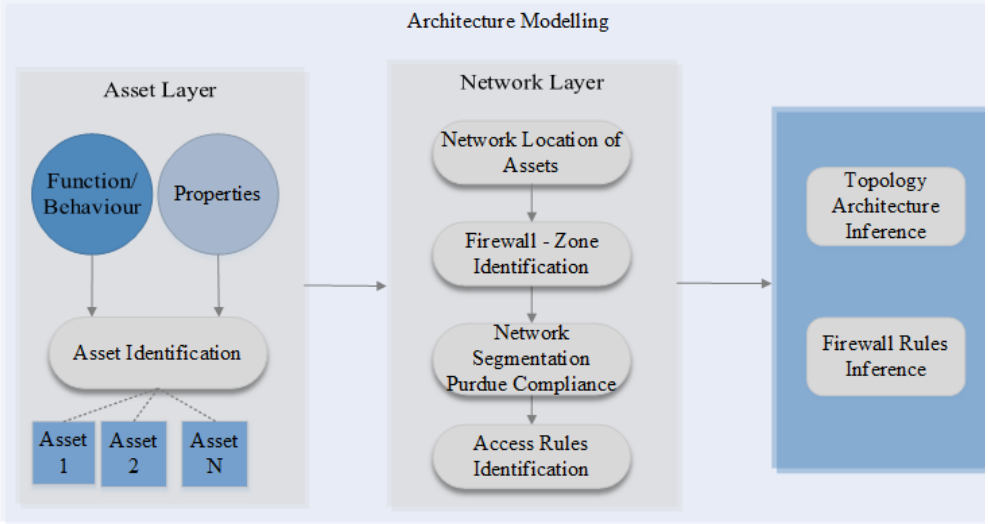


Figure A. ICS Architecture Modelling Workflow

Purpose: Inference of complex ICS architectures and firewall rules by the Purdue model is made. Thus, ICS assets and communication patterns in network locations where possible cyber-attacks can occur can be analyzed.

Theory and Methods: ICS assets were analyzed for their Purdue model levels according to their features and functions. The network zone where the assets are located, the services they offer to each other, and their communication models were inference through matrices. After the topology inference of the assets according to the Purdue model, the rules required for process communication in Firewall were also extracted.

Results: Topology and firewall rule inference of a wastewater station was performed according to the Purdue model with the matrices in the proposed method.

Conclusion: With the proposed method, Purdue-compatible topology and firewall rule inference can be done for every critical infrastructure. The compatibility of our proposed method with IEC 62443, NIST 800-82, and Defense in Depth security recommendations has also been matched.

Journal of the Faculty of Engineering and Architecture of Gazi University 41:1 (2026) 211-227

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

EKS için Purdue mimarisi uyumlu topoloji çıkarımı ve varlık iletişimine dayalı güvenlik kural önerisi yapan yeni bir model yaklaşımı

Firdevs Sevde Toker*, İbrahim Özçelik
Sakarya Üniversitesi, Bilgisayar ve Bilişim Bilimleri Fakültesi, Siber Güvenlik Mühendisliği Bölümü, 54187, Sakarya, Türkiye

ÖNEÇIKANLAR

- Karmaşık ICS yapısının Purdue uyumlu mimari çıkarımı
- Erişim analizini kullanarak ağ erişim kurallarının çıkarımı
- NIST 800-82, IEC 62443, Derinlemesine Savunma uyumluluğu ile topoloji çıkarımı

Makale Bilgileri
Araştırma Makalesi
Geliş: 14.01.2025
Kabul: 29.10.2025

DOI:
10.17341/gazimmfd.1619701

Anahtar Kelimeler:
Topoloji çıkarımı,
EKS mimarisi,
güvenli mimari,
EKS modelleme

ÖZ

Endüstriyel kontrol sistemleri (EKS), çalışma yapısı gereği farklı ağ mimarilerinde olan karmaşık iletişim yapısına sahip sistemlerdir. Güvenli ağ mimarisi kısıtları, global standartlar ile tanımlansa da farklı yorumlamalardan dolayı birbirinden farklı endüstriyel ağ mimarileri ortaya çıkmaktadır. Siber güvenlik kapsamında EKS ağ segmentasyonu ve varlıklar arası iletişim kurallarının çıkarımı uluslararası standartlar ile desteklenen önemli bir güvenlik konusudur. Bu çalışmada tercih edilen ağ mimarilerinden bağımsız bir şekilde varlıkların bulundukları ağ konumlarının ve birbirlerine sundukları hizmetlerin matrisler ile tanımlandığı ve oluşturulan matrislerden elde edilen sonuçlar ile de Firewall (Güvenlik Duvarı) üzerinde proses temelli erişim kurallarının çıkarımının yapıldığı bir yöntem önerilmiştir. Proses bağımlılığı olmayan, esnek bir modelleme sunan bu yöntem için test senaryosu olarak CENTER [1] altyapısındaki ağ mimarisi ve varlıkları kullanılmıştır. Geliştirilen çıkarım yöntemi sonucunda test ortamında kullanılan mimari ile proses temelli Firewall kurallarının birebir örtüştüğü tespit edilmiştir. Ayrıca yaygın kullanılan Derinlemesine Savunma (Defence in Depth-DiD) stratejisi, NIST 800-82 ve IEC 62443 standartlarının önerdiği güvenlik uyumu da test edilmiştir.

A new model approach for security rule recommendation based on Purdue architecture-aware topology inference and asset communication for ICS

HIGHLIGHTS

- Purdue-compatible architectural inference of complex ICS structure
- Inference network access rules using access analysis
- Topology inference with NIST 800-82, IEC 62443, Defense in Depth compliance

Article Info
Research Article
Received: 14.01.2025
Accepted: 29.10.2025

DOI:
10.17341/gazimmfd.1619701

Keywords:
Topology inference,
ICS architecture,
secure architecture,
ICS modelling

ABSTRACT

Industrial control systems (ICS) have complex communication structures with different network architectures due to their operating structure. Although secure network architecture constraints are defined by global standards, different industrial network architectures emerge due to different interpretations. Within the scope of cyber security, ICS network segmentation and extraction of communication rules between assets are important security issues supported by international standards. In this study, a method is proposed in which the network locations of the entities and the services they offer to each other are defined by matrices, independently of the preferred network architectures, and the process-based access rules on the Firewall are derived from the results obtained from the created matrices. The network architecture and assets in the CENTER [1] infrastructure were used as test scenarios for this method, which offers flexible modeling without process dependency. As a result of the developed inference method, it was determined that the architecture used in the test environment and the process-based Firewall rules matched one-to-one. In addition, the widely used Defense in Depth (DiD) strategy, the security compliance recommended by NIST 800-82, and IEC 62443 standards were also tested.

*Sorumlu Yazar / Yazarlar / *Corresponding Author / Authors: *firdevstoker@sakarya.edu.tr, ozcelik@sakarya.edu.tr / Tel: +90 264 295 5897

1. Giriş (Introduction)

EKS, farklı endüstriyel proseslerin işletilmesi için otomasyon sistemleri ile entegre edilmiş cihazlar ile ilişkili farklı alt sistemleri barındıran sistemler bütünüdür. Elektrik-enerji üretim/iletim/dağıtım, su arıtma sistemleri, doğalgaz üretim/iletim/dağıtım, imalat sistemleri, vb. altyapılar endüstriyel kontrol sistemlerine örnek olarak verilebilir. Gelişen teknoloji, EKS dünyasının proses yönetimini de kolaylaştırmaktadır. Ancak bu durum siber-fiziksel sistemlerin güvenlik anlamında daha çok kontrole ihtiyaç duymasına yol açmaktadır. EKS, siber-fiziksel sistemleri içerdiğinden katmanlı bir iletişim hiyerarşisine ihtiyaç duyar. Endüstriyel prosesin işletildiği saha ile prosesin kontrolünü sağlayan sistem farklı iletişim protokolleri kullanmak zorundadır. Bir kurum ya da şirket için proses kontrolünün haricinde iş ve kurumsal süreçlerin işletildiği farklı bir iletişim katmanı daha bulunması gerekir. Literatürde farklı iletişim modelleri ve varlıklarının oluşturduğu bu katmanlı yapı EKS için Purdue Referans Model (PERA) olarak tanımlanır [2]. Purdue model siber-fiziksel sistemlerin oluşturduğu hibrit sistemlerin mimarisini oluşturmaktadır. Mimari temel olarak ağ segmentasyonu ile altı seviyede farklı ağ ve proses servislerine hizmet edecek şekilde tasarlanmıştır. Otomasyon dünyası üreticilerinin farklı gerçekleme yaklaşımları, siber güvenlik firmalarının farklı güvenlik yaklaşımları (segmentasyon, mikro-segmentasyon, sıfır güven) veya endüstriyel proseslerin ihtiyaç duyduğu farklı servis gereksinimlerinden dolayı Purdue modelin farklı yorumları ile farklı endüstriyel ağ mimarileri ortaya çıkmıştır [3-6]. Bu da EKS'lerin benzer varlık ve servisler kullansa da farklı ağ mimarilerinin oluşmasına neden olmaktadır. Örneğin bir EKS'de saha seviyesinin kontrolü için SCADA (Supervisory Control and Data Acquisition) sistemlerinin kullanılması ile DCS (Distrubuted Control System) kullanılması arasında mimari model olarak farklılık bulunmaktadır. Bu farklılık hem varlıklar hem de varlıklar arası iletişim tarafını da etkiler. Bu gibi durumlar, kompleks olan EKS iletişim altyapısının siber güvenlik süreçlerinin uygulanması ve yönetimini de zorlaştırmaktadır. Hem varlık ve ağ yönetimi hem de güvenlik zafiyetlerinin analiz edilebilmesi için öncelikle ilgili EKS'nin doğru bir şekilde modellenmesi gerekmektedir.

Geçmişten günümüze artarak devam eden EKS saldırılarının (Havex, BlackEnergy, Duqu, TRITON vb.) olumsuz sonuçları tüm dünyada bilinmektedir [7]. Bu saldırıların kök kaynaklarına bakıldığında siber güvenlik kapsamında uygulanması gereken politikaların ve mimari çözümlerin yanlış ve/veya eksik uygulanmasından kaynaklandığı görülmektedir [7]. Diğer taraftan sadece siber saldırılar değil, EKS mimarilerinde sistem arızalarına karşı da dayanıklı topolojilerin oluşturulması bir ihtiyaç olarak karşımıza çıkmaktadır [8]. Bu çalışmada hem bu ihtiyaçları karşılamak hem de farklı ağ mimarilerinin ihtiyaç duyduğu farklı ağ mimarilerini doğru modellemek amacıyla topolojiyi oluşturan varlıkları ve servisleri modelleyerek bir EKS'nin topoloji çıkarımını yapan ve endüstriyel standartlar ile uyumluluğunu test eden bir öneride bulunulmuştur. Siber sistemleri modellerken birçok farklı yöntem bulunmaktadır. Ancak EKS gibi hem fiziksel hem de siber sistemleri içeren yapılarda durum biraz daha karmaşık hale gelir. Doğru tanımlanamayan sistemlerin siber güvenlik zafiyetlerinin belirlenmesi eksik veya yanlış olacaktır. Bu yüzden sistemi oluşturan varlıklar ve aralarındaki iletişimi proses ile ilişkilendirerek doğru modellemek; sonrasında yapılacak siber güvenlik analizlerinin de eksiksiz ve doğru yapılmasını sağlayacaktır. Yukarıda belirtilen problemlere öneri sunan bu çalışmada bir EKS'nin, varlık ve ağ iletişiminin doğru modellenmesi ile varlık yönetimi ve varlıkların birbirlerine sundukları hizmetlerde hem yönetilebilir hem de güvenlik zafiyet analizlerinin doğru bir şekilde uygulanması sağlanır.

EKS mimarilerinde temel ağ segmentasyonu Firewall cihazları ile sağlanır. Firewall cihazları, ağ trafiğini hem proses seviyesinde hem de kurumsal seviyede kontrol ederek temel çevre (perimeter) ve ağ güvenliğini sağlar. Uluslararası EKS standartlarından IEC 62443-3-2 bölümünde Güvenlik Bölgesi-Kanal (Security Zone-Conduit) konularının risk yönetimi için gerekliliği belirtilmiştir [9]. Güvenlik bölgesi; EKS mimarisinde benzer işlevsellik ve güvenlik gereksinimlere göre varlıkların ağ bölümlerine ayrıldığı gruplardır. Kanallar (Conduits) ise güvenlik bölgeleri arası iletişimi temsil eden protokollerdir. Bu konu ile ilgili ayrıntılar Bölüm 3'te detaylandırılmıştır. EKS modellemesi ve temel ağ segmentasyonunu sağlayan Firewall cihazlarının konumu ve üzerinde konfigüre edilen kuralların çıkarımı da yukarıda bahsedilen problemlerin temel çözümünü oluşturmaktadır. Bu amaç doğrultusunda bu çalışmada önerilen yaklaşım, EKS ağ mimarisinin matrisler kullanılarak çıkarımını ve ağ segmentasyonu ile katmanlı mimarinin oluşturulması için gerekli Firewall kurallarının çıkarımını da sağlamaktadır. Böylece herhangi bir siber-fiziksel sistemdeki tüm varlıklar ve aralarındaki iletişim için grafiksel gösterim sağlanarak sistem bütünü tanımlanmış hale gelmektedir. Grafik modellemede hem proses sistemini hem de siber sistemi kapsayan bileşenler, model kümesinde tanımlanmıştır. Model kümesindeki bileşenler hem sistemi tanımlamaya yardımcı olmakta hem de matrislerdeki ilişkisel durumların oluşmasına da zemin hazırlamaktadır. Matrislerin birbirleriyle ilişkisi yorumlandığında ve bir bütün olarak dikkate alındığında EKS'ne ait topolojinin çıkarımı farklı senaryolara uygulanabilir hale gelmektedir. Bütün bu bilgilere bağlı olarak bu çalışmanın katkıları aşağıda listelenmiştir:

- Bir EKS'nin matrisler ile varlık ve ağ temelli modellenmesi
- Bir EKS'nin Purdue model uyumluluğuna göre ağ mimari topolojisinin çıkarımı
- Topolojideki Firewall cihazlarının proses işlevselliğine göre temel kurallarının çıkarımı
- Bu çalışmada sunulan çözümün DiD, NIST 800-82, IEC 62443 güvenlik gereksinimlerine göre karşılaştırması/uyumluluğu

Çalışmanın kalan kısımlarının organizasyonu şu şekildedir: Bölüm 2; literatür araştırması, Bölüm 3; temel bilgiler, Bölüm 4; EKS model oluşturma (öneri), Bölüm 5; değerlendirme yöntemi, Bölüm 6; sonuç ve tartışma.

2. Literatür Araştırması (Literature Research)

EKS ağ mimarilerinin Purdue model uyumluluğuna göre modellenmesi ile ilgili literatür çalışmaları kısıtlı kalmaktadır. Yapılan çalışmalar genellikle proses seviyesi (L1-L2) veya kontrol seviyesi (L2-L3) için test edilmiştir. Ancak prosesler farklı olsa da endüstriyel kontrol sistem veya siber-fiziksel sistemlerin modellenmesi ile ilgili akademik çalışmalar bu bölüm içerisinde aktarılacaktır. Casola vd. [10], siber-fiziksel sistemlerin mevcut tehditlerini önlemek için gerekli güvenlik kontrollerini ve dayanıklılığını artırmayı ve entegre edilecek hareketli hedef savunma tekniklerinin tanımlanmasını desteklemeyi amaçlayan bir yöntem geliştirmişlerdir. Bu çalışmada, siber-fiziksel sistemlerin modellenmesi için önerilen yöntemde bulut katmanı, uç katmanı ve cihaz katmanı olmak üzere üç seviyeli bir yaklaşım ile Purdue modelin altı katmanlı yapısı eşleştirilmiştir. Purdue L0 ile cihaz katmanı, L1-L3 ile uç katmanı, BT (Bilgi Teknolojileri) ile bulut katmanı eşleştirilmiştir. Sistem modelleme içinde varlıklar; fiziksel/sanal proses düğümleri, iletişim kanalları, yazılım bileşenleri şeklinde üç alt başlıkta analiz edilmiştir. Ancak bir EKS mimarisinin temel ağ güvenliğinin sağlandığı Firewall cihazlarının kural işletimi, konumu ve erişim analizi ile ilgili testler [10]'da bulunmamaktadır. Carreno vd. [11], elektrik ve gaz dağıtım

sistemleri için Purdue mimarisini yönlendirilmiş graf ile modellemişlerdir. Güvenlik bölgelerine dayalı bir durum uzayı üzerinde sürekli zamanlı Markov zinciri kullanarak fiziksel sisteme yapılan siber saldırı vektörlerinin aktivasyonu modellenmiştir. Ancak modelleme sürecinde varlıkların birbirleri arasındaki ilişki ve Firewall kural çıkarımı ile ilgili bir çalışma bulunmamaktadır. Ayrıca modellenen sistemde ağ topolojisinin değişimi durumunda değişen iletişim modelleri de değerlendirilmemiştir. Önerdiğimiz yöntemde ise mimari değişiklik olması halinde ortaya çıkan iletişim kurallarının değişimi varlıkların detaylı analizi ile birbirlerine sundukları servisler sayesinde Firewall kuralları üzerinden çıkarımı yapılabilmektedir. Klaer vd. [8], ise genel bir mimari şablon kullanarak bir elektrik dağıtım şebekesi modelini temel alan akıllı altyapı modellerini otomatik olarak oluşturan bir yaklaşımı graf tabanlı olarak sunmuşlardır. SGAM tabanlı altyapının iletişim teknolojileri ile entegrasyonu olacak şekilde 3 adımda gerçekleştirilmiştir: (i) taslak, (ii) modelleme ve (iii) konfigürasyon. Modelleme aşamasında, SGAM bileşenleri nesne tabanlı olarak ele alınmıştır. İlgili çalışma SGAM tabanlı prosesler için geçerli olup Purdue mimarisi veya farklı proseslere uyum sağlayabilecek geniş bir modelleme yapısı sunmamaktadır. Hou vd. [12], bir ağın topoloji keşfinin önlenmesi için ProTO adında obfuscate eden bir yöntem geliştirmişlerdir. Bu çalışmada probing tekniği kullanılarak ağ modeli çıkarımı yapılmış ve topoloji tabanlı saldırıları proaktif olarak önlemek için sahte ağ topolojisi elde edilecek şekilde geciktiren yöntem geliştirilmiştir. Bu yöntemde ağda aktif keşif yapıldığından EKS'de gerçek zamanlı çalışma prensibinden dolayı ağ gecikmelerine neden olabilir. Bu yüzden ilgili yöntemin literatürde EKS için uygun olmadığı değerlendirilmektedir. Sharma vd. [13], bir ağın nedensel bağlantılarını keşfetmek için Transfer Entropi tabanlı yaklaşımla bir model geliştirmişlerdir. Bu model ile daha az hesaplama gereksinimine sahip olduğu belirlenmiştir. Fakat, ilgili topoloji çıkarım yöntemi Firewall güvenlik bölgeleri ve iletişim kanalları ile ilgili mimari çıkarımı sunmamaktadır. Testi vd. [14], kör kablosuz ağ topolojisi çıkarımı için makine öğrenmesi teknikleri kullanarak yeni bir çözüm sunmuşlardır. Ağ ortamındaki rastgele konumlandırılmış sensörler tarafından algılanan sinyaller ile ağdaki düğümlerin radyo frekansı arasında nedensel bir ilişki belirlenmiştir. Sinir ağı tabanlı çözümde 93% doğruluk oranı belirtilmiştir. Ancak bu topoloji belirleme yöntemi, kablosuz ağların kullanım oranının düşük olduğu EKS ortamlarının geneline uygulanması için uygun değildir. Sheng vd. [15], SCADA ağından gelen izinsiz girişleri tespit etmek için SCADA tabanlı siber-fiziksel model geliştirilmiştir. Geliştirilen modelde EKS varlıklarının iletişim şekilleri temel alınmıştır. Model oluşturma sürecinde sonlu durum makinelerinden yararlanarak altı bileşenli bir model kümesi oluşturulmuştur. Sistemlerin ve bileşenlerine ait analizini yapılmasına olanak tanıyan UML tabanlı SysML gibi araçlar da bulunmaktadır [16]. Elbüz vd. [16], nesnelerin interneti yoluyla toplanan verilerin blok zinciri teknolojisi kullanılarak güvenilir ve sağlıklı bir şekilde pazarlanabilmesi için SysML kullanarak sistem analizi yapmıştır. Ancak EKS gibi siber-fiziksel sistemlerin analizi için bu yöntemler yeterli olmamaktadır. Yukarıda bahsedilen akademik çalışmalarda EKS/OT (Operasyonel Teknolojiler) ağlarının modellenmesi ile ilgili prosese özel, ağa özel gibi spesifik konular ele alınmıştır. Bir EKS ağ mimarisinin hem kontrol merkezi hem de saha modellenmesi, Purdue seviyelerine göre uyumluluğunun kontrolü ve standartlar ile eşleştirilme aşamaları bulunmamaktadır.

Firewall cihazları EKS için temel güvenlik varlığıdır. Aynı zamanda ağ segmentasyonu ve Purdue sınırlarının belirlenmesinde de rol oynar. Firewall kurallarının doğru yapılandırılması hem proses işleyişi için gerekli komut ve saha verilerinin iletilmesinde hem de temel ağ güvenliğinin oluşmasında önemli bir konudur. Endüstriyel ortamlar için geliştirilen ticari yeni nesil Firewall [17] cihazları sadece ağ güvenliği sağlamakla kalmaz, aynı zamanda IT-OT geçişinde genel bir görünüm, gerçek zamanlı EKS tehdit tespiti, EKS spesifik ağ görünürlüğü gibi özellikler barındırır. Literatürdeki çalışmalarda Firewall tabanlı konfigürasyon hataları, tespit yöntemleri ve modellemeleri ile ilgili çalışmalar mevcuttur [17-19]. Ancak hiçbirinde EKS mimarisinin Purdue uygunluğuna göre bir kural çıkarımı bulunmamaktadır. EKS mimarilerinin ortak bir çerçevede güvenli mimari yaklaşımı için global ölçekte kullanılan standartlarda ağ segmentasyonu ve mimari ile ilgili temel gereklilikler vurgulanmıştır [20, 21]. Purdue model referans alınarak DiD kapsamında, güvenli bir mimari için EKS ağ mimarisi önemli bir rol oynamaktadır [23]. Bu yüzden varlıkların ağ mimarisindeki yeri ve iletişimi doğru belirlenmelidir. DiD ve IEC 62443-3-2 standardındaki sistem tasarımı ağ segmentasyonu ve güvenlik bölgesi-kanal bileşenleri güvenlik kapsamında vurgulanan süreçlerdir [9]. Yaygın kullanılan bu standartlarda mimari yapının güvenliği ve ağ segmentasyonunun önemi göz önüne alındığında bu çalışmanın amaçlarından biri olan EKS mimarisinin doğru bir şekilde çıkarımı literatüre katkı sağlayacaktır. Elde edilen mimari, ilgili standartlara uyum ve siber güvenlik kapsamındaki risk değerlendirmesi gibi konulara oldukça önemli katkılar sağlayacaktır.

Literatür çalışmalarında elektrik üretimi/iletimi, akıllı şebekeler gibi farklı prosesler için SGAM ve RAMI mimari yaklaşımları bulunmaktadır. Örneğin akıllı şebekler için beş katmanlı SGAM mimarisi kullanılmaktadır [23, 24]. Endüstri 4.0 için RAMI güvenlik temelli üç boyutlu katmanlı model ile siber-fiziksel sistemlerin modellenmesi kullanılmaktadır [25, 26]. Literatürde elektrik-enerji şebekesi, atık su/içme suyu yönetimi, doğalgaz üretim/iletim/dağıtım hattı, petrol iletim/dağıtım hattı gibi EKS altyapıları, birbiri ile ilişkili olmadan bağımsız dikkate alındığında SGAM ve RAMI mimarileri yerine Purdue referans modeli ile modellenirler. Bu çalışmada kritik altyapılardaki OT ağının kontrol merkezinden saha seviyesine kadar varlıklarının ve servislerinin hem operasyonel hem de BT iletişimi ile modellemesi yapılmıştır. Aynı zamanda proses için gerekli Firewall kurallarının çıkarımı elde edilmiştir. Modelleme sonucunda Purdue referans modeline göre katmanlı mimari oluşturularak güvenlik analizinin yapılması için bir yaklaşım sunulmuştur. Bu bölümde incelenen çalışmalarda, bir EKS'nin Purdue modele göre Seviye (Level)- Güvenlik Bölgesi-Sanal Ağ yaklaşımı ile mimari iletişim iskeletinin çıkarılması için sunulmuş herhangi bir yöntem bulunmamaktadır.

3. Temel Bilgiler (Background)

Bu bölümde çalışmanın kapsamı ile alakalı bilinmesi gereken EKS varlıkları, Purdue Mimarisi, EKS Güvenliği ve Standartları ile alakalı temel bilgiler verilecektir.

3.1. EKS Varlıkları (ICS Assets)

IEC 62443 standardına göre varlıklar; gömülü cihazlar, ağ cihazları, sunucular ve yazılım uygulamaları olmak üzere dört ana gruptan oluşmaktadır [28]. Her bir grup içerisindeki varlıklar kontrol, güvenlik ve tamamlayıcı fonksiyonları işleten farklı rollere sahiptirler. Gömülü cihazlar grubu içerisinde hem saha kontrol cihazları hem de sensör aktüatör cihazları bulunmaktadır. Sensör/Aktüatörler sahadan aldıkları dijital ve/veya analog proses verilerini saha kontrol cihazlarına iletirler. Saha kontrol cihazları farklı görev ve özelliklere sahip PLC (Programmable Logic Controller), RTU (Remote Terminal Unit), IED (Intelligent Electronic Device) ve SIS (Safety Instrumented System) cihazları olabilir. Bu cihazlar, BT varlıklarına göre düşük donanımsal özelliklere (hafıza, CPU (Central Processing Unit) döngüleri, vb.) sahip ve RTOS (Real-Time Operating System) bulunduran endüstriyel protokoller ile veri iletişimi sağlayan cihazlardır. Aynı zamanda proses verilerinin işlenmesini ve kontrol sunucularına endüstriyel protokol standartlarına göre verinin belli

mantıkta aktarımını sağlar. Saha varlıklarından bir diğeri HMI (Human Machine Interface) cihazlarıdır. Operasyonel süreçlerde saha verilerini görselleştirerek operatörlere yardımcı olur ve gerekiyorsa ilgili aksiyonun alınmasını sağlar. Kontrol cihazları, prosesin kontrolü ve cihaz bakımı/konfigürasyonunu sağlayan iş istasyonlarından oluşmaktadır. Bu grupta, saha cihazlarını konfigüre etmek, içerisindeki yazılımı güncellemek ve mantıksal programlama yapabilmek için Mühendislik İş İstasyonları bulunur. Mühendislik İş İstasyonları OT sistemlerinin güvenliğinde kritik varlıklardan biridir. Bu yüzden Mühendislik İş İstasyonlarının varlık güvenliği için ağ görünürlüğünün doğru yapılandırılmış olması gerekir. Bir başka kritik kontrol cihazı SCADA yazılımını bulunduran sunuculardır. SCADA yazılımları endüstriyel protokoller ile operasyonel komut ve kontrol sürecinin işletilmesini sağlar. Bu yazılımlar yerel veya uzakta konumlandırılabilir. OT spesifik varlıklar tek başına bir EKS ortamını oluşturamazlar. Bu varlıkların çoğunlukla endüstriyel protokoller aracılığı ile haberleşmesi gerekir. Ağ ara bağlantı cihazları grubunda bulunan Endüstriyel Switch, Router, Converter cihazları da kritik EKS varlıklarını oluşturmaktadır. Ağ güvenlik cihazlarında ise Data Diode, Firewall gibi ağ trafiğini denetleyen varlıklar bulunmaktadır. Saha ile sürekli iletişimde olan kontrol sunucularının erişim doğrulaması, yetkisiz kişilerin saha verilerinin manipülasyonuna karşı doğru ağ segmentasyonunun sağlanması Firewall kuralları ve Switch (Anahtar Cihaz) Sanal Ağ uygulamaları ile gerçekleştirilir. Her varlık gibi ağ cihazlarının da firmware ve cihaz üzerinde gerekli sıkılaştırma süreçlerinin işetilmesi ve takibinin yapılması gereklidir.

Yukarıda belirtildiği gibi EKS cihazları proses kontrolü ve izlemesi, saha cihazlarının yapılandırılması ve bakımı gibi kritik süreçlerde yer almaktadırlar. Bu yüzden bir kritik altyapıdaki varlıkların ve iletişim mimarilerinin belirlenmesi hem siber güvenlik hem de yönetilebilirlik açısından önemlidir.

3.2. Purdue Mimarisi (Purdue Architecture)

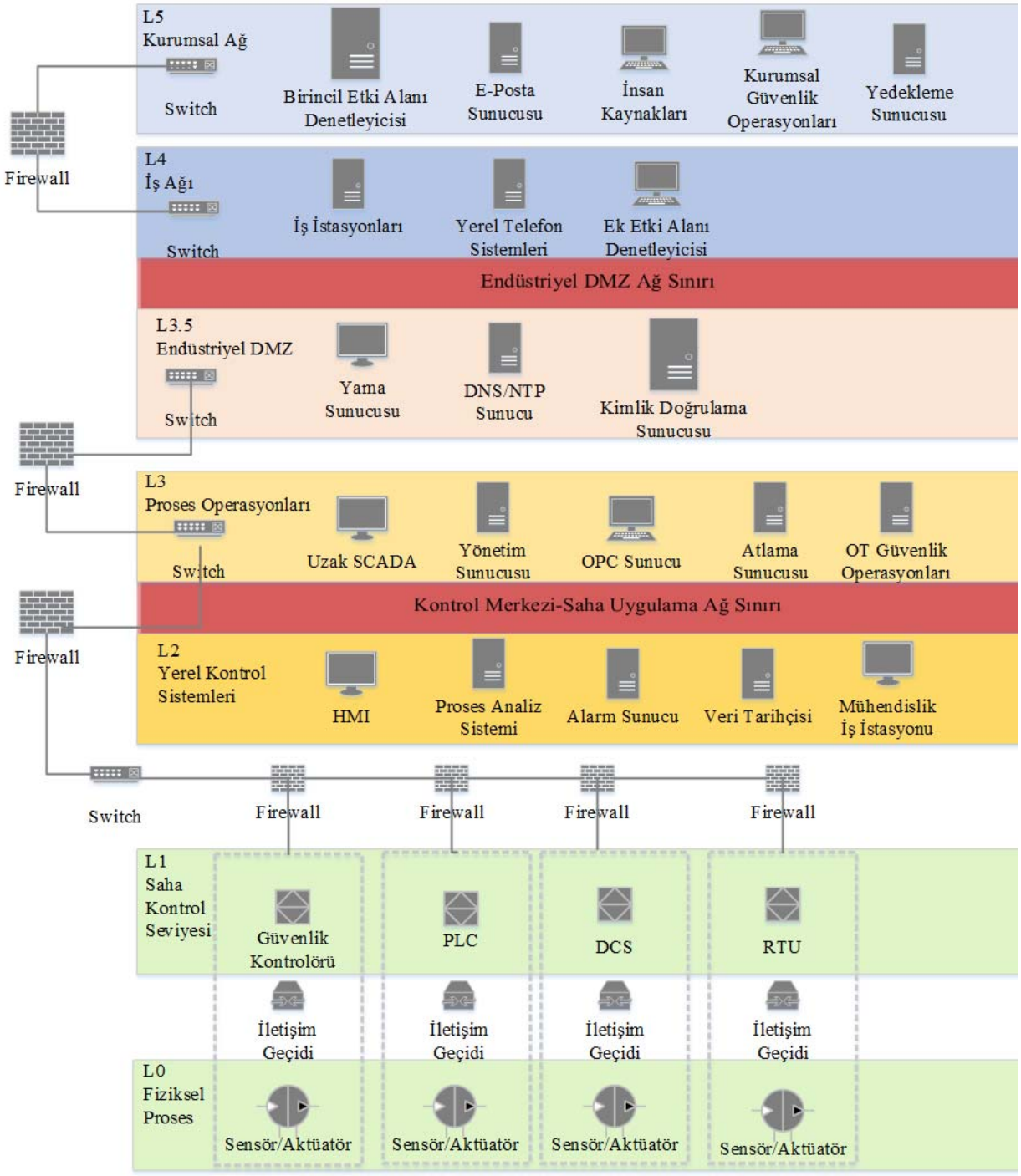
Endüstriyel tesisler, varlıkların ve operasyonel süreçlerin doğası gereği hem BT hem de OT ortamlarına sahiptirler ve literatürde hiyerarşik olarak seviyelerden oluşan ve Purdue Mimarisi olarak isimlendirilen bir mimari ile modellenirler. Bu mimaride BT ortamları üst seviyelerde (L5, L4) bulunurken, OT ortamları ise alt seviyelerde (L3, L2, L1, L0) tanımlanır. BT ve OT ortamlarının farklı varlıklara, veri akışlarına, iletişim protokollerine sahip olması ve bu ortamların da farklı zaman ve güvenlik gereksinimlerine ihtiyaç duyması her iki sistemin birbirleri arasında bir ağ sınırının konulmasını gerektirmektedir. Bu gereksinim mimaride ICS DMZ (Demilitarized Zone) (L3.5) olarak isimlendirilen bir seviye ile karşılanmaktadır. Global ölçekte standartlar ve EKS ürün üreticilerinin de referans aldığı Purdue model Şekil 1'de verilmiş olup, bir üst başlıkta verilen EKS varlıklarının seviyeler ile ilişkileri ve açıklamaları da aşağıda yapılmıştır [2]:

- L0 – Saha Seviyesi: Proses verilerinin toplanması için sensör/aktüatörlerin bulunduğu seviyedir.
- L1 – Yerel Denetleyici: L0 cihazlarından gelen proses verilerinin mantıksal kontrollerden geçirilip ilgili cihazlara aktarılmasını veya saha ile ilgili aksiyon alınmasını sağlayan varlıkların (PLC, RTU, IED, vb.) bulunduğu seviyedir.
- L2 – Yerel Kontrol Sistemleri: Saha cihazlarının komut ve kontrolü sağlayan varlıkların (SCADA, HMI, vb.) bulunduğu seviyedir.
- L3 – Proses Operasyonları: Bir tesisin veya EKS proses bölgesinin tamamı için izleme, denetleme ve operasyonel süreçleri kontrol eden Uzak (Remote) SCADA varlıkların bulunduğu seviyedir. Bu seviyede ek olarak veri tarihçisi, OT SIEM (Security Information And Event Management), OT IDS (Intrusion Detection System) gibi OT spesifik güvenlik ve analitik sistemler de bulunabilir. Farklı görev ve güvenlik seviyelerine sahip bu seviye birden fazla alt ağa bölünerek erişim denetim listelerinin işletilmesi güvenlik seviyesini arttırır.
- L3.5 (EKS DMZ): Purdue modelin ilk tasarlandığı zamanlarda bulunmayan bu seviye, BT ile OT ağları arasındaki doğrudan iletişimi kontrollü sağlamak, gerektiğinde engellemek için sonradan oluşturulan bir seviyedir. Bu seviyede, Proxy sunucular, uzak erişim sunucuları, veri tabanı sunucuları gibi aracı hizmetler bulunmaktadır.
- L4 – İş Ağı: Kurumsal BT süreçlerinin işletildiği varlıkların bulunduğu seviyedir. Bu seviyede, iş istasyonları, yerel dosya ve yazıcı sunucuları, kurumsal WAN (Wide Area Network) bağlantıları içeren cihazlar örnek verilebilir. Bu seviyedeki hiçbir varlık veya servis OT varlık veya servislerine erişmemelidir.
- L5 – Kurumsal Ağ: Kurumsal düzeydeki servisleri içeren varlıkların bulunduğu seviyedir. CRM (Customer Relationship Management) sistemleri, dahili E-Posta hizmetleri, İK sistemleri, yedekleme çözümleri ve kurumsal SOC (Security Operation Center) sağlayan teknolojiler bu seviyede bulunan varlıklara örnek olarak verilebilir. L4'e benzer olarak bu seviyeden de OT varlık veya servislerine erişim bulunmamaktadır.

OT sistemlerinde Purdue modeli referans alınarak farklı EKS mimarileri oluşturabilmektedir. Bu mimariler, farklı kabuller yapılarak ağ segmentasyonu ve izolasyonuna yönelik uygulama kontrolleri, Layer-3 Switch, Router, Firewall, tek yönlü ağ geçidi veya veri diyotları gibi cihazlar kullanılarak elde edilmektedir [29]. EKS mimarisi oluşturulduktan sonra mimarideki varlıklar üzerinde ve ağ trafiğinde gerçek zamanlı ağ tespitinin ve görünürlüğünün sağlanması, ilgili kritik altyapının siber saldırılara karşı saldırı yüzeyini minimize eden bir etki oluşturur. Geçmişte yapılan APT (Advanced Persistent Threat) saldırıları incelenmiştir [7, 29, 30]. Bu saldırılarda özellikle L1-L3 seviyelerindeki ağ görünürlüğünün eksikliği ve mimarideki saldırı tespit ve önleme sistemlerinin eksikliği, saldırıların başarılı olmasına neden olan büyük etkenler arasında görülmektedir. Global ölçekte kritik altyapı işletmeleri, siber güvenlik firmalarının ve otomasyon dünyası üreticilerinin kullandığı ya da önerdiği çözümlerin farklılığından dolayı farklı EKS mimarileri kullanabilmektedirler. Örneğin farklı karakteristik özelliklere sahip olsalar da saha kontrol cihazlarından olan PLC, RTU ve IED varlıkları Purdue modelin farklı katmanlarında yer alabilmektedir. Saha kontrol cihazları Fortinet ve Checkpoint tarafından L1'de konumlandırılır [3, 4]. Amerika enerji altyapısında saha cihazları ve SCADA sunucusu ile L0'da konumlandırılır [5]. SANS'ın önerdiği mimaride ise IED L0'da; PLC ve RTU L1'de yer almaktadır [6]. EKS'deki kritik varlıkların faklı Purdue seviyelerinde olması ya da tanımlanması farklı saldırı yüzeylerini oluşturmakla beraber güvenliğinin sağlanması noktasında da farklı yaklaşımların kullanılmasını gerektirebilir. Bu çalışmada topoloji çıkarımı ve mimari modelleme ile cihazların Purdue model uyumluluğu ve iletişim yapısı dikkate alınarak güvenlik ve risk değerlendirmesi için bir bakış açısı kazanımı sağlanmak istenmektedir. Aynı zamanda elektrik enerji şebekesi, doğalgaz üretim/iletim/dağıtım/depolama, çevrim santralleri, boru hattı iletim sistemleri gibi farklı kritik altyapılar, Purdue modelini referans alsalar da farklı çalışma prensiplerinden dolayı da farklı ağ mimarisi ortaya çıkartacaklardır. Her mimarinin güvenlik gereksinimlerinin ve kontrollerinin farklılık göstermesinden dolayı bu çalışmada önerilen modelleme yöntemi kritik altyapı bağımlılığı olmadan ağ güvenlik analizinin yapılmasını sağlayacak bir çıktı sunmaktadır.

3.3. EKS Güvenliği ve Standartlar (ICS Security and Standarts)

Günümüzde OT teknolojileri, operasyon süreçlerini ve bakımlarını hızlandırmak için sürekli gelişim halindedir. Gelişen teknoloji, kompleks bir yapı olan EKS'nin altyapısını değiştirmekte ve dolayısıyla güvenlik riskini de otomatik olarak etkilemektedir.



Şekil 1. Purdue mimarisi (Purdue architecture)

Standart kuruluşlar da bu değişen altyapılarda hem saldırı riskini azaltmak hem de sıfırıncı gün saldırılarına karşı dayanıklılığı artırmak için EKS güvenlik tasarımları ile alakalı önerilerde bulunmaktadırlar. IEC 62443 ve NIST 800-82 EKS alanına özgün standartlardır [9, 20]. Katmanlı DiD stratejisi de hem BT hem OT alanına uyarlanabilir güvenlik yaklaşımıdır. DiD ve diğer standartlar, EKS ürünlerinin üretimi ve güvenlik hizmetlerinin değerlendirilmesi için güvenlik yaklaşımları ve önlemleri ile alakalı bilgiler sunarlar. BT ortamları için geliştirilen standartlar OT ortamlarındaki karmaşık proses ve iletişim yapısı için yeterli değildir. BT sistemlerine yönelik siber saldırılarda yüksek maddi kayıplar ve veri sızıntıları yaşanır iken, OT sistemlerine yapılan saldırılarda ise, ciddi sağlık ve çevre sorunları ve insan yaşamını direkt etkileyecek olaylar ortaya çıkmaktadır. Bu yüzden farklı altyapılara sahip sistemler, farklı güvenlik gereksinimlerine ihtiyaç duyarlar. Bu farklı gereksinimleri karşılamak amacı ile ISA ve IEC (International Electrotechnical Commission) birlikte bir çalışma grubu oluşturarak OT spesifik çözümlerini Genel, Politika ve Prosedür, Sistem Gereklilikleri, Bileşen Gereklilikleri gibi dört ana kategoride inceleyen IEC 62443 standardını oluşturmuştur [9]. IEC 62443, yukarıda da belirtildiği gibi EKS için üretilen

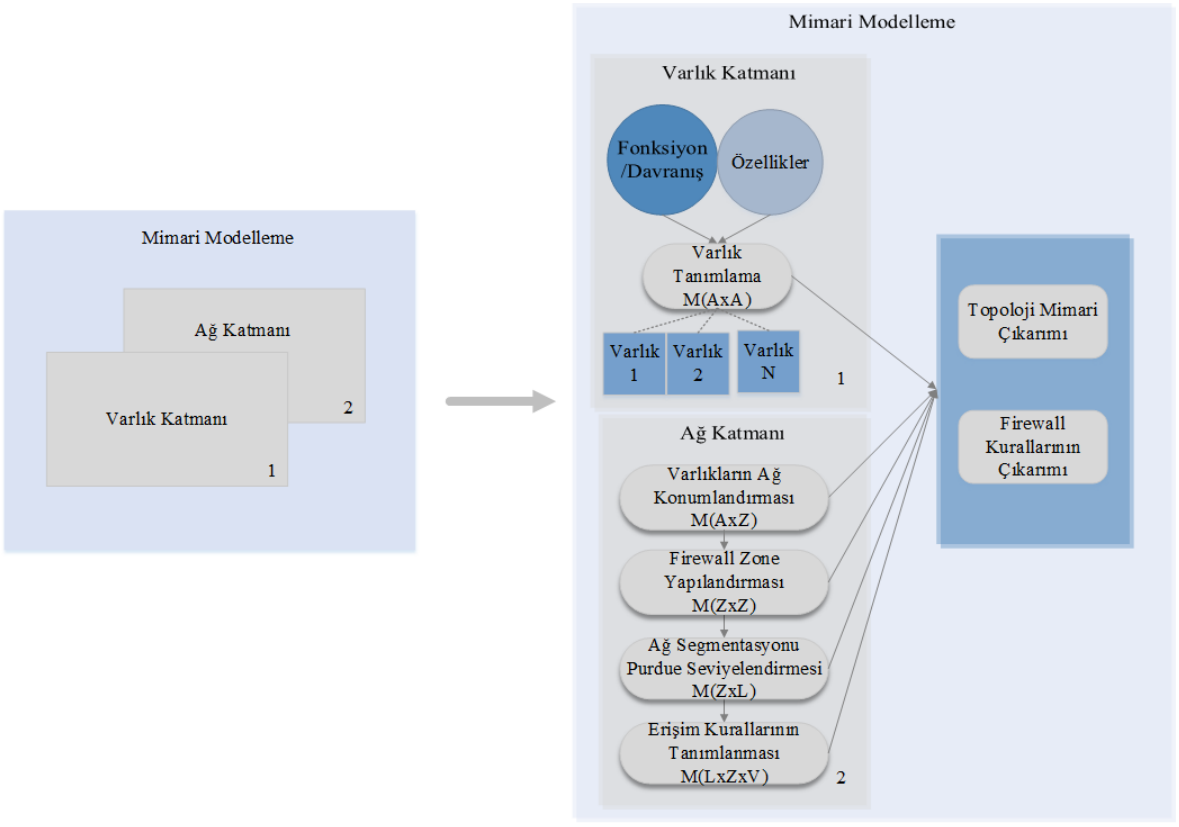
ürünlerin güvenlik süreçlerinden, sistem tasarımı ve bu aşamalarda görev alan insanların rol ve sorumluluklarına kadar tanımlayan kapsamlı bir standarttır. Bu standardın Sistem Gereklilikleri ana başlığının IEC 62443-3-2 bölümünde EKS ağında güvenlik bölgesi-iletişim kanalları ile ilgili gereklilikler, sistem tasarımına bağlı risk değerlendirmesi başlığında ele alınmıştır [9]. IEC 62443-3-2 güvenlik kanalı-iletişim kanalı modeli, mimarideki varlıkları benzer güvenlik gereksinimlerine sahip gruplara ayırarak bir grubu diğer bir gruba bağlayan bir kanal için gereksinimleri kısıtlayan bir yapı önerir. Güvenlik bölgeleri ile ilgili temel gereksinimler yedi farklı bakış açısı ile tanımlanmıştır [9]. Standartta yer alan "Sınırlı Veri Akışı" başlığında sistem gereksinimleri arasında; ağ segmentasyonu, güvenlik bölgesi ile ağ sınırı koruması yer almaktadır. EKS mimarilerindeki verilerin güvenlik bölgelerinden geçerken güvenli yöntemler ve kısıtların uygulanmasının gerekliliği vurgulanmıştır. Bu çalışmada da IEC 62443-3-2 temel gereksinimler başlığındaki sistem gerekliliklerinde istenen sınırlı veri akışının da ölçümlenebildiği bir mimari modelleme yöntemi sunulmuştur.

DiD, bir saldırıyı geciktirmek veya önlemek için birden fazla güvenlik korumasını katmanlar halinde sunar. Saldırganın tespit edilmeden hedefe yönelik saldırı vektörlerini daha fazla güvenlik katmanından geçmesini zorunlu kılar. DiD temel güvenlik katmanlarında endüstriyel sistemlere yönelik alt güvenlik başlıkları özelleştirilebilir [23]: Uygulama ve Veri Güvenliği, Sunucu Güvenliği, Ağ Güvenliği, Fiziksel Güvenlik, Risk Yönetimi. IEC 62443 standardında da vurgulanan DiD stratejisinde, EKS ağ mimarisi (güvenlik bölgeleri ve iletişim kanalları), ağ ve çevre güvenliği (Firewall ve atlama sunucuları) konuları EKS savunması için gereklilik olarak tanımlanmıştır. Bu çalışmada, ağ mimarisinin çıkarımı ile güvenlik bölgelerinde bulunan varlıkların benzer güvenlik gereksinimlerinin olup olmadığı ile ilgili analizler yapılması sağlanmaktadır. DiD stratejisinde bulunan ağ ve çevre güvenliği kapsamında Firewall cihazlarının hangi güvenlik bölgelerini bağladığı ve üzerinde oluşturulan kurallar ile iletişim kanallarının tanımlanması da bu çalışmanın katkılarından biridir.

NIST 800-82 standardında ise OT sistemlerinin güvenliğine yönelik risk yönetimi ve değerlendirmesi, kimlik doğrulama ve erişim kontrolü, ağ güvenliği, fiziksel güvenlik, olay müdahale ve izleme, varlık yönetimi ve konfigürasyon kontrolü, güvenlik zafiyeti yönetimi, yedekleme ve kurtarma, eğitim-farkındalık ve tedarikçi yönetimi konuları ele alınmaktadır [21]. Standardın ağ güvenliği konusunda, EKS ağ segmentasyonu, güvenlik duvarları, endüstriyel ağların izolasyonu ile EKS iletişim güvenliğinin belli bir seviyede olması gerektiği ve saldırı tespit sistemleri ile de desteklenmesi gerekliliği vurgulanmaktadır. Bu yüzden Purdue L1-L3 seviyelerindeki varlıkların hangi servisler ile birbirlerine erişmesi gerektiği Firewall kuralları ile doğru bir şekilde belirlenmelidir. Ağ anomalilerinin tespiti ve saldırıların önlenmesi için EKS mimarisinin çalışma yapısı dikkate alınarak Firewall kurallarının doğru yapılandırılmış olması gereklidir. Bu çalışmada EKS mimari modelleme yöntemi sayesinde güvenlik bölgelerinde bulunan varlıkların iletişim kanalları ile EKS proses verisinin ağdaki dolaşımının güvenlik analizini yapmak için bir ağ modeli oluşturularak Purdue Mimarisi ve EKS standartları çerçevesinde proses bağımsız bir topoloji modelleme yöntemi önerilmiştir.

4. EKS Model Oluşturma (ICS Model Creation)

EKS bileşenleri daha önce ifade edildiği üzere farklı rollere ve çalışma prensiplerine sahip varlıklardır [32]. Bu varlıklar, EKS proses işleyişinin saha seviyesindeki gerçek zamanlı veri akışını veya sahayı kontrol eden kontrol sunucularını kapsayan ve bir mimari oluşturan



Şekil 2. Mimari modelleme iş akışı (Architecture modelling workflow)

kritik varlıklardır. EKS mimarisinin tanımlanmasında, bu varlıkların mimarideki görevi, iletişim yapısı, erişim kontrolleri gibi hem proses işleyişi hem de güvenliği için öncelikle varlıkların doğru analiz edilerek modellenmesi ilk adımdır. Bu kapsamda önerdiğimiz modelde EKS topolojisinin bir bütün olarak tanımlanabilmesi için önce varlıkların doğru tanımlanması, ardından da ağ yapısının doğru analiz edilmesi gerekmektedir. Bu kapsamda önerilen mimari model, Varlık Katmanı (1) ve Ağ Katmanı (2) olarak iki ana bileşenden oluşmakta ve bu bileşenler ve mimari model ile ilgili çalışmanın genel akışı da Şekil 2'de verilmektedir.

4.1. Varlık Katmanı Modeli (Asset Layer Model)

Varlıklar EKS'nin en temel bileşenidir. Sistemde bir varlığı tanımlamadan varlığın oluşturduğu hizmetleri ve ağ akışını tanımlamak doğru bir yaklaşım değildir. Siber güvenlik kapsamında değerlendirildiğinde varlıkların hem kendi özelliklerinden hem de sunduğu hizmetlerden dolayı oluşan saldırı yüzeyi, kritik sonuçlara sebep olabilecek saldırılara ortam hazırlar. Örneğin PLC, RTU gibi proses kontrolünde direkt işlevsel olan saha cihazlarına zararlı yazılım içeren firmware yüklenmesi ile istenmeyen süreçlerin işletilmesine ortam hazırlanır. Elektrik şebekesine yapılan BlackEnergy zararlı yazılımında, sistemleri devre dışı bırakmak, kapatmak veya kurtarılamaz hale getirmek için seri-ethernet ağ geçitlerine özel bir firmware ile üzerine yazıldığı tespit edilmiştir [33]. Benzer şekilde TRITON zararlı yazılımının güvenlik denetleyicisinin belleğindeki kodu okuma, yazma ve çalıştırma işlemlerini yapabildiği tespit edilmiştir [34]. Diğer yandan SCADA, Mühendislik İş İstasyonları gibi kontrol katmanında görev alan varlıkların sunduğu proses verilerinin izlenmesi ile ilgili saldırıları yapmak da istenmeyen sonuçları ortaya çıkartmaktadır. Industroyer zararlı yazılımının, sabit sürücüdeki EKS konfigürasyon dosyalarının üzerine yazan ve özellikle ABB üreticisinin PCM600 konfigüratör aracını hedefleyen yıkıcı bir etkiye sahip davranış göstermesi örnek olarak verilebilir [35]. Verilen bu bilgiler ışığında bu çalışmada hem varlıkların özellikleri hem de sunduğu servisler/fonksiyonlar birlikte değerlendirilerek ağ mimarisinde dolaşan verinin varlıklarla eşleştirilmesini sağlayan bir yaklaşım sunulmuştur.

Bu çalışmada, bir EKS'de bulunan kontrol merkezi sunucuları, proses kontrol cihazları ve ara bağlantı cihazları gibi tüm bileşenleri kapsayacak şekilde modelleme bileşenleri oluşturulmuştur. Modeldeki bileşenler bir kümeyi veya alt bileşenleri içerebilir durumdadır. Bu model aynı zamanda dinamik bir yapıya sahiptir. Sisteme özgü bir işlevsellik ihtiyacı durumunda modele yeni bileşenler eklenebilir. Varlık Modeli için aşağıda belirtildiği üzere üç farklı bileşenden oluşacak şekilde bir yaklaşım sunulmaktadır:

Varlık Model = {Varlıklar (Q_A), Varlık Özellikleri (E_A), Varlık Fonksiyonları (E_S)}.

Varlık Modeli içerisindeki tanımlanan bileşenler ve özellikleri aşağıda verilmiştir:

1. Varlıklar (Q_A): Purdue mimarisindeki veya IEC 62443 kapsamı içerisindeki tüm varlıkların olduğu kümeyi belirtir. Bu kümenin bileşenleri Q_A kümesinde tanımlanmıştır. Bu kümede yaygın olarak kullanılan EKS varlıkları bulunmaktadır.

   Q_A = {Uygulama Sunucuları, Kontrol Sunucuları, Veri Ağ Geçidi, Veri Tarihçisi, Saha G/Ç, HMI, IED, Atlama Sunucuları, PLC, RTU, Ağ Yönlendiricileri, Güvenlik Kontrolörleri, VPN Sunucular, İş İstasyonları}

2. Varlık Özellikleri (E_A): Bir varlığın davranışlarını oluşturan özellikleri tanımlar. Bu özelliklerden yaygın olanlar E_A kümesinde tanımlanmıştır.

   E_A = {Firmware, İşletim sistemi versiyonu, Program belleği, I/O sayısı, Port sayısı, Port tipi, vb.}

3. Varlık Fonksiyonları (E_S): Sistemin bütün olarak doğru işleyebilmesi için varlıkların birbirlerine sundukları servisler/fonksiyonlar olarak tanımlanmıştır. Örneğin bir PLC varlığının SCADA varlığına saha verilerini aktaran fonksiyonu vardır. Benzer şekilde PLC'nin belleğinde barındırdığı verileri bir uygulama programına sunduğu bir Web Sunucu servisi bulunabilir. Bu servisler/fonksiyonlar E_S kümesinde tanımlanmıştır.

   E_S = {Proses İşletimi, Proses Komut-Kontrol, Web Sunucu, RBAC, Loglama, Alarm Yönetimi, Uzak Erişim}

Varlık modeli tanımına göre (1), bir EKS mimarisi (A) varlıklarından oluşur. Her varlığın sahip olduğu en az bir özelliği (E_A) ve iletişimde olduğu varlıklara sunduğu bir servisi (E_S) bulunur. Bu çalışmada EKS mimarilerinde Purdue Model L1-L3 seviyelerinde bulunan tüm varlıkların hem özellikleri hem de sunduğu servisler birlikte incelenmiş, önerdiğimiz varlık modeline göre de yaygın olarak kullanılan varlıklar ve varlıkların özellikleri ve bileşenleri Tablo 1'de detaylı olarak verilmiştir. Tablo 1'de verilen özellikler ve fonksiyonlar, ilgili varlıkların kullanım kılavuzlarından çıkarılarak oluşturulmuştur. Ayrıca Tablo 1'e göre varlıkların birbirlerine sundukları servislerin tanımlanması için her servise benzersiz olacak şekilde F1-F21 aralığında bir ID değeri atanmıştır. Tablo 1'de yer alan varlıklar hem fiziksel sistemin işleyişi hem de siber güvenlik kapsamında kontrol edilmesi gereken varlıklardır. Her EKS'de aynı varlıklar bulunmak zorunda değildir. Örneğin DCS her EKS'de olmayabilir. IED cihazları elektrik-enerji kritik altyapılarında bulunurken su yönetimi sistemlerinde bulunmaz. Ya da bir PLC ayrık kontrol sistemlerinde ana kontrol bileşeni olabilirken, SCADA veya DCS kontrol mimarisine sahip proseslerde yerel ve uç bir kontrol cihazı olarak kullanılabilir. Bu yüzden modeldeki varlık kümesi, incelenen EKS mimarisindeki prosese bağlı olarak değişkenlik gösterebilir. Önerilen model bu değişkenliği karşılayacak şekilde tasarlanmış ve böylece bir sonraki adımda matrislerle ilişkisel yapıların doğru tanımlanması için uygun bir model ortaya çıkartılmıştır. Varlıklar, fonksiyonlarını birbirlerine servis olarak sunar ve bu servislerde varlıkların davranışlarını oluşturur. Bu yüzden varlıkların arasındaki servis ilişkisini tanımlayan bir matris ile model verisi matematiksel olarak elde edilebilir. Varlık (M_{AxA}) matrisinde (Eş. 1) satır ve sütunlar mimarideki tüm varlıkları temsil eder. Satır ve sütun değerlerinde "0" olması varlıkların arasında herhangi bir iletişimin olmadığı anlamına gelirken "Fx, Fy" gibi ifadelerin olması varlıklar arasında Tablo 1'deki "ID" sütunundaki servis numaralarını ifade eden iletişimin varlığı anlamına gelir.

$$M(AxA)=\begin{bmatrix} 0 & \{0|Fx,Fy\} & \dots & \{0|Fx,Fy\} \\ \vdots & \ddots & & \vdots \\ \{0|Fx,Fy\} & \{0|Fx,Fy\} & \cdots & 0 \end{bmatrix} \quad (1)$$

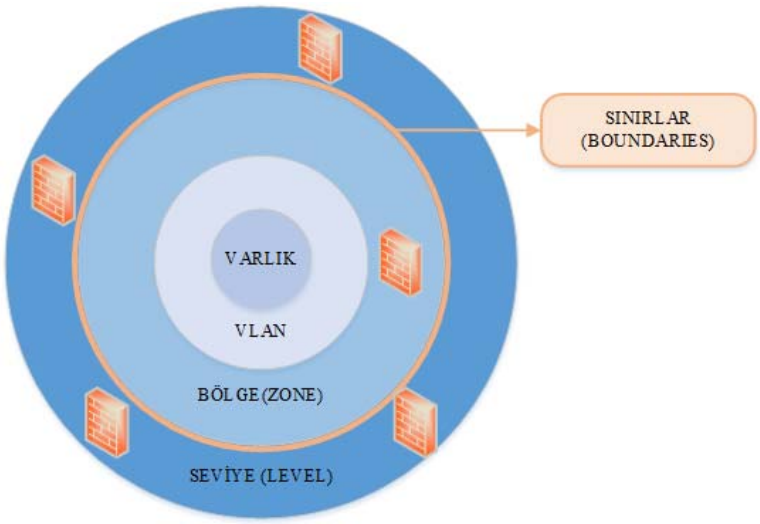
Matris yönlü bir matristir ve simetrik olmak zorunda değildir. Çünkü varlıkların birbirlerine aynı hizmeti sunma zorunluluğu yoktur. Bu yüzden ilgili matris, satırdaki bir varlığın sütundaki bir varlığa sunduğu hizmet şeklinde değerlendirilmelidir. Varlık tanımlama aşaması tamamlandıktan sonra varlıkların ağ mimarisinde bulundukları konum ve iletişim şekillerinin doğru belirlenmesi gerekmektedir. Bu aşama, bir sonraki bölümde varlıkların Sanal Ağ, Güvenlik Bölgesi ve Seviye bilgilerinin matrislerle tanımlanması ile açıklanacaktır.

4.2. Ağ Katmanı Modeli (Network Layer Model)

Mimari bir yapının doğru tanımlanması için varlıkların ağ içerisindeki konumlarının doğru belirlenmesi gerekmektedir. Varlıklar ve sundukları servisler ağ üzerinden seviyelere göre hem BT hem de OT protokolleri aracılığıyla haberleşmektedirler.

Tablo 1. Purdue modele göre EKS varlık özellikleri- Fonksiyonları (ICS Asset properties-Functions by Purdue levels)

Varlıklar (A)	Özellikler (E_A)	Fonksiyonlar/Davranışlar (E_S)	ID	Purdue Seviyesi
PLC	I/O Sayısı	Proses işletimi	F1	L1
	Donanım Yazılımı	OPC UA iletişimi	F2	
	Port Sayısı	Endüstriyel protokoller ile proses verisinin alınması/gönderilmesi	F3	
	Port Tipi			
	Bellek	Loglama	F4	
	Gerçek Zamanlı İşletim Sistemi			
RTU	I/O Sayısı	Proses işletimi	F1	L1
	Donanım Yazılımı	OPC UA iletişimi	F2	
	Port Sayısı	Endüstriyel protokoller ile proses verisinin alınması/gönderilmesi	F3	
	Port Tipi			
	Bellek	Loglama	F4	
	Gerçek Zamanlı İşletim Sistemi	Protokol geçidi (Gateway)	F5	
IED	Donanım Yazılımı	Endüstriyel protokoller ile proses komut işletimi ve kontrolü	F6	L1
	Port Sayısı	Web sunucu	F7	
	Port Tipi			
	Bellek	Rol tabanlı erişim kontrolü	F8	
	Gerçek Zamanlı İşletim Sistemi	Proses koruma, kontrol, görüntüleme fonksiyonları	F9	
SCADA	Uygulama Versiyonu	Proses kontrol	F10	L2-L3
	İşletim Sistemi Versiyonu/Tipi	Proses izleme	F11	
	SCADA Veri tabanı kayıtları	Alarm yönetimi	F12	
		Endüstriyel protokoller ile gerçek zamanlı proses veri erişimi/kontrolü	F13	
HMI	Grafik arayüzü	Proses verisi alma/gönderme	F3	L2
	Donanım Yazılımı	Proses izleme	F11	
OPC (Open Platform Communications)	Uygulama Versiyonu	Gerçek zamanlı proses verisine erişim	F14	L3
	İşletim Sistemi Versiyonu/Tipi	Alarm üretme	F15	
		Loglama	F4	
		OPC İstemcisi ile API iletişimi	F16	
Mühendislik İş İstasyonu	Uygulama Versiyonu	Endüstriyel cihaz yapılandırması	F17	L2-L3
	İşletim Sistemi Versiyonu/Tipi	Endüstriyel cihaz görüntülemesi	F18	
		Endüstriyel donanım yazılımı güncellemesi	F19	
Domain Etki Alanı	Uygulama Versiyonu	Etki alanı bilgisayar kısıtlama politikalarının uygulanması	F20	L3
	İşletim Sistemi Versiyonu/Tipi	Etki alanı kullanıcı kısıtlama politikalarının uygulanması	F21	



Şekil 3. Varlıkların EKS'de bulunabileceği ağ konumları (Network locations of assets in ICS)

Bir EKS mimarisinin ilk savunma hattını Sınırlar (Boundaries) oluşturmaktadır. Sınırlar ile herhangi iki ağ, keskin bir şekilde farklı cihazlar (Data Diode, Firewall, Router, L3 Switch, vb.) aracılığı ile ayrılır. Böylece bir tarafta oluşan herhangi bir siber olayın diğer tarafı etkileme ihtimali en aza düşürülmüş olur. EKS özelinde Sınırlar temel olarak dört alan için gereklidir [29]:

1. İnternet DMZ Sınırı & BT Uygulama Sınırı: EKS işletmesinin internete açılan sınırdır. WAN ağı ile trafiğin giriş-çıkış kontrol parametreleri belirlenir. Purdue mimarisinin L5 seviyesinin WAN ile iletişimi tanımlanır.
2. Endüstriyel DMZ Uygulama Sınırı: Purdue mimarisine göre L3 ile L4 arasındaki ağ sınırını tanımlar, temel BT-OT ağları arasındaki geçiş bölgesidir ve Purdue L3.5/OT DMZ olarak isimlendirilir. Bu sınır ile OT ağına kurumsal ağdan erişimin mümkün olduğunca olmaması istenir. Kurumsal ağ ile OT ağının erişimi bakım/güncelleme veya tedarikçi isteği ile gerekiyorsa mümkün olduğunca kısıtlı ve kontrollü bir iletişim olması beklenir.
3. Kontrol Merkezi-Saha Uygulama Sınırı: Purdue L2 ile L3 arasındaki ağ sınırını tanımlar. Endüstriyel DMZ Uygulama Sınırına göre daha az kısıtlı ancak yine de kontrollü ağ trafiği kısıtlama uygulamalarını içerir.
4. EKS / Emniyet Sınırı: Emniyet enstrümanlı sistemler (SIS) ile OT ağının geri kalanı arasındaki sınırdır. Hava boşluğu (airgap) uygulama sınırı olarak da tanımlanır.

OT sistemlerde kabul edilen temel Sınırlar yukarıda açıklamalı olarak verilmiştir. Sınırlar bir trafiğin giriş/çıkış noktalarını, içindeki varlıkların erişim yetkilerini ve iletişim protokollerinin kısıtlarını tanımlaması ve yetkili kişilerin/cihazların belli varlıklara/servislere erişmesi/erişmemesi gibi temel güvenlik önlemlerinin doğru karar verilmesine ve alınmasına önemli katkılar sunar. Bu çalışmada 2. ve 3. Maddede belirtilen Sınırlar dikkate alınarak bir model önerisi yapılmıştır. Diğer taraftan OT alanı ile alakalı uluslararası standartlar ve regülasyonlar varlıkların hem güvenlik hem de yönetilebilirlik açısından Sınırlar içinde daha küçük ve işlevsel ağ birimlerine bölünmesini ister ve gerekli kılar. Bu gereklilik bir varlığın konumunun tanımlanmasında ve/veya belirlenmesinde Purdue Seviyesi, Güvenlik Bölgesi (Zone) ve Sanal Ağ bilgilerinin de dikkat alınmasının önemini ortaya çıkartır. Bu bilgiye bağlı olarak önerilen modelde her bir varlık, bulunduğu Ağ Sınırı, Sanal Ağı, Güvenlik Bölgesi ve Purdue Seviye bilgileri matrisler yardımıyla tanımlanmış ve topoloji çıkarımı için gerekli veriler elde edilmiştir (Şekil 3). Önerilen modelde ağ mimari yaklaşımlarında Sıfır Güven (Zero Trust) mimarisi veya mikro-segmentasyon konuları değerlendirilmeye alınmamıştır.

Mimari yapıda topoloji çıkarımı yaparken en küçük birim olan Sanal Ağ (VLAN) yapılandırması incelenmiştir. Böylece katmanlı mimarinin tüm adımları en küçük birimden (Sanal Ağ) en büyük birime (Sınır) kadar ele alınmıştır. Bu çalışmadaki kabullerimiz aşağıda listelenmiştir:

- Bir varlık hiçbir sanal ağda olmayabilir veya bir sanal ağda bulunabilir.
- Bir varlık bir veya daha fazla güvenlik bölgesinde içinde bulunabilir (Varlık hem ana güvenlik bölgesi hem de alt güvenlik bölgesinde bulunabilir).
- Bir güvenlik bölgesi birden fazla seviyeyi kapsayabilir.
- Bir güvenlik bölgesi bir seviyeden oluşabilir.
- Güvenlik bölgeleri arasındaki iletişim bir veya birden fazla protokol içeren kanallar (conduit) ile sağlanır.
- Bir Sınır iki ayrı ağı birbirinden ayıran temel bir ağ geçiş sınırıdır.

Bu bilgilere göre her bir varlık bir güvenlik bölgesinde olabilir veya olmayabilir. Eğer bir güvenlik bölgesinde ise de bu bölgede yapılandırılan sanal ağ içinde olabilir veya olmayabilir. Buna göre varlıkların içinde bulunduğu konumu belirleyebilmek için Sanal Ağ ve Güvenlik Bölgesi bilgilerinin tanımlandığı Varlık- Güvenlik Bölgesi (M_{AxZ}) matrisi (Eş. 2) aşağıdaki kabullere göre oluşturulmuştur:

- Matristeki 0 değeri; varlığın ilgili sütundaki güvenlik bölgesinde bulunmadığını,
- Matristeki 1 değeri; ilgili güvenlik bölgesinde bulunduğunu,
- Matristeki Vx değeri ilgili güvenlik bölgesinde VLAN içerisinde bulunduğunu ifade eder.

$$M(AxZ) = \begin{bmatrix} \{0|1|Vx,Vy\} & \cdots & \{0|1|Vx,Vy\}\} \\ \vdots & \ddots & \vdots \\ \{0|1|Vx,Vy\} & \cdots & \{0|1|Vx,Vy\} \end{bmatrix} \quad (2)$$

Katmanlı mimarinin sonuçlarından biri olarak farklı güvenlik bölgesinde bulunan varlıkların birbirleri arasında haberleşmesi gerekebilir. IEC 62443 [9] standardında da belirtildiği üzere bu haberleşme işlemi kanallar (conduit) aracılığı ile gerçekleşir. Kanallar güvenlik bölgeleri arasında bir veya daha fazla protokol iletişimini içerebilir. Güvenlik bölgeleri arasındaki haberleşme gerekliliği, M_{AxA} matrisindeki varlıkların birbirlerine sunduğu servislerden çıkarılabilir. Bu durumun bir sonucu olarak güvenlik bölgeleri arasındaki haberleşme, Firewall cihazları üzerinde kural yapılandırmalarıyla sağlanır. Endüstriyel kontrol sisteminin ana topolojisini çıkarmadan önce uygulanacak son adım ise güvenlik bölgelerini Purdue modeli seviyelerine göre değerlendirmektir. Bu aşamada, güvenlik bölgelerinin içinde EKS varlıkları için tanımlanan M_{AxZ} matrisinden yararlanılmıştır. M_{AxZ} matrisinde, varlıkların içinde bulundukları güvenlik bölgeleri tanımlanmaktadır. Varlıkların Purdue modele göre bulunması gereken seviyeler Tablo 1 dikkate alınarak yorumlanmıştır. Modellemenin bu aşaması Bölüm 4.3 Adım 3'te daha detaylı aktarılmıştır.

Buraya kadar verilen bilgiler ile bu çalışmanın ana katkılarından biri olan ağ topolojisini modelleme ile ilgili gerekli olan tüm tanımlamalar tamamlanmıştır. Bir sonraki bölümde önerilen modelleme ile ana topolojinin Purdue modeline göre mimarisinin çıkarımı ve proses işlevselliğinin olması için gerekli Firewall kurallarının çıkarımı yapılacaktır. Varlıkların arasındaki haberleşme, varlıkların birbirlerine sundukları servisler aracılığıyla tanımlanmaktadır. Birbirleri ile haberleşen her varlık çifti için Firewall kuralı gerekmez. Örneğin Domain Sunucu ile aynı ağda bulunan OPC Sunucu varlıklarının birbirleri ile haberleşmeleri için herhangi bir Firewall kuralı yazılması (bir mikro-segmentasyon yapılmamışsa) gerekmez. Çünkü aynı ağ segmentasyonunda yer alırlar. Ancak SCADA Sunucu ile PLC/RTU/IED varlıkları arasında bir Firewall kuralının yazılması gereklidir. Çünkü her iki varlık farklı ağ segmentasyonunda olmalarına rağmen birbirlerine sundukları fonksiyon/servislerden dolayı farklı güvenlik bölgeleri veya sanal ağlar arası haberleşme gerekebilir. Bu yüzden Firewall cihazlarında ilgili varlıkların iletişimi için uygun kural yazımı gereklidir. Benzer şekilde ağ segmentasyonu içerisinde Sanal Ağ yapısı ile alt-segmentasyon da uygulanabilmektedir. Tüm bu ihtimaller (2^k, k=3 (Seviye-Güvenlik Bölgesi-Sanal Ağ)) farklı kombinasyonlar üretmektedir. İki varlığın mimarideki ağ bilgisi ve birbirlerine sundukları fonksiyon/servisler temel alınarak oluşabilecek durumların tanımlanması Tablo 2'de verilmiştir.

Bir EKS mimarisinde birbirlerine fonksiyon/servis sunan herhangi iki varlık, mimarideki konumlarına göre Tablo 2'deki durumlar temel alındığında, Firewall kurallarının yazılması ile ilgili durum ortaya çıkar. Tablo 2'ye göre geçersiz durumlar, LZV (1) ve LZV (5) hariç diğer tüm durumlar için Firewall üzerinde kural yazılması gereklidir.

Tablo 2. Seviye- Güvenlik bölgesi-Sanal ağ durum tablosu (Layer-Zone-Vlan state table)

Seviye/Güvenlik Bölgesi /Sanal Ağ	L	Z	V	Durum	Açıklama
1	1	1	1	(l,z,v)	Aynı seviye, aynı güvenlik bölgesi, aynı sanal ağ
2	1	1	0	(l,z,v')	Aynı seviye, aynı güvenlik bölgesi, farklı sanal ağ
3	1	0	1	-	Geçersiz Durum
4	1	0	0	(l,z',v')	Aynı seviye, farklı güvenlik bölgesi, farklı sanal ağ
5	0	1	1	(l',z,v)	Farklı seviye, aynı güvenlik bölgesi, aynı sanal ağ
6	0	1	0	(l',z,v')	Farklı seviye, aynı güvenlik bölgesi, farklı sanal ağ
7	0	0	1	-	Geçersiz durum
8	0	0	0	(l',z',v')	Varlıkların birbirinden bağımsız ağda olması

4.3. Mimari Modelleme (Architecture Modelling)

Bir EKS'de varlıkların tanımlanması, yönetilmesi ve konumlandırılması hem prosesin doğru işletilmesi hem de güvenliği açısından önemlidir. Varlıklar, bir EKS'de mimariyi oluşturan en küçük birimdir. Bu yüzden varlıkların birbirleri arasındaki iletişim, mimari yapının ağ segmentasyonunun oluşmasına etki etmektedir. Yönetilebilir ve güvenli bir mimari için ilgili varlıkların sunduğu hizmetlere göre Firewall kurallarının yazılması dikkat edilmesi gereken önemli bir konudur. Geçmişte büyük mali ve iş kaybına yol açmış EKS saldırıları incelendiğinde, bir varlığın mimarideki diğer varlığa kontrolsüzce erişiminden dolayı saldırganların sistem içerisinde ilerlediği ve saldırının başarılı olmasına neden olduğu bilinmektedir. Doğru ağ segmentasyonu, sistem ve ağ yapısının izlenebilirliği, erişim kontrollerinin doğru yapılandırılması gibi süreçler katmanlı mimaride gerekli ve kompleks süreçlerin oluşmasına neden olmaktadır. Bu çalışmanın ana katkılarından olan ağ mimarisinin çıkarımı, sistemin Purdue mimarisinin gerekliliklerini uygulama açısından yardımcı olacaktır. Çalışmanın bir diğer ana katkısı da EKS mimarisindeki ağ segmentasyonunda önemli rol oynayan Firewall cihazlarının üzerinde prosesin işlenebilirliğinin sağlanması için yazılan kurallarının çıkarımıdır. Bu bölümde, topolojinin çıkarımı ve Firewall cihazlarındaki olması gereken kural taslağının oluşturulması ile ilgili adımlar özet olarak sunulmaktadır. Purdue modelin seviyelerine göre ağ mimarisinin çıkarılması aşağıdaki adımlar uygulanarak oluşturulmuştur. Adım 1 ve Adım 2'de Bölüm 4.1 Varlık Katmanı ve Bölüm 4.2 Ağ Katmanında oluşturulan matrisler kullanılmıştır. Adım 3, Adım 4 ve Adım 5'te ise bu matrislerden çıkarımlar yapılarak sonuca gidilmiştir:

Adım 1- Varlıkların birbirleri arasındaki ilişkinin belirlenmesi: Bu adımla farklı seviyelerde bulunan varlıklar varsa birbirlerine sundukları servisler tanımlanmalıdır. Çünkü farklı güvenlik bölgesi veya seviyede bulunmaları durumunda Firewall kurallarının aralarındaki iletişime göre tanımlanması gerekir. Bu adımın gerçekleştirilmesi Bölüm 4.1'de M_{AxA} matrisinde tanımlanmıştır.

Adım 2- Varlıkların mimarideki konumunun belirlenmesi: Birinci adımda tanımlanan varlıkların verilen mimarideki konumlarının Sanal Ağ, Güvenlik Bölgesi ve Seviye ile tanımlanması sağlanır. Bu adımın gerçekleştirilmesi Bölüm 4.2'de M_{AxZ} matrisinde tanımlanmıştır.

Adım 3- Ağ segmentasyonun belirlenmesi: Bu aşamada iki ayrı tanımlama yapılmıştır. Birincisi; EKS mimarisindeki Firewall cihazları ile oluşturulan güvenlik bölgelerinin birbirleri arasında iletişim varsa belirlenmesi. İkincisi Sınırların hangi seviyeler arasında tanımlandığının belirlenmesi. Adım 2'de varlıkların bulundukları ağ konumlarına göre hangi varlıkların aynı güvenlik bölgesinde olduğu veya aynı güvenlik bölgesinde aynı sanal ağda olup olmadığı ile ilgili çıkarımlar yapılır. Belirlenen güvenlik bölgelerinin içinde bulunan varlıkların iletişimine göre (Adım 1) iletişim kanallarının tanımlanması sağlanır. Böylece Firewall kurallarının doğru oluşturulması için temel çıkarım elde edilmiş olur. Örneğin Z1 güvenlik bölgesinde bulunan SCADA varlığı Z2 güvenlik bölgesinde bulunan RTU varlığına bir komut göndermek istediğinde, Z1 ile Z2 güvenlik bölgelerinin arasında bir Firewall bulunması ve Firewall cihazında da Z1 ve Z2 arasında geçiş kuralının çift yönlü yazılması gerekir.

Adım 4- Ağ segmentasyonu ile Purdue modelin seviyelerinin eşleştirilmesi: EKS katmanlı mimarinin çıkarımı için oluşturulan ağ segmentasyonunun Purdue modelin seviyelerine göre eşleştirilmesi gerekir. Doğru eşleştirme için güvenlik bölgelerinde bulunan varlıkların Purdue mimarisinin hangi seviyesinde bulunduğu ile ilgili Tablo 1 verileri temel alınarak oluşturulur. Örneğin Güvenlik Bölgesi-1 içinde yer alan OPC varlığı Tablo 1'e göre L3 seviyesinde bulunmalıdır. Dolayısıyla Güvenlik Bölgesi-1 için Purdue mimarisinin Seviye-3 içinde bulunduğu yorumu yapılabilir. Bu adım, güvenlik bölgesinde bulunan varlıkların haberleşmesi için gerekli kural seti taslağının oluşturulması için önemlidir.

Adım 5- EKS mimarisi/topolojisi ve Firewall kural taslağının çıkarımı: Önceki adımlarda elde edilen veriler kullanılarak ağ mimarisi çıkarımı Purdue model referans alınarak yapılır. Sistemde kullanılan Firewall cihazları üzerindeki kuralların ana yapısı taslak olarak elde edilir.

Yukarıda belirtilen Adım 1 ve Adım 2'de ilgili ağ altyapıdan veri alınmış diğer adımlar Purdue model uyumluluğu ve temel EKS güvenlik sınırlarına göre bilgi çerçevesinde elde edilmiştir.

5. Sonuçlar ve Tartışmalar (Results and Discussions)

Bu bölümde önerilen modelin doğruluğunu ve işlevselliğini kanıtlamak amacıyla bir EKS mimarisinin Bölüm 4'te aktarılan çıkarım adımlarına göre işletilmesi ve işletilmesi sonrasında çıkarım yapılan ağ topolojisi ve Firewall kuralları ile alakalı sonuçları incelenecektir. Ele alınan EKS mimarisi, Kritik Altyapılar Ulusal Test Yatağı Merkezi'nde (CENTER) [1] bulunan Su Yönetimi kritik altyapısının [36] çalışan mimarisi olacaktır. Mimaride kullanılan aynı varlıklar, farklı ağ konumlarına alınarak iki farklı mimarinin (Mimari-1 ve Mimari-2) önerilen model sonrasında elde edilen sonuçları karşılaştırılacaktır. Mimari-1 ve Mimari-2 topolojileri Purdue Modelin L0, L1, L2 ve L3 seviyelerine sahip mimariler olarak tanımlanacaktır.

5.1. Test Çalışması-1: CENTER Su Yönetim Sistemi (Case Study-1: CENTER Water Management System)

CENTER Su Yönetimi [36] kritik altyapısındaki iletişim mimarisi, geliştirdiğimiz topoloji modellemesi ve kural çıkarımı ile merkezde çalışan gerçek sistemin karşılaştırması yapılarak test edilmiştir. İlk adımı uygulamadan önce varlık listesi modellemenin sonraki adımlarında kullanılmak üzere Tablo 3'teki gibi tanımlanmıştır.

Mimarideki varlıklar, Q_A = {SCADA, OPC, Domain Sunucu, EWS, HMI, PLC, I/O, BT Firewall, BT Switch, OT Firewall, OT Switch} kümesi ile tanımlanmıştır. Önerilen modellemeye uygun adımların Tablo 1'de verilen varlıklara göre sırasıyla uygulamaları aşağıda verilmiştir.

Adım 1: Varlıklar arası iletişim matrisinin (M_{AxA}) oluşturulması (Tablo 4): Tablo 4'te verilen Fx değerleri daha önceden ifade edildiği üzere varlıkların birbirlerine sunduğu hizmetleri tanımlayan fonksiyonlardır ve değerlerin hangi fonksiyona karşılık geldiği Tablo 1'de verilmiştir.

Adım 2- Varlıkların mimaride bulunduğu ağ bilgisinin (M_{AxZ}) tanımlanması (Tablo 5): Modellenen mimari 3 farklı güvenlik bölgesi ile yapılandırılmıştır. A1 (SCADA) – A3 (Domain Sunucu) varlıkları, Güvenlik Bölgesi -1 (Z1) içinde ve aynı zamanda bu güvenlik bölgesinde V50 olarak oluşturulan Sanal Ağda yer almaktadır. Aynı güvenlik bölgesinde A4 (EWS) varlığı da bulunmakta, ancak A4 farklı Sanal Ağ yapılandırmasında (V55) olduğu için bu varlıklar arasında haberleşme istenmemektedir. A5 (HMI) ve A6 (PLC) varlıkları ise Güvenlik Bölgesi -3 (Z3) içinde ve aynı zamanda bu güvenlik bölgesinde V41 olarak oluşturulan Sanal Ağda yer almaktadır.

Adım 3: Ağ Segmentasyonunun Belirlenmesi (M_{ZxZ}): Ağ mimarisinin oluşmasını sağlayan ve temel güvenlik parametrelerinden olan ağ segmentasyonu (M_{ZxZ}), Adım 1 ve Adım 2'de oluşturulan tablolar referans alınarak oluşturulmuştur (Tablo 6). Adım 2'deki Sanal Ağ-Güvenlik Bölgesi matrisinde üç farklı güvenlik bölgesi olduğu görülmektedir. Z1 güvenlik bölgesinde SCADA, OPC gibi sunucular bulunmaktadır. Bu sunucular Tablo 1'deki varlıkların Purdue seviyelerine göre gruplandırılmıştır. Aynı bölgede V50 etiketine sahip VLAN yapılandırması olduğu da anlaşılmaktadır. Buna göre ara bağlantı cihazlarından Switch ve Firewall iletişimi sağlayan ağ varlıkları da göz önüne alınarak Tablo 6'daki güvenlik bölgeleri arasındaki iletişim yapısı çıkarımı yapılmıştır. M_{ZxZ} matrisine göre Z1 güvenlik bölgesinin Z2 güvenlik bölgesi ile iletişimi A7 (BT Switch) ve A8 (BT/OT Geçiş Firewall) varlıkları ile sağlanırken, Z3 güvenlik bölgesi ile iletişimi A7-A10 (OT Switch) aralığındaki varlıklar aracılığı ile sağlanmaktadır. Diğer güvenlik bölgeleri Z2 ve Z3 için de aynı mantıkta iletişim yapısı kurulmuştur.

Adım 4: Ağ segmentasyonu ile Purdue modelin seviyelerinin eşleştirilmesi (M_{ZxL}): Bu adımda temel ağ segmentasyonunun EKS mimarilerinde sıklıkla referans alınan Purdue mimarisindeki Seviye karşılığı tanımlanmaktadır (Tablo 7). Z2'nin hiçbir seviyeye ait olmadığı net bir şekilde görülmektedir. Bu durumda Z2'nin bir geçiş güvenlik bölgesi ya da APN (Access Point Name) ağı olduğu çıkarımı yapılabilir. Bu çalışmanın ana katkılarından biri olan Firewall kurallarının proses seviyesinde çıkarımı için Adım 1, Adım 2 ve Adım 3'ten elde edilen bilgiler sonucunda M_{ZxL} matrisi elde edilmiştir. M_{ZxL} matrisine göre Z1 güvenlik bölgesi SCADA, OPC, vb. uygulama sunucularını barındırmasından dolayı Purdue modelin Seviye 3 (L3) bölgesine karşılık gelirken Z3 güvenlik bölgesi Purdue modelin Seviye 1 (L1) ve Seviye 2 (L2) bölgelerini kapsayacak şekilde oluşturuluştur. Z2 geçiş güvenlik bölgesi olduğu için L2-L3 aralığında bulunduğundan herhangi bir seviye ataması yapılmamıştır.

Adım 5: EKS mimarisi/topolojisi ve Firewall kural taslağının çıkarımı: Modelin son adımının işletimi ile öncelikle Şekil 4'te verilen EKS mimarisi ve topoloji çıkarımı yapılmıştır. Çıkarım yapılırken Adım 1, Adım 2 ve Adım 3'te yapılan tanımlar ve elde edilen bilgiler kullanılmıştır. Şekil 4'teki topoloji çıkarımı sonrasında Şekil 4 ve Adım 4'teki bilgiler kullanılarak Firewall cihazlarının üzerinde prosesin işleyebilmesi için gerekli temel kuralların çıkarımı öneri olarak sunulmuştur. Firewall kurallarının çıkarımında Tablo 2 referans alınarak Tablo 8 oluşturulmuştur. Bu bilgiler kullanılarak kurallar belirlenmiş ve önerilen bu mimari için kullanılması gereken kurallar da Tablo 9'da verilmiştir.

Tablo 3. Sunucu ve kontrol cihazları varlıkları (Server and controller assets)

Varlık ID	IT-OT Varlıkları	Varlık Tipi
A1	SCADA	Kontrol Sunucusu
A2	OPC	Uygulama Sunucusu
A3	Domain Sunucu	Uygulama Sunucusu
A4	EWS (Engineering Workstation)	Mühendislik İş İstasyonu
A5	HMI	İnsan-Makine Arayüzü Cihazı
A6	PLC	Kontrol Cihazı
A7	BT Switch	Ağ Cihazı
A8	BT/OT Geçiş Firewall	Ağ Güvenlik Cihazı
A9	OT Firewall	Ağ Güvenlik Cihazı
A10	OT Switch	Ağ Cihazı

Tablo 4. Varlıklar arası iletişim fonksiyonları (Inter-assets communication functions)

Varlık/Varlık	A1	A2	A3	A4	A5	A6
A1	0	0	F20, F21	0	0	F10, F11
A2	0	0	F20, F21	0	F14	F14
A3	F20, F21	F20, F21	0	F20, F21	0	0
A4	0	0	F20, F21	0	F17-F19	F17-F19
A5	0	F3	0	F17-F19	0	F3, F11
A6	F3	F14	0	F17-F19	F3	0

Tablo 5. Sanal ağ- Güvenlik bölgesi matrisi (Vlan-Zone matrix)

Varlık/ Güvenlik Bölgesi	Z1	Z2	Z3
A1 (SCADA)	V50	0	0
A2 (OPC)	V50	0	0
A3 (Domain Sunucu)	V50	0	0
A4 (EWS)	V55	0	0
A5 (HMI)	0	0	V41
A6 (PLC)	0	0	V41

Tablo 6. Güvenlik bölgesi- Güvenlik bölgesi matrisi (Zone-Zone matrix)

Güvenlik bölgesi / Güvenlik bölgesi	Z1	Z2	Z3
Z1	-	A7, A8	A7, A8, A9, A10
Z2	A7, A8	-	A9, A10
Z3	A7, A8, A9, A10	A9	-

Tablo 7. Güvenlik bölgesi -Seviye matrisi (Zone-Level matrix)

Güvenlik Bölgesi /Seviye	L1	L2	L3/L3.5
Z1	-	-	1
Z2	-	-	-
Z3	1	1	-

Tablo 8. Varlık-Varlık matrisi (Asset-Asset matrix)

Varlık/ Varlık	A1	A2	A3	A4	A5	A6
A1 (SCADA)	X	-	LZV (1)	-	-	LZV (8)
A2 (OPC)	-	X	LZV (1)	-	LZV (8)	LZV (8)
A3 (Domain Sunucu)	-	-	X	LZV (2)	-	-
A4 (EWS)	-	-	-	X	LZV (8)	LZV (8)
A5 (HMI)	-	-	-	-	X	LZV (5)
A6 (PLC)	-	-	-	-	-	X

Tablo 9. Proses temelli firewall kuralları (Process-based firewall rules)

Varlık Erişimi	Kural Grubu	Kural Formatı	Örnek İletişim Kanalları (Conduits)
A1(SCADA)'den A6 (PLC)'ya erişim	Proses Kontrol	{A8: Z1-V50<->Z2, A9:Z2<->Z3-V41}	DNP3, Modbus TCP
A2 (OPC)'den A5 (HMI)'e erişim	Saha Cihazı İzleme	{A8: Z1-V50<->Z2, A9:Z2<->Z3-V41}	Modbus TCP
A2'den A6'ya erişim	Proses İzleme, Saha Cihazı İzleme	{A8: Z1-V50<->Z2, A9:Z2<->Z3-V41}	Modbus TCP
A4 (EWS)'ten A5'e erişim	Cihaz bakımı ve Konfigürasyonu	{A8: Z1-V55<->Z2, A9:Z2<->Z3-V41}	Telnet, SSH, http(s)
A4'ten A6'ya erişim	Cihaz bakımı ve Konfigürasyonu	{A8: Z1-V55<->Z2, A9:Z2<->Z3-V41}	Telnet, SSH, http(s)
A3'ten A4'e erişim	Etki alanı kısıtlamaları	{A8: Z1-V50<->Z1-V55}	LDAP

5.2. Test Çalışması-2: CENTER Su Yönetim Sistemi Topoloji Değişikliği
(Case Study-2: CENTER Water Management System Topology Change)

Bu çalışmada önerilen model ve Firewall kural çıkarım yöntemi, gerekli olan matrislerde güncelleme yapılarak değişen EKS mimarilerine de çözüm üretebilmektedir. Bunun için Bölüm 5.1'de oluşturulan topolojiye göre A4 (EWS) varlığının A5 (HMI) varlığı ile aynı seviyede, ancak farklı sanal ağda olacak şekilde ağ konumunun değiştirilmesi durumunda yeni oluşan topoloji ve Firewall cihazlarındaki kural değişiminin çıkarımı aşağıdaki açıklanan adımlar takip edilerek yapılacaktır.

Adım 1: Mimariye yeni işlevi olan bir varlık eklenmemiş olmasından ve sadece bir varlığın ağ konumunun değiştirilmesinden dolayı varlıklar arası iletişim matrisinin (M_{AxA}) oluşturulmasında herhangi bir değişiklik olmayacaktır. Bu yüzden M_{AxA} matrisi, yukarıda verilen Tablo 4 ile aynı olacaktır.

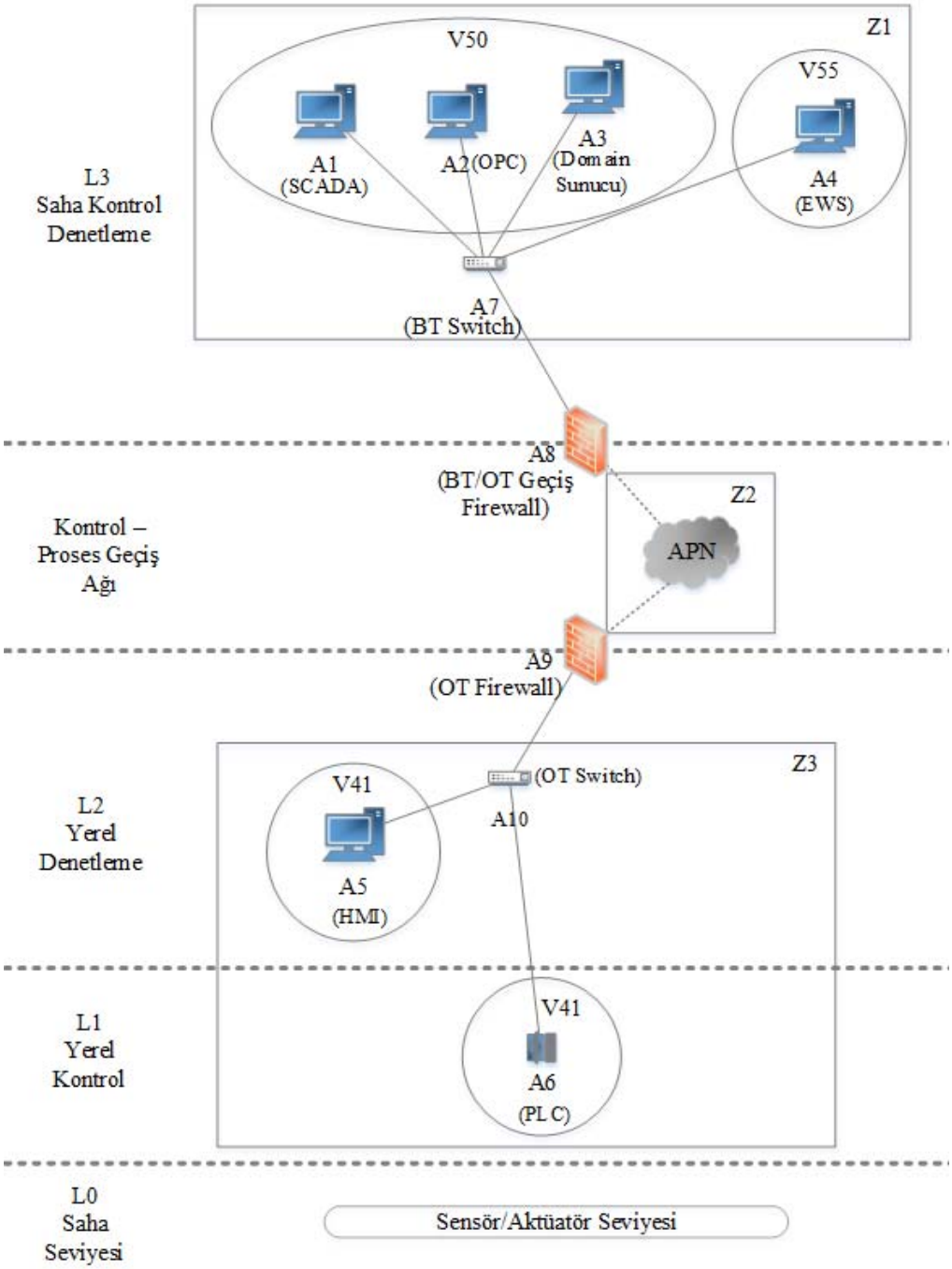
Adım 2: Varlıkların mimaride bulunduğu ağ bilgisinin (M_{AxZ}) tanımlanması: Mimari-1, 3 farklı güvenlik bölgesi ile yapılandırılmıştır. Değişen mimaride A4 varlığı VLAN 55 isimli sanal ağ ortamından çıkarılıp A5 ile aynı seviyede, aynı güvenlik bölgesinde, fakat farklı bir sanal ağ ortamında olduğu için A4 varlığının ağdaki konum değişimi Tablo 10'da kırmızı ile belirtilmiştir. [A4-Z3] hücresinde yazan V30 değeri, A4 varlığının Z3 güvenlik bölgesinde VLAN 30 sanal ağında olduğunu belirtmektedir.

Tablo 10. Sanal ağ- Güvenlik bölgesi matrisi (Vlan-Zone matrix)

Varlık/ Güvenlik Bölgesi	Z1	Z2	Z3
A1 (SCADA)	V50	0	0
A2 (OPC)	V50	0	0
A3 (Domain Sunucu)	V50	0	0
A4 (EWS)	*0*	0	*V30*
A5 (HMI)	0	0	V41
A6 (PLC)	0	0	V41

Bölüm 5.1 Adım 3'te oluşturulan M_{ZxZ} (Tablo 6) matrisinde, mimaride yeni bir güvenlik bölgesi veya Firewall ekleme/çıkarma yapılmadığından herhangi bir değişiklik oluşmaz ve dolayısıyla matris aynı kalır. Benzer şekilde Adım 4'te oluşturulan M_{ZxL} (Tablo 7) matrisinde de yeni bir güvenlik bölgesi eklenmediğinden/değiştirilmediğinden herhangi bir değişiklik oluşmaz ve dolayısıyla matris aynı kalır.

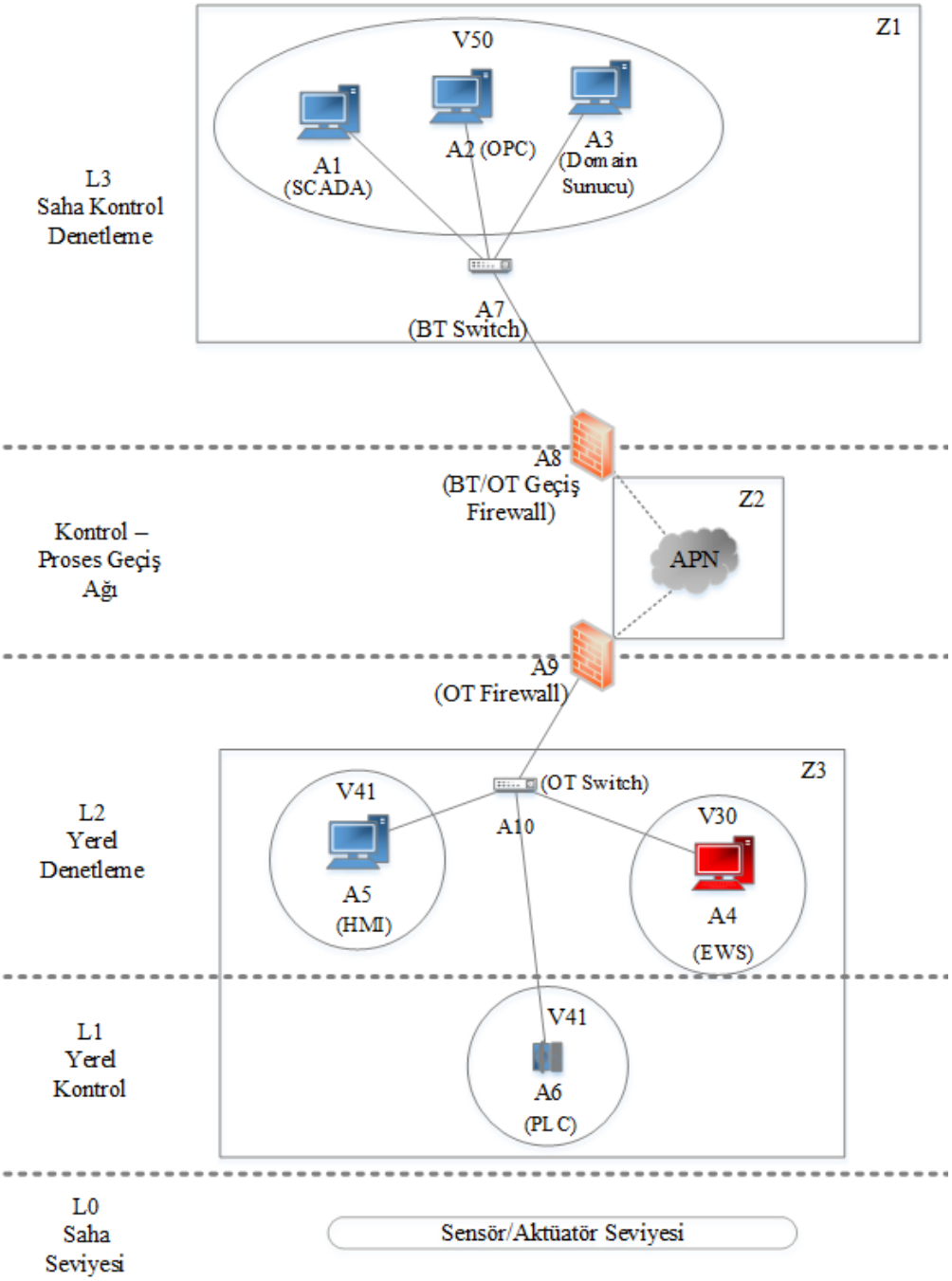
Adım 5: Bu adımda Mühendislik İş İstasyonunun (A4) değişimi ile bu varlıktan hizmet alan diğer varlıkların ağ konumlarına göre Seviye-Güvenlik Bölgesi-Sanal Ağ kapsamındaki Tablo 8 yenilenerek Tablo 11 oluşacak ve varlıklar arası iletişim için gerekli Firewall kural değişimi de ortaya çıkacaktır. Bölüm 5.1'de çıkarılan topolojide (Mimari-1) A3 ve A4 varlıkları için bir erişim kuralı gerekmezken yapılan değişiklik sonucunda yeni oluşan topoloji (Mimari-2) için bir kural eklenmesi (Tablo 12) gerekecektir.



Şekil 4. Topoloji çıkarımı – Mimari-1 (Topology inference-Architecture-1)

Tablo 11. Varlık-Varlık matrisi (Asset-Asset matrix)

Varlık/ Varlık	A1	A2	A3	A4	A5	A6
A1 (SCADA)	X	-	LZV (1)	-	-	LZV (8)
A2 (OPC)	-	X	LZV (1)	-	LZV (8)	LZV (8)
A3 (Domain Sunucu)	-	-	X	*LZV (8)*	-	-
A4 (EWS)	-	-	-	X	*LZV (2)*	*LZV (6)*
A5 (HMI)	-	-	-	-	X	LZV (5)
A6 (PLC)	-	-	-	-	-	X



Şekil 5. Topoloji çıkarımı – Mimari-2 (Topology inference-Architecture-2)

Varlıkların ağ değişikliği sonucu oluşan kurallara göre değişen topolojinin Purdue mimarisi ile uyumlu çıkarımı Şekil 5'te verilmiştir.

Buna göre Bölüm 5.1'de çıkarılan Firewall kurallarında saha cihazlarına erişimi bulunan mühendislik iş istasyonu Purdue L3 seviyesindedir. Tablo 9'da belirtildiği üzere mühendislik iş istasyonu ile saha cihazları arasında http ve telnet gibi açık metin güvenliksiz iletişim sunan protokoller kullanılmaktadır. L3 seviyesinde ağda bulunan herhangi yetkisiz bir kişi/cihaz bu ağ verisini kolaylıkla elde edebilir ve değiştirebilir. Bu bölümde ise mühendislik iş istasyonu L2 seviyesinde bir VLAN'da konumlandırılmıştır (Şekil 5). Bu durum, Tablo 12'de verilen Firewall kurallarının güncellenmesi ile sonuçlanmış ve saha cihazlarına erişim için kullanılan Mühendislik İş İstasyonunun atak yüzeyi, Mimari-1'e göre azaltıldığı için saldırı yayılımından daha az etkilenmesi sağlanmıştır.

5.3. Önerilen Yöntemin Standartlar ile Uyumluluğu
(Proposed Method Compliance with Standards)

Doğru ağ segmentasyonu özellikle OT sistemleri için temel kritik güvenlik kontrolleri arasında yer almaktadır [37]. Güvenli ağ segmentasyonu ile EKS görünürlüğü, varlık tanımlama/yönetimi, endüstriyel DMZ alanları, güvenli proses iletişim mimarisinin oluşumunda temel ve gerekli bir adımdır. Globalde DiD ve EKS

Tablo 12. Proses temelli firewall kuralları (Process-based firewall rules)

Varlık Erişimi	Kural Grubu	Kural Formatı	Örnek İletişim Kanalları
A1(SCADA)'den A6 (PLC)'ya erişim	Proses Kontrol	{A8: Z1-V50<->Z2, A9:Z2<->Z3-V41}	DNP3, Modbus TCP
A2 (OPC)'den A5 (HMI)'e erişim	Saha Cihazı İzleme	{A8: Z1-V50<->Z2, A9:Z2<->Z3-V41}	Modbus TCP
A2'den A6'ya erişim	Proses İzleme, Saha Cihazı İzleme	{A8: Z1-V50<->Z2, A9:Z2<->Z3-V41}	Modbus TCP
A4 (EWS)'ten A5'e erişim	Cihaz bakımı ve Konfigürasyonu	{A9:Z3-V41<->Z3-V30}*	Telnet, SSH, http(s)
A4'ten A6'ya erişim	Cihaz bakımı ve Konfigürasyonu	{A9:Z3-V30<->Z3-V41}*	Telnet, SSH, http(s)
A3'ten A4'e erişim	Etki alanı kısıtlamaları	{A8: Z1-V50<->Z2, A9:Z2<->Z3-V30}*	LDAP

*: Bölüm 5.1'de çıkarılan kurallar, mimari değişimden dolayı Şekil 5'teki topolojiye göre güncellenen yeni kurallar.

Tablo 13. Önerilen yöntemin standartlar ile uyumluluğu (Compliance of the proposed method with standards)

Derinlemesine Savunma Konuları (Desteklenen)	NIST 800-82	IEC 62443	Önerilen Yöntem
Çevre (Perimeter) Güvenliği	-	-	EKS Ağ Topoloji Çıkarımı
Ağ Güvenliği	Ağ Güvenliği	Ağ Segmentasyonu ve Koruma (Sınırlı Veri Akışı)	Firewall Kural Çıkarımı Varlıklar arası iletişimin tanımlanması M_{AxA} Seviye-Güvenlik Bölgesi Matrisi M_{LxZ}
Varlık Sıkılaştırması/Ekipman Güvenliği	Varlık Yönetimi ve Konfigürasyon Kontrolü	Konfigürasyon Yönetimi	EKS Ağ Topoloji Çıkarımı
Uygulama Güvenliği	-	-	Firewall Kural Çıkarımı

güvenlik kontrolleri ile ilgili standartlarda, EKS ağ segmentasyonu ve güvenli mimari için gereklilikler farklı başlıklarda ele alınmıştır. Bu çalışmada geliştirilen EKS modelleme ile ağ mimarisinin çıkarımında elde edilen topoloji ile standartlara göre kontrol edilebilen alanların çıkarımı bu bölüm içerisinde irdelenmiştir. DiD, gizlilik, bütünlük, erişilebilirlik çerçevesinde katmanlı siber güvenlik yaklaşımı sunmaktadır. Kurumların riskleri azaltmasına, tehditleri ele almasına ve güvenlik açıklarını doğru yönetimine yardımcı olan bir yaklaşım sunar [23]. DiD içerisinde istenilen EKS güvenlik düzeyinin (insan, süreç ve teknoloji) karşılanmasıyla ilgili yedi temel gereksinim tanımlanmıştır [9]. Bu çalışmada önerilen EKS mimarilerinin modellenmesi, Purdue uyumlu topolojinin belirlenmesi ve temel Firewall erişim kurallarının çıkarımı ile ilgili metodolojik yaklaşımın DiD, NIST 800-82 ve IEC 62443 katkısı ve uyumluluğu Tablo 13'te verilmiştir.

6. Sonuçlar (Conclusions)

Dijital dönüşümler ile OT sistemlerin yönetilebilirliğini kolaylaştırmak için geliştirilen teknolojiler BT ve OT sistemlerini birbirine yakınlaştırmıştır. Performans ve etkin yönetilebilirlik için bu durum olumlu bir gelişme olsa da siber güvenlik perspektifinden büyük riskleri de beraberinde getirmektedir. Bu çalışmada OT teknolojilerini içinde barındıran EKS ağ mimarilerinin Purdue mimarisi referans alınarak modellemesi yapılmıştır. Modellemeden iki ana önemli sonuç çıkarılmıştır: (i) EKS ağ topolojisinin Purdue mimarisine göre ağ topolojisinin çıkarımı, (ii) Firewall cihazlarında yazılması gereken temel kuralların çıkarımı. Tüm bu süreçlerde EKS mimarilerini oluşturan temel bileşenler olan varlıklar temel alınarak ağ seviyesinde servislerin iletişimine kadar matrisler aracılığı ile matematiksel modeller oluşturulmuştur. Sunduğumuz model ve matris tanımlarının doğruluğunu test etmek için fiziksel test ortamı olan CENTER Su Yönetimi [36] test yatağında bulunan varlık ve ağ mimarileri kullanılmıştır. Geliştirdiğimiz model EKS siber güvenliği temel alınarak oluşturulmuştur. Geçmişte yapılan EKS saldırıları analiz edilmiştir [29, 37]. Bu saldırılarda yanlış ağ segmentasyonu veya yanlış/eksik Firewall kural yazımlarından dolayı BT ağından OT ağına ağ pivot yöntemleri [39] ile saldırılar yapılmış ve bu saldırılar sonrasında da yıkıcı etkiler ortaya çıkmıştır. Bu açıdan EKS mimarilerinin doğru modellenmesi, sürdürülebilir ve izlenebilir olması açısından oldukça önem arz eden bir konudur. Mimari-1 ve Mimari-2 çalışmaları ile EKS için kritik varlıklardan biri olan mühendislik iş istasyonunun ağ konumuna bağlı olarak ilişkili olduğu varlıklar ile iletişiminin erişim kuralları ile değiştiği gözlemlenmiştir. Saha cihazları ile aynı erişim şekline sahip ancak saldırı zorluğundan dolayı saldırı olasılığı ilk topolojiye göre daha azaldığı yorumu yapılabilir. Böylece bu çalışmanın katkılarından biri olan mimarilerin güvenlik perspektifinden değerlendirilmesi için sistemin analiz edilmesi de sağlanmıştır. Varlıkların tanımlanması ve ağ mimarilerindeki iletişimleri, CENTER [1] altyapısındaki Su Yönetimi mimarisi ile karşılaştırılmış ve ilgili altyapıda kullanılan topoloji ve Firewall kuralları ile örtüştüğü belirlenmiştir. Bu model sadece Su Yönetimi için değil aynı zamanda elektrik enerji şebekesi, boru hattı, doğal gaz iletim/dağıtım, LNG (Liquified Natural Gas) gibi farklı kritik altyapıların modellenmesinde de kullanılabilir esnek bir yapı sunmaktadır. Farklı bir kritik altyapının modellenmesinde yapılması gereken ilk adım, ilgili kritik altyapının varlıklarının belirlenmesi olacaktır. Su yönetimi test çalışmasında PLC varlığı kullanılarak model işletilmiştir. Elektrik şebekesi modellenmek istendiğinde bu altyapıda RTU ve IED cihazları yaygın olarak kullanıldığı için bu varlıklar üzerinden modelin işletilmesi gerekmektedir. EKS'de yaygın kullanılan tüm varlıklar ve bu varlıkların farklı özellik ve servisleri ile alakalı tüm bilgiler, bu çalışmanın varlık katmanı modeli bölümünde verilmiştir. Ağ katmanı tarafında ise prosesin işlemesi için de IEC 61850 ve IEC 104 gibi su yönetimi altyapısında kullanılmayan iletişim kanallarının çıkarımı aynı yöntemler ile uygulanabilir. Böylece makalede önerilen varlık ve ağ modellemesi ile farklı proseslere ait Purdue uyumlu topoloji ve Firewall kurallarının çıkarımı sağlanabilir. Ayrıca geliştirilen ağ mimarisi çıkarım modeli ile IEC 62443, NIST 800-82 gibi yaygın kullanılan kritik altyapı sistemlerinde istenen ağ segmentasyonu için uyumluluk kontrolü de modelleme üzerinden yapılabilir. Aynı zamanda ilgili EKS'de herhangi bir cihaz entegrasyonu veya kullanım süresi tamamlanmış ürünlerin değişimi veya kaldırılması gibi süreçlerde, alternatif EKS

mimarilerinin de sunduğumuz model üzerinden doğrulanması, standartlara uygunluğunun sürekli olarak izlenebilmesi ve test edilebilmesi gibi çıktılar da ortaya konmuştur.

Kaynaklar (References)

1. Kritik Altyapılar Ulusal Test Yatağı Merkezi. https://center.sakarya.edu.tr/. Erişim tarihi Şubat 02, 2024.
2. SANS, ICS410 SCADA Reference Model. https://sansorg.egnyte.com/dl/eQu4hT5fCW Yayın tarihi Eylül 1, 2021. Erişim tarihi Şubat 11, 2024.
3. Fortinet. OT asset visibility and network topology. https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/880597/ot-asset-visibility-and-network-topology. Erişim tarihi Şubat 11, 2024.
4. Checkpoint. Blueprint for Securing Industrial Control Systems. https://www.checkpoint.com/downloads/products/cp-industrial-control-ics-security-blueprint.pdf Yayın tarihi Mayıs, 2020. Erişim tarihi Şubat 11, 2024.
5. David Garton. https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf. Yayın tarihi Aralık 12, 2019. Erişim tarihi Mart 15, 2024.
6. Stephen Mathezer. Introduction to ICS Security Part 3. https://www.sans.org/blog/introduction-to-ics-security-part-3/. Yayın tarihi Ekim 1, 2021. Erişim tarihi Mart 15, 2024.
7. Makrakis G. M., Kolias C., Kambourakis G., Rieger C., Benjamin J, Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents, IEEE Access, 9, 165295–165325, 2021.
8. Klaer B., Sen O., Van Der Velde D., Hacker I., Andres M., Henze M., Graph-based model of smart grid architectures, International Conference on Smart Energy Systems and Technologies (SEST), İstanbul- Türkiye, 5-7 Eylül, 2020.
9. ISA. Quick Start Guide: An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control Systems. https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf. Yayın tarihi Haziran, 2020. Erişim tarihi Mart 15, 2024.
10. Casola V., De Benedictis A., Mazzocca C., Montanari R., Designing Secure and Resilient Cyber-Physical Systems: A Model-Based Moving Target Defense Approach, IEEE Trans. Emerg. Top. Comput., 12 (2) 631–642, 2024.
11. Carreño I. L., Scaglione A., Zlotnik A., Deka D., Sundar K., An adversarial model for attack vector vulnerability analysis on power and gas delivery operations, Electr. Power Syst. Res.,189, 106777, 2020.
12. Hou T., Wang T., Lu Z., Liu Y., Combating Adversarial Network Topology Inference by Proactive Topology Obfuscation, IEEE/ACM Trans. Netw., 29 (6) 2779–2792, 2021.
13. Sharma P., Bucci D. J., Brahma S. K., Varshney P. K., Communication Network Topology Inference via Transfer Entropy, IEEE Trans. Netw. Sci. Eng., 7 (1) 562–575, 2020.
14. Testi E., Favarelli E., Pucci L., Giorgetti A., Machine Learning for Wireless Network Topology Inference, 13th International Conference on Signal Processing and Communication Systems (ICSPCS), Australia, 1-7, 2019.
15. Sheng C., Yao Y., Fu Q., Yang W., A cyber-physical model for SCADA system and its intrusion detection, Comput. Networks, 185, 107677, 2021.
16. Elbüz A., Osmanoğlu M., ve Tanrıöver Ö., A SysML-based approach for designing an ideal blockchain-based data trading platform, Journal of the Faculty of Engineering and Architecture of Gazi University. 39 (1), 509–519, 2023.
17. Checkpoint. Claroty Continuous Threat Detection & Check Point Next-Generation Firewall. https://web-assets.claroty.com/resource-downloads/2021_q1_global_check_point_ngfw_integration_brief.pdf. Erişim tarihi Mart 15, 2024.
18. Seno L., Cheminod M., Bertolotti I. C., Durante L. and Valenzano A., Improving performance and cyber-attack resilience in multi-firewall industrial networks, IEEE 18th International Conference on Factory Communication Systems (WFCS), Pavia- Italy, 1-8, 2022.
19. Alicea M., Alsmadi I., Misconfiguration in firewalls and network access controls: Literature review, Futur. Internet, 13 (11), 2021.
20. D. Ranathunga, M. Roughan, P. Tune, P. Kernick, and N. Falkner, ForestFirewalls: Getting Firewall Configuration Right in Critical Networks (Technical Report), Available: http://arxiv.org/abs/1902.05689, 2019
21. Keith Stouffer, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, and Suzanne Lightman, Adam Hahn, Stephanie Saravia, Aslam Sherule, Michael Thompson, Guide to Operational Technology (OT) Security. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf. Yayın tarihi Eylül, 2023. Erişim tarihi Mart 15, 2024.
22. Forescout. How to Effectively Implement ISA 99 / IEC 62443. https://tech-resource.biz-tech-insights.com/landing-pages/Forescout/How_to_Effectively_Implement/how-to-effectively-implement-isa-99-iec-62443-lp.pdf. Erişim tarihi Mart 15, 2024.
23. Ozcelik I., Iskefiyeli M., Balta M., Toker F. S., Testbed Infrastructure Proposal (Center Energy) for Electricity Power Grid and Defence in Depth Practice on The Proposal, IJISS, 11 (2), 52–68, 2022.
24. Uslar M., Rohjans S., Neureiter C., Andrén F.P., Velasquez J., Steinbrink C., Efthymiou V., Migliavacca G., Horsmanheimo S., Brunner H., Strasser T.I, Applying the smart grid architecture model for designing and validating system-of-systems in the power and energy domain: A European perspective, Energies, 12 (2), 2019.
25. Hooshyar H., Vanfretti L., A SGAM-based architecture for synchrophasor applications facilitating TSO/DSO interactions, IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf., Washington DC-USA, 23-26 Nisan, 2017.
26. Elkhawas A. I., Azer M. A., Security Perspective in RAMI 4.0, 13th Int. Conf. Comput. Eng. Syst. Cairo- Egypt, 151–156, 18-19 Aralık, 2019.
27. Ma Z., Hudic A., Shaaban A., Plosz S., Security viewpoint in a reference architecture model for cyber-physical production systems, IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris- Fransa, 153-159, 26-28 Nisan, 2017
28. IEC. IEC 62443 Background. https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62443/. Erişim tarihi Mart 25, 2024.
29. Muhammad Yousuf Faisal. OT Security Dozen Part 3: Network Security Architecture & Segmentation. https://gca.isa.org/blog/ot-security-dozen-part-3-network-security-architecture-segmentation. Erişim tarihi Nisan 15, 2024.
30. Siddhant Shrivastava. BlackEnergy- Malware for Cyber-Physical Attacks. https://itrust.sutd.edu.sg/wp-content/uploads/2016/10/itrust-analysis-blackenergy.pdf Yayın tarihi Mayıs, 2016. Erişim tarihi Ocak 25, 2024.
31. S4Events. Havex Deep Dive. https://www.youtube.com/watch?v=SyupAcnURtA Yayın tarihi Eylül 4, 2017. Erişim tarihi Mart 25, 2024.
32. MITRE ATT&CK. Assets. https://attack.mitre.org/assets/. Erişim tarihi Mart 25, 2024.
33. Michael Assante; Tim Conway; Robert Lee. Analysis of the Cyber Attack on the Ukrainian Power Grid. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf. Yayın tarihi Mart 18, 2016. Erişim tarihi Şubat 5, 2024.
34. CISA. Safety System Targeted Malware (Update B) https://www.us-cert.gov/sites/default/files/documents/MAR-17-352-01 HatMan- Safety System Targeted Malware %28Update B%29.pdf. Yayın tarihi Şubat 27, 2019. Erişim tarihi Şubat 5, 2024.
35. Dragos Inc. CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf. Yayın tarihi 2017. Erişim tarihi Şubat 5, 2024.
36. Ozcelik I., Iskefiyeli M., Balta M., Akpinar K. O., Toker F. S., CENTER Water: A Secure Testbed Infrastructure Proposal for Waste and Potable Water Management, 9th Int. Symp. Digit. Forensics Secur. Elazığ- Türkiye, 1-7, 28- 29 Haziran, 2021.
37. Robert M. Lee, Tim Conway. The Five ICS Cybersecurity Critical Controls. https://sansorg.egnyte.com/dl/R0r9qGEhEe. Yayın tarihi Ekim, 2022. Erişim tarihi Şubat 5, 2024.
38. Joe Slowik. Anatomy of an attack: Detecting and defeating Crashoverride. https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Slowik.pdf. Yayın tarihi Ekim 12, 2018. Erişim tarihi Şubat 5, 2024.
39. Christopher Nourrie. Pivoting Between Corporate IT and OT Networks with Network Shell. https://www.dragos.com/blog/pivoting-between-corporate-it-and-ot-networks-with-network-shell/. Yayın tarihi Eylül 3, 2022. Erişim tarihi Şubat 5, 2024.