T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ZAFİYET VERİTABANLARINA GÖRE TRAFO MERKEZLERİNDEKİ AKILLI ELEKTRONİK CİHAZLARIN FİRMWARE ANALİZÖRÜ

YÜKSEK LİSANS TEZİ

Khouloud GARGOURI

Bilgisayar Mühendisliği Anabilim Dalı

Siber Güvenlik Bilim Dalı

Eylül 2025

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ZAFİYET VERİTABANLARINA GÖRE TRAFO MERKEZLERİNDEKİ AKILLI ELEKTRONİK CİHAZLARIN FİRMWARE ANALİZÖRÜ

YÜKSEK LİSANS TEZİ

Khouloud GARGOURI

Bilgisayar Mühendisliği Anabilim Dalı

Siber Güvenlik Bilim Dalı

Tez Danışmanı: Doç.Dr. Murat İSKEFİYELİ

Eylül 2025

Khouloud GARGOURI tarafından hazırlanan “Zafiyet Veritabanlarına Göre Trafo Merkezlerindeki Akıllı Elektronik Cihazların Firmware Analizörü” adlı tez çalışması 08.09.2025 tarihinde aşağıdaki jüri tarafından oy birliği ile Sakarya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Siber Güvenlik Bilim Dalı’nda Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Jürisi

Jüri Başkanı :	**Prof. Dr. Halit ÖZTEKİN** Sakarya Uygulamalı Bilimler Üniversitesi	.....
Jüri Üyesi :	**Doç. Dr. Murat İSKEFİYELİ** (Danışman) Sakarya Üniversitesi	.....
Jüri Üyesi :	**Dr. Öğr. Üyesi Musa BALTA** Sakarya Üniversitesi	.....

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Sakarya Üniversitesi Fen Bilimleri Enstitüsü Lisansüstü Eğitim-Öğretim Yönetmeliğine ve Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesine uygun olarak hazırlamış olduğum "Zafiyet Veritabanlarına Göre Trafo Merkezlerindeki Akıllı Elektronik Cihazların Firmware Analizörü" başlıklı tezin bana ait, özgün bir çalışma olduğunu; çalışmamın tüm aşamalarında yukarıda belirtilen yönetmelik ve yönergeye uygun davrandığımı, tezin içerdiği yenilik ve sonuçları başka bir yerden almadığımı, tezde kullandığım eserleri usulüne göre kaynak olarak gösterdiğimi, bu tezi başka bir bilim kuruluna akademik amaç ve unvan almak amacıyla vermediğimi ve 20.04.2016 tarihli Resmi Gazete'de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince Sakarya Üniversitesi'nin abonesi olduğu intihal yazılım programı kullanılarak Enstitü tarafından belirlenmiş ölçütlere uygun rapor alındığını, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun ortaya çıkması halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi beyan ederim.

(08/09/2025)

Khouloud GARGOURI

“Hayallerimin peşinden koşmam için beni cesaretlendiren aile ve dostlarıma… İthafımdır.”

TEŞEKKÜR

Öncelikle, bu çalışmayı tamamlamamı nasip eden, bana sağlık, sabır ve güç veren Yüce Allah'a sonsuz şükürlerimi sunarım. Bu yolculuk boyunca karşılaştığım her zorlukta bana dayanma gücü veren ve başarıya ulaşmamı sağlayan O'nun lütfudur.

Yüksek lisans tezimin hazırlanma sürecinde, bana yol gösteren, her aşamada desteğini ve sabrını esirgemeyen değerli danışmanım Doç. Dr. Murat İSKEFİYELİ'ye en içten teşekkürlerimi sunarım. Kendisinin bilgi birikimi, rehberliği ve yönlendirmeleri bu çalışmanın şekillenmesinde büyük rol oynamıştır. Akademik anlamda bana kazandırdığı bakış açısı ve araştırma disiplininin, bundan sonraki çalışmalarımda da yol gösterici olacağına inanıyorum.

Kritik Altyapılar Ulusal Test Yatağı Merkezi'nin (CENTER Energy) geliştirilmesi, uygulanması ve sürdürülmesine katkıda bulunan herkese içten teşekkürlerimi sunarım. Böyle sağlam ve pratik bir deneysel araştırma ortamı oluşturmaya yönelik çabaları, bu çalışmayı önemli ölçüde zenginleştirmiştir. Özellikle deneylerimi böylesine donanımlı ve gerçekçi bir ortamda yürütmeme imkân tanıdıkları için kendilerine teşekkür ederim. Bu ortam, çalışmamın pratik olarak doğrulanmasında kritik bir rol oynamıştır.

Hayatım boyunca yanımda olan, bana koşulsuz sevgi, sabır ve destek veren aileme şükranlarımı sunarım. Zorluklarla karşılaştığımda beni cesaretlendiren, moral kaynağım olan ve her zaman yanımda olduklarını hissettiren ailem, bu süreçte en büyük dayanağım olmuştur. Onların desteği olmasaydı, bu noktaya gelmem mümkün olmayacaktı.

Ayrıca, tez sürecinde moralimi yüksek tutmamı sağlayan, yanımda olduklarını hissettiren ve güzel dostluklarıyla bana güç katan arkadaşlarıma da teşekkür etmek isterim. Bu süreçte beraber paylaştığımız sohbetler, motivasyon ve dayanışma, benim için çok kıymetli olmuştur.

Son olarak, bu tezin hazırlanma sürecinde doğrudan ya da dolaylı olarak katkıda bulunan herkese içtenlikle teşekkür ederim.

Khouloud GARGOURI

İÇİNDEKİLER

Sayfa

KISALTMALAR

ABD : Amerika Birleşik Devletleri

A/D : Analog-Dijital dönüşümü

AZT : Aktif Zafiyet Tarama

BT : Bilgi Teknolojisi

CDC : Common Data Class
Ortak Veri Sınıfı

CID : Configured IED Description
Yapılandırılmış IED Açıklaması

CISA : Cybersecurity and Infrastructure Security Agency
ABD hükümeti, Siber Güvenlik ve Altyapı Ajansı

CPE : Common Platform Enumeration
Ortak Platform Numaralandırması

CVE : Common Vulnerabilities and Exposures
Ortak Güvenlik Açıkları ve Riskler

CVSS : Common Vulnerability Scoring System
Ortak Güvenlik Açığı Puanlama Sistemi

CWE : Common Weakness Enumeration
Ortak Zayıflıklar Sınıflandırması

DA : Data Attribute
Veri Özniteliği

D/A : Dijital-Analog Dönüşümü

DC : Decription
Açıklama

DKS : Distributed Control System
Dağıtılmış Kontrol Sistemi

DO : Data Object
Veri Öğesi

DoS : Denial of Service
Hizmet Reddi

DPL : Device name plate

Cihaz İsim Plakası

EKS : Endüstriyel Kontrol Sistemi

ENTSO-E : European Network of Transmission System Operators for Electricity
Avrupa Elektrik İletim Sistemi İşletmecileri Ağı

EX : Extended Definition
Genişletilmiş tanım

FC : Functional Constraint
İşlevsel Kısıtlama

FDIA : False Data Injection Attack
Yanlış Veri Enjeksiyon Saldırısı

HMI : Human-Machine Interface
İnsan-Makine Arayüzü

ICD : IED Capability Description
IED Yetenek Açıklaması

ICT : Information and Communication Technology
Bilgi ve İletişim Teknolojisi

IEC : International Electrotechnical Commission
Uluslararası Elektroteknik Komisyonu

IED : Intelligent Electronic Devices
Akıllı Elektronik Cihaz

IID : Instantiated IED Description
Örneklenmiş IED Açıklaması

LD : Logical Device
Mantıksal Cihaz

LN : Logical Node
Mantıksal Düğüm

LPHD : Logical node of physical device information
Fiziksel Cihaz Bilgilerinin Mantıksal Düğümü

MU : Merging Units
Birleştirme Üniteleri

NIST : US National Institute Standards and Technology
ABD Ulusal Standartlar ve Teknoloji Enstitüsü

NSM : Network Security Monitoring
Ağ güvenliği izleme aracı

NVD : National Vulnerability Database

Ulusal Güvenlik Açığı Veritabanı

OO : Object-Oriented
Nesne yönelimli

OT : Operasyonel Teknoloji

OUI : Organizationally Unique Identifier
Kurumsal Benzersiz Tanımlayıcı

PDC : Phasor Data Concentrator
Fazör Veri Yoğunlaştırıcıları

PLC : Programmable Logic Controller
Programlanabilir Mantık Denetleyicileri

PMU : Phasor Measurement Unit
Fazör Ölçüm Ünitesi

PZT : Pasif Zafiyet Tespiti

RAS : Remedial Action Schemes
Düzeltici Eylem Planı

SAS : Substation Automation System
Trafo Merkezi Otomasyon Sistemi

SBO : Select Before Operate
Seç ve Sonra İşlet

SCADA : Supervisory Control and Data Acquisition
Denetleyici Kontrol ve Veri Toplama

SCD : Substation Configuration Description
Trafo Merkezi Yapılandırma Açıklaması

SCL : Substation Configuration Language
Trafo Merkezi Yapılandırma Açıklama Dili

SIS : Safety Instrumented System
Güvenlik Enstrümanlı Sistemi

SSD : System Specification Description
Sistem Spesifikasyon Açıklaması

WAN : Wide Area Network
Geniş Alan Ağları

WLS : Weighted Least Squares
Ağırlıklı en Küçük Kareler

XML : eXtensible Markup Language
Genişletilebilir İşaretleme Dili

TABLO LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

ZAFİYET VERİTABANLARINA GÖRE TRAFO MERKEZLERİNDEKİ AKILLI ELEKTRONIK CİHAZLARIN FİRMWARE ANALİZÖRÜ

ÖZET

Modern toplum, kritik altyapılarının düzgün işleyişine büyük ölçüde bağımlıdır. Gelişmekte olan teknolojiler, yüksek yaşam standartlarına katkı sağlarken; sanayileşmiş ülkeler ulaşım, iletişim, finansal işlemler, gıda temini ve sağlık hizmetleri gibi alanlarda bilgi ve iletişim sistemlerine güvenmektedir. Endüstriyel Kontrol Sistemleri (EKS), bu kritik altyapıların izlenmesi, sürdürülmesi ve yönetilmesi açısından hayati öneme sahiptir. Enerji sektöründe ise EKS, elektrik üretimi, iletimi ve dağıtımı süreçlerinde vazgeçilmezdir.

Akıllı Şebeke'nin artan bağlantılı yapısıyla birlikte, koruma, kontrol ve izleme gibi işlevler hızla gelişen iletişim altyapılarına bağımlı hale gelmiştir. Bu dijital entegrasyon, Kritik Altyapıların performansını önemli ölçüde artırmış; hizmet kalitesini yükseltmiş, operasyonel verimlilik sağlamış, otomasyonu desteklemiş ve maliyetleri düşürmüştür. Ancak aynı zamanda, endüstriyel cihazların internete maruz kalmasıyla birlikte siber saldırıların sayısında ciddi bir artışa yol açmıştır. Bu bağlantılı yapı, saldırı yüzeyini genişleterek tehdit aktörlerinin kritik sistemleri tehlikeye atmasını kolaylaştırmıştır. Elektrik şebekesine yönelik iyi planlanmış bir siber saldırı, ciddi ekipman hasarlarına ve yaygın elektrik kesintilerine neden olabilir.

Akıllı şebekeler içerisinde, Akıllı Elektronik Cihazlar (IED'ler), SCADA haberleşmesi, gerçek zamanlı izleme ve istasyonlardaki olaylara özgü veri kaydı gibi işlevleri mümkün kılan temel bileşenlerdir. Ancak bu IED'lerde yerleşik olarak bulunan üretici yazılımları (firmware), çoğunlukla istismar edilebilir zafiyetler içermekte olup, onları siber saldırılar için cazip hedefler haline getirmektedir. Bu zafiyetlerin tespit edilmesi ve giderilmesi, siber güvenlik uzmanları için kritik bir görevdir. Teknik olarak zafiyet tespitleri pasif ya da aktif tarama yöntemleriyle gerçekleştirilmektedir. Yapılan araştırmalar, pasif yöntemlerin genellikle daha verimli olduğunu, daha kısa sürede, doğru sonuçlar verdiğini ve ağda rahatsız edici trafik oluşturmadan çalıştığını ortaya koymaktadır. Bu durum, özellikle aktif tarayıcıların oluşturduğu yoğun trafik nedeniyle dengesizleşebilen ya da durma riski taşıyan EKS ortamlarında büyük önem taşır. Bu nedenle, Pasif Zafiyet Tespiti (PZT), Operasyonel Teknoloji (OT) ortamları için daha uygun kabul edilmektedir.

Her zafiyet tarama sürecinin temelinde, özellikle pasif tarama cihazların doğru şekilde tanımlanması yatmaktadır. Eğer bir cihazın statik özelliklerinden herhangi biri hatalı belirlenirse, zafiyet tarama sonuçları da hatalı olabilir. Bu tür cihaz bilgileri genellikle OT varlık envanterinde tutulur ve her endüstriyel kuruluşun bu envantere sahip olması gerekir. Ancak, özellikle Programlanabilir Lojik Kontrolörler (PLC'ler) ve IED'ler gibi gömülü endüstriyel cihazlar söz konusu olduğunda, eksiksiz ve doğru bir varlık envanterinin sürdürülmesi büyük bir zorluk oluşturmaktadır. Bu zorlukları göz önünde bulunduran bu çalışma, mevcut envanterlerde eksiklikler bulunduğu varsayımıyla, zafiyet taramasına başlamadan önce cihazlara ait üretici,

model, seri numarası ve donanım/yazılım sürümleri gibi detaylı bilgilerin yapılandırma dosyalarından çıkarılmasını amaçlamaktadır.

Bu çalışma, Akıllı Şebeke uygulamaları için özel olarak tasarlanmış, Endüstriyel Kontrol Sistemlerindeki (EKS) IED'lerde zafiyet tespiti amacıyla yarı otomatik ve müdahalesiz bir yaklaşım sunmaktadır. Önerilen yöntem, IEC 61850 standardı ile uyumlu Trafo Merkezi Yapılandırma Dili (SCL) dosyalarını kullanarak IED'lerin üretici, model, donanım ve yazılım/firmware sürümleri gibi statik özelliklerini operasyonel ağlara doğrudan müdahale etmeden çıkarmaktadır. Bu çıkarılan özellikler, cihaz üreticilerinin (örneğin ABB, Siemens) yayınladığı güvenlik duyuruları, Ulusal Zafiyet Veritabanı (NVD) ve Ortak Zayıflık Sınıflandırması (CWE) ile eşleştirilerek her bir IED için kapsamlı bir zafiyet raporu üretilmektedir.

Raporlar, EKS şirketlerinin %60'ından fazlasının ekipmanlarındaki açıkları tespit etmek için üretici güvenlik duyurularına güvendiğini ortaya koymaktadır. Bu çalışma özellikle bu süreci sadeleştirmeye odaklanmakta ve bir veya daha fazla IED için zafiyet raporlamasını otomatikleştiren bir araç sunmaktadır. Bu sayede operatörler zaman ve çabadan tasarruf etmektedir.

Geleneksel Aktif Zafiyet Taraması (AVS) araçlarının yüksek ağ trafiği ya da müdahaleci sorgularla OT sistemlerini bozma riski bulunurken, önerilen Pasif Zafiyet Tespiti (PVD) yaklaşımı, herhangi bir paket enjeksiyonu ya da müdahaleci işlem gerçekleştirmediği için güvenli bir şekilde çalışmaktadır. Üretilen zafiyet raporları yalnızca her bir IED'yi etkileyen bilinen CVE'leri listelemekle kalmaz; aynı zamanda risk puanları, saldırı vektörleri, zayıflık sınıflandırmaları, etkilenen sürümler, üretici tarafından yayınlanan yamalar ve önerilen önlemler gibi kritik meta verileri de içerir. Bu kapsamlı veri seti, operasyon mühendisleri ve siber güvenlik analistlerinin EKS altyapılarının açıklık ve dayanıklılık düzeyini değerlendirmelerine yardımcı olmak amacıyla yapılandırılmış ve aranabilir bir veritabanında toplanmaktadır.

Sistemin deneysel doğrulaması, Sakarya Üniversitesi Ulusal Kritik Altyapılar Test Merkezi (CENTER Energy) bünyesindeki üretim, iletim, dağıtım ve tüketimi kapsayan gerçekçi bir enerji sistemleri test ortamında gerçekleştirilmiştir. ABB'nin REF615, REL650 ve RET670 IED cihazları üzerinde başarıyla test edilmiş ve önerilen çözüm, her cihazı etkileyen bilinen tüm zafiyetleri doğru bir şekilde tespit etmiştir. Sonuçlar, IEC 61850 yapılandırma dosyası analizinin pasif zafiyet tespitiyle bütünleştirilmesinin, trafo merkezleri ve diğer EKS bileşenlerinin siber güvenlik duruşunu güçlendirmede etkili ve uygulanabilir bir yöntem olduğunu göstermektedir.

Bilindiği kadarıyla, bu çalışma, SCL dosyalarından IED bilgilerini çıkarma ve bu bilgileri NVD, CWE ve üretici duyuruları ile zenginleştirerek eyleme geçirilebilir zafiyet değerlendirmeleri oluşturma sürecini uçtan uca otomatikleştiren ilk çalışmadır. Ayrıca bu araştırma, yeniden kullanılabilir ve genişletilebilir bir veritabanı modeli sunarak çoklu cihaz üreticilerini destekleyebilecek şekilde ölçeklenebilir bir yapı ortaya koymakta ve gerçek dünyadaki OT/EKS ortamlarında yaygın olarak uygulanabilirliği mümkün kılmaktadır. Önerilen metodoloji, varlık görünürlüğü ve zafiyet istihbaratının sıklıkla parçalı ve güncel olmayan yapısını bütünleyerek EKS siber güvenliğinde önemli bir boşluğu doldurmaktadır.

Sonuç olarak, bu tez, kritik altyapı ortamlarında zafiyet değerlendirmesi için pratik, ölçeklenebilir ve doğru bir yaklaşım sunmaktadır. Standartlaştırılmış yapılandırma analizini tehdit istihbarat kaynaklarıyla entegre ederek, EKS için otomatik, gerçek

zamanlı ve üretici bağımsız siber güvenlik çözümlerinin gelecekteki gelişimine zemin hazırlamaktadır.

Gelecekteki iyileştirmeler arasında, aracın veritabanının farklı üreticilere ait IED'leri kapsayacak şekilde genişletilmesi ve hem veritabanı oluşturma hem de yapılandırma dosyalarının elde edilmesi süreçlerinin tamamen otomatik hale getirilmesi yer almaktadır.

FIRMWARE ANALYZER OF INTELLIGENT ELECTRONIC DEVICES IN SUBSTATIONS BASED ON VULNERABILITY DATABASES

SUMMARY

Modern society relies heavily on the smooth operation of its critical infrastructure. Emerging technologies contribute to high living standards, while industrialized countries depend on information and communication systems for transportation, communication, financial transactions, food supply, and healthcare services. Industrial Control Systems (ICS) are essential for overseeing, maintaining, and managing these critical infrastructures. In the energy sector, ICS is vital for power generation, transmission, and distribution.

With the increasing interconnectivity of the Smart Grid, functions such as protection, control, and monitoring have become heavily dependent on rapidly evolving communication infrastructures. Substations play a central role in the distribution process by transforming high-voltage electricity into low voltage, and digital substations offer additional advantages such as improved measurement accuracy, ease of configuration, and real-time performance. These substations also incorporate additional digital components, including electronic relays, merging units, SCADA gateways, HMIs, time synchronization devices, and networking equipment.

While this digital integration has significantly enhanced the performance of the energy systems—offering benefits like improved service quality, operational efficiency, automation, and cost savings—it has also led to a surge in cyber-attacks due to the exposure of industrial devices to the internet. This connectivity has broadened the attack surface, giving threat actors more opportunities to compromise critical systems. A well-orchestrated cyber-attack on the power grid could result in severe equipment damage and widespread blackouts.

Within smart grids, Intelligent Electronic Devices (IEDs) serve as essential elements, providing functions such as protection, control, real-time monitoring, measurement, and communication. Categorized into control, monitoring, and protection types, IEDs work together to enhance the reliability, maintainability, and quality of the power system and are generally compatible with protocols such as IEC 61850, Modbus, and DNP3. A single multifunctional IED can simultaneously incorporate protection functions, communication protocols, and monitoring capabilities. However, the widespread adoption of Ethernet and TCP/IP-based communication has exposed these devices to the internet and wide-area networks, leaving them vulnerable to cyberattacks. Compromising an IED can lead to the takeover of substation equipment control, manipulation of measurements, and cascading failures that put the entire grid at risk. Therefore, identifying software vulnerabilities in IEDs and implementing protective measures against them is a vital task for cybersecurity experts.

Technically, vulnerability detections are carried out using either passive or active scanning techniques. Research indicates that passive methods are generally more efficient, providing accurate results with minimal scanning time and without

introducing disruptive traffic into the network. This is particularly important for ICS systems, which are highly sensitive and can be destabilized or shut down by the intrusive traffic generated by active scanners. Therefore, Passive Vulnerability Detection (PVD) is typically more suitable for Operational Technology (OT) environments.

The cornerstone of any vulnerability scanning process—especially passive scanning—is the precise identification of devices. If any static attribute of a device is incorrectly defined, the vulnerability scanning results may be inaccurate. This device information is typically maintained in the OT asset inventory, which every industrial organization should possess. Despite its importance for cybersecurity and vulnerability management, maintaining a complete and accurate asset inventory remains a major challenge—especially for embedded industrial devices like Programmable Logic Controllers (PLCs) and IEDs. Acknowledging these challenges, this study assumes the presence of gaps in current asset inventories and proposes a method to extract detailed device information (such as manufacturer, model, serial number, and hardware/software versions) from configuration files before initiating vulnerability scans.

In the Passive Vulnerability Detection (PVD) method, system components are generally matched with CVE–CPE records. However, this approach has limitations: some CVE entries lack CPE identifiers, there may be gaps or outdated data in CPE–CVE mappings, and inconsistent CPE assignments for the same product can be observed across different sources. Moreover, in security advisories and notices issued by vendors, instead of the devices' CPEs, static information such as models, software and hardware versions, and design standards is provided. For these reasons, in this work, vulnerabilities are identified by matching based on this device information rather than relying on CPE.

IEC 61850 is an international standard designed to standardize communication between Intelligent Electronic Devices (IEDs) in substations. It organizes device data using a hierarchical, object-oriented model, allowing each data object to be uniquely identified and accessed across the network through the MMS protocol. In addition, the standard introduces the Substation Configuration Language (SCL), an XML-based format that describes the configuration of IEC 61850 systems. SCL files serve as comprehensive documentation, detailing device characteristics and the overall system topology.

This work presents a semi-automated and non-intrusive approach to vulnerability detection in IEDs within Industrial Control Systems (ICS), specifically designed for smart grid applications. The proposed method utilizes Substation Configuration Language (SCL) files compliant with the IEC 61850 standard to extract static attributes of IEDs — including vendor, model, hardware, and firmware versions — without requiring direct interaction with operational networks. These extracted attributes are then correlated with publicly available security advisories from device manufacturers (e.g., ABB), the National Vulnerability Database (NVD), and the Common Weakness Enumeration (CWE) database to generate a comprehensive vulnerability report for each identified IED.

Reports reveal that over 60% of ICS companies rely on vendor-issued security advisories to detect flaws in their equipment. This study focuses particularly on streamlining this process, introducing a tool that automates vulnerability reporting for one or more IEDs, helping operators save time and effort.

A three-stage method is proposed for identifying vulnerabilities in IEDs:

- Preparation stage: A comprehensive vulnerability database was created using data obtained from sources such as ABB security bulletins, the NVD, and the CWE. The vulnerability data were stored in a MySQL database.
- Manual operations stage: The IP addresses of the IEDs in the target system were identified through Nmap's ARP scan, after which the SCL files were extracted using IEDExplorer and stored for analysis.
- Automated processing stage: A Python-based program parsed these files to determine the static information of the device, which was then matched with the database to generate device-specific reports containing the relevant vulnerabilities and mitigation recommendations. Additionally, the user may manually enter the information of a device. In this case, the vulnerability detection process is carried out in the same way without parsing SCL files.

Unlike injectionsal Active Vulnerability Scanning (AVS) tools, which may disrupt OT systems due to high network traffic or intrusive queries, the proposed Passive Vulnerability Detection (PVD) approach ensures safe operation by avoiding any packet injection or intrusive actions. The generated vulnerability reports not only list known CVEs affecting each IED but also include critical metadata such as risk scores, attack vectors, weakness classifications, affected versions, vendor-issued patches, and suggested mitigations. This extensive dataset is assembled into a structured and searchable database that can serve both operational engineers and cybersecurity analysts in evaluating the exposure and resilience of their ICS infrastructure.

Experimental validation of the system was conducted using a realistic test environment, the energy systems—covering production, transmission, distribution, and consumption—at the National Critical Infrastructures Testbed Center at Sakarya University (CENTER Energy). It was successfully evaluated on ABB's REF615, REL650, and RET670 IED devices and the proposed solution produced accurate results including all the known vulnerabilities affecting each device. The results highlight the feasibility and effectiveness of combining IEC 61850 configuration parsing with passive vulnerability detection correlation for enhancing the cybersecurity posture of substations and other ICS components.

To the best of our knowledge, this is the first study to automate the end-to-end process of extracting IED information from SCL files and enriching it with data from NVD, CWE, and vendor disclosures to produce actionable vulnerability assessments. Furthermore, this research contributes a reusable and extensible database model that can be scaled to support multiple device vendors, enabling wider applicability in real-world OT/ICS environments. The proposed methodology bridges a crucial gap in ICS cybersecurity, where asset visibility and vulnerability intelligence often remain fragmented and outdated.

In conclusion, this thesis provides a practical, scalable, and accurate approach to vulnerability assessment in critical infrastructure environments. By integrating standardized configuration analysis with threat intelligence sources, it lays the groundwork for future developments in automated, real-time, and vendor-agnostic cybersecurity solutions for ICS.

Future improvements may include expanding the tool's database to include IEDs from various vendors and automating both the database generation and configuration files retrieval processes.

1. GİRİŞ

Kritik Altyapılar, ülke için hayati önem taşıyan ve devre dışı kalmaları veya tahrip olmaları ulusal güvenliği etkileyebilecek tüm sistem ve bileşenleri olarak tanımlanmaktadır (Abedi ve ark., 2019; Pinto ve ark., 2023). Son birkaç on yılda, çeşitli endüstri sektörlerindeki cihaz ve sistemlere kademeli olarak entegre edilen elektronik, bilgi ve iletişim teknolojilerinde önemli gelişmeler yaşanmıştır (Lloret ve ark., 2007). Bu gelişmelerle üretim, ulaşım ve enerji gibi kritik altyapı endüstrilerini destekleyen Operasyonel Teknolojiler (OT), izleme ve kontrol açısından büyük ölçüde bilgi sistemlerine bağımlı haline gelmiştir (Weerathunga ve Cioraca, 2017b). Endüstriyel Kontrol Sistemi (EKS), Operasyonel Teknolojiye (OT) dayanıp Denetleyici Kontrol ve Veri Toplama (SCADA) sistemleri, Dağıtılmış Kontrol Sistemleri (DKS) ve Programlanabilir Mantık Denetleyicileri (PLC) gibi diğer kontrol sistemi yapılandırmalarını temsil etmek için kullanılan genel bir terimdir (Stouffer ve ark., 2015).

Yıllar içinde, bu teknolojiler, sistemler ve bileşenler yüksek gerilim trafo merkezlerinin tüm operasyonel koşullarında güvenilirliklerini kanıtlamıştır. Bu nedenle, trafo merkezi otomasyonu dünya çapında kabul görmüş, bu gelişmelerin çoğu hayata geçirilmiştir ve artık enerji sektörü kuruluşları; güç üretmek, iletmek ve dağıtmak için EKS'lere dayanmaktadır (McCarthy ve ark., 2020). Analog rölelerin yerini dijital cihazlar almıştır ve trafo merkezlerinde kontrol, koruma, izleme ve haberleşme kapasiteleri artmıştır (Lloret ve ark., 2007).

Siber savaş senaryosunda, finans sektörünün yanı sıra enerji sektörü ülkenin güvenliği için en kritik sektör olarak kabul edilir. Bunun sebebi, elektrik şebekesinin; petrol ve doğal gaz, su, ulaşım, telekomünikasyon ve finans sektörleri de dahil olmak üzere diğer kritik altyapı sektörlerini desteklemesi ve güçlendirmesidir. Akıllı şehirlerin, akıllı arabaların ve akıllı evlerin gelişmesiyle birlikte elektriğe olan bağımlılığımız katlanarak artmaya devam etmektedir (Weerathunga ve Cioraca, 2017b).

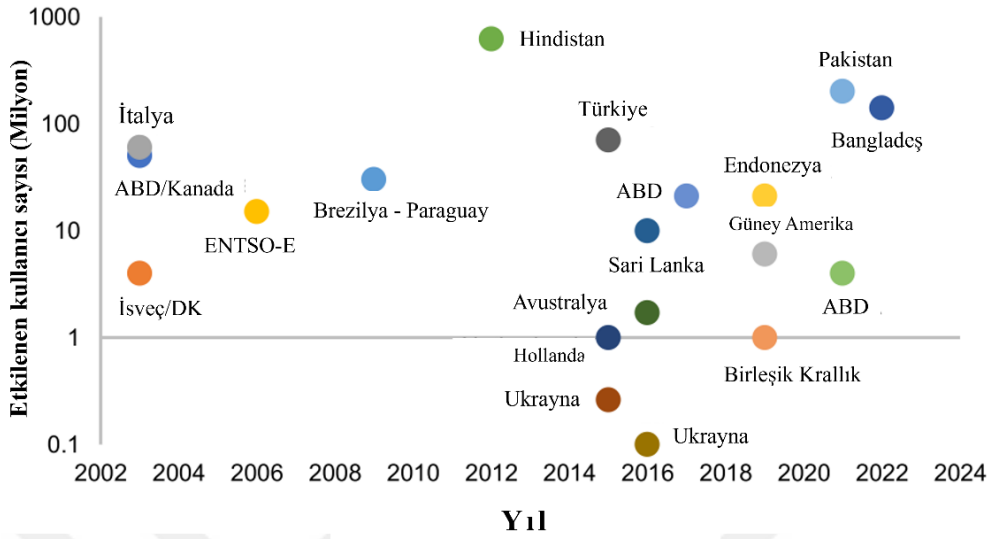
Elektrik enerji sistemleri hem desteklediği kritik altyapı sektörleri hem günlük hayatta kullanıldığı geniş alanlar, hem de şebekesinin kapsadığı büyük coğrafi alanlar göz önüne alındığında ne kadar önemli sistemler olduğu anlaşılır. Türkiye Elektrik İletim A.Ş. (TEİAŞ)'ın istatistiklerine göre şirketin işlettiği elektrik iletim sistemi 2023 yılında 74.441,6 km uzunluğunda bir yüksek gerilim iletim hattından (TEİAŞ, 2024a) ve 2.146 adet trafodan (TEİAŞ, 2024b) oluşmaktadır. Türkiye Elektrik Dağıtım A.Ş (TEDAŞ)'ın istatistiklerine göre ise, 2022 yılında dağıtım hatlarının uzunluğu 1.269.706,4 km'ye ulaşmıştır (TEDAŞ, 2024). Bu, Türkiye enerji dağıtım sistemini Avrupa'nın en büyük üçüncü şebekesi yapmaktadır (Düzgün, 2018).

Elektrik şebekesi, dünya çapında elektrik sağlayan en karmaşık insan yapımı sistemlerden biridir. Ancak, diğer tüm büyük ölçekli sistemler gibi, büyük ölçekli arızalara ve felaketlere maruzdur. Bu sorun, kıtalar ve ülkeler genelindeki elektrik şebekelerinin giderek artan şekilde birbirine bağlanmasıyla daha da kötüleşmektedir. Bu tür arızalar, güç kaynağının kesintiye uğramasına veya temel güç kalitesi gereksinimlerinin karşılanamamasıyla sonuçlanabilir. Sonuç olarak, ulaşım, iletişim, evsel güç kaynağı vb. gibi kamu hizmetlerinde kesintiler meydana gelebilir. Ayrıca, bu kesintiler sistem operatörleri için büyük cezalara yol açmaktadır (Rajkumar ve ark., 2023).

2003-2022 döneminde bazı büyük küresel elektrik kesintilerinin etkilendiği kullanıcı sayısı, kaynak ülke ve yıl bilgileri Şekil 1.1'de gösterilmektedir.

Şekilden de görüldüğü gibi, son 10 yılda dünya çapında birçok önemli elektrik kesintisi yaşanmıştır. 2003 yılında Amerika Birleşik Devletleri (ABD) ve Kanada, 50 milyon kişiyi etkileyen 48 saatlik bir elektrik kesintisi yaşarken, İtalya 60 milyon kişiyi etkileyen 12 saatlik bir elektrik kesintisi yaşamıştır. 2006 yılında, Avrupa Elektrik İletim Sistemi İşletmecileri Ağı (ENTSO-E) bölgesinde 15 milyon kişiyi etkileyen 3 saatlik bir elektrik kesintisi yaşanmıştır. Etkilenen tüketiciler açısından en büyük elektrik kesintisi, 2012 yılında Hindistan'da meydana gelen ve 620 milyon kişiyi etkileyen 15 saatlik şiddetli bir elektrik kesintisi sırasında yaşanmıştır. 2015 yılında Türkiye'de yaklaşık 8 saat süren ve 70 milyon kişiyi etkileyen elektrik kesintileri meydana gelmiştir. Diğer önemli elektrik kesintileri arasında da 2021

yılında Pakistan'da 9 saat süren ve 200 milyon kişiyi etkileyen elektrik kesintileri yer almaktadır (Abedi ve ark., 2019; Rajkumar ve ark., 2023).



Şekil 1.1. 2003-2022 yılları arasında yaşanan küresel elektrik sistemi kesintileri ve toplumsal etkileri (Rajkumar ve ark., 2023).

Elektrik kesintileri; doğal afetler, olumsuz hava koşulları, aşırı yüklenen sistemler vs. gibi kasıtsız nedenlerden meydana gelebileceği gibi kasıtlı olarak fiziksel saldırılar veya hacker ve/veya siber saldırganlar tarafından düzenlenen siber güvenlik saldırının bir sonucu da olabilir (Abedi ve ark., 2019).

Bu karmaşık ve dinamik güç sistemleri ağını izlemek ve kontrol etmek için invertörler, dijital röleler ve fazör ölçüm üniteleri (PMU'lar) gibi çeşitli akıllı elektronik cihazlar (IED'ler) kullanılmaktadır. Ayrıca, üretimden son kullanıcılara kadar akıllı şebekenin fiziksel bileşenleri; fiziksel süreç odaklı kontrol, hesaplama kaynakları ve bilgi teknolojisi tabanlı iletişim sistemlerinden oluşan bir siber ağ ile sıkı bir şekilde bağlantılıdır. Sonuç olarak, güç sisteminin izleme, kontrol ve operasyonlarında siber saldırılar gibi yeni tür beklenmedik durumlar, yüksek sıklıkta meydana gelmektedir (Amin ve ark., 2021).

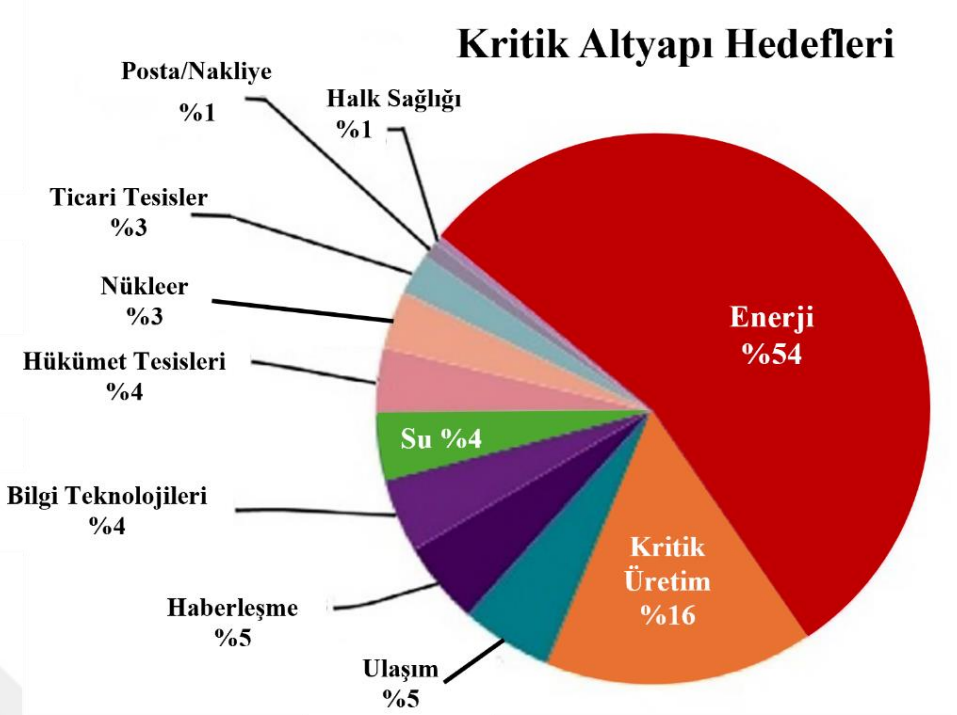
Geleneksel olarak, elektrik güç sistemleri da dahil olmak üzere EKS sistemlerinin ortamları izole edilmiş ortamlardır, iletişim özel hatlar ve belirli kuruluşların sahip olduğu kaynakları açık olmayan veya sınırlı şekilde paylaşılan protokoller üzerinden gerçekleştirilir ve izolasyon ve gizlilik yoluyla bir tür güvenlik sağlanır. Onun için bu sistemler, yıllar önce siber güvenliğe pek önem verilmeden tasarlanmışlardır.

Örneğin, elektrik iletim/dağıtım şirketlerinde fiziksel güvenliğin tek ihtiyaç olduğuna inanmak gibi bir alışkanlık vardı ve bu nedenle, trafo merkezlerine personel erişimi için çok güçlü politikalar geliştirmişlerdir. Bunlar iyi önlemler olsa da günümüz dünyasında yeterli olmaktan çok uzaktır. Bu duruma katkıda bulunan birkaç neden bulunmaktadır (IEEE, 2025; Weerathunga ve Cioraca, 2017a; Xia ve ark., 2020):

- Birincisi, iletişim artık izole değildir. IED'ler, IP tabanlı bir ağ, hatta İnternet üzerinden SCADA ve kontrol sistemleriyle iletişim kurabilir.
- İkincisi, iletişim protokolleri artık özel ve gizli değil. IEC 61850 gibi çeşitli üreticiler arasında birlikte çalışabilirlik sağlamak amacıyla IED protokol iletişimleri için birçok standart geliştirilmiştir.
- Üçüncüsü, kötü amaçlı saldırılarda belirgin bir artış söz konusudur. Artık tehdit aktörleri; sadece amatör saldırganlar veya memnuniyetsiz çalışanlar değil, büyük grupları ve tesisleri etkilemeyi amaçlayan kasıtlı suç ve/veya terörist gruplardır. Bu faaliyetleri engellemek için yalnızca fiziksel güvenlik yetersiz kalır.

Elektrik şebekeleri ve endüstriyel sistemler giderek artan sayıda siber tehditle karşı karşıya olduğundan, kritik altyapılara yönelik siber güvenlik saldırıları artık teorik olarak değerlendirilemez. Son raporlar, operasyonel teknoloji (OT) ortamları, tehdit aktörleri için giderek daha çekici hale geldiğini ve kontrol merkezleri, nükleer santraller ve trafo merkezleri gibi kritik altyapılara yönelik siber saldırılarının sayısı giderek arttığını göstermektedir (Hong ve Liu, 2019; Pöhler ve ark., 2024). ABD'de bildirilen saldırılar üzerine yapılan bir çalışma, saldırı sayısı artmaya devam etse bile Şekil 1.2'nin gösterdiği gibi enerji altyapısının %54 ile saldırıların ana hedefi olduğunu ortaya koymuştur (Kimani ve ark., 2019).

Bir trafo merkezine yönelik doğru tasarlanmış bir saldırı veya aynı anda gerçekleştirilen birden fazla saldırı ekipmanlarda feci hasara ve büyük ölçekli elektrik kesintilerine yol açarak felaketle sonuçlanabilir. Elektrik enerji sistemleri, kendi başına bir kritik altyapıları kategorisi olduğu için, bu durum bir dalgalanma etkisi yaratarak farklı kritik altyapı sektörlerindeki hayati hizmetlerde önemli bir kesintiye yol açarak bir ülkenin güvenliğini tehlikeye atabilir. Bundan dolayı, saldırıları olabildiği kadar engellemek, saldırgan(lar)ın bağlantısını kesmek, trafo merkezlerinin siber güvenliğini ve elektrik şebekelerinin dayanıklılığını artırmak için siber ve fiziksel güvenliği tek bir entegre yapı olarak analiz etmek hayati önem taşımaktadır (Hong ve Liu, 2019).



Şekil 1.2. Siber saldırıların kritik altyapıya etkisi (Kimani ve ark., 2019).

Enerji sistemlerinde zafiyetler; politika ve prosedür, mimari ve tasarım, konfigürasyon, bakım, iletişim ve ağ yapılandırmasındaki eksiklikler ve/veya hatalardan kaynaklandığı gibi kontrol birimindeki cihazların yazılımlarındaki hatalardan da kaynaklı olabilir (Stouffer ve ark., 2023). Tüm güvenlik açıklarını tek seferde çözmek aşılmaz bir engel gibi görünebilir (Alshawish ve de Meer, 2019). Çeşitli kaynaklardan sağlanan bilgiler ışığında, EKS ve enerji sistemlerine özel olarak tasarlanmış cihazlar, deney ve araştırmaların odak noktası olmalıdır. Bunların arasında; İnsan-Makine Arayüzleri (HMI'ler), programlanabilir mantık denetleyicileri (PLC'ler), Uzak Terminal Birimleri (RTU'lar), Ana Terminal Birimleri (MTU'lar) ve Akıllı Elektronik Cihazlar (IED'ler) yer almaktadır (Coffey ve ark., 2018; Hagman ve ark., 2016; Huang ve ark., 2018; Motorola, 2012; Weerathunga ve Cioraca, 2017b). Bu çalışmada, IED'lerin yazılımlarında bulunan güvenlik açıklarının yol açtığı tehditlere karşı korumaya odaklanılacaktır. Bunlar, kötü tasarım ve kodlama nedeniyle yazılıma yanlışlıkla eklenen güvenlik zafiyetleridir.

Akıllı elektronik cihazlar (IED'ler), güç şebekesindeki ve güç ekipmanlarındaki sensörlerden veri alan ve voltaj, akım veya frekans anormallikleri algıladığında devre kesicileri devreye sokmak veya istenen seviyeyi korumak için voltaj seviyelerini yükseltmek/düşürmek gibi kontrol komutları verebilen cihazlardır. Bu cihazlar akıllı

şebekede daha kritik roller üstlendikçe, yazılım güncellemeleri tarafından kolayca saldırıya uğramamasını, sahte bir uzak cihaz tarafından ele geçirilmemesini veya değiştirilmemesini sağlama ihtiyacı artmaktadır (NISTIR 7628, 2014). SANS 2019 OT/EKS Siber Güvenlik Durumu Anketi'ne katılan EKS güvenlik uzmanları, saha kontrol ağ bağlantılarının ve PLC ve IED'ler gibi gömülü bileşenlerin ele geçirilip istismar edilmesi; üretim güvenliği, emniyeti ve süreç bütünlüğü üzerinde en büyük etkiye sahip olduğunu düşünmektedirler (Filkins ve Wylie, 2019). Bu etki 2021 yılında dördüncü sıraya geçmiş olsa da hala risk bileşenlerinin ¾'ünden daha önemlidir (Bristow, 2021).

ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST)'e göre, yama uygulanmamış yazılımlar, bir sistemdeki en büyük güvenlik açıklarından birini temsil eder (IEEE, 2025; Stouffer ve ark., 2015, 2023). Bu zafiyete bağlı olarak, saldırganlar tarafından çeşitli sızma planları uygulanabilir. Örneğin; saldırganlar, kimlik avı (Phishing) veya sahtekarlığı (spoofing) saldırıları yoluyla kötü amaçlı yazılımlar dağıtarak bir bilgisayara veya endüstriyel kontrol sistemine (EKS) erişim sağlayabilir ve sistemin tamamını veya bir bölümünü ele geçirerek operasyonu yanıltabilir veya belirli bir süre devre dışı bırakabilirler. Ayrıca, IED'lerin işlevselliğini uzlaştırarak veya yazılım ve iletişim protokollerindeki kusur ve güvenlik açıklarından yararlanarak güç sistemine yanlış veriler enjekte edilebilir (Amin ve ark., 2021). Bu nedenle, bu cihazların yazılımındaki bilinen güvenlik açıklıklarının mümkün olabildiği kadar en erken zamanda ve kesinlikle saldırganlar harekete geçmeden önce keşfedilmeli, gerekli yamalar yüklenerek ve önlemler alınarak giderilmelidir (Ecik, 2021; Weerathunga ve Cioraca, 2017a). Yamalar uygulanarak ve sistemler güncel tutularak, saldırganların istismar edebileceği güvenlik açığı sayısı sınırlanarak tehdit yüzeyi daraltılabilir (Weerathunga ve Cioraca, 2017b).

Geleneksel sistemlerde, cihaz sayısı az olduğu için ve o kadar varyant olmadığından dolayı yama seviyelerini ve güvenlik açıklarını belirlemek için cihazları tek tek araştırmak kolaydır. Fakat; dijital trafo merkezi teknolojisinin benimsenmesinin kaçırılmaz bir sonucu, trafo merkezlerindeki ortalama elektronik cihaz sayısının artmasıdır. Bir çalışma, dijital trafo merkezindeki toplam cihaz sayısının geleneksel tasarımlara göre 1,5 ile 2 kat daha fazla olacağını tahmin etmektedir (Arnaud ve ark., 2014). Sistem güvenlik açıkları, potansiyel saldırı noktalarının eklenmesiyle; yani cihaz sayısının artmasıyla artmaktadır (NISTIR 7628, 2014). Buna ek olarak, bu

cihazların her biri; tasarım, donanım, yazılım, ek bileşenler, üçüncü taraf işletim sistemleri ve yazılımlar, vs. gibi özellikler açısından farklı olmaları, sistemde çeşitli kötü amaçlı gruplar tarafından istismar edilebilecek güvenlik açıklarının çeşitliğini artırır ve bunların tespit edilmesini geleneksel trafo merkezlerine göre çok daha zor hale getirir. Bu, endüstriyi ve akademiyi zafiyet tespitini otomatik hale getirmek için araştırma yapmaya teşvik etmiştir.

Güvenlik açığı tespitinin yaygın bir yolu, pasif veya aktif tarama yaparak sürekli izleme yapmaktır. Zafiyet yönetimini destekleyen otomatik araçlar genellikle tercih edilse de, aracın bilgileri nasıl topladığını ve bu toplama yönteminin OT sistemlerine zarar verip vermeyeceğini değerlendirmelidir (Stouffer ve ark., 2023). Pasif Zafiyet Tarama (PZT) teknikleri; donamım modeli ve sürümü, yazılım sürümü, işletim sistemi sürümü, vs. gibi sisteme/cihaza özgü özellikleri bilinen güvenlik açıklarının veri tabanlarıyla karşılaştırmaya amaçlarken Aktif Zafiyet Tarama (AZT) araçları, ağ bağlantılı varlıklara bağlanarak bu varlıkları etkileyen olası güvenlik açıklarını belirlemek için bileşenlerin ayrıntılı sorgularını ve analizlerini gerçekleştirir (Samtani ve ark., 2016; Stouffer ve ark., 2023). AZT; yüksek yanlış pozitif oranları, uzun tarama süreleri ve istenmeyen yan etkilere sahip olmaları nedeniyle sıklıkla eleştirilmiştir. Bu yan etkiler arasında, tarama sırasında oluşan yüksek trafik hacimleri ve kullanılan tarama komut dosyalarının müdahaleci (intrusive) doğası nedeniyle ağlarda kesintilere, cihazlarda bozulmalara ve sistemlerde çökmelere yol açmaları da bulunmaktadır (Ecik, 2021; Kennedy ve ark., 2011).

Kesintisiz bir teknik olan PZT; diğer adıyla Taramasız Zafiyet Tespiti, AZT'ye kıyasla önemli ölçüde daha hızlıdır. Dahası, düşük yanlış pozitif oranlarıyla daha fazla güvenlik açığı tespit edebilir (Ecik, 2021). Bundan dolayı, bu çalışmada IED cihazlarının zafiyet raporunu elde etmek için PZT yaklaşımına dayanan bir yöntem kullanılmıştır. Bir PZT tarayıcısı ilgili cihaza ait bulabildiği özellikler kadar iyi tarama yapıp doğru ve kapsamlı sonuçlar verebilir. Bunun için PZT tarayıcıları genellikle ya envanter yönetim sistemlerindeki varlıkların bilgilerinden yararlanır, ya da pasif tarama ve konfigürasyon analizi gibi varlık tespit yöntemlerinden birine başvurur (Ecik, 2021).

EKS sistemlerinin kapsamlı bir varlık envanterinin tutulması zorlu bir süreçtir ve (Filkins ve Wylie, 2019)'te birçok EKS sistemine sahip şirket, özellikle saha kontrol ağlarında bulunan varlıkları ve PLC ve IED gibi gömülü denetleyiciler ve

bileşenlerin ayrıntılarını varlık envanterinde ya eksik bir şekilde yer aldığı ya da hiç yer almadığı ifade edilmiştir. Bu bilgi ile hareketle, bu çalışmada zafiyet taraması yapılacak kuruluşun envanterindeki bilgiler eksik olduğunu ya da güncel olmadığını kabul edip IEC 61850 tabanlı sistemlerin yapılandırmasını tanımlayan SCL dosyalarından faydalanarak IED cihazlarının zafiyetlerinin tespit edilmesine yarayan üretici, model, donanım ve yazılım sürümleri vs. gibi bilgiler elde edilecektir.

ABB (ABB, 2025a), Rockwell Automation (Rockwell Automation, 2025a), Siemens (Siemens ProductCERT, 2025) gibi tüm büyük akıllı elektronik cihaz tedarikçileri, müşterilerini uyarmak için ürünlerini etkileyen güvenlik açıklarını yayınlarlar. SANS'in raporuna göre EKS operatörleri kontrol sistemleri ağlarındaki yazılım ve donanım güvenlik açıklarını tespit etmek için ne kadar pasif ağ izleme, aktif zafiyet tarama, vs. gibi araçlar kullansalar da yine %61.2'si tedarikçilerin ve ilgili kurumların herkese açık olarak yayınladığı güvenlik bildirimleri ve yama dokümanlarını takip ettikleri açıklanmıştır (Bristow, 2021). Bu çalışmada bu süreci otomatikleştirmeyi amaçlayan üreticinin bir IED cihazıyla ilgili yayınladığı güvenlik bildirimlerini kapsamlı bir zafiyet raporu haline dönüştüren bir yaklaşım sunmaktayız. Geliştireceğimiz yarı otomatik araç çıktı olarak sadece o cihaz/cihazların yazılımında bulunan güvenlik açığı listesi değil, buna ek olarak Ulusal Zafiyet Veritabanı (NVD)'deki açıklaması, risk seviyesi, önemi ve atak vektörü, Ortak Zayıflıklar Sınıflandırması (CWE)'ye göre bu zafiyete yol açan yazılım kusurları ve tedarikçinin bu zafiyetle ilgili açıkladığı etkilenen donanım ve yazılım sürümleri, buna karşı geliştirdiği yamalar ve gereksinimleri ve/veya önerdiği önlemler, vs… gibi farklı bilgiler içeren kapsamlı bir zafiyet raporu döndürecektir. Bu amaçla, belirli IED cihazlarının yazılımlarında bilinen zafiyet verilerini bu farklı kaynaklardan bir araya getirecek bir veritabanı oluşturulacaktır.

Temel katkılarımız aşağıdaki gibidir:

- Bildiğimiz kadarıyla tedarikçilerin yayınladıkları güvenlik bildirimleri ve uyarılarını analiz edip IED cihazın donanım ve yazılım özelliklerine göre zafiyet raporu oluşturan tek çalışma budur.
- Hem NVD hem CWE hem de tedarikçinin belgelerinden bir IED cihazında bilinen güvenlik açıklarıyla ilgili bütün bilgileri bir araya getirerek kapsamlı bir veritabanı oluşturulacaktır. Bu bir yandan EKS operatörüne sistemindeki cihazlarla ilgili kapsamlı bir bakış sağlamaktadır. Öbür yandan da bu uygulama

piyasadaki farklı tedarikçilerin çeşitli ürünlerini kapsayacak şekilde geliştirilirse daha kapsamlı bir veritabanı elde edilip sektörün durumuna genel bir bakış sunan bir IED veritabanını oluşturulmuş olur. Bu çaba, akıllı şebeke IED'leri üzerine gelecekteki araştırmalar için kullanılabilir ve farklı kritik altyapı sektörlerinden kuruluşlarının ayrıntılı olarak hazırlanmış ve dağıtılmış IED yazılımlarının güvenliğini değerlendirmeleri için faydalı olabilir.

- Cihazın güvenlik açıklarını filtrelemekte kritik olan cihazın üreticisi, modeli, donanım ve yazılım sürümleri, vs. gibi statik bilgilerini konfigürasyon dosyalarından çekerek bu bilgiler hataya mahal vermeyecek şekilde tespit edilecektir. Bu, aracın daha net ve eksiksiz sonuçlar vermesine yardımcı olacaktır.
- Önerilen yaklaşım varlıkları tanımlamak için konfigürasyon dosyaları, zafiyet tespiti için de pasif bir yöntem kullanacağından doğruluğu korurken cihazlar ve sistemlerin gerçek zamanlı operasyonlarında aksatmalara neden olmayacaktır.
- Deneysel çalışmalarımız, önerilen yaklaşımdan beklenen sonuçları doğru ve eksiksiz bir şekilde elde edildiğini göstermektedir. Bu sonuç manuel analiz ile veritabanını kontrol ederek doğrulanmıştır.

Çalışmanın geri kalanı şu şekilde düzenlenmiştir:

2. bölümde, çalışmanın teorik altyapısını oluşturmak için temel kavramların tanımlarını, kritik altyapılara karşı daha önce yaşanmış saldırıları, IED’lere karşı düzenlenebilecek saldırı türlerini ve bunlara yol açabilecek zafiyet kaynaklarını sunduktan sonra EKS sistemlerinde zafiyet ve varlık taramanın temel yöntemlerini anlamak için öncelikle literatürü sonra da bu yöntemlerin teknik detayları ile avantaj ve dezavantajları incelenecektir. Ardından, IED’lerin haberleşmesini ve cihaz modeli ve işlevlerini standartlaştıran IEC 61850’nin özellikleri ve bu çalışmayla ilişkili yönleri anlatılacaktır.

3. bölümde araştırmanın test ortamı, önerilen yaklaşım ve gerçekleştirimi ayrıntılı olarak açıklanacaktır. Ardından, temel sonuçlar sunulup tartışıldıktan sonra gelecekteki araştırmalar birkaç bir yöne yönlendirme yapılacaktır.

Son olarak, 4. bölümde çalışmanın bulgu ve sonuçlar özetlenip araştırma sonlandırılacaktır.

2. TEKNOLOJİK ALTYAPI

Bu bölüm, bu çalışmanın bir parçası olan ana kavramları tanıtmayı amaçlamaktadır. İlk olarak, Kritik Altyapı, Operasyonel Teknoloji (OT), Endüstriyel Kontrol Sistemleri (EKS), akıllı güç sistemi ve dijital trafo merkezi, akıllı elektronik cihazlar (IED)'lerin tanımı, bunlara yönelik yapılan saldırılar ve bunları güvence altına alınması gereken sistemler yapan özelliklere odaklanılacaktır. Ardından, bu sistemlerin güvenliğiyle ilgili yapılan çalışmaların literatürü gözden geçirilecektir. Son olarak, bu bölümde varlık ve zafiyet taraması ve IEC 61850 standardı teknik açıdan anlatılacaktır.

2.1. Tanımlar

2.1.1. Kritik altyapıları

Kritik altyapının ne olduğu ve kritik altyapı terimini kullanırken hangi altyapılardan bahsettiğimiz konusunda ortak bir anlayış yoktur (Genco, 2020; Henten ve Windekilde, 2020; Pinto ve ark., 2023). Kritik altyapı kavramı ilk kez 1996 yılında dönemin ABD Başkanı Bill Clinton'un imzaladığı 13010 sayılı "Kritik Altyapı Koruması" başlıklı yürütmede (Clinton, 1996) tanıtılmıştır. Söz konusu yürütme; Telekomünikasyon, Elektrik Güç Sistemleri, Gaz ve Petrol Depolama ve Taşımacılığı, Bankacılık ve Finans, Taşımacılık, Su Temin Sistemleri, Acil Durum Hizmetleri (Tıbbi, Polis, İtfaiye ve Kurtarma dahil) ve Hükümetin Sürekliliği olmak üzere 8 kritik altyapı sistemi içermiştir (Clinton, 1996; Henten ve Windekilde, 2020).

Kritik altyapılarının tanımı her ne kadar kaynağa bağlı olarak farklılık gösterse de akademisyenlerin bakış açısına göre, Kritik Altyapılarını toplumun işlevini sürdürmesini sağlayan ve bunun bozulması bir veya birden fazla ulusu etkileyerek sosyoekonomik ve politik bir krize neden olabilecek temel bir ulusal varlık olarak tanımlama konusunda bir fikir birliği vardır (Genco, 2020; Pinto ve ark., 2023).

Ülkeler kendi özellikleri ve çıkarlarıyla uyumlu olarak kendi Kritik Altyapıları tanımlarını yayınlamışlardır. Örneğin, ABD hükümeti Kritik Altyapılarını şöyle tanımlamıştır: Fiziksel veya sanal olsun, Amerika Birleşik Devletleri için o kadar

hayati önem taşıyan sistemler ve varlıklar ki, bu tür sistemlerin ve varlıkların etkisiz hale getirilmesi veya yok edilmesi güvenlik, ulusal ekonomik güvenlik, ulusal kamu sağlığı veya güvenliği veya bu konuların herhangi bir kombinasyonu üzerinde zayıflatıcı bir etkiye sahip olacaktır (Henten ve Windekilde, 2020; NIST, 2018; NIST SP800-53, 2020; A.B.D Hükümeti, 2001). ABD hükümeti, Siber Güvenlik ve Altyapı Ajansı (CISA) aracılığıyla 16 sektörü kritik altyapı olarak tanımlamaktadır. Bunlar; Kimya, Ticari Tesisler, İletişim, Kritik Üretim, Barajlar, Savunma Sanayi Üssü, Acil Durum Hizmetleri, Enerji, Finansal Hizmetler, Gıda ve Tarım, Devlet Tesisleri, Sağlık ve Halk Sağlığı, Bilişim Teknolojileri, Nükleer Reaktörler, Malzemeler ve Atık, Ulaştırma Sistemleri ve Su ve Atıksu Sistemleri Sektörüdür (Henten ve Windekilde, 2020; Stouffer ve ark., 2023).

Avrupa Komisyonu ayrıca terörle mücadelede kritik altyapı korumasına yönelik adımlar atmıştır. 2008/114/EC Direktifte, Kritik Altyapının anlamını ve önemini açıklığa kavuşturarak şöyle ifade etmiştir: Kritik altyapı; Üye Devletlerde bulunan ve hayati toplumsal işlevlerin, sağlık, emniyet, güvenlik, insanların ekonomik veya sosyal refahının sürdürülmesi için elzem olan ve bunların bozulması veya yok edilmesi, bu işlevlerin sürdürülememesi sonucu bir üye devlette önemli bir etkiye sahip olacak bir varlık, sistem veya bunun bir parçası anlamına gelir (Avrupa Birliği Konseyi, 2008).

Türkiye Cumhuriyeti Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı AFAD kritik altyapılarını şu şekilde tanımlamaktadır:

> İşlevini kısmen veya tamamen yerine getiremediğinde çevrenin, toplumsal düzenin ve kamu hizmetlerinin yürütülmesinin olumsuz etkilenmesi neticesinde, vatandaşların sağlık, güvenlik ve ekonomisi üzerinde ciddi etkiler oluşturacak ağ, varlık, sistem ve yapıların bütünüdür (AFAD, 2014a, 2014b).

20 Haziran 2013 tarihinde Bakanlar Kurulu Kararı olarak yayımlanan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013) Siber Güvenlik Kurulu'nca Türkiye'nin kritik altyapıları; Kamu kurumları yanında enerji, su kaynakları, sağlık, ulaşım, haberleşme, ve finansal hizmetler olarak belirlenmiştir.

Kritik altyapıyı oluşturan sistemlerin çağdaş tanımları ve sektörleri bir ülkeden diğerine değişir. Kritik Altyapı'nın tanımlarının daha kapsamlı bir sunumu Smith ve Wilson (2023), INTERPOL (2018) ve Gallais ve Filiol (2017)'de yer almaktadır.

Ayrıca, Amerikan, Afrika, Asya Avrupa ve Pasifik ulus/devletlerinin kritik sektörlerinin listesi (Gallais ve Filiol, 2017) çalışmasında sunulmuştur. Yazarlar 30'dan fazla kritik sektörü belirlemişlerdir. Uzun bir kritik sektör listesi elde edilmiş olsa da bunların en önemlileri şunlardır: Ulaştırma, Enerji, İletişim Teknolojisi, Finans, Su, Gıda, Sağlık, Bilgi Teknolojisi, Savunma, Bankacılık, Acil Durum Hizmetleri ve Hükümettir.

Her kritik endüstrinin kendine ait bir altyapısı olmasına rağmen, bunlar genellikle Operasyonel Teknoloji (OT) kullanarak Endüstriyel Kontrol Sistemlerinden (EKS) oluşur (Pinto ve ark., 2023; Stouffer ve ark., 2023).

2.1.2. Operasyonel teknoloji (OT)

Operasyonel Teknoloji (OT), fiziksel ortamla etkileşime giren veya fiziksel ortamla etkileşime giren cihazları yöneten geniş bir programlanabilir sistem ve cihaz yelpazesini kapsamaktadır. Bu sistemler ve cihazlar; cihazları, süreçleri ve olayları izleyerek ve/veya kontrol ederek doğrudan bir değişikliği algılar veya neden olur. Örnekler arasında endüstriyel kontrol sistemleri, bina otomasyon sistemleri, ulaşım sistemleri, fiziksel erişim kontrol sistemleri, fiziksel çevre izleme sistemleri ve fiziksel çevre ölçüm sistemleri yer almaktadır. OT sistemleri, bir hedefe (örneğin, üretim, madde veya enerjinin taşınması) ulaşmak için birlikte hareket eden kontrol bileşenlerinin (örneğin, elektrik, mekanik, hidrolik, pnömatik) kombinasyonlarından oluşur (Stouffer ve ark., 2023).

OT, kritik altyapı sektörleri olarak tanımlananlar da dahil olmak üzere birçok endüstri ve altyapıda da kullanılmaktadır. OT, sıklıkla fiziksel olarak ve çok sayıda bilgi ve iletişim teknolojisi aracılığıyla birbirine yüksek oranda bağlı ve karşılıklı olarak bağımlı olan kritik altyapıların işletilmesi için hayati öneme sahiptir.

2.1.3. Endüstriyel kontrol sistemleri (EKS)

Endüstriyel Kontrol Sistemi (EKS); Denetleyici Kontrol ve Veri Toplama (SCADA) sistemleri, Dağıtılmış Kontrol Sistemleri (DKS) ve endüstriyel sektörlerde ve kritik altyapılarda sıklıkla bulunan programlanabilir mantık denetleyicileri (PLC) gibi diğer kontrol sistemi yapılandırmaları dahil olmak üzere çeşitli kontrol sistemi türlerini kapsayan genel bir terimdir (Stouffer ve ark., 2023).

Endüstriyel Kontrol Sistemleri (EKS), genellikle elektrik, su ve atık su, petrol ve doğal gaz, ulaşım, kimya, ilaç, kağıt ve kağıt hamuru, gıda ve içecek ve ayrık üretim (örneğin otomotiv, havacılık ve dayanıklı tüketim malları) gibi endüstrilerde kullanılır. Denetleyici kontrol ve veri toplama (SCADA) sistemleri, genellikle merkezi veri toplama ve gözetim kontrolü kullanarak dağıtılmış varlıkları kontrol etmek için kullanılır. Dağıtık Kontrol Sistemleri (DKS), genellikle bir fabrika gibi yerel bir alandaki üretim sistemlerini gözetim ve düzenleyici kontrol kullanarak kontrol etmeyi hedefler. Programlanabilir Mantık Denetleyicileri (PLC) genellikle belirli uygulamalar için ayrık kontrol amacıyla kullanılır ve genellikle düzenleyici kontrol sağlar. Bu kontrol sistemleri, genellikle yüksek oranda birbirine bağlı ve karşılıklı olarak bağımlı sistemler olan altyapıların işletimi için hayati önem taşır (IEEE, 2025; Stouffer ve ark., 2015).

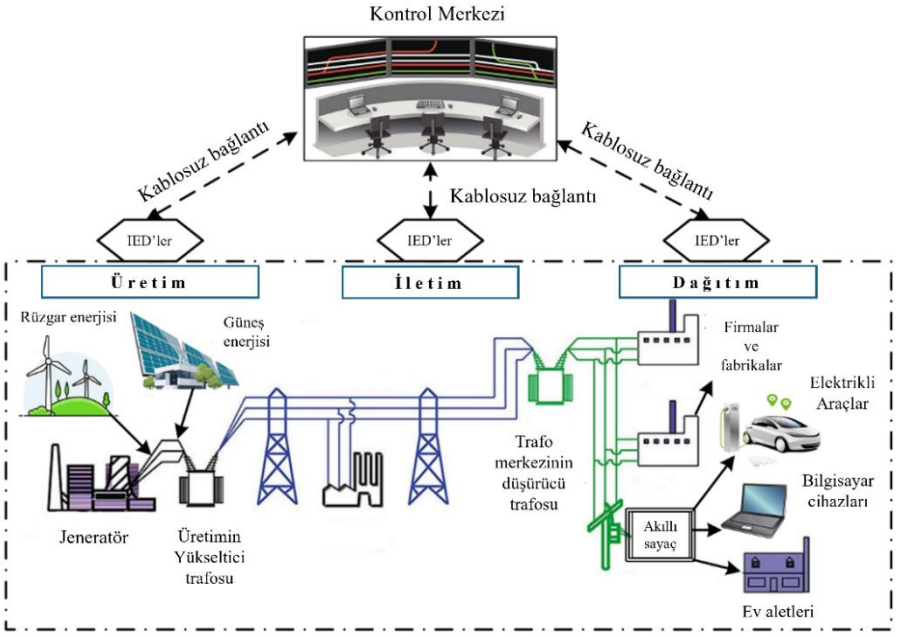
2.1.4. IED tabanlı akıllı güç sistemi ve trafo merkezi

Akıllı güç sistemi, sıkı bir şekilde birbirine bağlı fiziksel ve siber ağlardan oluşan karmaşık bir altyapıdır. Bu büyük ve karmaşık siber-fiziksel ağda, PMU'lar gibi birkaç IED'den oluşan gelişmiş bir ölçüm altyapısı, bir güç sistemi içindeki çeşitli veri yolu ve düğüm noktalarındaki voltajlar, akımlar, güç ve açılar dahil olmak üzere önemli fiziksel nicelikleri izlemek ve ölçmek için kullanılır. IED ile ölçülen tüm veriler, Şekil 2.1'de gösterildiği gibi kontrol kararları almak için yüksek hızlı bir iletişim ağı aracılığıyla kontrol merkezine gönderilir. Kontrol merkezi, alınan ölçüm verilerini işler ve aktüatörlere kontrol komutları gönderir (Amin ve ark., 2021).

Trafo merkezleri, günümüz akıllı şebeke elektrik enerji sistemlerinin en önemli bileşenlerindendir. Bu sistemler, işletimleri için bilgisayar tabanlı uzaktan kontrol ve otomasyona giderek daha fazla bağımlı hale gelmiştir. Trafo merkezleri, güç dağıtım süreci için olmazsa olmazdır. Elektrik enerjisi, elektrik santrallerinde üretilir; ancak çeşitli cihaz ve aygıtları çalıştırmak üzere prizlere ulaşmadan önce genellikle trafo merkezlerinden geçmesi gerekir. Trafo merkezleri, santrallerde üretilen yüksek voltajlı elektriği alır ve dağıtım sistemlerindeki yükü karşılayan daha düşük voltajlı elektriğe dönüştürür (Hong ve Liu, 2019; Shirani ve ark., 2018).

Dijital bir trafo merkezi, gelişmiş ölçüm doğruluğu, cihaz yapılandırma kolaylığı ve gerçek zamanlı performansla sınırlı olmayan birçok avantaj sunar (Rajkumar ve ark., 2020). Geleneksel trafo merkezinde bulunan cihazların yanı sıra dijital trafo

merkezinde ek dijital cihazlar bulunmaktadır. Ek cihazlar şunları içerir: elektronik koruma röleleri, Birleştirme Üniteleri (MU) ve/veya dijital gösterge trafoları, SCADA ağ geçitleri, mühendislik erişimi ve İnsan Makine Arayüzleri (HMI'ler) için endüstriyel PC donanımı, IEEE1588 ana saatler gibi zaman senkronizasyon cihazları, Ethernet yönlendiricileri ve anahtarları gibi ağ ekipmanları, IP Üzerinden Ses (VoIP) telefoni ve IP tabanlı video gözetimi gibi operasyonel destek hizmetleridir (Arnaud ve ark., 2014). Trafo Merkezi Otomasyon Sistemi (SAS), enstrümantasyon ve kontrol cihazları aracılığıyla güç sistemini kontrol eder (Weerathunga ve Cioraca, 2017b).



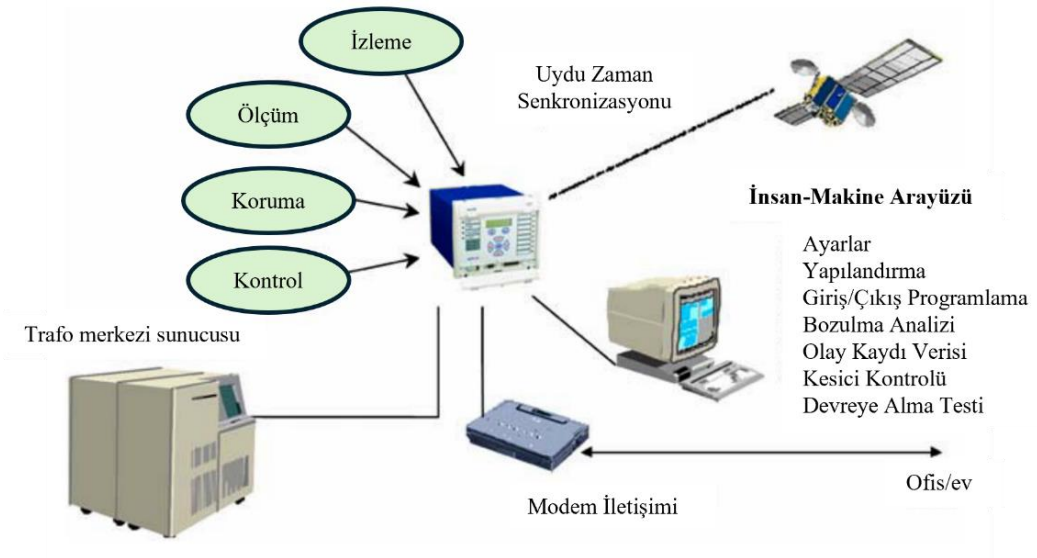
Şekil 2.1. Akıllı elektronik cihaz (IED) tabanlı akıllı güç sistemi (Amin ve ark., 2021).

Trafo merkezlerinin işletimi ve performansı otomasyonla giderek daha verimli hale geldikçe, trafo merkezi güvenliği de oldukça karmaşık hale gelmiştir. Trafo merkezinin fiziksel sistemi, kontrol, izleme ve işletim için siber sisteme dayanmaktadır. Sonuç olarak, trafo merkezlerinin güvenilir bir şekilde çalışması, ilgili siber altyapılara büyük ölçüde bağımlıdır. Trafo merkezlerinin bütünleşmiş siber ve fiziksel sistemi, büyük ve karmaşık bir altyapı oluşturur. Bilgi ve İletişim Teknolojileri (ICT) kullanımının yaygınlaşması nedeniyle, Denetleyici Kontrol ve Veri Toplama (SCADA) sistemleri birbiriyle bağlantılı hale gelmiştir. Bu da siber saldırılara karşı daha yüksek bir güvenlik açığına yol açmaktadır (Hong ve Liu,

2019). Dijital bir trafo merkezine yapılan siber saldırı, bir saldırganın en az bir koruma, otomasyon veya kontrol cihazının hizmetini değiştirdiği, bozduğu veya devre dışı bıraktığı kötü amaçlı bir olaydır. Bu durum, siber saldırıların gerçekleştirildiği yollar ve araçlar, yani saldırı vektörleri konusunda soru işaretleri doğurur (Rajkumar ve ark., 2020). Siber-fiziksel bir sistem olarak, milyonlarca cihazı olan akıllı şebeke sistemi büyük risk altındadır. Çünkü ağdaki bir cihaz ele geçilirse, tüm ağ savunmasız hale gelir. Dolayısıyla, IED tabanlı bir akıllı şebekede çok sayıda cihazın olmasına rağmen, bu cihazları ve içerdikleri güvenlik açıklarını tespit etmek ve cihazları olası risklere karşı savunmak son derece önemlidir.

2.1.5. Akıllı elektronik cihazlar (IED)

Genel tanımı ile IED; elektronik çok işlevli sayaçlar, sensörler, kontrolörler vs. gibi harici bir kaynaktan veri/kontrol alabilen/gönderebilen bir veya daha fazla işlemci içeren bir cihazdır (Hor ve Crossley, 2005; McDonald, 2003). Gelişmiş mikroişlemci ve iletişim teknolojisiyle bu cihazlar; koruma, kontrol, izleme, ölçüm ve iletişim gibi işlevler sağlar (Abdulrazzaq ve Wei, 2018; Hor ve Crossley, 2005). IED'ler, herhangi bir uzaktan güç yönetim sisteminin gözü ve kulağı olarak düşünülebilir ve ortamdaki olanları algılama biçimleri, sistemin güvenilirliği ve etkinliği üzerinde önemli bir etkiye sahiptir. IED kullanımının önemli ekonomik faydaları nedeniyle, elektrik enerji sistemlerinde hızla ana akım ürün haline gelmiştir. Şekil 2.2, geleneksel bir röle şemasıyla ilişkili tüm işlevleri içeren tek bir paket IED'nin yapısını göstermektedir (Hor ve Crossley, 2005).



Şekil 2.2. Akıllı elektronik cihazın genel işlevsel bakışı (Hor ve Crossley, 2005).

Gelişmiş IED'ler, güç sistemlerinin gerçek zamanlı izlenmesini ve kontrolünü sağlamış ve şebekenin güvenilirliğini, bakımını ve güç kalitesini iyileştirmiştir. Enerji sistemlerindeki farklı IED kategorilerinin kısa bir açıklaması aşağıda verilmiştir (Amin ve ark., 2021; Huang ve ark., 2018; Shirani ve ark., 2018; Wang ve Shi, 2018):

- Kontrol IED'leri: Yük atma, devre kesici ve anahtar gibi sistem davranışını uzaktan kontrol etmek için komut gönderir ve alır.
- İzleme ve röle IED'leri: Birincil ekipmandan alınan akımlar, voltajlar, güç değerleri gibi analog girişi, fazör ölçüm üniteleri (PMU'lar) ve fazör veri yoğunlaştırıcıları (PDC'ler) gibi ağ genelinde kullanılabilecek dijital bir formata dönüştürür.
- Koruma IED'leri: Bir trafo merkezinin otomasyon sistemindeki son derece kritik cihazlardır. İletim hattı, bara ve trafo koruması ve doğrudan devre kesici kontrolü gibi koruma ve kontrol işlevlerini yerine getirmek için tasarlanmıştır. Bu cihazların rolü, devre kesicilerini açarak veya uygun koruma şemalarını kullanarak diğer koruma IED'lerle koordine olarak güç sistemindeki bir arızayı tespit etmek ve gidermektir. Ayrıca, operatörden, örneğin; kullanıcı arayüzünden, ağ geçidinden veya kontrol merkezinden bir kontrol komutu alabilir ve iletişim protokolü veya sabit kablolu çıkış (dijital Giriş/Çıkış) aracılığıyla devre kesicileri açıp kapatabilir.

Genellikle, birkaç IED'nin bazı görevleri tamamlamak için birlikte çalışması gerekmektedir. Birlikte çalışabilirliği artırmak için, farklı üreticiler tarafından üretilen IED'ler genellikle Modbus, DNP3, IEC 61850, IEC 60870-5 vb. gibi bazı tescilli olmayan protokolleri destekler (Huang ve ark., 2018; Wang ve Shi, 2018).

Tek bir IED, birçok işlevi barındıran built-in bir mikroişlemci bulundurmaktadır. Yani, çok işlevli bir IED; mesafe, diferansiyel ve aşırı akım olmak üzere koruma fonksiyonlarını, iletişim protokollerini, web sunucusunu ve izlemeyi aynı anda işleme kapasitesine sahiptir (Hong ve Liu, 2019; Wang ve Shi, 2018).

Ethernet ve TCP/IP tabanlı iletişimin kullanımı, IED'lerin veri toplamasını ve kontrol sağlamasını daha verimli hale getirmekle birlikte, IED'leri internete veya geniş alan ağlarına (WAN) açık hale getirecektir. Bu cihazların gerek donanım olarak gerekse yazılım olarak karmaşık yapısı ve geniş kullanım alanları göz önüne alındığında, bu

cihazlarda siber saldırılar başlatmak için kullanılabilecek potansiyel güvenlik açıklarının bulunmasına şaşırmamak lazım (Wang ve Shi, 2018).

Bir IED tehlikeye atıldığında, saldırganlar trafo merkezlerindeki fiziksel varlıkların kontrolünü ele geçirebilir. Anahtar cihazlarının normal işleyişini kesintiye uğratabilir, birincil ekipmanı sabote edebilir ve güç kaynağının istikrarını etkilemek için ölçümleri manipüle edebilirler. Birden fazla ilişkili saldırı aynı anda başlatılırsa, saldırganlar sonuçları genellikle felaket olan ardışık arızalara bile neden olabilir (Wang ve Shi, 2018). Bu nedenle, IED'lerin siber güvenliğini artırmak çok önemli ve bunun için ilk adım bu cihazların yazılımlarındaki zafiyetlerden bilinçli olup bunların istismar edilmesine karşı gerekli önlemleri almaktır.

2.1.6. Güvenlik açığı

NIST, zafiyeti (güvenlik açığını); bir bilgi sisteminde, sistem güvenlik prosedürlerinde, iç kontrollerde veya uygulamada bir tehdit kaynağı tarafından istismar edilebilecek veya tetiklenebilecek bir zayıflık olarak tanımlamaktadır (NIST, 2006). Farklı bir deyişle zafiyet, bir saldırganın güvenlik kontrollerini atlatmasına ve sistemleri geliştiricinin asla amaçlamadığı şekillerde manipüle etmesine olanak tanıyan bir sistem, uygulama veya hizmet içinde bir kusurdur (Ecik, 2021; Samtani ve ark., 2016).

Sızma, elektronik güvenlik çevresinin içerisinden veya dışarısından yapılabilir. Güvenlik açıkları, yayınlanan yazılımda kasıtlı olarak bırakılan arka kapılar veya kötü tasarım ve kodlama uygulamalarının neden olduğu kasıtsız zayıflıklar nedeniyle cihazda bulunabilir. Kasıtlı bir güvenlik açığına örnek olarak, bir programcı hata ayıklama amacıyla aygıt yazılımında bir arka kapıyı açık bırakabilir ve bu, dışarıdan gelen saldırganların hassas donanıma erişmesine olanak tanır. Saldırgan açık arka kapıyı hassas bilgilere erişmek için kullanabilir. Kasıtsız güvenlik açıklarına ise; üretim hataları, programlama hataları veya tasarım kusurları örnek verilebilir (Weerathunga ve Cioraca, 2017a).

Güvenlik açıkları, bir cihazdaki en zayıf noktalardır. Saldırganlar, cihaz iletişimini kesintiye uğratmak veya cihazı tamamen devre dışı bırakmak için bu güvenlik açıklarından yararlanabilirler. Bu nedenle, mevcut bir güvenlik açığından faydalanılarak yapılan bir güvenlik ihlalinin etkisi büyüktür. Keşfedilip açıklanmış bilgi güvenliği açıkları ve riskleri, Ortak Güvenlik Açıkları ve Riskler (CVE) (CVE

Numaralandırma Yetkilisi (CNA), 2000) sisteminde listelenmiştir (Ecik, 2021; Weerathunga ve Cioraca, 2017a).

2.1.7. Zafiyet tespiti

Zafiyet yönetimi, 4 adımlı bir süreçten oluşan genel bir sistem güvenlik programının vazgeçilmez bir bileşenidir. Bu 4 adım şunlardır: zafiyet tespiti, zafiyet doğrulaması, zafiyet değerlendirmesi ve zafiyet giderilmesi. Zafiyet yönetimi sürecinin ilk ve en önemli adımı, zafiyeti olan donanım, yazılım ve firmware'lerdeki bilinen güvenlik açıklarını ve zayıf noktaları tespit etmektir. Bilinen güvenlik açıklarını belirleyerek, güvenlik uzmanlarının sistemlerde mevcut bu zafiyetleri gidermelerine yardımcı olur (Ecik, 2021). Taranacak hedef türlerine bağlı olarak zafiyet tarayıcıları, ağ tabanlı veya cihaz/uygulama tabanlı güvenlik açığı tarayıcıları olarak sınıflandırılabilir (Ecik, 2021; Xia ve ark., 2020). Bu çalışmanın geri kalanında, güvenlik açığı/zafiyet taraması/tespiti terimleri, cihaz tabanlı güvenlik açığı tarayıcılarını ifade edecektir.

2.1.8. Ulusal zafiyet veritabanı (NVD)

Zafiyet veritabanı, bilinen zafiyetler hakkında bilgi toplayan, depolayan ve paylaşan bir platformdur. NVD, 300.000'den fazla CVE zafiyetiyle en büyük ve en yaygın kullanılan zafiyet veritabanı olarak kabul edilir. NVD; zafiyetin açıklaması, risk puanı, önem derecesi, saldırı vektörü, CWE kategorisi vb. gibi özellikleri içeren bir CVE listesine sahiptir (NIST, 2025b). Bu bağlamda, NVD bilinen zafiyetlerin analiz edilmesini kolaylaştırmaktadır.

2.1.9. Ortak zayıflıklar sınıflandırması (CWE)

CWE, güvenlik sorunlarına yol açabilecek yaygın yazılım ve donanım zayıflık türlerinin bir listesidir. Zayıflık, bir yazılım, donanım yazılımı (firmware), donanım veya hizmet bileşeninde, belirli koşullar altında güvenlik açıklarının ortaya çıkmasına katkıda bulunabilecek bir durumdur. Zayıflık koşulları, çoğu durumda, ürünün geliştirilmesi sırasında geliştirici tarafından oluşur. Geliştiricilerin kodlama uygulamaları çok farklı olsa da hepsi aynı yaygın zayıflık türlerini üretebilir ve bu da geliştirdikleri ürünlerde güvenlik açıklarına yol açabilir. CWE Listesi ve ilgili taksonomiler ve sınıflandırma şemaları, bu zayıflıkları (CWE'ler) açısından belirlemek ve tanımlamak için kullanılabilecek bir dil görevi görür (MITRE, 2025).

2.2. Kritik Altyapılarına Yönelik Gerçekleştirilmiş Saldırılar ve Etkileri

Enerji sistemleri de dahil olmak üzere kritik altyapılar, saldırganlar için birincil hedef haline gelmiştir. Olgun tehdit gruplarının sürekli kampanyalarından, hacktivistlerin veya fidye yazılımı operatörlerinin fırsatçı saldırılarına kadar, saldırganlar hedeflerine ulaşmak için OT/EKS ortamlarının potansiyel saldırı vektörleri olarak giderek artan bir farkındalık gösterdiler (Dragos Inc., 2025; Wallace ve Proctor, 2018). Dolayısıyla, kamu hizmetleri hem fiziksel hem de siber saldırılarla karşı karşıya haline gelmiştir. Kritik altyapılara yönelik siber saldırıların oluşturduğu tehlikeleri daha iyi anlamak için, son 20 yıl içerisinde dünya genelinde bazı dikkat çekici rapor sonuçları ve saldırı örneklerini inceleyeceğiz:

2008 yılında Polonya'nın Lodz şehrinde bir tramvay sistemine yönelik saldırı, bir düzine yolcunun yaralanmasına yol açacak kadar büyümüştür. Bu, insan yaralanmasına neden olan ilk siber-kinetik saldırı olmuştur (Kimani ve ark., 2019).

2009 yılında, ABD ve İsrail hükümetleri tarafından oluşturulan ve İran'ın uranyum zenginleştirme cihazlarını hedef alan bir solucanın, İran'daki bir nükleer tesisteki uranyum zenginleştirme santrifüjlerini yok ederek İran'ın nükleer programına önemli zararlar verdiği düşünülmektedir. Stuxnet, elektromekanik süreçlerin otomasyonunu sağlayan programlanabilir mantık denetleyicilerini (PLC'ler) hedef alarak SCADA sistemlerini hedef alan kötü amaçlı bir bilgisayar solucanıdır (Chen ve Abu-Nimeh, 2011; Karnouskos, 2011).

Federal kayıtların incelenmesinde bildirildiği üzere, saldırganların 2010 ve 2014 yılları arasında 150'den fazla siber saldırı düzenleyerek ABD Enerji Bakanlığı bilgisayar sistemlerini başarıyla tehlikeye attığı bildirilmiştir (Reilly, 2015). Yine ABD'de ve 2011 ve 2014 yılları arasında elektrik dağıtım şirketleri, elektrik kesintilerine neden olan 362 hedefli saldırı bildirmiştir. Enerji Bakanlığı'na bildirilen elektrik dağıtım şirketi verilerine göre, bu saldırıların 14'ü siber saldırı, geri kalanı ise fiziksel saldırılardır (CNA Askeri Danışma Kurulu, 2015). Bunlardan; 16 Nisan 2013'te Kaliforniya'daki Pacific Gas and Electric'in (PG&E) Metcalf iletim trafo merkezinde meydana gelen fiziksel saldırıdır. Bu saldırıda, trafo merkezinin yakınından geçen iki fiber optik hat kesilmiş ve trafo merkezlerinin trafolarına 100'den fazla tüfek atışı yapılmıştır (Weerathunga ve Cioraca, 2017b).

Yine 2013 yılında New York'taki Bowman Avenue Barajı'nda bir ihlal gerçekleşmiş; bilgisayar korsanları baraj kapaklarının kontrolünü ele geçirmeyi başarmıştır. Yapılan incelemeler, su akışıyla ilgili ayarları veya hatta su arıtımında kullanılan kimyasal miktarını kolayca değiştirebileceklerini göstermiştir. Bu, felaket sonuçlara yol açabilirdi (Kimani ve ark., 2019).

23 Aralık 2015'te Ukrayna'nın elektrik şebekesi, üç bölgesel elektrik dağıtım şirketine (Oblenergos) düzenlenen uzaktan siber saldırılar nedeniyle yaklaşık 225.000 müşteriyi etkileyen ve birkaç saat süren elektrik kesintileri yaşamıştır (CISA, 2021; ISA, 2017; Kimani ve ark., 2019). Ukrayna elektrik sisteminde, bu siber saldırılar bölgesel dağıtım seviyesine yönelik olup 7 adet 110 kV ve 23 adet 35 kV trafo merkezinin şebeke bağlantısı kesilerek gerçekleştirilmiştir. Saldırganlar, sanal özel ağ (VPN) ve KillDisk ve BlackEnergy adlı kötü amaçlı yazılım virüsleri aracılığıyla dağıtım şirketinin endüstriyel kontrol sistemini başarıyla ele geçirmiştir (Hong ve Liu, 2019; Rajkumar ve ark., 2020; Wang ve Shi, 2018; Weerathunga ve Cioraca, 2017b).

17 Aralık 2016'da yine Ukrayna'da bir siber saldırı daha başlatılmıştır. Bu saldırı, iletim seviyesindeki SCADA sistemini etkileyerek tek bir 330 kV trafo merkezini hedef almıştır. Bu saldırı, dağıtım şebekesinde toplam 200 MW'lık bir yükün kaybedildiği bir elektrik kesintisine neden olmuştur. Bu, elektrik sistemlerini hedef alan ve elektrik kesintisine yol açan ilk kamuya açık kötü amaçlı yazılımdır (Rajkumar ve ark., 2020; Weerathunga ve Cioraca, 2017b).

12 Mayıs 2017'de, Windows'un bir güvenlik açığından yararlanan WannaCry adlı oldukça yıkıcı bir kötü amaçlı yazılım gözlemlenmiştir. WannaCry, özellikle kritik sistemlerde olmak üzere 150 ülkede yaklaşık 250.000 bilgisayarı etkileyip yaklaşık 4 milyar dolar olarak tahmin edilen büyük hasar maliyetlerine yol açmıştır (Alshawish ve de Meer, 2019; Berr, 2017).

Ağustos 2017'de de Triton (Trisis) diye bir kötü amaçlı yazılım, Suudi Arabistan'daki bir petrokimya tesisinin Güvenlik Enstrümanlı Sistemine (SIS) karşı konuşlandırılarak kritik güvenlik kontrolleri devre dışı bırakılmıştır. Bu siber saldırı yalnızca tesisin faaliyetlerini sabote etmekle kalmayıp aynı zamanda insanların ölümüne yol açabilecek bir patlamaya neden olmayı da amaçlamıştır. Neyse ki,

saldırganların kullandığı bilgisayar kodundaki bir hata patlamayı engellemiştir (Kimani ve ark., 2019).

7 Mart 2019'da Venezuela'da Raul Leoni Hidroelektrik Santrali'ne yapılan bir saldırı, ülkenin elektrik sisteminin çökmesine neden olmuştur (Xia ve ark., 2020).

2021 yılında farklı ülkelerdeki farklı kritik altyapılarına karşı önemli saldırılar düzenlenmiştir. Bunlardan; Mayıs'ta ABD'deki Colonial Pipeline'ın büyük yakıt boru hattında konuşlandırılan DarkSide isimli fidye yazılımı saldırısıdır. Saldırganlar, bu hattın operasyonlarını durdurarak ABD'nin Doğu Kıyısı genelinde yakıt kıtlığına neden olmuştur. Saldırı BT sistemlerini etkilemesine rağmen ihtiyati tedbir olarak boru hattının kapatılmasına yol açmıştır (Kamu Güvenliği İstihbarat Teşkilatı, 2022). Bu saldırının yanı sıra, Temmuz'da Durban ve diğer yerlerdeki Transnet firmasının konteyner terminallerini vuran bir fidye yazılımı saldırısı, yakıt ve mal taşımacılığına sıkı sıkıya bağlı lojistik altyapısını bozmuştur ve Güney Afrika'nın en kötü altyapı saldırılarından biri olmuştur (Timcke ve ark., 2023).

2022'nin başlarında, Almanya, Belçika ve Hollanda genelindeki 17 petrol rafineri terminaldeki sistemler siber saldırılar sonucunda ele geçirilmiştir. Bu durum, ARA merkezinden kargo hareketini geciktirmiş ve artan jeopolitik gerginlikler sırasında tedarik zincirlerine yük bindirmiştir (Tidy, 2022).

2024 yılında, saldırgan siber faaliyetler devam eden jeopolitik çatışmalarla bağlantılı olarak hareket ettiği görülmüştür (Dragos Inc., 2025). Hacktivistler de dahil olmak üzere tehdit grupları, kendi taraflarının hedeflerine uygun daha açık siber operasyonlara yönelirken, daha olgun gruplar yıkıcı etkiler yaratmaya çalışmıştır. Örneklerin arasında; Ukrayna'daki bir belediye enerji şirketine yapılan ve yüzlerce apartmanın ısıtma sistemini bozan siber saldırı (GRAHAM ve ark., 2024), Ukrayna yanlısı Blackjack grubunun gerçekleştirdiği Rusya'daki kritik altyapı izleme cihazlarına zarar veren saldırı (Radiflow, 2024), ve İran yanlısı CyberAv3ngers İsrail'deki yakıt yönetim sistemlerine karşı düzenlenen saldırıdır (Lyons, 2024) bulunmaktadır.

Ayrıca, ABD'nin Siber Tehdit İstihbarat Entegrasyon Merkezi'nin (CTIIC, 2024) raporunda 23 Kasım 2023 ile 24 Nisan 2024 arasındaki 5 ay içerisinde İran bağlantılı ve Rusya yanlısı siber aktörler; gıda ve tarım, sağlık, su ve atık su yönetimi, enerji, telekomünikasyon, eğitim, eyalet ve yerel yönetimler ve özel sektör üretimi

sektörlerindeki ABD'nin kritik EKS sistemlerine karşı toplamda 36 saldırı düzenleyerek erişim sağlamayı ve bazı durumlarda manipüle etmeyi başarmışlardır.

Endüstriyel Kontrol Sistemleri Siber Acil Durum Müdahale Ekibi'ne ICS-CERT, 2025'e göre, 2025 yılının ilk çeyreğinde dünya genelinde çeşitli endüstriyel sektörlerden kuruluşlarda siber saldırıların neden olduğu yaşandığı açıklanmıştır. Bu saldırılar, gizli verilerin kaybına ve BT hizmetlerinin ve ürün üretimi ve tedariki de dahil olmak üzere temel operasyonel süreçlerin kesintiye uğramasına neden olmuştur. Çeyreğin en dikkat çeken olayı, kalkış ve varış panoları, check-in terminalleri ve bagaj taşıma sistemleri de dahil olmak üzere birçok bilgi sisteminin 10 saat boyunca devre dışı kalmasına neden olan Kuala Lumpur Havalimanı saldırısıydı.

Dragos Inc., (2025) 2025 OT/EKS Siber Güvenlik Raporu'nda ise endüstriyel kuruluşlara yönelik fidye yazılımı saldırıları bir önceki yıla göre %87 arttığı, tüm fidye yazılımı saldırılarının %69'u 26 farklı üretim alt sektöründeki 1.171 üretim kuruluşunu hedef aldığı açıklanmıştır.

Bu saldırılar, raporlar ve istatistikler, akıllı şebekeler de dahil olmak üzere kritik altyapılara yönelik siber saldırıların potansiyelini ve ciddiyetini ve bu sektörlerdeki siber güvenliğin önemini açık bir şekilde göstermektedir. EKS sistemlerinin siber güvenliğinin önemli bileşenlerinden olan zafiyet tarama çalışmaları, sistemdeki güvenlik açıklarını siber saldırganlar tarafından istismar edilmeden önce tespit ederek siber saldırıları önlerler. Sonuç olarak, EKS/OT sistemlerinin varlık ve zafiyet taraması/yönetimi önemli bir araştırma alanı olarak ortaya çıkmıştır.

2.3. IED'lere Yönelik Siber Saldırı Türleri

Bir cihaza karşı yapılan bir saldırı, bir şebeke ağ cihazını ele geçirmeyi ve kontrol etmeyi amaçlar. Genellikle, ele geçirilen bir cihazın giriş noktası olarak kullanıldığı ve daha fazla saldırı başlatılarak akıllı şebeke ağının geri kalanının tehlikeye atıldığı büyük bir saldırının ilk adımıdır (Kimani ve ark., 2019). Aşağıda IED cihazlarına karşı bazı siber saldırı türleri anlatılacaktır:

2.3.1. Aktüatörlerin doğrudan kontrolü

Saldırganlar bir trafo merkezinin teknik özelliklerine erişebilirse, siber saldırı başlatmaları için en basit yol, kendilerini yetkili operatörler gibi gösterip devre kesiciler gibi aktüatör IED'lerine komutlar göndermek olabilir. Bu tür bir saldırıyı başlatmanın birçok olası yolu vardır. Bir aktüatörü ele geçirerek saldırganlar aynı anda birden fazla elektrik kesintisine neden olabilirler. Arıza sonrası kontrol stratejileri beklendiği gibi çalışmazsa, bu durum ardışık arızalara bile yol açabilir (Wang ve Shi, 2018). 2007 yılında, bir kesicinin kasıtlı olarak açılıp kapatılmasıyla bağlı döner ekipmanın faz dışı çalıştırılmasını sağlayarak Aurora güvenlik açığı ortaya çıkarılmıştır (Salmon ve ark., 2009). 2015 Ukrayna elektrik sistemine karşı yapılan saldırılar, birden fazla saldırgan tarafından işletim sistemi düzeyinde mevcut uzaktan yönetim araçları veya sanal özel ağ (VPN) bağlantıları üzerinden uzaktan endüstriyel kontrol sistemi (EKS) istemci yazılımı kullanılarak kesicilerin kötü amaçlı uzaktan çalıştırılmasıyla başlatılmıştır. Saldırganların uzaktan erişimden önce geçerli kullanıcı bilgileri elde ettiği düşünülmektedir (NCCIC, 2016).

2.3.2. Ölçüm manipülasyon saldırıları

Otomatik üretim kontrolü, otomatik voltaj regülasyonu, optimum güç akışı ve geçici kararlılık değerlendirmesi gibi enerji yönetim sistemlerindeki birçok uygulama, güç sistemlerinin durumundan farkında olmak ve kontrol kararları almak için büyük ölçüde doğru ölçümlere dayanır. IED'lerden alınan ölçümler manipüle edildiğinde, istenmeyen kontrol eylemleri gerçekleştirilebilir ve bu da kararlı güç kaynağını tehdit edebilir (Sridhar ve Govindarasu, 2014). Operatörler yanıltılırsa, manuel işlemler etkileri daha da kötüleştirebilir. İki tür tipik ölçüm manipülasyon saldırısı olan Yanlış Veri Enjeksiyon Saldırısı (FDIA) ve Tekrarlama Saldırısı (Diğer adıyla; Yeniden Oynatma Saldırısı) aşağıda tartışılmaktadır:

Başlangıçta ağırlıklı en küçük kareler (WLS) tabanlı durum kestirimi için önerilen Yanıltıcı Veri Enjeksiyon Saldırıları (FDIA) (Youssef ve Labeau, 2018), kısa sürede enerji sistemleri siber güvenliği alanında en popüler konulardan biri haline gelmiştir. Bu saldırı türüyle, stratejik olarak seçilmiş bazı ölçüm verilerinin ele geçirilmesiyle, hatalı veri tespit mekanizmalarının atlatılarak durum kestirimlerine sahte veriler enjekte edilebilir. Saldırganlar, kârlarını en üst düzeye çıkarmak için FDIA'lar

elektrik piyasaları alanına dahil edilebilirler (Mangalwedekar ve ark., 2015; Wang ve Shi, 2018).

Tekrarlama saldırısıyla, saldırganların sensörleri ele geçirip okumalarını belirli bir süre kaydedip daha sonra tekrar oynatabilirler. Normal ölçümlerin görüntülenmesi, operatörlerin anormal durumlara karşı dikkatli olmalarını engelleyebilir. Buna karşılık, gerçekte bir arızanın olmaması halde operatörler ekranda bir yerde bir arızanın olduğunu ve otomatik olarak giderilmediğini görürlerse, röle koruma sisteminin arızalı olduğunu düşünebilir ve buna müdahale etmeye çalışırlar. Otomatik kontrol sürecini veya insan operatörlerini yanıltarak, bu tür bir saldırı güç sistemleri üzerinde ciddi sonuçlara yol açabilir (Tran ve ark., 2013; Wang ve Shi, 2018).

2.3.3. Kaynak tükenmesi ve tepki geciktirici siber saldırılar

Saldırganlar, IED'lere çok sayıda gereksiz paket göndererek yalnızca iletim yollarını tıkamakla kalmaz, aynı zamanda cihazların iletişim ve hesaplama kaynaklarını tüketerek devre dışı bırakabilirler (Kalluri ve ark., 2016; Wang ve Shi, 2018). Böylece, yasal paketler bu cihazlar tarafından zamanında aktarılamaz ve işlenemez; bu durum Hizmet Reddi (DoS) olarak bilinir. Birçok güç sistemi de dahil olmak üzere EKS uygulaması gecikmeye duyarlıdır. Örneğin, düzeltici eylem planları (RAS'ler), önceden belirlenmiş sistem koşullarını algılar ve küçük bir kesintinin büyük ölçekli bir olaya yayılmasını azaltmak için otomatik düzeltici eylemlerle yanıt verir. Bu tür eylemler genellikle yük veya üretim kesintisi ve sistem yapılandırmalarında değişiklikleri içerir. RAS'ler zaman gecikmelerine karşı son derece hassastır ve genellikle 50 ms mertebesinde olan katı zamanlama gereksinimlerine sahiptir (Ashok ve ark., 2017). Bu nedenle, veri iletimindeki gecikme, ilgili fiziksel sistemleri etkileyecektir (Wang ve Shi, 2018).

2.3.4. Zaman senkronizasyon saldırısı

Elektrik şebekelerinde arıza tespiti, olay yeri tespiti, gerilim kararlılığı izleme ve dalga koruma gibi birçok işlem, hassas zamanlama bilgilerine bağlıdır. Şebeke genelinde zaman referansı olarak GPS zamanı uygulandığında, akıllı şebekedeki tüm IED'ler senkronize olarak çalışabilir. Saldırganlar, gerçek GPS sinyallerinin alımına müdahale ederek ve sahte GPS sinyalleri ekleyerek örnekleme zaman damgasını değiştirebilirse, söz konusu güç sistemi uygulamaları artık düzgün çalışamaz (Z.

Zhang ve ark., 2013). GPS sinyallerinin iletim mesafeleri çok uzun olduğundan, GPS alıcılarının yerleşik uydu saatini kalibre etmek için saat ofsetini hesaplaması gerekir. Saldırganlar sahte bir GPS sinyalini simüle edip bir IED'nin GPS alıcısının, gerçek GPS sinyalini kademeli olarak bastırarak yeni sinyale bağlanmasına neden olursa, hesaplanan alıcı saat ofseti yanlış olabilir (Jiang ve ark., 2013). GPS tabanlı olmayan IED'ler için, sorunlu A/D ve D/A dönüşümü nedeniyle zaman senkronizasyonu kaybı da meydana gelebilir (Corcoran ve Melvin, 2011).

2.3.5. Röle koruma şemalarına yönelik saldırılar

Son araştırmalar, bağımsız röle IED'lerini kontrol etmenin yanı sıra, röle koruma şemalarına yönelik dikkatlice planlanmış saldırılara da dikkat çekmiştir. Düğüm arızaları çok sayıda jeneratör, yük ve hattın bağlantısını keserek sistem istikrarsızlığına neden olur. Bundan dolayı, veri yolu diferansiyel koruması önemli bir röle koruma şeması olarak kabullenmiştir. Saldırı alanını stratejik olarak belirleyerek saldırganlar saldırı beklentilerini en üst düzeye çıkarabilirler (Bulbul ve ark., 2014; Wang ve Shi, 2018). Yeni önerilen ajan tabanlı röle koruma şemalarında, eş (peer) röleler, yerel röle sensörleri bir sorun algıladığında hangi eylemin gerçekleştirileceğine karar vermek için birbirleriyle bilgi alışverişinde bulunur. Bu röle IED'leri arasındaki iletişim, normal hatları devre dışı bırakmayı amaçlayan siber saldırıların hedefi olabilirler (Rahman ve ark., 2014; Wang ve Shi, 2018; J. Zhang ve Dong, 2017).

2.4. IED'nin Bazı Güvenlik Açığı Kaynakları

Saldırganlar, IED de dahil olmak üzere bir cihaza bir siber saldırıyı başlatmak için o cihazda bulunan bir veya birden fazla zafiyetlerden yararlanırlar. Tablo 2.1'de, IED'lere özgü bazı güvenlik açığı kaynakları ve bunların istismar edilmesinden gerçekleştirilebilir saldırı yöntemleri listelenmektedir.

Bu çalışmada, cihazın firmware'inde ve ilgili üçüncü taraf yazılım bileşenleri ve işletim sistemlerinden kaynaklanan daha önce açıklanmış güvenlik açıklarına odaklanılacaktır.

Tablo 2.1. IED'lerde bulunan bazı zafiyet kaynakları ve ilgili saldırı yöntemleri.

Güvenlik Açığı	Açıklama
Değiştirilmemiş varsayılan parolalar veya zayıf parola politikaları ve başarısız kimlik doğrulama girişimi sayısında sınırın olmaması	Varsayılan parolalar değiştirilmezse, saldırganlar kullanıcı kılavuzlarında ve el kitaplarında bulunan varsayılan oturum açma bilgilerini kullanarak cihaza erişebilirler. Zayıf parolalar ise; tahmin, sözlük saldırıları veya kaba kuvvet saldırıları yoluyla kırılabilir (Wang ve Shi, 2018; Weerathunga ve Cioraca, 2017a).
Kod Enjeksiyonu	Web tabanlı uzaktan erişim sayfalarında, saldırganlar SQL enjeksiyonu veya XSS yürütme gibi kötü amaçlı kodlar enjekte ederek orijinal işlevi genişletebilir (Wang ve Shi, 2018).
Gelen paket hızlarında sınırın olmaması	Paket fırtınası saldırıları, ağ hizmetinin CPU kullanımını artırarak ve aşırı ağ tıkanıklığına yol açarak Hizmet Reddine (DoS) neden olabilir (Weerathunga ve Cioraca, 2017a).
Kötü Tasarım ve Kodlama Uygulamaları	Bu kategoride, karmaşıklık derecesi değişen birçok durum bulunmaktadır. Bunlar arasında yetersiz giriş doğrulaması (MITRE, 2023c), yarış koşulları (MITRE, 2023d), arabellek taşmaları (MITRE, 2023a, 2023b) ve bellek sızıntıları örnek verilebilir. Saldırı türü, güvenlik açığına bağlıdır. Örneğin (Wang ve Shi, 2018; Weerathunga ve Cioraca, 2017a): - Giriş doğrulaması eksik/yetersizse, saldırgan dahili tasarım tarafından tolere edilemeyecek aralık dışı değerler girerek cihazın çökmesine yol açabilir. - Bellek sızıntıları, tüm belleği tüketerek ve cihazı kullanılamaz hale getirerek istismar edilebilir. - Arabellek taşmalarından faydalanıldığında, saldırgan tahsis edilen belleğin dışına yazarak cihazı çökertebilir. Kullanım oranlarında herhangi bir sınırın olmaması, hesaplama kaynaklarını tüketmek için istismar edilebilir.

Tablo 2.1. (Devamı) IED'lerde bulunan bazı zafiyet kaynakları ve ilgili saldırı yöntemleri.

Güvenlik Açığı	Açıklama
Üçüncü taraf yazılım bileşenleri ve işletim sistemlerinden kaynaklanan güvenlik açıkları	Üçüncü taraf yazılımlar kapsamlı bir şekilde test edilmemiş olabilir ve güvenlik açıkları içerebilir. İlgili cihaza entegre edildikten sonra, bu güvenlik açıkları cihaza aktarılır (Wang ve Shi, 2018; Weerathunga ve Cioraca, 2017a). TCP/IP yığını (ABB, 2016; NIST, 2020), güvenlik yığını ve işletim sistemi (ABB, 2020; NIST, 2022) örnek olarak verilebilir.
Üretim sürümünde bırakılan test ve hata ayıklama özellikleri	Hata ayıklama bilgilerinin görüntülenmesi, cihaz işlevselliğini ortaya çıkararak saldırganların cihazların dahili davranışlarını anlamalarına olanak tanır (Wang ve Shi, 2018; Weerathunga ve Cioraca, 2017a). Hata ayıklamayı kolaylaştırmak için açılan arka kapılar, saldırganların kullanıcı haklarını artırmasına ve hassas bilgilere erişmesine olanak tanır (Wang ve Shi, 2018; Weerathunga ve Cioraca, 2017a).
Şifrelenmemiş/ İmzalanmamış hassas bilgiler	Akıllı cihazların sınırlı hesaplama kapasitesi, hesaplama açısından yoğun görevleri yerine getirmelerini zorlaştırmaktadır. Birçok cihaz düşük karmaşıklıkta şifreleme algoritmaları kullanır veya şifrelemeden tamamen yoksundur. Şifreleme kullanılmazsa, ağ trafiği dinleme (sniffing), sahtecilik (spoofing) ve manipülasyona karşı savunmasız olacaktır. Ayrıca, IED'lerin işletim paneline doğrudan düz parolalar basılması da yasaklanmalıdır (Wang ve Shi, 2018; Weerathunga ve Cioraca, 2017a).

2.5. Literatür taraması

IED'lerin yazılımlarındaki güvenlik açıklarını ve bunların nasıl giderilebileceğini belirlemek, akıllı şebeke sistemlerinin güvenliğini sağlamanın olmazsa olmazıdır. EKS operatörlerinin %60'tan fazlası cihazlarındaki zafiyetleri ve ilgili yamalarıyla ilgili haberdar olmak için tedarikçilerin güvenlik bildirim ve uyarılarını takip

etmelerine rağmen gördüğümüz kadarıyla hiçbir çalışma bu süreci otomatikleştirmeye çalışmamıştır.

Literatürdeki çalışmalar, ya var olan zafiyet tarama araçlarını/yöntemlerini EKS bağlamında karşılaştırmaya ya da yeni yaklaşımlar ortaya koymaya odaklanmaktadırlar. Örneğin; El ve ark. (2017) ve El (2017) Nessus ve Burp Suite zafiyet değerlendirme araçlarını SCADA cihazları bağlamında taramaların doğruluğu, ölçeklenebilirliği ve zafiyet sonuçları açısından karşılaştırmayı amaçlamışlardır. McMahon ve ark. (2018) ve McMahon (2018) ise EKS ve enerji sistemleri de dahil olmak üzere siber-fiziksel sistemler bağlamında iki popüler zafiyet değerlendirme aracı olan Nessus ve OpenVAS'ın doğruluğunu ve ölçeklenebilirliğini değerlendirip karşılaştırmışlardır.

Ecik (2021) de Pasif Zafiyet Tespiti (PZT) ve Aktif Zafiyet Taraması (AZT) yaklaşımlarını bir test ortamında deneysel olarak karşılaştırarak verimlilik ve etkinlik açısından değerlendirmektedir. Bu çalışmada, toplam doğruluk ve kesinlik açısından, PZT'nin sonuçları AZT'den daha yüksek olduğu sonucuna varılmıştır. Ayrıca, PZT'nin AZT'ye kıyasla önemli ölçüde daha kısa tarama süreleriyle ve ağlar üzerinde hiçbir yan etki olmadan daha doğru sonuçlar verdiği ispatlanmıştır. Bu sonuçları elde etmek için aktif taramada Nessus, Nexpose ve OpenVAS yazılımları kullanılırken pasif tarama için güvenlik açığı deposu olarak NVD ve Ortak Platform Numaralandırması (CPE) veritabanlarından yararlanan yarı otomatik bir yaklaşım geliştirilmiştir. Bu çalışmalar, bir EKS ortamında test edilmemiş olsalar da sonuçları hem IT hem de OT için geçerlidir. Çalışmanın sonunda da NVD ve CPE'ye dayanan pasif tarama yaklaşımının eksikleri ve yanlış pozitif ve yanlış negatif döndürme nedenleri tartışılmıştır.

Samtani ve ark. (2016) da İnternet destekli SCADA sistemlerinin güvenlik açıklarını belirlemek amacıyla pasif ve aktif zafiyet değerlendirme tekniklerini kullanmışlardır. Fakat, Shodan'da bulunan IoT cihazlarının zafiyetlerini pasif olarak değerlendirmek için CPE ve NVD korelasyonu değil, bu çalışmaya benzer bir yaklaşım kullanarak cihazların banner verilerinde sağlanan satıcı, ürün ve sürüm numarası bilgilerini otomatik olarak ayıklayıp NVD kayıtlarıyla çapraz referanslama yapan bir Python betiği geliştirilmiştir. Aktif zafiyet değerlendirme aracı olarak ise Nessus yazılımı kullanılmıştır. Çalışma, SCADA'daki IoT cihazlarının en çok içerdiği güvenlik açıklarını tespit etmekle ilgilendiği için ne bu iki zafiyet değerlendirme yöntemlerini

karşılaştırmış ne de pasif değerlendirme yapmak için geliştirilmiş betiğin verimliliği tartışmıştır.

Görüldüğü gibi birçok çalışmada EKS güvenlik açığı taramalarında OpenVAS ve Nessus gibi aslında IT için tasarlanmış araçlar kullanılmaktadır. Bu tür araçlar OT sistemlerinde bulunan bir takım güvenlik açığı tespit etmeyi başarsalar da hem veritabanlarındaki sınırlı zafiyet testleri hem de güvenlik açıklarını sisteme sorgular göndererek aktif olarak tespit ettiğinden dolayı yetersiz kalmasının yanında dikkatli bir şekilde kullanılmazlarsa sisteme yıkıcı zararlar verebilirler. Bunun için; NISTIR 7628 (2014), Pöhler ve ark. (2024) ve Samanis ve ark. (2022) vs. gibi çalışmalarda EKS ağlarına ve bunların güvenlik, güvenilirlik ve sağlamlık gibi kritik özelliklerine odaklanarak daha özel zafiyet tarayıcılarına ihtiyaç duyulduğu vurgulanmaktadır.

Son yıllarda, EKS sistemlerine özgü çözümler ve bunlarla ilgili çalışmaların sayısı artmıştır. Örneğin; Shirani ve ark. (2018) ve Collard (2018) ARM mimarisine dayanan akıllı şebeke IED'lerin yazılımlarındaki zafiyetli/kusurlu fonksiyonları tespit etmek için pasif bir tarama yaklaşımı sunmuşlardır. Bu amaçla, akıllı şebeke IED yazılım görüntülerindeki yaygın güvenlik açıklarından oluşan bir güvenlik açığı veritabanı oluşturmuşlardır ve uyumsuz adayları filtreleyerek giderek karmaşıklaşan üç aşama kullanan bir tespit motoru tasarlamışlardır.

Xia ve ark. (2020) akıllı trafo merkezinin EKS ağının özelliklerine uygun OpenVAS tabanlı bir güvenlik açığı tarama aracı tasarlayıp uygulamışlardır. Deneysel sonuçlar, tasarlanan zafiyet tarama aracının performansının orijinal OpenVAS tarama aracına kıyasla önemli ölçüde iyileştirildiğini göstermektedir. Ancak; OpenVAS da OpenVAS'tan türetilen bu araç da ağ tabanlı tarama yaptıkları için cihaz ve yazılım gibi ağ dışı platformlar için zayıf güvenlik açığı tespit yeteneklerine sahiptirler. Teorik olarak bu tür araçlar ağ üzerinden iletilen tüm güvenlik açıkları tespit edebilse de pratikte ağ üzerinden iletilmeyen bazı güvenlik açıkları da mevcuttur. Bu tür güvenlik açıkları sürüm tespiti yoluyla keşfedilebilse de erişim izni verilen cihazlar taranırken spoofing'e uğrayabilirler.

Alhasawi (2020), Alonso ve ark. (2021), Ani ve ark. (2024), Qassim ve ark. (2019), Shang ve ark. (2023) ve Wen (2023) gibi çalışmalarda zafiyet tarama ve tespitinden ziyade EKS ve akıllı şebeke sistemlerindeki güvenlik açıklarının analizi ve bunların yol açabileceği siber saldırı riskini değerlendirmekle ilgilenilmiştir.

Diğer yandan, bu çalışmanın kapsamında olan ve güvenlik sağlamanın ve zafiyet tespitinin temelini oluşturan varlık taraması OT bağlamındaki son teknoloji durumu incelenmiştir.

EKS sistemlerinde varlık taraması ve yönetimi, yeni konular değildir. ABB Switzerland Ltd. firması, 2005'in başlarında kendi endüstriyel otomasyon sistemi 800xA için özel bir çözüm üretmiştir. 800xA sisteminde; PC, Ağ ve Yazılım İzleme (PNSM) uygulaması operatöre kontrol ağının durumu ve ona bağlı cihazlar hakkında genel bir bakış sağlayarak varlıkların izlenmesini sağlamaktadır. ABB, yeni varlık türlerinin bir EKS sisteminde yapılandırma sürecini otomatikleştirmek için ayrıca Ağ ve Cihaz Tarama Aracı'nı (NDS) geliştirmiştir. NDS, otomasyon ağından ve MIB dosyaları gibi diğer kaynaklardan IP ve SNMP verilerini toplamaktadır (Gelle ve ark., 2005). PNSM ve NDS, varlık taraması ve yönetimi için genel çözümler değil, ABB'nin kendi otomasyon sistemi 800xA için özel bir çözümlerdir. Benzer çözümler, endüstriyel sektördeki birçok üreticide bulunabilir. Ancak, çok az tesis yalnızca tek bir üreticinin tek ürününü/varyantını içerdiğinden dolayı bu çözümler genellikle kullanılamaz.

Wiberg (2006), bir ağdaki kontrol sistemi cihazlarını bulmak için aktif ve pasif trafik analizini kullanan SCADAScan aracını geliştirmiştir. Bu araç, cihazları ağda bulup aktif IP adresleri, koşturulan protokol ve servisleri ve dağıtımla ilgili bilgilerini başarılı bir şekilde tespit edebilirken açık portları ve bu çalışma için gerekli olan cihazların statik bilgilerini tespit edememektedir ve yalnızca DNP 3 ve Modbus protokollerini desteklemektedir. Ayrıca, SCADAScan aracı 26 Ekim 2011'den beri hiç güncellenmemiştir (Google, 2011; Samanis ve ark., 2022).

O yıllardan bu yana EKS sistemlerinin varlık taraması ve/veya yönetimi için kimisi lisanslı kimisi açık kaynaklı birçok araç geliştirilmiştir. Aynı zamanda genel amaçlı araçlardan da faydalanılmıştır. Bu araçların birçoğu Samanis ve ark. (2022) tarafından önerilen EKS tarama taksonomisine dayalı olarak sistematik bir şekilde yetenekleri ve özellikleri karşılaştırılmıştır. Yazarlar hem araçların belgelerini inceleyerek hem de deneysel olarak araçların hangi iletişim protokollerini desteklediklerini, nasıl kullanıldıklarını, nasıl çalıştıklarını ne tür sonuçlar verdiklerini ve ne derinlikte tarama yapabildiklerini araştırmışlardır. Ayrıca deneysel çalışmaları sırasında, özellikle Nmap ve OpenVAS ile aktif tarama yaparken bazı cihazların arızalandığını gözlemledikleri için aktif taramanın EKS sistemleri

üzerindeki dezavantajlarından bahsetmişlerdir. Sonuç olarak bu çalışma, daha fazla EKS iletişim protokollerini destekleyen daha özel araçlara ihtiyaç duyulduğunu vurgulamıştır. Ayrıca, daha fazla EKS cihazı türünü desteklemek ve taramanın sonuçlarına daha fazla cihaz bilgisi dahil ederek daha iyi bir tarama kalitesi sunmak için araçların parmak izi yeteneklerinin geliştirilmesi ihtiyacını da vurgulamaktadır.

Varlık tarama ve tanımlama araçlarının OT sistemlerinin genel güvenlik programındaki kritik rolünden dolayı, bu tür araçların sonuçlarının eksiksiz, doğru ve zamanında olması ve ağlar üzerinde minimum veya hiç yan etki yaratmayan sonuçlar üretmesi çok önemlidir. Bu hedeflere ulaşmak için daha güncel çalışmalar, pasif taramaya odaklanarak çözümler üretmeye çalışmışlardır. Aşağıdaki çalışmalar örnek olarak verilebilir.

Niedermaier ve ark. (2018), ARP yayın (broadcast) paketlerinde bulunan MAC adresine göre endüstriyel cihazları tanımlamak için bir pasif izleme aracı geliştirmişlerdir. Araç, bilinen cihazların MAC adresini, satıcı bilgilerini ve model adlarını içeren önceden oluşturulmuş bir veri havuzundan yararlanır ve bir MAC adresi korelasyon stratejisini kullanır. Akabininde, NVD'yi kullanarak cihazla ilişkili güvenlik açıklarını belirlemeye çalışır. Bu yaklaşımın endüstriyel bileşenlerin yüksek tanımlama oranı ve hassas EKS ağlarında ek ağ trafiği oluşturmamasına rağmen şöyle dezavantajları vardır: Birincisi, statik ortamlarda ARP yayın paketlerinin olmaması nedeniyle cihazı tanımlamak neredeyse imkansızdır. İkincisi, cihazı tanımlamak için MAC adresi korelasyon yaklaşımı kullandığından, birden fazla ürünün aynı MAC Kurumsal Benzersiz Tanımlayıcı (OUI) adresini paylaşması durumunda cihazın yanlış tanımlanabilme ihtimali vardır. Üçüncüsü, firmware ve yazılım sürümleri, bu yöntemle tespit edilemediğinden dolayı, güvenlik açıkları yazılım sürümü dikkate alınmadan belirlenmiştir.

Wallace ve Proctor (2018) ise varlık envanterini gerçek zamanlı ve pasif olarak takip etmeyi sağlayan bir yaklaşım geliştirmişlerdir. Önerilen yaklaşımda, bir ağ anahtarının bir portu, SPAN portu olarak yapılandırılarak bu porta bir ağ güvenliği izleme aracı (NSM) yerleştirilir. SPAN portuna yansıtılacak her iletişim paketi NSM tarafından ayrıntılı bir şekilde analiz edilecektir. Bu, tüm gelen ve giden trafiğin yanı sıra şebeke kenarındaki her akıllı elektronik cihaz (IED) arasındaki trafiğin de izlenmesini sağlayacaktır. Araç, sürekli izleme yaptığı için bir cihaz kaldırıldığında, değiştiğinde ya da firmware'i güncellendiğinde ilgili paketleri analiz ederek

farkedecektir ve ona göre varlık envanterini gerçek zamanlı olarak güncelleyecektir. Yazarlar, NSM aracı, her cihaza yüklenen mevcut firmware sürümünün doğru bir şekilde tespit ettiği için, söz konusu firmware sürümü, protokoller ve tespit edilen yazılımla ilişkili bilinen güvenlik açıklarını CVE standardına dayanarak tespit edebildiğini iddia etmişlerdir. Fakat; zafiyet tespit yöntemiyle ilgili ayrıntı vermemişlerdir.

Thomas ve ark. (2022) de bir varlık envanteri oluşturmak için pasif bir tarama tekniğini kullanarak hafif bir çözüm önerip geliştirmişlerdir. Önerilen sistemde, yine SPAN port yeteneğine sahip bir anahtara bağlı bilgisayar ve diğer cihazlardan oluşan bir ağ vardır. Anahtarın tüm portlarından gelen trafik, önerilen programın çalıştığı makineye bağlı olan SPAN portuna yansıtılır. Program, mevcut bir pcap dosyasından paketleri okuyabilir veya Wireshark ve Python modülü olan Pyshark'ı bir koklayıcı modül olarak kullanarak canlı paket yakalama işlemi gerçekleştirebilir. Araç, yakalanan paketleri ayrıştırır ve ardından bir ağdaki çeşitli cihazları türlerine göre (bilgisayar, yazıcı, HMI, PLC, IED, saha cihazları, anahtarlar, vb.) tanımlamak için çeşitli yaklaşımlar kullanır. Bu, her donanımın kullandığı protokoller ile ilgili varsayılan portlarının korelasyonu ve paketlerden çekilen MAC adresleri ile üretici OUI'siyle korelasyonundan faydalanarak yapılmıştır. Bu araç hem OT hem de BT varlıklarını tespit edebilir. Fakat, bilgisayarlarda işletim sistemlerini tespit edebilirken HMI, PLC, IED, vs. gibi OT cihazlarında firmware sürümlerii tespit edememektedir. Ayrıca, bir EKS ortamında port yansıtmanın geleneksel bir ortamda olduğu kadar etkili olmadığı unutulmamalıdır. Bunun nedeni, basit anahtarlarla birbirine bağlanan çok sayıda küçük cihaz grubunun olmasıdır (Niedermaier ve ark., 2018).

Son olarak, Pöhler ve ark. (2024) OT cihazlarının belirli özelliklerini, üretim ortamlarının hassasiyetini ve birçok gerçek makine operatörünün tipik olarak ilkel başlangıç koşullarını dikkate alarak OT varlık yönetimine yönelik yeni bir yaklaşım sunup bunu bir web uygulaması olarak uygulamıştır. Varlık keşif fonksiyonu, farklı yoğunluk profilleri için Netdiscover, Nmap ve Crackmapexec tarama yazılımlarını kullanan bir Python ağ keşif betiği aracılığıyla oluşturulmuştur. Araç, çeşitli endüstriyel cihazlardan oluşan bir test ortamında test edilmiş olsa da IED cihazları için test edilmemiştir. Test edilse de kullandığı teknolojiler ve tarama araçlarından dolayı cihazların firmware sürümleriyle ilgili bilgi veremeyecektir.

Piyasada bir de OT için geliştirildiği iddia edilen lisanslı araçlar da vardır. İlginçtir ki, bu araçların vaat ettiği işlevler çoğunlukla aynıdır. Bunlardan; Almanya, Norderstedt merkezli Langner Communications GmbH şirketinin OT için sunduğu varlık yönetim sistemi: OT-BASE aracıdır. Langner, OT-BASE aracının "otomasyon mühendislerini, siber güvenlik uzmanlarını ve bakım personelini daha verimli hale getireceğini" vaat etmektedir (Langner, 2025). ABD, Chicago merkezli Verve Industrial Protection, Verve ürününün OT için en derin, en geniş ve en verimli varlık envanter yönetimi çözümünü sunduğunu iddia etmektedir (Rockwell Automation, 2025). Verve, bu sayede varlıklar hakkında belirli bir derinlikte bilgi edinme vaadinde bulunmaktadır. ABD, Foxborough merkezli Industrial Defender ise varlık ve risk yönetimi için başka bir yazılım sunmaktadır (Industrial Defender, 2025). OT için özel olarak geliştirilen diğer lisanslı varlık yönetim sistemleri şunlardır: Asset Guardian (Asset Guardian, 2025), Claroty (Claroty, 2025), Dragos (Dragos, 2025), Microsoft Defender for IoT (Microsoft, 2025), Nozomi (Nozomi Networks, 2025) ve PAS Cyber Integrity (Hexagon, 2025).

EKS üzerine literatür taramasının ardından bu sistemlerin özellikleri ve hassasiyetine uygun varlık ve zafiyet tarama araçlarını geliştirmek için önemli çabalar sarf edildiği görülmektedir. Ancak, önerilen yöntemlerin çoğu IED cihazları için yetersiz kaldığını da görmekteyiz. Bu çalışmalar çok farklı yaklaşımlar geliştirerek çok sayıda OT sisteminde iyi çalışılmış olsa da ya IED için test edilmemiş ya IED için test edilip istenilen bilgiler döndürememiş ya da eksik sonuçlar vermiştir.

Bu bölümün geri kalan kısmında zafiyet ve varlık tarama ve tespitinin farklı yöntemleri, bunların avantajları ve dezavantajları, bu çalışmada seçilen yöntemlerin tercih edilme nedenleri ve IEC 61850 standardının tanımı, kısa bir açıklaması ve bu çalışmada yararlandığımız özellikleri anlatılacaktır.

2.6. Zafiyet Tarama/Tespit Teknikleri

Güvenlik açığı tarama çalışmaları, açıklanan yeni güvenlik açıklarını istismar edilmeden önce tespit etmek için sürekli olarak gerçekleştirilmelidir (Stouffer ve ark., 2023). Manuel yöntemleri kullanarak arzulanan doğrululuğu ve sürekliliği sağlamak neredeyse imkansızdır. Dolayısıyla, zafiyet tarama/tespit araçları kullanmak şarttır. Bir zafiyet tarama aracı, bilgisayarlarda, bilgisayar sistemlerinde, ağlarda ve uygulamalardaki güvenlik açığı aramak üzere tasarlanmış otomatik bir

programdır (Kennedy ve ark., 2011). Günümüzde, yaygın olarak kabul görmüş iki güvenlik açığı tarama yöntemi vardır: aktif (AZT) ve pasif (PZT) (Samtani ve ark., 2016).

2.6.1. Aktif zafiyet taraması (AZT)

AZT, zafiyet tespit araçları veritabanlarından yararlanarak taranan ağlardaki ana bilgisayarlara veri gönderir ve geri dönen yanıtları inceleyerek zafiyetlerin varlığını tespit ederler (Ecik, 2021; Kennedy ve ark., 2011). Çeşitli işletim sistemleri ve yazılımlar, kullanılan farklı ağ uygulamaları nedeniyle belirli ağ araştırmaları gönderildiğinde farklı yanıtlar verme eğilimindedir. Bu benzersiz yanıtlar, zafiyet tarayıcısının işletim sistemi sürümünü ve hatta yama düzeyini belirlemek için kullandığı bir parmak izi görevi görür. Bir zafiyet tarayıcısı, uzak sisteme giriş yapmak ve yazılım ve hizmetleri sıralayarak yama uygulanıp uygulanmadıklarını belirlemek için belirli bir kullanıcı kimlik bilgisi kümesini de kullanabilir (Kennedy ve ark., 2011).

Tarayıcı, tespit ettiği sistemin türü ve özelliklerine göre çeşitli zafiyet testi paketleri gönderir. Bu tür testlere örnek olarak port tarama, SQL enjeksiyonunu kontrol etme, parola ile oturum açma girişimleri, ağ trafiğini izleme ve kötü amaçlı veya istismar amaçlı yükleri kaldırma verilebilir. Elde ettiği sonuçlarla tarayıcı, sistemde tespit edilen tüm güvenlik açıklarını özetleyen bir rapor sunar (Kennedy ve ark., 2011; Samtani ve ark., 2016).

Pasif taramanın aksine, aktif tarama yöntemlerini kullanan çeşitli açık kaynaklı ve kurumsal araçlar mevcuttur. Bunlardan; Nmap ve Zmap port tarayıcıları, Burpsuite web uygulama tarayıcısı, SQLMap veritabanı tarayıcısı ve Nessus ve OpenVAS gibi çok yönlü tarayıcılar (Samtani ve ark., 2016).

AZT, çalışma prensibi nedeniyle mücadeleci (intrusive) bir yaklaşım olarak değerlendirilmektedir (Ecik, 2021). Sonuç olarak, AZT taramanın kapsamındaki cihazlarla doğrudan etkileşime girer (Niedermaier ve ark., 2018; Stouffer ve ark., 2023). Sıkı zamanlama kısıtlamalarına bağlı olarak, ek ağ trafiğinin enjeksiyonu endüstriyel sistemlerdeki bağlı cihazların istikrarsızlığına neden olabilir veya cihaz işlem durumunu etkileyebilir. Standart bir zafiyet taraması, Hizmet Reddi'ne (DoS), cihazların arızalanmasına ve/veya süreçlerin yanlış bir şekilde işlenmesine yol

açabilir (Niedermaier ve ark., 2018; Stouffer ve ark., 2023; Wedgbury ve Jones, 2015).

Aktif taramanın neden olduğu olumuz durumlarla bağlı olarak, NIST (2023)'de yaşanmış 2 olay anlatılmıştır (Stouffer ve ark., 2023). Birincisi; 9 fitlik robotik kolları kontrol eden aktif bir SCADA ağında ping taraması yapılırken, bir kol aktif hale gelip 180 derece dönmüştür. Ping taraması başlatılmadan önce kolun kontrolörü bekleme modundaydı. İkinci bir olayda, envanter amacıyla ağa bağlı ana bilgisayarları belirlemek için bir EKS ağında ping taraması gerçekleştirilmekteydi ve bu, üretim tesisinde entegre devrelerin oluşturulmasını kontrol eden bir sistemin kilitlenmesine neden olmuştur. Bu test, 50.000 dolar değerinde yonga plakasının (Wafer) imha edilmesiyle sonuçlanmıştır.

2.6.2. Pasif zafiyet tespiti (PZT)

PZT, ağda müdahaleci olmayan bir teknik olarak önerilmiştir. Başlangıçta ağdaki ana bilgisayarlar, yüklü yazılım/donanım, açık portlar ve çalışan hizmetler gibi bilgiler mevcut verilerden elde edilecektir. Ana bilgisayarların ve varlıkların bir envanteri oluşturulduktan sonra, NVD veya zafiyet istihbarat depoları gibi güvenlik açığı veritabanları, zafiyeti olan ürün sürümlerini ve ilgili güvenlik açıklarını belirlemek için kullanılabilir (Ecik, 2021).

PZT aracılığıyla güvenlik açıklarını tespit etmek için ağdaki yazılım/donanımlar ve çalışan hizmetler ya varlık envanteri yönetim sistemlerinde bulunan ve kolayca erişilebilen bilgilerinden yararlanarak çekilir, ya da zafiyet tespitinden önce ağ trafiği analizörlerini kullanılarak varlık taraması yapılır (Ecik, 2021; Stouffer ve ark., 2023). Bir ağda bulunan ürünlerin bir listesi derlendikten sonra, CVE girişlerinin CPE spesifikasyon formatında olan güvenlik açığı bulunan yazılım açıklamaları, kullanımda olan ürünlerle karşılaştırılarak bir güvenlik açığından etkilenen ürünler belirlenir (Ecik, 2021).

2.6.3. AZT ve PZT tekniklerinin genel karşılaştırması

AZT'ler ağdaki düğüm/cihazlara paket gönderirken, PZT hedefe müdahale etmez. Bu bağlamda, iki yaklaşımın verdiği sonuçlar farklılık göstermektedir. Aşağıda AZT ve PZT yöntemlerinin kapsam, vakitlilik (Timeliness), görünürlük, hız,

ölçeklenebilirlik, yan etkiler, tarama aralıkları ve güvenilirlik açısından genel bir karşılaştırması sunulacaktır:

- Kapsam: Bir zafiyet değerlendirme aracının kapasitesi, yalnızca bilinen istismarların veritabanına dayanır (Ecik, 2021; Kennedy ve ark., 2011). Bu çalışmanın yapıldığı tarihte (Temmuz 2025), NVD'de 300.000'den fazla CVE bulunurken (NIST, 2025b) önde gelen zafiyet tarayıcılarından biri olan Nessus, bir AZT aracı örneği olarak, resmi web sitesinde yalnızca 100.000'den fazla CVE kapsadığını beyan etmektedir (Tenable® Inc, 2025). Diğer yandan PZT, güvenlik açığı veritabanlarında veya güvenlik açığı istihbarat depolarında bulunan tüm bilinen güvenlik açıklarını kapsayabilir.
- Vakitlilik/Zamanındalık (Timeliness): AZT, en son güvenlik açıklarını kapsayacak en güncel güvenlik açığı veritabanını kullanmalıdır. Ancak bu durumda bile, yakın zamanda açıklanan güvenlik açıkları için test betiklerinin oluşturulması zaman aldığından, tarama sonuçlarının eksiksizliği garanti değildir (Gawron ve ark., 2017). CVE beslemeleri için NVD kullanıldığında PZT tarayıcılarda da benzer bir sorun mevcuttur. Bunun nedeni, bir CPE tanımlayıcısının bir güvenlik açığı için oluşturulması ile NVD'de yayınlanması arasında değişken bir gecikme süresinin olmasıdır (Ecik, 2021).
- Görünürlük: Eksik veya hatalı ağ görünürlüğü, güvenlik uzmanlarının güvenlik duvarlarının arkasında AZT araçlarını yürütürken sıklıkla karşılaştıkları bir diğer sorundur. Bu durumda, TCP sorgulama paketleri engellendiğinde AZT tarayıcıları genellikle çalışan hizmetleri kaçırır; yani yanlış negatif sonuçlar verir. Ayrıca, güvenlik duvarları UDP sorgulamalarına yanıt vermediğinde yanlış pozitif sonuçlar elde edilir. Benzer şekilde, tarama sırasında çevrimdışı olan sistemler AZT tarafından tespit edilemez. AZT'nin aksine, PZT, ağ ile herhangi bir etkileşim olmadığı için bu tür görünürlük sorunlarından etkilenmez.
- Hız: AZT'ler, ilgili güvenlik açıklarını tespit etmek için ağda aktif olan varlıkları listelemek üzere çok sayıda test gerçekleştirir. Bu süreç, ağın boyutuna ve taramaların yapılandırmasına, yani taramanın ayrıntı düzeyine bağlı olarak önemli miktarda zaman alabilir (Deraison ve ark., 2003; Gula, 1999). Ancak, PZT kullanılarak, ek tarama çabası gerektirmeden güvenlik açıklarını tespit edebildiğinden, genel tespit performansı önemli ölçüde artırılabilir.

- Ölçeklenebilirlik: Hız konusunda tartışıldığı gibi, ağ boyutu ne kadar büyükse, AZT'ler için tarama süresi de o kadar uzun olur. Ancak, PZT durumunda güvenlik açığı bilgilerinin zafiyet veritabanlarından pasif olarak çıkarılması, ağ boyutuna o kadar bağlı değildir.
- Yan Etkiler: AZT'nin ağ üzerinden paket göndermesi gerektiğinden, önemli miktarda ağ bant genişliği tüketir ve bu da ağın performansını yavaşlatabilir. Ayrıca, tarama betikleri taranan ana bilgisayarların ve ağdaki cihazların mevcut durumunu değiştirebilir ve bu da üzerlerinde çalışan hizmetleri aksatabilir (Ecik, 2021; Gula, 1999; Stouffer ve ark., 2023). Özellikle OT sistemlerinde bu yan etkiler felaketlere yol açabilir. PZT yaklaşımı ise, gerekli tüm veriler mevcut envanter/yama yönetimi çözümlerinden alındığından, hiçbir ana bilgisayara dokunulmadığı veya incelenmediği için bu tür ağ kesintisi sorunlarını ortadan kaldırır (Deraison ve ark., 2003).
- Tarama Aralıkları: Uzun tarama süreleri ve istenmeyen olası yan etkiler nedeniyle, AZT haftalık veya aylık gibi aralıklarla gerçekleştirilir. Taramalar arasındaki bu aralık kritiktir; çünkü bu durumda tarama işlemi güncel olmayan sonuçlar üreterek güvenlik uzmanlarının güncel ağ zafiyet durumunu görmesini engeller ve ağları yeni tehditlere açık hale getirir. Buna karşılık, PZT sürekli izleme olanağı sağlayabilir (Deraison ve ark., 2003) ve ağ üzerinde canlı güvenlik açığı ve ana bilgisayar bilgileri sunar (Ecik, 2021).
- Güvenilirlik: Gerek AZT gerekse PVT, yanlış pozitifler ve yanlış pozitifler döndürebilir. Başka bir deyişle; sırasıyla ağın varlıklarında gerçekte mevcut olmayan CVE sonuçları döndürebilir ve mevcut bazı CVE'leri gözden kaçırabilir. AZT durumunda bu tespit hataları; önceki maddelerde anlatılan kapsam, görünürlüğün yanında, aracın yaptığı kimlik doğrulanmış ve doğrulanmamış taramalar ve komut dosyalarının statik yapısından kaynaklanır. PZT tarayıcıları ise zafiyet tespiti için ürünün CPE tanımlayıcısına dayandığı için; CPE tanımlayıcısı olmayan CVE girişleri, CPE ve CVE senkronizasyon sorunu ve belirsiz CPE atamaları ve bu tür tarayıcılar güvensiz yapılandırma zafiyetlerine bakmadığı için yanlış veya eksik sonuçlar döndürebilir (Ecik, 2021).

Sonuç olarak, PZT potansiyel olarak AZT'ye göre önemli avantajlar sunduğu görülmektedir. Bu avantajlarından dolayı, bu çalışmada pasif zafiyet tespiti (PZT)

olarak sınıflandırılabilecek güvenlik açıklarını filtrelemek için tedarikçi, cihaz modeli, donanım ve yazılım sürümlerini kullanacak bir yaklaşım geliştirilecektir.

2.6.4. CPE ile ilgili sorun

Pasif Zafiyet Tespiti yönteminde en yaygın kullanılan yaklaşım; donanım, yazılım veya uygulamanın CPE tanımlayıcısı ile NVD vs. gibi güvenlik açığı veritabanlarında depolanan zafiyetlerin ilgili CPE'lerinin korelasyonunu gerçekleştirmektir. Ancak; bu yaklaşımın da bazı eksiklikleri vardır.

Ortak Platform Numaralandırması (CPE), NIST tarafından geliştirilen ve sürdürülen bir dizi uygulama, işletim sistemi ve donanım aygıtını tanımlamak ve belirlemek için standartlaştırılmış bir yöntemdir. CPE öznitelikleri, parça, satıcı, donanım sürümü, yazılım sürümü, işletim ortamı, mimari ve dili tanımlayan bir dizi karakterlerden oluşmaktadır (Ecik, 2021). Bu yaklaşımda bir ürünün CPE'si CVE deposundaki CPE'lerle karşılaştırılır ve aynı CPE'lerin CVE'leri elde edilir. PZT'nin bu yaklaşımı ne kadar AZT'ye göre daha doğru sonuçlar verse de bazı sorunları vardır. Bunlardan (Ecik, 2021; Sanguino ve Uetz, 2017; R. J. Thomas ve ark., 2020);

- CPE Tanımlayıcıları Olmayan CVE Girişleri: NVD'deki bazı CVE girişlerinde herhangi bir CPE tanımlayıcısı bulunmamaktadır. Bu sorun, CVE kayıtlarındaki güvenlik açığı bulunan ürün tanımlarını kontrol ederek güvenlik açıklarının tespit edilmesini engellemekte ve PZT'nin yanlış negatif sonuçlar döndürmesine neden olmaktadır. Bu sorun, PVD için daha güvenilir bir güvenlik açığı veritabanı kullanılarak ortadan kaldırılabilir.
- CPE ve CVE Senkronizasyon Sorunu: Örneğin, CPE sözlüğünde bulunmayan CPE tanımlayıcıları atanmış CVE'ler vardır. Ayrıca, bazı CPE'lerin kullanımdan kaldırılmasına rağmen CVE kayıtlarında güncellenmemiştir.
- Belirsiz CPE Atamalarını Belirleme: Bazı veri kaynaklarındaki CPE'ler, tedarikçi güvenlik bültenlerinde bildirilen CPE'lerden farklı olur. Bu durumda, hangi veri kaynağının en güncel ve güvenilir verilere sahip olduğunu belirlemek zordur.

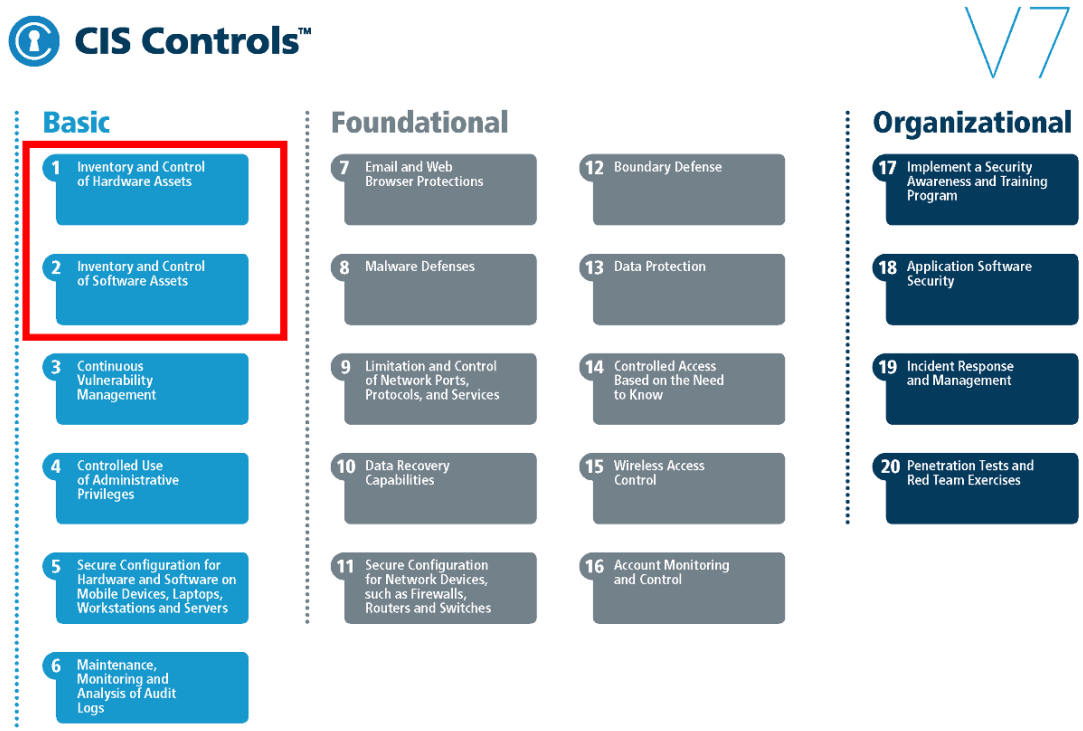
2.7. Varlık Tanımlaması/Taraması ve Varlık Envanteri

Doğru envanter bilgileri, zafiyet taraması ve yönetimi, risk değerlendirmesi ve varlıkların eskime takibi gibi birden fazla risk yönetimi hedefini destekler. Ağda bulunan cihazlar, yazılımlar ve servislerin tespiti ve doğru bir şekilde tanımlanması,

zafiyet taramasının temelini oluşturmaktadır (Niedermaier ve ark., 2018). Gerek PZT gerekse AZT'de her iki tarama yönteminde de güvenlik açığı tespiti ile ilgili temel sorun, ürün envanterinin doğru ve kesin bir şekilde tespit edilememesidir (Ecik, 2021).

Doğru bir varlık envanteri listesi tutulmadan ve ağdaki varlıklar hakkında sağlam bir anlayışa sahip olmadan, sadece güvenlik açığı tespiti değil, risk yönetmek ve güvenilir operasyonlar sağlamak için bir strateji geliştirmek ve uygulamak imkanız olduğuna dair bütün kaynaklarda bir fikir birliği vardır. Çünkü bir kuruluşun, sahip olduğunu bilmediği bir şeyi koruması ve savunması zordur (McCarthy ve ark., 2020; Parsons, 2018; Stouffer ve ark., 2023; A. M. Thomas ve ark., 2022; ABD İç Güvenlik Bakanlığı, 2016; Wallace ve Proctor, 2018). Şekil 2.3'te de görüldüğü gibi varlık envanteri, SANS'ın kritik siber güvenlik kontrollerinin en başında yer almaktadır (İnternet Güvenliği Merkezi (CIS), 2018).

Aktif tarama, pasif tarama, yapılandırma analizi ve fiziksel inceleme olmak üzere dört etkili varlık tanımlama metodolojisi vardır (Bristow, 2020; Parsons, 2018).



Şekil 2.3. SANS'ın kritik siber güvenlik kontrolleri (İnternet Güvenliği Merkezi (CIS), 2018)**.**

2.7.1. Pasif ağ taraması

Pasif ağ taramaları, ağ anahtarlarından veya diğer özel ağ yakalama cihazlarından geçen trafiği izleyerek mevcut ağ trafiğini inceleyen bir ağ keşif biçimidir. Pasif ağ taramalarını uygulayan sistemler, ağa herhangi bir ek trafik getirmez. Bu, doğrudan araştırıldığında beklenmedik davranışlar gösterebilecek OT ağlarında bulunan hassas cihazlar için idealdir. Pasif tarama, izlenen ağ segmentlerinde aktif olarak iletişim kuran tüm cihazları belirleyebilir (Samanis ve ark., 2022; Stouffer ve ark., 2023).

Pasif tarama araçları, Ethernet veya TCP/IP gibi geleneksel ağ teknolojileri ve protokolleri için daha sağlam iken Profibus veya Modbus gibi endüstriyel protokoller için ise daha az sağlamdır. Pasif tarama, Purdue Modelinin 2. seviye ve üzeri varlıkları hızla tespit etmek için harika bir araç olabilir. Ancak, iletişim içeriğinden varlıklarını göremediği saha cihazlarını tespit etmekte zorluk çekebilir. Bu da kritik cihazları tespit edememesine neden olabilir (Bristow, 2020). Ayrıca, pasif tarama aktif olarak iletişim kurmayan cihazları belirleyemez ve şifrelenmiş trafiği (özel bir düzenleme olmadan) denetleyemez. Ek olarak, pasif bir taramanın tamamlanması, mevcut ağ trafiğine olan bağımlılığı nedeniyle genellikle günler sürer (Bristow, 2020; Samanis ve ark., 2022; Stouffer ve ark., 2023).

2.7.2. Aktif ağ taraması

Aktif ağ taramaları, ağa bağlı cihazları doğrudan araştıran bir ağ keşfi biçimidir. Aktif tarama kullanan sistemler ağ ortamına ek paketleri yayınlar ve ortaya çıkan trafiği izler. Aktif tarama, ağda normalde aktif olmayan cihazları da tespit edebilir. Ancak, yalnızca belirli koşullar altında yanıt verecek şekilde yapılandırılmış cihazları gözden kaçırabilir. Aktif keşif, uyumlu olmayan protokol uygulamalarına sahip bazı eski ekipmanlarla olumsuz etkileşimlere neden olarak ağ arayüzlerini kilitlemelerine veya CPU kaynaklarını tüketmelerine yol açabilir. Aktif zafiyet tarama (AZT)'nin sahip olduğu çalışma prensibiyle aynı şekilde işlediği için hassas OT cihazları ve sistemine aynı olumsuz durumlara neden olabilir (Bristow, 2020; Niedermaier ve ark., 2018; Samanis ve ark., 2022; Stouffer ve ark., 2023; Wedgbury ve Jones, 2015). Bunun için OT ağ sahipleri, hedef ağdaki cihaz hassasiyeti nedeniyle operasyonel bir ağda aktif taramaya izin verirken aşırı dikkatli olmalıdır ve aktif taramalar mümkün olduğunca planlı OT kesintileri sırasında gerçekleşecek şekilde planlanmalıdır (Bristow, 2020; Stouffer ve ark., 2023).

Bazı OT'ye özgü tarama sistemleri, aktif taramanın daha güvenli bir versiyonunu uygulamak için pasif ve aktif taramayı birleştirir. Güvenli aktif tarama, öncelikle pasif yollarla bağlı ekipman hakkında bilgi edinir, ardından OT operasyonları için risk oluşturmadan bağlı ekipman hakkında ek bilgi edinmek için cihaza özgü iletişim biçimini kullanır (Stouffer ve ark., 2023).

2.7.3. Yapılandırma analizi

Yapılandırma analizi, bilinen varlıkların bir resmini oluşturmak için proses kontrol sistemlerinden, ağ cihazlarından, proses diyagramlarından ve diğer yapılandırma kaynaklarından mevcut yapılandırma verilerini alan bir tekniktir. Yapılandırma analizi, statik yapılandırmalardan yararlanan pasif taramaya benzer şekilde tamamen pasif veya yapılandırmaları sürekli olarak değerlendirmek için otomasyondan yararlanarak daha aktif olabilir (Bristow, 2020).

OT sistem yapılandırma bilgilerini kullanmak, kapsamlı bir envanter oluşturmak için Purdue Modelinin 0. ve 1. seviye cihazlarından gerekli bilgileri almanın en ekonomik yoludur. Yapılandırma verisi analizindeki zorluk, yapılandırmaları işleyip kullanılabilecek formatına dönüştürmek için birden fazla tedarikçi veya model içeren homojen olmayan kontrol ortamlarından veri çekmektir (Bristow, 2020). Ancak; farklı üreticilerden gelen IED'ler arasında birlikte çalışabilirliği sağlamak, yapılandırma verilerini standartlaştırmak ve kullanılabilir hale getirmek için ortaya çıkan IEC 61850 standardı ve bu standarttan türetilmiş protokolleri kullanan dijital trafo merkezlerinde böyle bir sorun artık söz konusu değildir (Weerathunga ve Cioraca, 2017b).

Piyasadaki çoğu yapılandırma analiz aracı ve metodolojisi, ağ anahtarı ve güvenlik duvarı yapılandırmaları gibi daha geleneksel BT cihazlarına odaklanır. OT ortamlarında, bu cihazlar genellikle yüksek derecede izin verici şekillerde yapılandırılır; örneğin, güvenlik duvarı kuralları bir segmentte herhangi bir veriye izin verir ve bu nedenle kapsamlı sonuçlar sağlamak için yeterince yüksek çözünürlüğe sahip değildir. OT ortamlarında, genellikle kontrol sisteminden yapılandırma analizi için zengin veri kümeleri bulunur. Bazı EKS'ye özgü yapılandırma analiz araçları; mantık dosyaları, denetleyici, G/Ç yapılandırmaları veya mühendislik iş istasyonundan gelen diğer işlem yapılandırma verilerini işlerler (Bristow, 2020).

IEC 61850'nin soyut veri ve nesne modelleri, güç sistemi cihazlarını tanımlamak için standartlaştırılmış bir yöntem tanımlar ve tüm IED'lerin güç sistemi işlevleriyle doğrudan ilgili aynı yapıları kullanarak veri sunmasını sağlar. Bu veriler Trafo Merkezi Yapılandırma Açıklama Dili (SCL) formatında sistemden elde edilebilir ve sistem/cihazın işleyişi, statik ve dinamik özelliklerini tanımlar. Bu çalışmada bu dosyalardan yararlanıp IED'lerin statik bilgileri çıkarılacaktır.

Yapılandırma analizi, varlık envanterine kapsamlı OT bilgisi eklemenin en iyi yollarından biridir ve diğer varlık tanımlama teknikleriyle elde edilemeyen temel ve bağlamsal bir süreç bilgisi sağlayabilir. Bu, güvenlik sistemleri gibi izole ve bağlantısız ortamlarda kullanılabilecek tek pratik teknik olabilir (Bristow, 2020).

2.7.4. Fiziksel inceleme

Ağ mimarileri veya diğer OT ortamı sorunları nedeniyle otomatik araçlar uygun olmadığında, kuruluş güncel bir envanter tutmak için fiziksel inceleme başta olmak üzere manuel süreçleri göz önünde bulundurmalıdır (Stouffer ve ark., 2023). Fiziksel incelemede, hangi sistemlerin bağlı olduğunu doğrulamak için proses tesisinin genelindeki her bir fiber, Ethernet, seri kablo ve tel parçasının izlenir. Doğru bir şekilde gerçekleştirilirse, bu yöntem genellikle en kapsamlı verilerin toplanmasını sağlar ve başka yöntemlerle tespit edilemeyecek varlıkları ortaya çıkarır. Ancak, pasif ve aktif taramada bulunan ölçeklenebilir avantajlara ve otomatik güncellemelerin kolaylığına ve yapılandırma analizinde bulunan ek içeriğe sahip değildir (Bristow, 2020; Parsons, 2018).

2.7.5. Varlık envanteri ile ilgili sorun

Sağlam bir varlık envanterinin oluşturulması kolay bir iş olmadığı, hem bilgi teknolojisi (BT) hem de operasyonel teknoloji (OT) profesyonellerinin hemfikir olduğu bir konudur. Tarihsel olarak, varlık tanımlama, doğru bir envanteri belirlemek ve sürdürmek için zaman alıcı ve maliyetli çabalarla ilişkilendirilmiştir ve operatörlerin yarısından fazlası zamanlarının %20-80'ini yalnızca tesis bilgilerini bulup doğrulamakla geçirmiştir (Bristow, 2020; Wallace ve Proctor, 2018).

Ayrıca, varlık tanımlama, SANS 2019 OT/EKS Siber Güvenlik Durumu Anketi'ne katılan 338 EKS güvenlik uzmanının 1 numaralı endişesiydi. Aynı anket raporunda uzmanalar; sistemin karmaşıklığı nedeniyle sistem varlıklarının, özellikle de PLC ve

IED’ler gibi endüstriyel gömülü cihazların kapsamlı bir envanteri elde etmek daha da zor hale geldiğini belirtmişlerdir (Filkins ve Wylie, 2019).

Varlık envanterinin tutulmasının kritik öneme sahip olduğu aşikâr görünse de, bu zorluklardan dolayı birçok tesisin kapsamlı ve güncel bir envanter tutmaması şaşırtıcı değildir. Bir kuruluş bir aşamada kapsamlı bir envantere sahip olsa da sistemlere bileşenler eklendiğinde, kaldırıldığında veya değiştirildiğinde; örneğin yama uygulandığında, yeni aygıt yazılımı yüklendiğinde, bakım sırasında bileşen değiştirildiğinde, envanterdeki bilgiler güncellenmelidir (Stouffer ve ark., 2023). Fakat; kuruluşun belli bir varlık yönetimi sistemi bulundurduğu durumlar hariç genellikle sahada değişiklikler yapılıp bu değişikliklerin envantere girilmesi gözden kaçabilir. Bu da, pasif zafiyet tarayıcısı için yanıltıcı olur.

Bu sebeplerden dolayı, bu çalışmada kuruluşun tuttuğu varlık envanterindeki IED’lerle ilgili bilgiler eksik olabileceği kabul edip zafiyet taramasına başlamadan önce bu cihazların üretici, model, seri numarası, donanım ve yazılım sürüm numaraları dahil olmak cihazların detaylarını konfigürasyon dosyalarından elde edilmeye çalışılacaktır.

2.8. IEC 61850

2.8.1. Tanımı ve özellikleri

IEC 61850, trafo merkezlerinde IED'ler arası iletişimin tüm potansiyelinden yararlanmak ve Kontrol ve Otomasyon iletişim işlevlerinin tüm yönlerini standartlaştırmak amacıyla Uluslararası Elektroteknik Komisyonu (IEC) tarafından geliştirilen ve 2003 yılında yayınlanan küresel bir standarttır (Hadbah ve ark., 2014; Mackiewicz, 2006). Standart, trafo merkezi otomasyon sistemlerine ilişkin gereksinimlerden bir iletişim protokolünün ayrıntılarına kadar çeşitli bölümlerden oluşmaktadır (ABB, 2012).

Trafo merkezi otomasyonunda kullanılan diğer iletişim protokolleri ile IEC 61850 arasındaki en önemli farklardan biri, IEC 61850'nin yalnızca bir iletişim protokolü değil, aynı zamanda trafo merkezi otomasyon sistemlerini belirlemek, tasarlamak ve işletmek için bütünsel bir çerçevenin olmasıdır (ABB, 2012). Dünyanın dört bir yanından uzmanlar tarafından özetlenen ve trafo merkezi otomasyon endüstrisinde genel kullanım için tasarlanan bu model, Ethernet teknolojisi protokollerine ve

uygulama programlama arayüzleri (API'ler) için bir geliştirme kılavuzuna ek olarak, soyut düzeyde kapsamlı bir nesne yönelimli veri modeli sunmayı amaçlamaktadır (Hadbah ve ark., 2014). Dolayısıyla, IEC 61850, güç sistemi cihazlarının verileri her tür ve marka cihazda tutarlı olacak şekilde nasıl düzenlemesi gerektiğine dair kapsamlı bir model sunmuştur. Bu, cihazların kendi kendilerini yapılandırabildiğini sağladığı için sıkıcı yapılandırma çalışmalarının çoğunu ortadan kaldırır (Mackiewicz, 2006).

Standart, ayrıca trafo merkezi otomasyon sistemleri için bir XML bir tanımlama dili tanımlamıştır: Trafo Merkezi Yapılandırma Dili (SCL). Bu dil, cihazların sistemlere otomatik bir şekilde verimli bir şekilde entegre edilmesini kolaylaştırır; mühendis cihazı yapılandırmak için yalnızca SCL dosyasını cihaza aktarması yeterlidir. Ardından, IEC 61850 istemci uygulaması, nesne tanımlarını ağ üzerinden cihazdan çıkarabilir (ABB, 2012; Mackiewicz, 2006). Zira; standardın 6. bölümünde belirtildiği gibi standart, yalnızca cihazları değil, aynı zamanda araçlarını ve sistemlerini de birlikte çalışabilir hale getiren kapsamlı ve tutarlı bir sistem tanımı ve mühendisliğini destekler (ABB, 2012).

2.8.2. IEC 61850 cihaz modeli

IEC 61850 standardında veriler, nesne yönelimli kavramlar kullanılarak nesne yönelimli hiyerarşik bir yapıda tanımlanır. Dolayısıyla, fiziksel bir cihazın özellikleri ve işlev dağılımlarını tanımlayan cihaz modelleri bulunur (Hadbah ve ark., 2014).

IEC 61850 cihaz modeli, fiziksel bir cihazla başlar. Fiziksel cihaz, ağa bağlanan cihazdır. Bu cihaz genellikle ağ adresiyle; yani IP adresi ile tanımlanır. Her fiziksel cihazda bir veya daha fazla mantıksal cihaz (LD) bulunabilir. IEC 61850 mantıksal cihaz modeli, tek bir fiziksel cihazın birden fazla cihaz için proxy veya ağ geçidi görevi görmesini sağlayarak standart bir veri yoğunlaştırıcısı temsilini sağlar. Her bir mantıksal cihaz bir veya daha fazla mantıksal düğüm (LN) içerir. Mantıksal düğüm, bir güç sistemi işleviyle mantıksal olarak ilişkili olan, adlandırılmış bir veri ve ilişkili hizmet grubudur (ABB, 2009; Mackiewicz, 2006).

Mantıksal düğümlerin adları, türlerini belirten harflerle başlar. Örneğin; Otomatik Kontrol (A), Ölçüm (M), Denetleyici Kontrol (C), Genel Fonksiyonlar (G), Arayüz/Arşivleme (I), Koruma (P), Korumayla İlgili (R), Sensörler (S), Enstrüman Trafoları (T), Şalt Cihazları (X), Güç Transformatörleri (Y) ve Diğer Ekipmanlar (Z).

Ayrıca, adları "L" harfiyle başlayan Sistem Mantıksal Düğümleri de vardır (Mackiewicz, 2006). LPHD bunlardan bir tanesidir. LPHD, mantıksal cihazın başına özel bir mantıksal düğümdür ve fiziksel cihazın (IED) durumunu tanımlayan veri nesneleri içerir (ABB, 2009; Apostolov, 2017).

Her bir mantıksal düğüm, bir veya daha fazla veri öğesi (DO) içerir. Her veri öğesinin benzersiz bir adı vardır. Bu veri adları standart tarafından belirlenir ve işlevsel olarak güç sistemi amacıyla ilişkilidir (ABB, 2009; Mackiewicz, 2006). Örneğin, fiziksel cihaz bir LPHD mantıksal düğümü olarak modellenir ve fiziksel cihazın bilgilerinin saklandığı PhyNam, IED dahili veya sistem yapılandırma arızalarını gösteren PhyHealth gibi çeşitli veri nesnelerini (DO) içerir (ABB, 2009, 2012).

Mantıksal düğüm (LN) içindeki her veri öğesi (DO), IEC 61850-7-3 standardına göre ortak bir veri sınıfının (CDC) spesifikasyonuna uygundur. Her CDC, mantıksal düğüm içindeki verilerin türünü ve yapısını açıklar. Her CDC'nin tanımlanmış bir adı ve her biri tanımlanmış bir ada, tanımlanmış bir türe ve belirli bir amaca sahip bir dizi CDC özniteliği (DA) vardır. Bir CDC'nin her bir özniteliği, öznitelikleri kategorilere ayıran bir dizi işlevsel kısıtlamaya (FC) aittir (ABB, 2009; Mackiewicz, 2006).

Örneğin, Şekil 2.4'te açıklanan Cihaz isim plakası (DPL) CDC'sinde, açıklama (DC) öznitelikleri ve genişletilmiş tanım (EX) öznitelikleri için işlevsel kısıtlamalar vardır.

Bu örnekte, DPL sınıfının açıklama (DC) öznitelikleri şunlardan oluşur: üretici (vendor), donanım sürümü (hwRev), firmware sürümü (swRev), seri numarası (serNum), cihazın modeli (model) ve konum (location) bilgileridir.

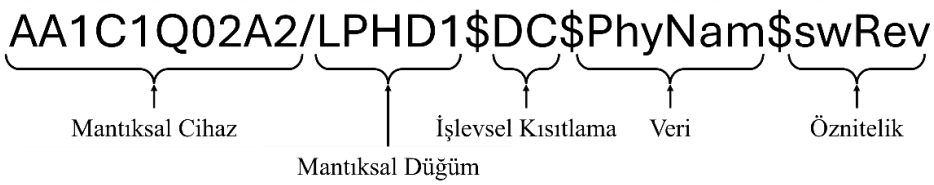
Bir cihazın IEC 61850 modeli, cihazın ve nesnelerinin soyut bir görünümüyle başlayan ve IEC 61850'in 7. bölümünde tanımlanan sanallaştırılmış bir modeldir. Daha sonra, bu soyut model, IEC 61850-8-1 bölümünde MMS (ISO9506), TCP/IP ve Ethernet'e dayalı belirli bir protokol yığınına eşlenmiştir. IEC 61850 nesnelerinin MMS'ye eşlenmesi sürecinde, IEC 61850-8-1, model bilgilerini adlandırılmış bir MMS değişken nesnesine dönüştürme yöntemini belirtir. Bunun sonucu, modeldeki her veri öğesinin benzersiz ve açık bir referansının olmasıdır (Mackiewicz, 2006). Örneğin, bir IED'den oluşan "AA1C1Q02A2" adlı bir mantıksal cihazımızın

olduğunu ve bu cihazın firmware'inin sürümünü belirlemek istediğimizi varsayalım. Bunu yapmak için Şekil 2.5'te gösterilen nesneyi okumamız gerekmektedir.

Name	Type	FC	Value/ Value range	M/O	OPC Data Type
vendor	VISIBLE STRING255	DC		M	VT_BSTR
hwRev	VISIBLE STRING255	DC		O	VT_BSTR
swRev	VISIBLE STRING255	DC		O	VT_BSTR
serNum	VISIBLE STRING255	DC		O	VT_BSTR
model	VISIBLE STRING255	DC		O	VT_BSTR
location	VISIBLE STRING255	DC		O	VT_BSTR
cdcNs	VISIBLE STRING255	EX		O	VT_BSTR
cdcName	VISIBLE STRING255	EX			VT_BSTR
dataNs	VISIBLE STRING255	EX		O	VT_BSTR

Öznitelik İşlevsel Kısıtlama Zorunlu/İsteğe Bağlı

Şekil 2.4. IEC 61850'deki cihaz isim plakası ortak veri sınıfının anatomisi (ABB, 2004).



Şekil 2.5. IEC 61850-8-1 nesne adı anatomisi.

2.8.3. Trafo merkezi yapılandırma dili (SCL)

Trafo Merkezi Yapılandırma Dili (SCL), IEC 61850 tabanlı sistemlerin yapılandırmasını tanımlayan XML tabanlı bir tanımlama dilidir. SCL, sistemin birden fazla seviyesinin açık ve standartlaştırılmış XML dosyalarında tanımlanmasını sağlayan bir yapılandırma dosyaları hiyerarşisi belirler (Lloret ve ark., 2007; Mackiewicz, 2006).

Bu tanımlama dili; bir IEC 61850 trafo merkeziyle ilgili tüm bilgilerin tutarlı bir şekilde belgelenmesini ve trafo merkezinin otomasyon sistemi (SAS) ile trafo merkezi (şalt sahası) arasındaki ilişkilerin tanımlanmasını sağlar. Bu nedenle, bu format, farklı üreticilerden gelseler bile, farklı uygulamalar arasında IEC 61850'ye

özgü verilerin alışverişi için uygundur. Uygulama düzeyinde, şalt sahasının topolojisinin kendisi ve şalt sahası yapısının IED'ler üzerinde yapılandırılan SAS fonksiyonlarıyla (mantıksal düğümler) ilişkisi açıklanabilir (Mackiewicz, 2006; Siemens, 2024).

SCL sözdizimi, her biri belirli bir amaca sahip farklı dosya türlerini destekler (Energinet, 2019; Lloret ve ark., 2007; Mackiewicz, 2006):

- ICD (IED Yetenek Açıklaması) dosyası: bir satıcının bir cihazın tüm yeteneklerini tanımladığı dosyadır.
- IID dosyası: ICD dosyasıyla birlikte, IED mühendisliği, yeteneklerin cihazda nasıl kullanıldığını açıklayan bir IID (Örneklenmiş IED Açıklaması) dosyası oluşturabilir. IID dosyası daha sonra sistem mühendisliği tarafından bir CID (Yapılandırılmış IED Açıklaması) veya bir SCD (Sistem Yapılandırma Açıklaması) dosyası oluşturmak için kullanılabilir.
- CID dosyası: Yalnızca bir IED'nin yapılandırmasını açıklar ve bir IED'ye yüklendiğinde, söz konusu IED'nin davranışını yapılandırır.
- SCD dosyası, CID'dekiyle aynı ayrıntıları içeren bir veya daha fazla IED'yi ve bunların birbirleriyle ve sistemle nasıl ilişkili olduğunu açıklar. Bu dosya ayrıca bir IED'nin davranışını yapılandırmak için de yüklenebilir.
- Sistem Spesifikasyon Açıklaması (SSD) dosyası: Bu dosya, trafo merkezi ve işlevleri (mantıksal düğümler) için tek hat şeması da dahil olmak üzere bir trafo merkezi otomasyon sisteminin eksiksiz özelliklerini içerir.

Tüm bu dosyalar aynı yöntem ve formatta oluşturulur, ancak ihtiyaca bağlı olarak farklı kapsamlara sahiptir (Mackiewicz, 2006). Bu dosyaların kullanımı, trafo merkezi sistem elemanlarının öz tanımını sağlar (Lloret ve ark., 2007). Her cihaz, kendi yapılandırmasını açıklayan bir SCL dosyası sağlamalıdır.

Bir IEC 61850 istemcisi, bir ağ üzerinden IED'ye bağlandığında IED'nin yapılandırmasını IED'den çıkarabilse de, SCL gibi resmi bir çevrimdışı tanımlama dilinin kullanılabilirliğinin, IEC 61850 istemci uygulamalarını yapılandırmanın dışında kullanıcılara çok büyük faydalar sağlayabileceği çeşitli senaryolar vardır. SCL, her kullanıcının ihtiyaçlarına en uygun şekilde kullanılabilir. Bu çalışmada cihazlara zarar verebilecek aktif varlık ve/veya zafiyet tarama yöntemlerine

başvurmadan pasif bir yoldan cihazların zafiyetlerini araştırabilmek için IED cihazlarının özellikleri ve bilgileri SCL dosyalarından çekilecektir.

SCL dosyaları; Omicron'un IED analiz, simülasyon ve test aracı olan IEDScout (Omicron, 2024), ABB'nin koruma ve kontrol IED yöneticisi olan PCM600 (ABB, 2025f), vs. gibi ticari araçlarla üretilebileceği gibi (ABB, 2012; Hadbah ve ark., 2014), açık kaynaklı yazılım olan IEC 61850 istemcisi IEDExplorer (Charvat, 2013) aracıyla de elde edilebilir.

3. UYGULAMA

Bu bölümde, önerdiğimiz metodolojiyi açıkladıktan sonra geliştirdiğimiz yaklaşımı test edeceğiz ve ürettiği sonuçların doğruluğunu kontrol edeceğiz.

3.1. Test Yatağı

Bu çalışma, EKS sistemlerinin modeli olarak Sakarya Üniversitesi'nde bulunan Kritik Altyapılar Ulusal Test Yatağı Merkezi'ndeki enerji üretim, iletim ve dağıtım sistemleri kullanılmıştır. CENTER Energy isimli bu test yatağı merkezi, kritik altyapıların güvenliği ile ilgilenen araştırmacılara ve profesyonellere çözümlerin araştırılması, geliştirilmesi ve test edilmesi için bir çalışma ortamı sunmaktadır (Sakarya Üniversitesi, 2023).

CENTER Energy test yatağı, TM-1 ve TM-2 olmak üzere iki trafo merkezinden oluşmaktadır. Üretim tarafında farklı enerji kaynakları tarafından üretilen enerji, TM-1'i orta gerilim enerjisiyle besleyip TM-2'ye iletilmek üzere yüksek gerilime dönüştürülür. Daha sonra, dağıtım merkezi için yine orta gerilime dönüştürülür. Yüksek gerilim ve orta gerilim fiderlerinde hat olaylarının izlenmesi ve kontrolü için trafo diferansiyel, mesafe kontrol ve aşırı akım röleleri kullanılmakta ve koruma konfigürasyonları yapılmaktadır. Yardımcı röleler, trafo merkezlerinde ve dağıtım merkezlerinde trafo, kesici ve ayırıcı cihazlarının saha sinyallerini modellemek için kullanılır. TM-1'de üretim, iletim ve dağıtım prosesleri SICAM SCC SCADA, Siemens, ABB ve GE marka röleler ve Siemens marka RTU kullanılarak kontrol edilirken TM-2'de iletim ve dağıtım prosesleri ABB Micro SCADA, ABB ve Schneider marka röleler ve ABB marka RTU kullanılarak kontrol edilmektedir (Ozcelik ve ark., 2021).

Tüm çalışmalarımız ve deneylerimiz, TM-2'de bulunan ABB'nin Relion® ürün ailesinin üyeleri olan REF615, REL650 ve RET670 üzerinde yapılmıştır. Relion®, IEC ve ANSI uygulamaları için güç sistemlerinin korunması, kontrolü, ölçümü ve denetimi için IEC 61850 standardının temel değerlerini uygulamak üzere tasarlanmış ürünler içermektedir. Bu, IED'lerin işlevselliği standarda uygun bir veri modelinde

temsil edildiği ve IED'lerin standart tarafından sağlanan çeşitli hizmetleri desteklediği anlamına gelir (ABB, 2025e). Bunlardan (ABB, 2012);

- Proses verileri: durum bilgilerinin izlenmesi ve ölçümler,
- Uygulama verileri: koruma aktivasyonları, anahtar açma, arıza kayıtları,
- Bozulma kayıt dosyaları,
- Kontrol komutları,
- Koruma ayarları,
- Ayar grupları,
- Yapılandırma verileri,
- Özdenetim mesajları,
- Cihazlar arasında hızlı yatay iletişim,
- ve zaman senkronizasyonudur.

3.1.1. REL650

REL650, doğrudan topraklanmış veya empedans topraklı şebekelerde havai hatların ve kabloların korunması, kontrolü ve izlenmesi için kullanılır. Bu IED cihazı, bir ve/veya üç fazlı açma gerektiren, ağır yüklü hatlar ve çok terminalli hatlar olmak üzere her türlü havai hat, kablo ve elektrik şebekesi topraklaması için mesafe koruması sağlamaktadır. Ayrıca, bir devre kesici için yedek koruma ve cihaz kontrolü yapabilir (ABB, 2010, 2017).

3.1.2. RET670

RET670, iki ve üç sargılı trafolar, ototrafolar, jeneratör-trafo üniteleri, faz kaydırmalı trafolar, özel demiryolu trafolar ve şönt reaktörler için koruma, izleme ve kontrol sağlayan bir diferansiyel koruma cihazıdır (ABB, 2007).

3.1.3. REF615

REF615, dağıtılmış güç üretimi olan veya olmayan trafo merkezlerinin ve endüstriyel güç sistemlerinin korunması, kontrolü, ölçümü ve denetimi için tasarlanmış özel bir fider koruma ve kontrol rölesidir. REF615, ABB'nin Relion® ürün ailesinin bir üyesi ve 615 koruma ve kontrol ürün serisinin bir parçasıdır (ABB, 2021). 615 serisi altyapı trafo merkezlerinin ve endüstriyel şalt ekipmanlarının düşük seviyeli koruma ve denetim uygulamaları için sayısal IED serisidir (ABB, 2012).

3.2. Kullanılacak Yöntemler

3.2.1. Zafiyet veritabanının oluşturulmasıyla ilgili

Bu çalışma, belirli bir üreticinin bir veya birden fazla cihazına ilişkin yayımladığı güvenlik uyarıları ve bildirimlerini sistematik bir rapora dönüştürmeyi amaçlamaktadır. Bu amaç doğrultusunda pasif tarama yöntemi kullanılacaktır. Pasif zafiyet tespitinde yaygın olarak kullanılan yöntemlerden biri, CVE (Common Vulnerabilities and Exposures) ile CPE (Common Platform Enumeration) korelasyonudur. Ancak, ABB tarafından yayımlanan dokümanlar incelendiğinde, bu dokümanların bir zafiyetten etkilenen cihazın CPE tanımlayıcısından ziyade cihazın modeli, tasarım standardı, donanım ve yazılım sürümleri gibi bilgileri içerdiği görülmektedir. Ayrıca, önceki bölümde de açıklandığı üzere CVE-CPE korelasyonu çeşitli sınırlılıklara sahiptir. Bu nedenle, bu çalışmada bir cihazın sahip olduğu güvenlik açıkları, üretici, model, desteklediği uygulamalar ile donanım ve yazılım sürümleri temel alınarak araştırılacaktır. Bununla birlikte, yapılan incelemeler sonucunda, bu ihtiyacı doğrudan karşılayacak nitelikte ve istenilen formatta bir veritabanının bulunmadığı tespit edilmiştir.

NVD gibi güvenlik veritabanları, bir cihazda kullanılan üçüncü taraf yazılım bileşenleri veya işletim sistemlerinden kaynaklanan güvenlik açıklarını belirleme konusunda yetersiz kalmaktadır. Örneğin, ABB'nin yayımladığı bir güvenlik duyurusuna (ABB, 2019) göre, 2.1 donanım sürümüne sahip 650 ve 670 serisi ürünlerinde (REL650 ve RET670 dahil olmak üzere) kullanılan OpenSSL kütüphanesindeki zayıflıklar nedeniyle bu cihazların CVE-2016-2177, CVE-2016-2178, CVE-2016-2182, CVE-2016-2183, CVE-2016-6304 ve CVE-2016-6306 zafiyetlerinden etkilendiği belirtilmektedir. Ancak, NVD'nin (2016) kayıtları incelendiğinde, söz konusu CVE girdilerinde bu cihazların üreticisine, modeline veya benzeri tanımlayıcı bilgilerine dair herhangi bir ifadenin yer almadığı görülmektedir (NIST, 2016a, 2016b, 2016c, 2016d, 2016e, 2016f). Bu durum, NVD'nin doğrudan üretici, cihaz modeli, donanım ya da yazılım sürümleri gibi parametreler kullanılarak filtreleme yapmaya imkân tanımadığını ortaya koymaktadır.

Bu bilgilerle hareketle, bu çalışmada tedarikçinin yayımladıkları dokümanları baz alarak cihazların ilgili özellikleri ve bilgilerini içerecek bir zafiyet veritabanı

oluşturmaya karar verilmiştir. Bu veritabanında güvenlik açığıyla ilgili ekstra bilgiler içerip bu bilgiler CWE ve NVD'den alınacaktır.

3.2.2. SCL dosyalarının ayrıştırılması ile ilgili

IEC 61850 standardının dokümanları ve CENTER Energy test yatağında bulunan ABB'nin REF615, REL650 ve RET670 cihazlarının HMI'ları ve bu IED'lerde elde ettiğimiz SCL dosyalarını inceleyerek IED'nin;

- üretici bilgisi "LPHD1DCPhyNam$vendor",
- model bilgisi "LPHD1DCPhyNam$model",
- yazılım sürüm bilgisi "LPHD1DCPhyNam$swRev",
- seri numarası bilgisi "LPHD1DCPhyNam$serNum",
- sipariş kodu bilgisi (varsa) "LDEV1EXNamPlt$eOrdNum",
- ve donanım sürüm bilgisi (varsa) "LINF1EXNamPlt$eDevRev",

nesnelerinde bulunduğu görülmüştür.

3.2.3. Veritabanında zafiyet filtreleme işlemi ile ilgili

ABB'nin ürün kılavuzları, teknik dokümanları ve yayımladığı güvenlik uyarı ve bildirimleri incelendiğinde aşağıdaki bulgulara ulaşılmıştır:

- Tasarım standartlarına göre çeşitlendirme: ABB, bazı Akıllı Elektronik Cihazlarını (IED), örneğin REF615'i, IEC (ABB, 2025b), ANSI (ABB, 2025c, 2007a) ve CN olmak üzere üç farklı tasarım standardına uygun şekilde üretmekte ve piyasaya sunmaktadır. Bu cihazların donanım ve/veya yazılım sürümleri isim olarak aynı olsa da, etkilendikleri güvenlik açıkları ile bu açıkların giderilmesine yönelik yamalar, tasarım standardına bağlı olarak farklılık gösterebilmektedir (ABB, 2025d).
- Sipariş kodlarının önemi: Cihazların sipariş kodları, rölenin donanım ve yazılım modüllerinden türetilen alfanümerik karakterlerden oluşmakta ve cihazla ilgili kritik bilgiler barındırmaktadır. Bu kod, özellikle cihazın tasarım standardı ve donanım sürümü hakkında bilgi sağlamaktadır. Tasarım standardına ilişkin bilgi SCL dosyalarında veya cihazın HMI arayüzünde bulunmazken, sipariş kodu her iki yerde de mevcuttur. Dolayısıyla, sipariş kodunun çözümlenmesiyle cihazın tasarım standardına ulaşmak mümkündür. Nitekim, sipariş kodunun soldan ikinci

karakteri “A” olduğunda cihaz ANSI, “B” olduğunda IEC, “C” olduğunda ise CN standardına göre tasarlanmış olmaktadır (ABB, 2007a; ABB Oy., 2010).

- Ürün serileri: ABB’nin dijital trafo merkezlerinde kullanılan IED’leri belirli ürün serilerine ayrılmaktadır. Bu seriler yalnızca sayılardan oluşan isimlerle ifade edilmektedir (ör. 650, 670, 630, 615). Örneğin REF615, 615 koruma ve kontrol ürün serisine; REL650 ve RET670 ise sırasıyla 650 ve 670 ürün serilerine dahildir (ABB, 2021).
- Relion ürün ailesi: ABB’nin “Relion” olarak adlandırılan bir IED ürün ailesi mevcuttur. Bu aile, 615, 650 ve 670 serilerinin yanı sıra 630 IEC serisi, 620 IEC serisi, 611 serisi, 605 serisi gibi farklı serileri de kapsamaktadır (ABB, 2025e).
- Güvenlik bildirimlerindeki tanımlama çeşitliliği: ABB’nin güvenlik bildirimlerinde, bir güvenlik açığından etkilenen cihazlar farklı biçimlerde tanımlanabilmektedir. Bu tanımlar cihazın modeli, ait olduğu ürün ailesi veya ürün serisi ile yapılabildiği gibi, bunların çeşitli kombinasyonlarını da içerebilmektedir. Ayrıca, farklı tasarım standartlarına sahip cihazlarda bu bilginin cihaz ismine eklenerek belirtildiği gözlemlenmiştir. Örneğin, bir güvenlik açığından etkilenen cihaz şu şekilde ifade edilebilmektedir: REF615, Relion 650 series, Relion 670 series, 615 series IEC 5.0 FP1 vb...

Bu çalışma kapsamında geliştirilen program, cihazların etkilendiği güvenlik açıklarının gözden kaçırılmaması amacıyla, olası tüm varyasyonları dikkate alacak biçimde tasarlanmıştır.

3.3. Kullanılacak Araçlar

Bu cihazların konfigürasyon dosyalarını elde etmek için IEC 61850 istemcisi olan IEDExplorer yazılımı kullanılmıştır. Geliştirilecek program, Python dilinde yazılmıştır ve tüm güvenlik açıkları ve ilgili verileri depolamak için Mysql veritabanı yönetim sistemi tercih edilmiştir. Bu araçlarla ilgili ayrıntılar aşağıda verilmiştir.

3.3.1. Python ve Mysql

Python, esnek yapısı, geniş kütüphane desteği ve kolay öğrenilebilirliği sayesinde siber güvenlik alanında sıklıkla tercih edilen bir programlama dilidir. Özellikle saldırı tespiti, zafiyet analizi, olay müdahalesi ve log yönetimi gibi alanlarda yaygın kullanım alanı bulmaktadır. MySQL ise açık kaynaklı ve yaygın olarak kullanılan bir

ilişkisel veritabanı yönetim sistemi olup hem kurumsal hem de bireysel sistemlerde kritik verilerin depolanmasında önemli rol oynamaktadır.

Bu çalışmada önerilen yaklaşım Python ile gerçekleştirilecektir. Her bir güvenlik açığına ilişkin bilgiler bir Mysql veritabanında saklanıp basit bir SQL sorgusu kullanılarak, belirli statik bilgilere sahip bir cihazın etkilendiği zafiyetler ve ilgili ayrıntıları listelenecektir.

3.3.2. IEDExplorer

Bu çalışmada, (EKS) operatörlerinin varlık envanterlerinde IED cihazlarına ilişkin bilgilerin eksik olduğu varsayılmıştır. Bu nedenle, söz konusu bilgilerin SCL dosyaları üzerinden elde edilmesi hedeflenmiştir. SCL dosyaları genellikle IEC 61850 istemci araçları aracılığıyla temin edilebilmektedir. Örneğin, ABB'nin Relion serisi koruma ve kontrol IED uygulamaları için geliştirdiği PCM600 aracı bu işlevi sağlayabilmektedir (ABB, 2025e).

Bu çalışmada her ne kadar yalnızca ABB ürünleri üzerinde testler gerçekleştirilmiş olsa da önerilen yaklaşım, farklı üreticilerin ürünlerini de kapsayacak şekilde genişletilebilir niteliktedir. Bu doğrultuda, üreticiye özgü yazılımlar kullanılabilmektedir. Örneğin, Omicron tarafından geliştirilen IEDScout yazılımı, farklı tedarikçilere ait IEC 61850 tabanlı IED cihazlarının konuşlandırılması, yapılandırılması ve yönetilmesine olanak tanıyan ticari bir çözümdür (Hadbah ve ark., 2014). Ancak, bu yazılımın lisanslı olması ve yalnızca 30 günlük deneme sürümü sunması nedeniyle bu çalışmada tercih edilmemiştir.

Bunun yerine, açık kaynaklı ve ücretsiz bir IEC 61850 istemci aracı olan IEDExplorer kullanılmıştır. Test ve eğitim amaçlı geliştirilen IEDExplorer, MMS (ISO/IEC 9506-1 ve ISO/IEC 9506-2) iletişim protokolü üzerinden IEC 61850 cihazlarına (IED'lere) bağlanabilmektedir. Araç, saf C# diliyle geliştirilmiş olup Windows işletim sistemi üzerinde .NET ortamında çalışmaktadır. BinaryNotes ASN.1 aracına dayanan bir MMS ASN.1 ayrıştırıcısını da bünyesinde barındırmaktadır.

IEDExplorer yazılımının temel özellikleri şu şekilde özetlenebilir (Charvat, 2013):

- Bir IEC 61850 cihazına (IED'ye) bağlanabilir.
- Ağaç yapısındaki MMS değişkenlerini inceleyebilir.

- Değerleri okuyabilir/yazabilir.
- "Seç ve Sonra İşlet" (SBO) kontrol komutları dahil olmak üzere komutlar verebilir.
- Dinamik değişken listeleri oluşturabilir veya silebilir.
- Dinamik veya statik değişken listeleri aracılığıyla arabelleğe alınmış/alınmamış raporları etkinleştirebilir ve okuyabilir.
- Dizinleri ve dosyaları okuyabilir (örneğin COMTRADE koruma olay kayıtları için).
- MMS paketlerini yakalayabilir, XML veya ağaç biçiminde inceleyebilir.
- GOOSE mesajlarını inceleyebilir.
- GOOSE mesajları gönderebilir.
- SCL dosyalarını inceleyebilir.
- SCL verilerini kullanarak IED simülasyonu yapabilir (özellik, yerel libiec61850.dll kullanılarak deneysel ALPHA durumundadır).

3.3.3. Nmap

Nmap (Network Mapper), açık kaynaklı ve komut satırı tabanlı bir ağ keşif ve güvenlik tarama aracıdır. Sistem yöneticileri ve siber güvenlik uzmanları tarafından hedef sistemlerdeki açık portları, çalışan servisleri, işletim sistemi bilgilerini ve ağ üzerindeki cihazları tespit etmek amacıyla yaygın olarak kullanılmaktadır (Nmap, 1997).

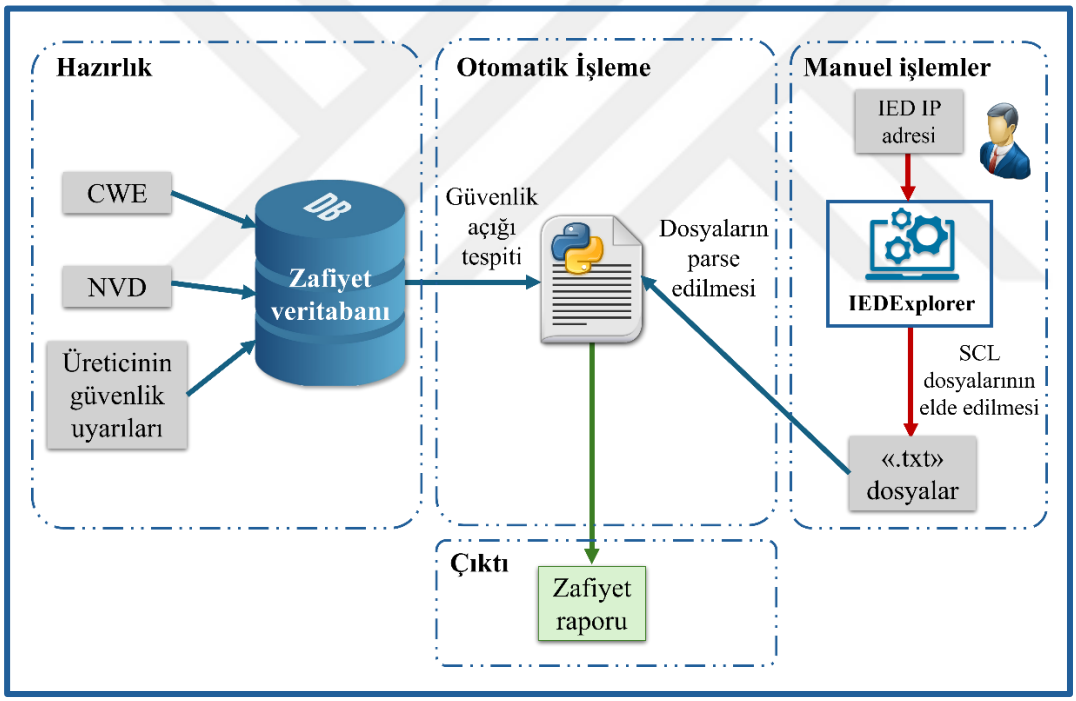
Nmap, host tarama yaparak ana bilgisayarları ve üzerlerinde çalışan hizmetleri belirlemek için kullanıcının isteğine göre aşağıdaki yöntemlerden bir tanesini kullanabilir (Samanis ve ark., 2022):

- Port tarama: Cihazlardaki açık portları tespit etmek için tüm bir ağ veya alt ağda arama yapmak için kullanılır.
- ICMP tarama: Canlı cihazlara hangi IP adreslerinin eşleneceğini belirlemek için tek bir ICMP ping paketi içeren basit bir tarama tekniğidir. Nmap, bir ana bilgisayarın canlı olup olmadığını belirlemek için ICMP zaman damgası istekleri gönderebilir ve ICMP zaman damgası yanıtlarını bekleyebilir.
- ARP tarama: Kullanıcının ARP paketleri aracılığıyla IPv4 ağına bağlı tüm cihazları keşfetmesini sağlar. Bu teknikle IP adresleri MAC adreslerine eşlenir. Bu yöntem, OT sistemleri için güvenli bir yöntemdir (Pöhler ve ark., 2024).

IEDExplorer gibi IEC 61850 istemci uygulamaları aracılığıyla SCL dosyalarının elde edilebilmesi için ilgili cihazın IP adresinin bilinmesi gerekmektedir. Ancak, bu cihazların kurumun varlık envanterinde kayıtlı olmaması ya da IP adreslerinin herhangi bir şekilde belirlenememesi durumunda, bu çalışmada alternatif bir yöntem olarak **Nmap** aracı kullanılmıştır. Nmap üzerinden gerçekleştirilen **ARP taramaları** sayesinde ağda bulunan hostların listesi, IP adresleriyle birlikte tespit edilerek cihazlara erişim mümkün hale getirilmektedir.

3.4. Önerilen Yaklaşım

Bu çalışmada önerilen yaklaşımın genel çerçevesi, hazırlık, manuel işlemler ve otomatik işleme olmak üzere üç temel aşamadan oluşmakta olup, söz konusu süreç Şekil 3.1'de görselleştirilmiştir.



Şekil 3.1. Çalışmanın kapsamında önerilen yaklaşıma genel bakış.

3.4.1. Hazırlık aşaması

Hazırlık aşaması, IED cihazlarına ilişkin bilinen güvenlik açıklarını içeren kapsamlı bir veritabanının oluşturulmasını kapsamaktadır. Bu veritabanında yer alan bilgiler aşağıda özetlenmiştir:

- Güvenlik açığının CVE tanımlayıcısı,
- Güvenlik açığının CWE tanımlayıcısı ve adı,

- Üretici tarafından ilgili zafiyete atanan tanımlayıcı,
- Zafiyetin kısa açıklaması,
- CVSS (Common Vulnerability Scoring System) puanı (0–10 arası), önem derecesi (kritik, yüksek, orta veya düşük) ve atak vektörü,
- Zafiyetin bulunduğu cihaz modeli ve etkilenen firmware sürümü/sürümleri,
- Zafiyetin giderildiği yama sürümü,
- Yamanın uygulanabileceği cihaz özellikleri (ör. belirli donanım sürümü, tasarım standardı vb.),
- Yamaya ek olarak ya da yamanın bulunmadığı veya cihaza uygun olmadığı durumlarda alınabilecek alternatif önlemler,
- NVD, CWE ve üretici web sitelerindeki ilgili bağlantılar aracılığıyla güvenlik uzmanlarının ulaşabileceği ek bilgi ve kaynaklar.

Bu kapsamda, ABB'nin resmi web sitesinde (ABB, 2025a) yayımlanan güvenlik uyarıları ve bildirimleri incelenmiş ve IED'lerle ilişkili olanlar belirlenmiştir. Ardından, bu belgelerden elde edilen veriler NVD (NIST, 2025a) ve CWE (MITRE, 2025) platformlarından toplanan bilgilerle birlikte manuel olarak veritabanına aktarılmıştır. Ayrıca, ABB'nin firmware güncellemelerine ilişkin dokümanları (ABB, 2025d) incelenerek yamaların cihazlarla uyumluluğu kontrol edilmiş ve ilgili bilgiler veritabanına eklenmiştir.

Bu çalışmada yalnızca ABB'ye ait IED cihazları ele alındığından, zafiyet veritabanı tek bir tablo ("ABB" tablosu) olacak şekilde tasarlanmıştır. Bununla birlikte, bu yapı ileride Siemens, General Electric, Schneider Electric gibi diğer üreticilerin ürünlerine ilişkin zafiyetlerin de ayrı tablolar halinde eklenmesine olanak sağlayacak biçimde genişletilebilir şekilde planlanmıştır.

Oluşturulan veritabanı, sonraki aşamalarda SCL dosyalarından elde edilecek IED cihaz özellikleriyle çapraz karşılaştırma yapılarak cihazların etkilendiği güvenlik açıklarının tespit edilmesini ve buna uygun zafiyet raporlarının üretilmesini mümkün kılacaktır. Bu veritabanının temel amacı, sistem güvenliğini sağlamakla görevli güvenlik uzmanlarına, cihazların zafiyetleri ve korunma yöntemlerine ilişkin mümkün olan en kapsamlı bilgiyi sunmaktır.

3.4.2. Manuel işlemler aşaması

Sürecin işleyişini somut bir örnek üzerinden açıklamak gerekirse; bir kurumun sisteminde konuşlandırdığı IED cihazlarının bilinen güvenlik açıklarından etkilenip etkilenmediğini kontrol etmek ve olası zafiyetlerin nasıl giderilebileceğine dair bilgi edinmek istediği varsayılsın. Bu durumda, Şekil 3.1'de sunulan metodoloji izlenmektedir.

İlk olarak, sistemdeki IED cihazlarının IP adresleri kurumun tuttuğu varlık envanterinden elde edilir. Envanterde bu bilgilerin bulunmaması halinde ise, OT sistemleri açısından güvenli ve zararsız bir yöntem olan Nmap tabanlı ARP taraması kullanılarak ağdaki hostların keşfi yapılır ve IP adresleri tespit edilir.

Elde edilen IP adresleri, IEDExplorer yazılımı aracılığıyla her bir cihaza bağlanmak ve bu cihazlara ait SCL dosyalarını temin etmek için kullanılır. Elde edilen her bir konfigürasyon dosyası, cihazın IP adresini dosya adı olacak şekilde ".txt" formatında kaydedilir.

Bu noktaya kadar olan işlemler manuel olarak yürütülmekte olup, süreç tamamlandıktan sonra sisteme doğrudan bağlı kalmaya gerek bulunmamaktadır. Kalan tüm işlemler, çevrimdışı ortamda ve bu çalışma kapsamında geliştirilen program aracılığıyla otomatik olarak gerçekleştirilecektir.

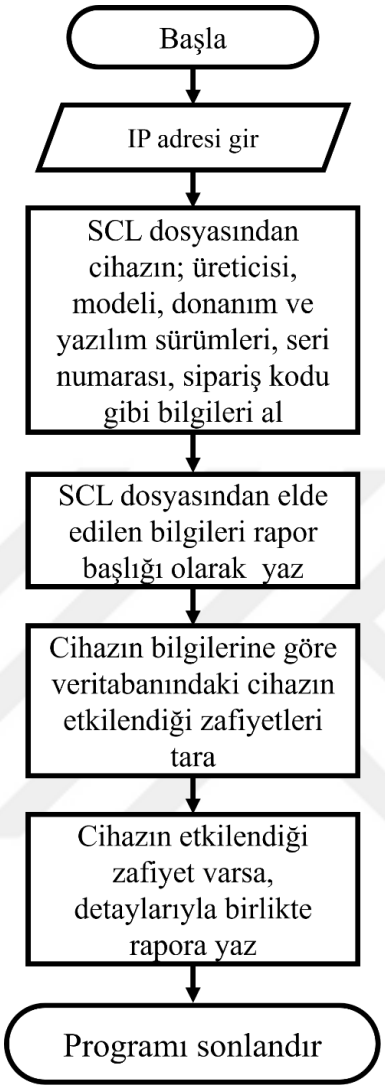
3.4.3. Otomatik işleme aşaması

Otomatik işlemenin akışı Şekil 3.2'deki gibidir.

Bu aşamada, kullanıcıya üç farklı seçenek sunulmaktadır (bkz. Şekil 3.3):

- Tek cihaz analizi: Kullanıcı, tek bir IP adresi girerek ilgili cihaza ait SCL dosyasının ayrıştırılmasını sağlayabilir. Bu işlem sonucunda cihazın statik bilgilerini (ör. üretici, model, donanım/yazılım sürümleri) ve etkilendiği güvenlik açıklarının detaylarını içeren bir rapor üretilmektedir.
- IP aralığı analizi: Kullanıcı, belirli bir IP adresi aralığı girerek bu aralıkta yer alan cihazları analiz edebilir. SCL dosyaları elde edilebilen cihazların bilgileri ilgili dosyalardan çıkarılmakta ve her bir cihaz için belirlenen güvenlik açıkları ve detayları tek bir raporda birleştirilmektedir.
- Manuel bilgi girişi: Kullanıcı, bir cihaza ait bilgileri manuel olarak girerek, veritabanıyla karşılaştırmalı bir analiz yapılmasını sağlayabilir. Bu yöntemle de

ilgili güvenlik açıklarını ve bunlara ilişkin ayrıntıları içeren rapor elde edilmektedir.



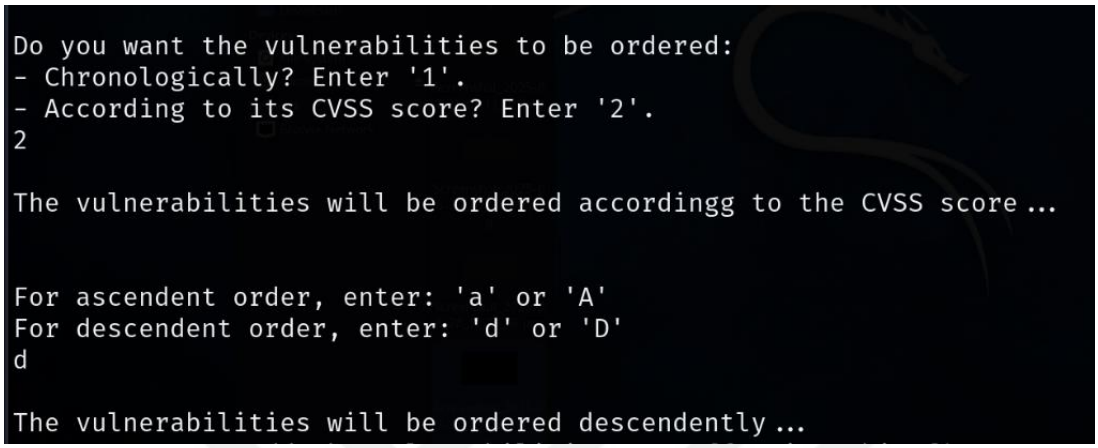
Şekil 3.2. Otomatik işlemenin akışı.

```
**************
Starting Menu
**************
If you want to enter:
- an IP address, enter "1".
- an IP range, enter "2".
- a device model, enter "3".

Enter 'q' or 'Q' to quit.
_
```

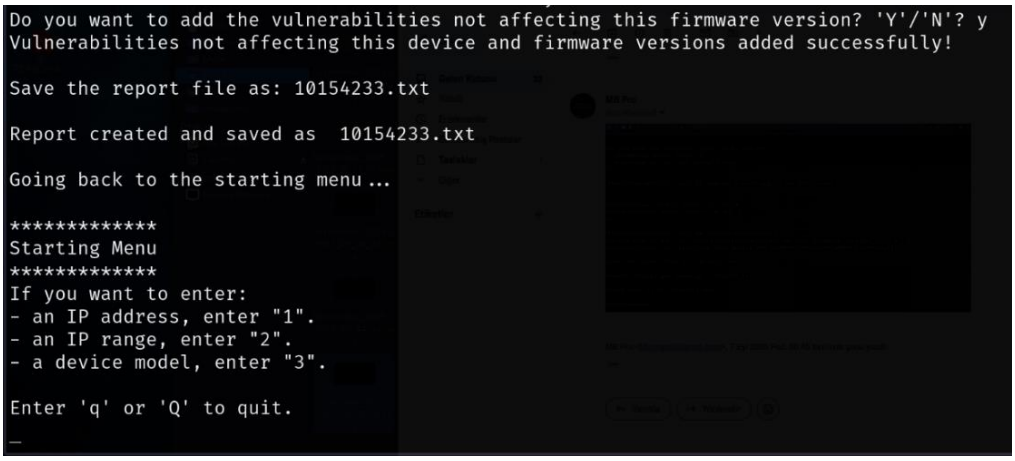
Şekil 3.3. Geliştirilen programın ana menüsü.

Buna ek olarak, Şekil 3.4'te gösterildiği gibi kullanıcı zafiyet raporunun güvenlik açıklarının sıralanma kriterlerini belirleyebilir. Raporda sıralama, güvenlik açıklarının yayınlanma tarihine (kronolojik) veya CVSS puanına göre yapılabilir. Ayrıca, kullanıcı sıralamanın yönünü artan veya azalan olarak seçme olanağına sahiptir.



Şekil 3.4. Zafiyetlerin sıralama kriterleri ve yönü seçeneklerinin örneği.

Şekil 3.5'te gösterildiği üzere, kullanıcı, ilgili cihazın muaf olduğu güvenlik açıklarını zafiyet raporuna dahil etme seçeneğine sahiptir ve bu bilgiler rapor üzerinde görüntülenebilir. Bu seçeneğin tercih edilmesinin ardından, kullanıcı oluşturulacak zafiyet raporuna bir isim atar. Daha sonra, program otomatik olarak ana menüye dönmektedir. Söz konusu zafiyet raporlarında cihazlara ait teknik bilgiler yer almakta; cihazın etkilendiği güvenlik açıkları, bu açıkların detayları, giderildiği yamalar ve alınması gereken ek önlemler gibi bilgiler düzenli bir biçimde sunulmaktadır.



Şekil 3.5. Cihazın muaf olduğu zafiyetlerin ekleme seçeneği ve oluşturulacak raporun isimlendirilmesi.

SCL dosyalarının ayrıştırılma ve zafiyetlerin filtrelenme süreçleri otomatik olarak yürütülmektedir.

Kullanıcının IP adresi veya IP adres aralığı girdiği durumlarda, Python 3 ile geliştirilen program, girdi olarak ".txt" formatında kaydedilen SCL dosyalarını almaktadır. Program, önceki bölümde belirtilen nesneleri kontrol ederek bu dosyaları ayrıştırmakta ve cihazın adı, üreticisi, modeli, donanım ve yazılım sürümleri, seri numarası, sipariş kodu gibi bilgileri çıkarmaktadır. Eğer sipariş kodu mevcutsa, program bu kodu çözümleyerek cihazın hangi standarda göre tasarlandığını belirlemekte; model bilgisine bakarak da cihazın hangi ürün serisine ve ürün ailesine ait olduğunu tespit etmektedir. Elde edilen tüm bu bilgiler program tarafından oluşturulan ve kullanıcı tarafından isimlendirilen bir dosyaya eklenmektedir.

Bir cihazın ayrıntıları çıkarıldıktan sonra program, öncelikle üretici bilgisine dayanarak veritabanından ilgili tabloyu çağırmaktadır. Daha sonra cihazın modeli, ürün ailesi, ait olduğu seri, tasarım standardı ve donanım sürümü dikkate alınarak, veritabanında cihazı etkileyen olası güvenlik açıkları aranmakta; yazılım sürümü ise bu güvenlik açıklarının etkilediği sürümlerle karşılaştırılmaktadır. Cihazın yazılım sürümünün söz konusu güvenlik açığını içerdiği tespit edilirse, program bu zafiyetin tüm bilgilerini düzenli bir şekilde rapor dosyasına eklemektedir.

Bir IP adres aralığı girildiği durumda, tüm cihazlar için bu işlem sırasıyla tekrarlanmakta; her bir cihazın SCL dosyası ayrıştırılmakta, ilgili güvenlik açıkları veritabanından çekilmekte ve elde edilen bulgular rapora işlenmektedir. Sürecin sonunda, bütün cihazların ve bunların etkilendiği güvenlik açıklarının detaylarını içeren kapsamlı bir rapor üretilmektedir.

Kullanıcı, bir cihazın bilgilerini manuel olarak girdiği durumda ise, herhangi bir SCL dosyası ayrıştırılmasına gerek kalmaksızın, kullanıcının sağladığı bilgiler temel alınarak zafiyet filtreleme ve belirleme işlemleri aynı şekilde yürütülmektedir.

3.5. Tarama Sonuçları

Önerilen programın değerlendirilmesi amacıyla, TM-2'de bulunan ve sırasıyla 10.154.23.1, 10.154.23.2 ve 10.154.23.3 IP adreslerine sahip REL650, RET670 ve REF615 cihazları üzerinde testler gerçekleştirilmiştir. Bu üç cihazın SCL dosyalarının ayrıştırılması ve zafiyetlerin filtrelenmesi sonucunda elde edilen

bilgiler, program tarafından oluşturulan zafiyet raporunda sırasıyla Şekil 3.6, Şekil 3.7 ve Şekil 3.8'de gösterildiği biçimde yer almaktadır.

SCL dosyaslarının ayrıştırılmasından elde edilen sonuçlar hem SCL dosyalarına hem de cihazların HMI'larına bakarak doğrulanmıştır.

Şekil 3.8'de gösterildiği üzere, programın çıktı olarak ürettiği zafiyet raporunda, her bir cihazın statik bilgileri altında, o cihaza ait güvenlik açıkları ve detayları ile birlikte sunulmaktadır. Şekilde, REF615 modelinde tespit edilen güvenlik açıklarından bir örneğin raporda nasıl yer aldığı gösterilmiştir.

```
****************************************
Details of Device of IP: 10.154.23.1
****************************************

Device Name: AA1C1Q02A1
Device Vendor: ABB
Device Model: REL650
Product Version: The file does not contain Product Version
Firmware Version: 2.2.9.6
Device Serial Number: T2018236
Device Order Number: The file does not contain Order Number

-------------------------

No known vulnerabilities for this device version
```

Şekil 3.6. REL650'nin cihaz bilgileri ve etkilendiği zafiyetler.

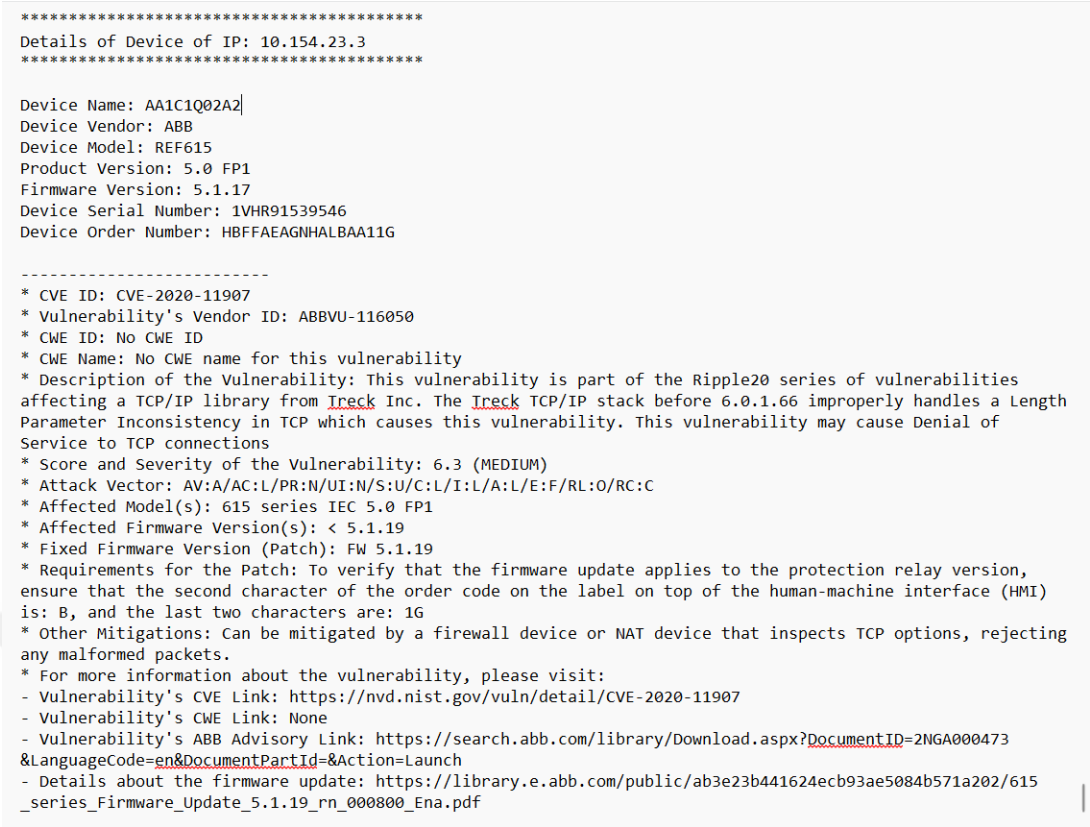
```
****************************************
Details of Device of IP: 10.154.23.2
****************************************

Device Name: AA1C1Q01A1
Device Vendor: ABB
Device Model: RET670
Product Version: The file does not contain Product Version
Firmware Version: 2.2.9.6
Device Serial Number: T2018237
Device Order Number: The file does not contain Order Number

-------------------------

No known vulnerabilities for this device version
```

Şekil 3.7. RET670'in cihaz bilgileri ve etkilendiği zafiyetler.



Şekil 3.8. REF615'in cihaz bilgileri ve etkilendiği zafiyet örneği.

Cihazın bilgileri ve etkilendiği güvenlik açıklarının ardından, kullanıcı tercihi doğrultusunda, etkilenmediği güvenlik açıkları da detaylarıyla birlikte rapora dahil edilebilir. Bu duruma ilişkin bir örnek Şekil 3.9'de gösterilmiştir.

Zafiyet tarama sonuçlarının doğruluğu, veritabanı üzerinden manuel kontrol yapılarak değerlendirilmiştir. Sonuçlar, programın cihazların etkilendiği güvenlik açıklarını doğru ve eksiksiz bir şekilde tespit ettiğini göstermektedir. Test ortamındaki REL650 ve RET670 IED'leri, 2.2.9.6 yazılım sürümüne sahip olup, bilinen herhangi bir güvenlik açığı içermemektedir. Buna karşılık, REF615 cihazı, IEC standardına göre tasarlanmış 5.0 FP1 donanım sürümüne ve 5.1.17 yazılım sürümüne sahip olup, orta seviyede 7 güvenlik açığı içermektedir. REF615'te tespit edilen güvenlik açıklarının listesi Tablo 3.1'de özetlenmiştir.

3.6. Sonuçların Tartışması

Bu çalışmada, akıllı şebeke cihaz üreticilerinin yayınladığı güvenlik bildirimleri ve uyarılarını yarı otomatik bir şekilde kapsamlı bir rapora dönüştüren bir yaklaşım sunulmuştur. Geliştirilen program, cihazın statik bilgileri SCL dosyasından elde

ettikten ya da kullanıcı tarafından girildikten sonra, veritabanındaki CVE kayıtlarını cihazın özelliklerine göre filtreleyerek, istenilen sonuçları eksiksiz bir şekilde ortaya koyabilmektedir.

```
----------------------------------------
*** The details of the vulnerabilities not affecting this device and firmware versions ***

* CVE ID: CVE-2014-3566
* Vulnerability's Vendor ID: ABB-VU-PPMV-1MRS758301
* CWE ID: CWE-310
* CWE Name: Cryptographic Issues
* Description of the Vulnerability: This is a vulnerability discovered in the SSL protocol 3.0.
 To work with legacy servers, many TLS clients implement a downgrade operation: In a first handshake attempt,
TLS clients offer the highest protocol version supported by them; if this handshake fails, retry (possibly
repeatedly) with earlier protocol versions. This downgrade can also be triggered by network glitches, and by
active attackers. If an attacker that controls the network between the client and the server interferes with
any attempted handshake offering TLS 1.0 or later, such clients/servers will readily confine themselves to
SSL 3.0.
 The SSL protocol 3.0, as used in the openSSL cryptographic software library uses nondeterministic CBC
padding, which make it easier for man-in-the-middle attackers to obtain clear text data via padding-oracle
attack aka, POODLE attack (Padding Oracle On Downgraded Legacy Encryption).
 An attacker who successfully exploits this vulnerability could get hold of the user credentials and
cryptographic keys used to login to the device.
* Score and Severity of the Vulnerability: 3.4 (Low)
* Attack Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
* Affected Model(s): Relion 615 series
* Affected Firmware Version(s): >= 5.0.0 & <= 5.0.4
* Fixed Firmware Version (Patch): 5.0.5
* Requirements for the Patch: None
* Other Mitigations: Recommended security practices and firewall configurations can help protect an
industrial control network from attacks that originate from outside the network. Such practices include that
industrial control systems are physically protected from direct access by unauthorized personnel, have no
direct connections to the Internet, and are separated from other networks by means of a firewall system that
has a minimal number of ports exposed, and others that have to be evaluated case by case. Industrial control
systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers
and removable storage media should be carefully scanned for viruses before they are connected to a control
system.
* For more information about the vulnerability, please visit:
- Vulnerability's CVE Link: https://nvd.nist.gov/vuln/detail/cve-2014-3566
- Vulnerability's CWE Link: https://cwe.mitre.org/data/definitions/310.html
- Vulnerability's ABB Advisory Link: https://search.abb.com/library/Download.aspx?DocumentID=1MRS758301
&LanguageCode=en&DocumentPartId=&Action=Launch
- Details about the firmware update: None
```

Şekil 3.9. REF615'in etkilenmediği bir güvenlik açığının rapora dahil edilmesi.

Önerilen yaklaşımın temel zorluğu, veritabanında arama yaparak doğru, net ve eksiksiz sonuçlar elde edebilmek için, farklı tedarikçilerin birbirlerinden farklı cihaz dokümantasyonları, güvenlik bildirimleri ve yama belgelerinden veri çekerek bunları uygun ve standart bir yapıya (veritabanı) dönüştürmektir. Bu normalizasyon süreci, her bir tedarikçinin ürün varyantları ve sınıfları, güvenlik açıkları ve yamalarının belgelendirilme ve yayınlanma biçimlerinin incelenmesini ve kavranmasını gerektirmektedir. Tedarikçi sayısının ve ürün çeşitliliğinin fazlalığı göz önünde bulundurulduğunda, piyasadaki IED üreticilerini kapsayacak bir veritabanı oluşturmak zaman alıcı ve zahmetli bir süreç olabilir. Ancak bu veritabanı bir kez oluşturulduğunda kalıcı olup tekrar kullanılabilir, genişletilebilir ve sektöre genel bir bakış sunarak, gelecekteki araştırmacıların çalışmalarına da katkı sağlayabilir.

Tablo 3.1. REF615'in etkilendiği güvenlik açıklarının özeti.

CVE Tanımlayıcısı	CWE Tanımlayıcısı ve Adı	CVSS risk puanı ve seviyesi	Etkilenmiş yazılım sürüm(ü/leri)	Yama
CVE-2020-11907	CWE ID'si ve ismi bulunmamaktadır	6.3 (Orta)	5.1.19	FW 5.1.19
CVE-2020-11909	CWE-191: Tamsayı Taşması (Alt Sınır Aşımı veya Sarmalanma)	5.3 (Orta)	< 5.1.19	FW 5.1.19
CVE-2020-11910 ve CVE-2020-11912	CWE-125: Sınır Dışı Okuma	5.3 (Orta)	< 5.1.19	FW 5.1.19
CVE-2020-11911	CWE-732: Kritik Kaynak İçin Hatalı İzin Ataması	5.3 (Orta)	< 5.1.19	FW 5.1.19
CVE-2021-22283	CWE-665: Hatalı (Uygun Olmayan Başlatma)	6.2 (Orta)	< 5.1.20	FW 5.1.20
CVE-2024-8036	CWE-347: Kriptografik İmzanın Hatalı Doğrulanması	5.9 (Orta)	Bütün sürümler	Yama bulunma-maktadır

ABB'nin 2025 yılı öncesinde yayımladığı güvenlik bildirimleri ve uyarıları PDF formatında olup, içerikleri zamanla değişebilmektedir. Bu nedenle, çalışmadaki zafiyet veritabanı bu dosyaları otomatik olarak ayrıştırmak yerine manuel olarak oluşturulmuştur. Ancak, 2025 yılı ve sonrasında açıklanan güvenlik açıkları için bu durum sorun teşkil etmemektedir; zira ABB, 2025 yılından itibaren güvenlik

uyarılarını ".json" formatında yayımlamakta ve bu dosyalar belirli bir standart çerçevesinde düzenlenmektedir. Dolayısıyla, manuel olarak veritabanı oluşturma zorunluluğu ortadan kalkmış durumdadır. Bu gelişme, yaklaşımın hazırlık aşamasının gelecekte otomatikleştirilebilmesine olanak tanımaktadır.

3.7. Gelecek Çalışmalar

Gelecekteki araştırmalar açısından çeşitli umut vadeden genişleme alanları bulunmaktadır. Bunlar arasında:

- SCL dosyalarının otomatik elde edilmesi: IEDExplorer aracılığıyla cihazların SCL dosyalarının otomatik olarak temin edilmesini sağlayacak ek çalışmalar yapılabilir.
- Veritabanının genişletilmesi: ABB'nin kalan IED cihazlarının yanı sıra farklı üreticilerin IED cihazları ve ilgili zafiyetlerini kapsayacak şekilde veritabanı geliştirilerek, programın ekstra cihazlar için de zafiyet tarama yapması mümkün hale getirilebilir.
- Otomatik güncelleme: Zafiyet veritabanının güncel tutulabilmesi için, ileride yayınlanacak güvenlik uyarılarını takip eden ve web kazıma tekniklerini kullanarak bu dosyaları otomatik olarak ayrıştırıp veritabanına ekleyen bir bileşen eklenebilir.
- Varlık yönetimi entegrasyonu: SCL dosyalarının ayrıştırılmasıyla elde edilen cihaz bilgileri, farklı formatlarda kaydedilip kurumun varlık yönetimi sistemine aktarılabilir ve böylece mevcut bilgiler güncellenebilir.
- Diğer EKS sistemlerine genişletme: Program yalnızca IED cihazlarını değil, diğer EKS sistemlerinin de zafiyet analiz raporlarını üretecek şekilde genişletilebilir. Aslında, mevcut veritabanı yapısı ve filtreleme algoritması bu tür bir genişletmeye uygundur. IEC 61850 standardı IED'ler arası iletişimi kapsadığı ve SCL dosyaları bu standarda özgü olduğu için, IED dışındaki cihazlarda zorluklar, ilgili cihaz veya sistemlerin statik bilgilerinin elde edilmesiyle ilgilidir. Bu bilgiler, kurumun güvenilir ve güncel bir varlık envanteri üzerinden temin edilebilir ya da söz konusu bilgilerin elde edilmesi için ek araştırmalar yapılabilir.

4. SONUÇ VE ÖNERİLER

Kritik altyapılar, bir ülkenin ulusal güvenliği, kamu sağlığı ve ekonomik istikrarı açısından hayati öneme sahiptir. Bu altyapıların çoğu, operasyonel teknoloji (OT) temelli Endüstriyel Kontrol Sistemleri (EKS) ile izlenmekte ve kontrol edilmektedir. Son yıllarda dijitalleşmenin artmasıyla birlikte, özellikle enerji iletim ve dağıtım sistemlerinde kullanılan Akıllı Elektronik Cihazlar (IED), siber tehditlerin ana hedefi haline gelmiştir. IED'ler, şebeke kontrol ve koruma işlevlerinde kritik roller üstlenmekte ve bu cihazlara yönelik siber saldırılar, tüm sistemin işleyişini tehlikeye atabilecek potansiyele sahiptir. Yama uygulanmamış yazılımlar, bir sistemdeki en büyük güvenlik açıklarından birini temsil etmektedir.

EKS sistemindeki cihaz ve uygulama fazlalığı ve çeşitliliği, IED'lerin yazılımlarında bulunan güvenlik açıklarının tespiti ve yönetimini zorlaştırmış; sistem güvenliğini ciddi anlamda tehdit eder hale getirmiştir. Modern sistemlerde yaygın olarak kabul görmüş iki temel zafiyet tarama yöntemi bulunmaktadır: Aktif Zafiyet Taraması (AZT) ve Pasif Zafiyet Tespiti (PZT).

Raporlar, Endüstriyel Kontrol Sistemleri (EKS) operatörleri; kontrol sistemlerine ait ağlarda mevcut olan yazılım ve donanım güvenlik açıklarını tespit edebilmek amacıyla pasif ağ izleme, aktif zafiyet tarama gibi çeşitli yöntemler ve araçlar kullanmalarına rağmen operatörlerin %61,2'sinin aynı zamanda üreticiler ve yetkili kuruluşlar tarafından kamuya açık şekilde yayımlanan güvenlik duyuruları ile yama belgelerini düzenli olarak takip ettiklerini açıklamaktadır. Bununla birlikte, literatürdeki çalışmalar ve piyasadaki gerek ticari gerekse açık kaynaklı araçların bildiğimiz kadarıyla hiçbiri bu süreci otomatikleştirmeye çalışmamıştır.

Bu çalışmada, kritik altyapıların en önemli sektörlerinden biri olan enerji sistemlerinde kullanılan IED cihazlarının üretici bültenlerini temel alarak söz konusu manuel süreci otomatikleştirmeyi amaçlayan pasif zafiyet tarama (PZT) temelli bir yöntem önerilmiştir. Önerilen yaklaşım, bir üreticiye ait Akıllı Elektronik Cihaz (IED) ile ilgili yayımlanan güvenlik bildirimlerinin işlenerek, cihaz özelinde kapsamlı ve sistematik bir zafiyet raporuna dönüştürülmesini sağlamaktadır. Bu

sayede, güvenlik açıklarının daha etkin ve hızlı bir şekilde izlenmesi ve yönetilmesi hedefine ulaşılabilir.

Pasif Zafiyet Tespit yönteminde genellikle sistem bileşenleri ile CVE-CPE kayıtları eşleştirilir. Ancak bu yaklaşımın sınırlılıkları vardır: bazı CVE kayıtlarında CPE tanımı yoktur, CPE-CVE eşleştirmelerinde eksiklikler veya güncellenmemiş veriler bulunabilir ve farklı kaynaklarda aynı ürün için tutarsız CPE atamaları görülebilir. Ayrıca, üreticinin güvenlik bildirimleri ve uyarılarında cihazların CPE'lerinden ziyade modelleri, yazılım ve donanım sürümleri, tasarım standartları vs. gibi statik bilgileri yer almaktadır. Bu nedenlerden dolayı bu çalışmada, güvenlik açıklarının belirlenmesinde CPE'yi kullanmaksızın, cihazın bu bilgileriyle eşleştirme yapılması tercih edilmiştir.

Mevcut zafiyet veritabanları, örneğin NVD, genellikle cihazların statik bilgilerini değil yalnızca CPE (Common Platform Enumeration) bilgilerini içermektedir. Dolayısıyla, bir cihazın yazılımında kullanılan üçüncü taraf bileşenlerde bir güvenlik açığı tespit edildiğinde, söz konusu veritabanlarında bu açığın hangi cihazları etkilediği belirtilmemektedir. Bundan dolayı, bu çalışmanın amacına ulaşabilmek için, bir tedarikçinin belirli cihazlarına ilişkin yayımladığı güvenlik bildirimlerini temel alarak özel bir zafiyet veritabanı oluşturulması gerekmiştir.

Deneysel analizler, Sakarya Üniversitesi'ndeki Kritik Altyapılar Ulusal Test Yatağı Merkezi (CENTER Energy) üzerinde yürütülmüştür. Çalışmada, ABB'nin Relion® ailesine ait IEC 61850 standardına dayalı olan üç farklı IED modeli (REF615, REL650, RET670) üzerinde testler yapılmıştır. Dolayısıyla, çalışma kapsamında oluşturulan zafiyet veritabanı bu üç modele odaklanarak oluşturulmuştur. Bu veritabanı, NVD, CWE ve ABB firmasının güvenlik bildirimlerindeki bilgileri birleştirerek kapsamlı bir zafiyet raporunun üretilmesine olanak sağlamaktadır.

Belirli bir cihazın zafiyetlerinin veritabanında doğru bir şekilde tespit edilebilmesi için, öncelikle cihazın bilgilerinin doğruluğu sağlanmalıdır. Bu amacı gerçekleştirmek için, çalışma kapsamında IEC 61850 standardına uygun yapılandırma dosyaları (SCL) kullanılmıştır. Bu dosyalar aracılığıyla cihazların üretici, model, donanım ve yazılım sürümleri gibi özellikleri otomatik olarak elde edilmiş ve elde edilen bilgiler, veritabanındaki cihaz özelliklerine göre filtreleme yapmak için kullanılmıştır.

Bu çalışmada, IED'lerin güvenlik açıklarını belirlemeye yönelik üç aşamalı bir yöntem önerilmiştir:

- Hazırlık aşamasında ABB bültenleri, NVD ve CWE gibi kaynaklardan elde edilen verilerle kapsamlı bir zafiyet veritabanı oluşturulmuş; zafiyet verileri, ilişkisel bir yapı sunan MySQL veritabanında saklanmıştır.
- Manuel işlemler aşamasında hedef sistemdeki IED'lerin Nmap'in ARP taraması ile IP adresleri tespit edilerek IEDExplorer aracılığıyla SCL dosyaları çıkarılmış ve analiz için kaydedilmiştir.
- Otomatik işleme aşamasında ise Python tabanlı program bu dosyaları ayrıştırarak cihazın statik bilgileri belirlenmiş, ardından veritabanıyla eşleştirilerek ilgili zafiyetler ve çözüm önerileri cihaz bazlı raporlanmıştır. Kullanıcı ayrıca, bir cihazın bilgilerini manuel olarak girebilir. Bu durumda, SCL dosyaları ayrıştırmaksızın zafiyet tespit işlemi aynen yürütülmektedir.

Bu yöntemle, dijital trafo merkezlerindeki IED'lerin güvenlik açıkları etkin şekilde tespit edilmekte ve güvenlik uzmanlarına kapsamlı, cihaz odaklı öneriler sunulmaktadır. Ayrıca, önerilen bu sistem, aktif tarama yöntemlerine kıyasla hem daha hızlı hem de daha az müdahaleci bir yapı sunarak EKS sistemlerinin operasyonel sürekliliğini riske atmadan güvenlik değerlendirmesi yapabilmektedir.

Uygulanan deneysel çalışmalar sonucunda sistem tam olarak istenilen sonuçları verdiği veritabanını manuel olarak kontrol ederek görülmüştür. Her cihazın sahip olduğu statik bilgileri, yüklü mevcut yazılım sürümünün doğru bir şekilde tespit edilmesi sayesinde araç, ilgili ürün donanım ve yazılım sürümleriyle ilişkili bilinen güvenlik açıklarını net bir şekilde tespit edebilmiştir.

Bu güvenlik açıkları, bir yandan üreticinin belgelerine dayandıkları için cihaza özgü daha derin bilgiler sunup yamanın olup olmadığı ve cihazı koruyabilmek için alınabilecek önlemler belirtilmektedir. Ayrıca, güvenlik açıkları CVE sınıflandırma standardına da dayanmaktadır. Dolayısıyla, güvenlik açığının sistem üzerindeki etkisini belirleyen bir risk puanına sahiptir, atak vektörü de belirtilmektedir. Ek olarak, güvenlik açığına yol açan zayıflıklar da CWE'den faydalanarak veritabanında da raporda da yer almaktadır. Bu, güvenlik uzmanının cihazın içerdiği zafiyetlerle ilgili farklı açılardan bilgi edinmesini sağlayacaktır. Son olarak, raporda bulunan zafiyetle ilgili üreticinin güvenlik uyarı ve yama bildirim linki, NVD linki, CWE

linki ekstra bilgiye ulamayı sağlamaktadır. Bu özellikler, olası saldırı yüzeylerini büyük ölçüde azaltır ve bir dizi uyumluluk ve bakım gereksinimini karşılamanın getirdiği yükü hafifletmeye yardımcı olur.

Bu tez çalışması, literatürde bilinen zafiyetleri yarı otomatik olarak analiz edip cihaz özelinde güvenlik raporu sunan az sayıdaki çalışmadan biri olup, OT sistemlerinde siber güvenliğin artırılmasına katkı sağlamayı hedeflemektedir. Gelecekte bu sistemin farklı üreticilerin cihazlarını kapsayacak şekilde genişletilebilir, cihaz bilgilerinin varlık yönetimi sistemleriyle entegrasyonu sağlanabilir, SCL dosyalarının ile otomatik olarak elde edilebilmesi ve zafiyet veritabanının otomatik güncellenmesi için ekstra çalışmalar yapılıp tam otomatik bir sistem haline getirilebilir.

KAYNAKLAR

ABB. (2004). *COM 600 Station Automation Series IEC 61850 Master Protocol (OPC) 3.0: User's Guide* (C/16.10.20).

ABB. (2007a). *Feeder protection relay REF615 ANSI Prouct Guide* (Yayın no. 1VAD386601).

ABB. (2007b). *Transformer protection IED RET 670 Buyer's Guide* (Yayın no. 1MRK 504 090-BEN).

ABB. (2009). *630 series IEC 61850 Communication Protocol Manual* (A).

ABB. (2010). *Line Distance Protection REL650 Product Guide*.

ABB. (2012). *615 series IEC 61850 Engineering Guide* (G).

ABB. (2016). *TCP Predictability Vulnerability in Relion® 670 series version 2.0 ABB-VU-PGGA-1MRG019772* (Yayın no. 1MRG023264). Erişim adresi https://publisher.hitachienergy.com/preview?DocumentID=1MRG023264&LanguageCode=en&DocumentPartId=&Action=Launch

ABB. (2017). *Line distance protection REL650 2.1 IEC Product Guide* (B). ABB.

ABB. (2019). *OpenSSL vulnerabilities in Relion® 650 series version 2.1 and Relion® 670 series version 2.1 ABB-VU-PGGA-1MRG024369 ABB-VU-PGGA-1MRG025160* (Yayın no. 1MRG025160). Erişim adresi https://publisher.hitachienergy.com/preview?DocumentID=9AKK107492A9254&LanguageCode=en&DocumentPartId=&Action=Launch

ABB. (2020). *WindRiver VxWorks IPNet Vulnerabilities , impact on Relion 670 , Relion 650 , SAM600-IO series ABBVU-PGGA-Relion670-1MRG035814 ABBVU-PGGA-Relion650-1MRG035815 ABBVU-PGGA-SAM600-IO-1MRG035816* (Yayın no. 1MRG037536). Erişim adresi https://device.report/m/6b0850dd3f66a375b47f30730f75243a64672806995ae4acdb8d542aaeb4649f.pdf

ABB. (2021). *RELION® 615 SERIES: Feeder Protection and Control REF615 Application Manual*. ABB.

ABB. (2025, 21 Haziran). Cyber security alerts and notifications. ABB. https://global.abb/group/en/technology/cyber-security/alerts-and-notifications

ABB. (2025, 15 Temmuz). Feeder protection and control REF615 IEC. ABB. https://new.abb.com/medium-voltage/digital-substations/protection-relays/feeder-protection-and-control/feeder-protection-and-control-ref615-iec

ABB. (2025, 15 Temmuz). Feeder protection relay REF615 ANSI. ABB. https://new.abb.com/medium-voltage/digital-substations/protection-relays/feeder-protection-and-control/feeder-protection-relay-ref615-ansi

ABB. (2025, 06 Temmuz). Firmware update releases for digital substation products. ABB. https://new.abb.com/medium-voltage/digital-substations/protection-relay-services/firmware-update-release

ABB. (2025, 06 Temmuz). Relion protection and control. ABB. https://new.abb.com/medium-voltage/digital-substations/relion

ABB. (2025, 10 Temmuz). Simplifying management of protection and control relays with PCM600 - Protection and control IED manager. ABB. https://new.abb.com/medium-voltage/digital-substations/software-products/protection-and-control-ied-manager-pcm600

ABB Oy. (2010). *Feeder Protection and Control REf615 Product Guide*.

ABD İç Güvenlik Bakanlığı. (2016). *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies* (Ics-Cert Eylül). Erişim adresi https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

Abdulrazzaq, M. ve Wei, Y. (2018). *Industrial Control System (ICS) Network Asset Identification and Risk Management* [Yüksek lisans tezi]. Halmstad University.

Abedi, A., Gaudard, L. ve Romerio, F. (2019). Review of major approaches to analyze vulnerability in power system. *Reliability Engineering & System Safety*, 183(November), 153–172. https://doi.org/10.1016/j.ress.2018.11.019

AFAD. (2014a). *2014-2023 Kritik Altyapıların Korunması: Yol Haritası Belgesi*. Erişim adresi https://afyonluoglu.org/PublicWebFiles/Reports-TR-SG/2014-2023-AFAD-Kritik%20Altyap%C4%B1larin%20Korunmasi%20Yol%20Haritasi.pdf

AFAD. (2014b). *2014-2023 TEKNOLOJİK AFETLER: Yol Haritası Belgesi*. Erişim adresi https://www.afad.gov.tr/kurumlar/afad.gov.tr/3906/xfiles/teknolojik-afetler-son.pdf

Alhasawi, S. (2020). *ICSrank: A Security Assessment Framework for Industrial Control Systems (ICS)* [Doktora tezi]. Liverpool John Moores University.

Alonso, M., Turanzas, J., Amaris, H. ve Ledo, A. T. (2021). Cyber-physical vulnerability assessment in smart grids based on multilayer complex networks. *Sensors*, 21(17), 5826. https://doi.org/10.3390/s21175826

Alshawish, A. ve de Meer, H. (2019). Risk mitigation in electric power systems: Where to start? *Energy Informatics*, 2(1), 34. https://doi.org/10.1186/s42162-019-0099-6

Amin, B. M. R., Hossain, M. J., Anwar, A. ve Zaman, S. (2021). Cyber Attacks and Faults Discrimination in Intelligent Electronic Device-Based Energy Management Systems. *Electronics*, 10(6), 650. https://doi.org/10.3390/electronics10060650

Ani, U. D., Watson, J., He, H., Radanliev, P. ve Epiphaniou, G. (2024). Minimising cybersecurity risk exposures in industrial control system environments: a techno-human vulnerability analysis approach. *Journal of Cyber Security Technology*, *00*(00), 1–40. https://doi.org/10.1080/23742917.2024.2421589

Apostolov, A. (2017). Efficient maintenance testing in digital substations based on IEC 61850 edition 2. *Protection and Control of Modern Power Systems*, *2*(1). https://doi.org/10.1186/s41601-017-0054-0

Arnaud, J., Jenkins, D., Yau, M., Thompson, S. ve Wright, J. (2014). Version Control and Patch Management of Protection and Automation Systems. *12th IET International Conference on Developments in Power System Protection (DPSP 2014)*, *2014*(626 CP), 12.80-12.80. https://doi.org/10.1049/cp.2014.0152

Ashok, A., Govindarasu, M. ve Wang, J. (2017). Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid. *Proceedings of the IEEE*, *105*(7), 1389–1407. https://doi.org/10.1109/JPROC.2017.2686394

Asset Guardian. (2025, 25 Temmuz). Asset Guardian. https://www.assetguardian.com/

Berr, J. (2017). "WannaCry" ransomware attack losses could reach $4 billion. CBS NEWS. https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/ adresinden 19 Temmuz 2025 tarihinde alınmıştır.

Bristow, M. (2020). *SANS White Paper - ICS Asset Identification: It's More Than Just Security*. https://www.sans.org/white-papers/39650/

Bristow, M. (2021). *A SANS 2021 Survey: OT/ICS Cybersecurity*. Erişim adresi https://www.sans.org/white-papers/SANS-2021-Survey-OTICS-Cybersecurity/

Bulbul, R., Gong, Y., Ten, C.-W., Ginter, A. ve Mei, S. (2014, 18-22 Ağustos). Impact quantification of hypothesized attack scenarios on bus differential relays. *2014 Power Systems Computation Conference* içinde. Wroclaw, Poland

Charvat, P. (2013). IEDExplorer. https://sourceforge.net/projects/iedexplorer/ adresinden 15 Haziran 2025 tarihinde alınmıştır.

Chen, T. M. ve Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer*, 44(4), 91–93. https://doi.org/10.1109/MC.2011.115

CISA. (2021). Cyber-Attack Against Ukrainian Critical Infrastructure. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 adresinden 14 Temmuz 2025 tarihinde alınmıştır.

Claroty. (2025). Claroty. https://claroty.com/ adresinden 25 Temmuz 2025 tarihinde alınmıştır.

Clinton, B. (1996). Executive Order 13010: Critical Infrastructure Protection. *Presidential Documents* (C. 61, Sayı 138, ss. 37347–37350) içinde. Erişim adresi https://www.govinfo.gov/content/pkg/FR-1996-07-17/pdf/96-18351.pdf

CNA Askeri Danışma Kurulu. (2015). *National Security and Assured U.S. Electrical Power* (Kasım). Erişim adresi https://www.cna.org/cna_files/pdf/national-security-assured-electrical-power.pdf

Coffey, K., Smith, R., Maglaras, L. ve Janicke, H. (2018). Vulnerability Analysis of Network Scanning on SCADA Systems. *Security and Communication* Networks, 2018, 1–21. https://doi.org/10.1155/2018/3794603

Collard, L. (2018). *Fingerprinting Vulnerabilities In Intelligent Electronic Device Firmware* [Yüksek lisans tezi]. Concordia University.

Corcoran, P. M. ve Melvin, H. (2011). Synchronization Issues for Smart Grids. *University of Galway Research Repository*.

CTIIC. (2024). *Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems* (Haziran). Erişim adresi https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf

CVE Numaralandırma Yetkilisi (CNA). (2000). Common Vulnerabilities and Exposures. https://www.cve.org/ adresinden 12 Temmuz 2025 tarihinde alınmıştır.

Deraison, R., Gula, R. ve Hayton, T. (2003). Passive vulnerability scanning: Introduction to NeVO. Erişim adresi https://ouah.lescigales.org/passive_scanning_tenable.pdf

Dragos. (2025). Dragos. https://www.dragos.com/cybersecurity-platform/asset-visibility/ adresinden 25 Temmuz 2025 tarihinde alınmıştır.

Dragos Inc. (2025). *2025 OT/ICS Cyber Security Report - Year in Review*. Erişim adresi https://www.dragos.com/ot-cybersecurity-year-in-review/#anchor-report

Düzgün, B. (2018). Türkiye Elektrik İletim ve Dağıtım Şebekesinin Enerji Verimliliğinin Değerlendirilmesi ve 2023 Projeksiyonları. *Journal of Polytechnic*, 0900(3), 621–632. https://doi.org/10.2339/politeknik.389604

COUNCIL DIRECTIVE 2008/114/EC, of 8 December 2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union 77 (2008). https://doi.org/10.4324/9781003062226-4

Ecik, H. (2021). Comparison of Active Vulnerability Scanning vs. Passive Vulnerability Detection. *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*, *December*, 87–92. https://doi.org/10.1109/ISCTURKEY53027.2021.9654331

EL, M. (2017). *Benchmarking vulnerability scanners: An experiment on SCADA devices and scientific instruments* [Yüksek lisans tezi]. The University of Arizona.

El, M., McMahon, E., Samtani, S., Patton, M. ve Chen, H. (2017). Benchmarking vulnerability scanners: An experiment on SCADA devices and scientific instruments. *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 83–88. https://doi.org/10.1109/ISI.2017.8004879

Energinet. (2019). *DRAFTrev16: Specification of IEC 61850 Information Exchange between DER and Power System Actors, including TSO, DSO and BRP*.

Filkins, B. ve Wylie, D. (2019). *SANS 2019 State of OT/ICS Cybersecurity Survey*. Erişim adresi https://sansorg.egnyte.com/dl/6hWfMGKRKWqx

Gallais, C. ve Filiol, E. (2017). Critical Infrastructure: Where Do We Stand Today? A Comprehensive and Comparative Study of the Definitions of a Critical Infrastructure. *Journal of Information Warfare*, 16(1), 64–87.

Gawron, M., Cheng, F. ve Meinel, C. (2017). PVD: Passive vulnerability detection. *2017 8th International Conference on Information and Communication Systems (ICICS)*, 322–327. https://doi.org/10.1109/IACS.2017.7921992

Gelle, E., Koch, T. E. ve Sager, P. (2005). IT Asset Management of Industrial Automation Systems. *12th IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'05)*, 123–128. https://doi.org/10.1109/ECBS.2005.49

Genco, A. (2020). Türkiye'de Kritik Altyapı ve Kritk Altyapıya Yönelik Tehditler. *Kaytek Dergisi*, *2*(2), 38–46.

Google. (2011). Scadascan. Google Code Archive. https://code.google.com/archive/p/scadascan/ adresinden 25 Temmuz 2025 tarihinde alınmıştır.

GRAHAM, M., AHLERS, C. ve O'MEARA, K. (2024). *Impact of FrostyGoop ICS Malware on Connected OT Systems*. (Temmuz). Erişim adresi https://hub.dragos.com/report/frostygoop-ics-malware-impacting-operational-technology

Gula, R. (1999). Passive Vulnerability Detection. *Network Security Wizards*, *9*, 1-5.

Hadbah, A., Ustun, T. S. ve Kalam, A. (2014). Using IEDScout software for managing multivendor IEC61850 IEDs in substation automation systems. *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 67–72. https://doi.org/10.1109/SmartGridComm.2014.7007624

Hagman, K., Frisk, L., Menezes, J. ve Saha, M. M. (2016). Cyber Security measures in Protection and Control IEDs. *13th International Conference on Development in Power System Protection 2016 (DPSP)*, *2016*(CP671), 1-5. https://doi.org/10.1049/cp.2016.0014

Henten, A. ve Windekilde, I. (2020). Critical infrastructure - what is it, and what are the implications? *2020 13th CMI Conference on Cybersecurity and Privacy (CMI) - Digital Transformation - Potentials and Challenges(51275)*, 1–9. https://doi.org/10.1109/CMI51275.2020.9322690

Hexagon. (2025). PAS Cyber Integrity®. https://hexagon.com/products/pas-cyber-integrity adresinden 25 Temmuz 2025 tarihinde alınmıştır.

Hong, J. ve Liu, C.-C. (2019). Intelligent Electronic Devices With Collaborative Intrusion Detection Systems. *IEEE Transactions on Smart Grid*, *10*(1), 271–281. https://doi.org/10.1109/TSG.2017.2737826

Hor, CL., Crossley ve P.A. (2005). Knowledge Extraction from Intelligent Electronic Devices. *Transactions on Rough Sets III. Lecture Notes in Computer Science*, 3400, 82–111. https://doi.org/10.1007/11427834_4

Huang, X., Qin, Z. ve Liu, H. (2018). A Survey on Power Grid Cyber Security: From Component-Wise Vulnerability Assessment to System-Wide Impact Analysis. *IEEE Access*, *6*, 69023–69035. https://doi.org/10.1109/ACCESS.2018.2879996

ICS-CERT. (2025). *A brief overview of main incidents in industrial cybersecurity Q1 2025*. Erişim adresi https://ics-cert.kaspersky.com/publications/reports/2025/06/26/a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity-q1-2025/

IEEE. (2025). Cybersecurity of Critical Infrastructure with ICS/SCADA Systems. IEEE Public Safety Technology. https://publicsafety.ieee.org/topics/cybersecurity-of-critical-infrastructure-with-ics-scada-systems/ adresinden 15 Temmuz 2025 tarihinde alınmıştır.

Industrial Defender. (2025). Industrial Defender. https://www.industrialdefender.com/ adresinden 25 Temmuz 2025 tarihinde alınmıştır.

INTERPOL. (2018). *The Protection of Critical infrastructures against terrorist attacks: Compendium of good practices*. Erişim adresi https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf

ISA. (2017). Ukrainian power grids cyberattack. ISA's Flagship Publications. https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack adresinden 15 Temmuz 2025 tarihinde alınmıştır.

İnternet Güvenliği Merkezi (CIS). (2018). CIS Critical Security Controls Version 7 – What's Old, What's New. CIS Controls. https://www.cisecurity.org/insights/blog/cis-controls-version-7-whats-old-whats-new adresinden 17 Mayıs 2025 tarihinde alınmıştır.

Jiang, X., Zhang, J., Harding, B. J., Makela, J. J. ve Dominguez-Garcia, A. D. (2013). Spoofing GPS Receiver Clock Offset of Phasor Measurement Units. *IEEE Transactions on Power Systems*, *28*(3), 3253–3262. https://doi.org/10.1109/TPWRS.2013.2240706

Kalluri, R., Mahendra, L., Kumar, R. K. S. ve Prasad, G. L. G. (2016). Simulation and impact analysis of denial-of-service attacks on power SCADA. *2016 National Power Systems Conference (NPSC)*, *1*, 1–5. https://doi.org/10.1109/NPSC.2016.7858908

Kamu Güvenliği İstihbarat Teşkilatı. (2022). *Overview of Threats in Cyberspace 2021*. Erişim adresi https://www.moj.go.jp/content/001381943.pdf

Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, 4490–4494. https://doi.org/10.1109/IECON.2011.6120048

Kennedy, D., O'Gorman, J., Kearns, D. ve Aharoni, M. (2011). *Metasploit: The Penetration Tester's Guide.* William Pollock.

Kimani, K., Oduol, V. ve Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49. https://doi.org/10.1016/j.ijcip.2019.01.001

Langner. (2025). OTbase. https://www.langner.com/ adresinden 25 Temmuz 2025 tarihinde alınmıştır.

Lloret, P., Velasquez, J. L., Molas-Balada, L., Villafafila, R., Sumper, A. ve Galceran-Arellano, S. (2007). IEC 61850 as a flexible tool for electrical systems monitoring. *2007 9th International Conference on Electrical Power Quality and Utilisation*, 1–6. https://doi.org/10.1109/EPQU.2007.4424193

Lyons, J. (2024). Iran-linked crew used custom “cyberweapon” in US critical infrastructure attacks. The Register. https://www.theregister.com/2024/12/13/iran_cyberweapon_us_attacks/ adresinden 19 Temmuz 2025 alınmıştır.

Mackiewicz, R. E. (2006). Overview of IEC 61850 and Benefits. *2006 IEEE PES Power Systems Conference and Exposition*, *57*(57), 623–630. https://doi.org/10.1109/PSCE.2006.296392

Mangalwedekar, S., Surve, S. K. ve Mangalvedekar, H. A. (2015). False Data Injection Attacks and detection scenarios in the power system. *2015 Annual IEEE India Conference (INDICON)*, *8*, 1–6. https://doi.org/10.1109/INDICON.2015.7443817

McCarthy, J., Acierto, L., Joy, G., Kuruvilla, J., Ogunyale, T., Urlaub, N., Wiltberger, J. ve Wynne, D. (2020). *Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry* (Nist Special Publication 1800-23). https://doi.org/10.6028/NIST.SP.1800-23

McDonald, J. D. (2003). Substation automation. IED integration and availability of information. *IEEE Power and Energy Magazine*, *1*(2), 22–31. https://doi.org/10.1109/MPAE.2003.1192023

McMahon, E. (2018). *Benchmarking Vulnerability Assessment Tools for Enhanced Cyber-Physical System (CPS) Resiliency* [Yüksek lisans tezi]. The University of Arizona].

McMahon, E., Patton, M., Samtani, S. ve Chen, H. (2018). Benchmarking Vulnerability Assessment Tools for Enhanced Cyber-Physical System (CPS) Resiliency. *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, *945*(05 0), 100–105. https://doi.org/10.1109/ISI.2018.8587353

Microsoft. (2025). Microsoft Defender for IoT. Microsoft Security. https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-iot adresinden 25 Temmuz 2025 tarihinde alınmıştır.

MITRE. (2023a). *CWE*-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow’). CWE. https://cwe.mitre.org/data/definitions/120.html adresinden 29 Haziran 2024 tarihinde alınmıştır.

MITRE. (2023b). CWE-121: Stack-based Buffer Overflow. CWE. https://cwe.mitre.org/data/definitions/121.html adresinden 16 Mayıs 2024 tarihinde alınmıştır.

MITRE. (2023c). CWE-20: Improper Input Validation. CWE. https://cwe.mitre.org/data/definitions/20.html adresinden 25 Nisan 2024 tarihinde alınmıştır.

MITRE. (2023d). CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition’). CWE. https://cwe.mitre.org/data/definitions/362.html adresinden 16 Mayıs 2024 tarihinde alınmıştır.

MITRE. (2025). Common Weakness Enumeration (CWE). https://cwe.mitre.org/ adresinden 21 Haziran 2025 tarihinde alınmıştır.

Motorola. (2012). *Protecting Our Critical Utilities With Integrated Control Systems*. Erişim adresi https://www.motorolasolutions.com/content/dam/msi/docs/business/products/scada_products/ace3600/_documents/static_files/ics_security_protecting_critical_utilities.pdf

NCCIC. (2016). *IR-ALERT-H-16-043-01AP CYBER-ATTACK AGAINST UKRAINIAN CRITICAL INFRASTRUCTURE*. Erişim adresi https://nsarchive.gwu.edu/sites/default/files/documents/4164304/Department-of-Homeland-Security-NCCIS-ICS-CERT.pdf?utm_source=chatgpt.com

Niedermaier, M., Hanka, T., Plaga, S., von Bodisco, A. ve Merli, D. (2018). Efficient Passive ICS Device Discovery and Identification by MAC Address Correlation. *Proceedings of ICS & SCADA 2018*, 21–30. https://doi.org/10.14236/ewic/ICS2018.3

NIST. (2006). *Minimum security requirements for federal information and information systems* (Mayıs). https://doi.org/10.6028/NIST.FIPS.200

NIST. (2016a). CVE-2016-2177 Detail. NVD. https://nvd.nist.gov/vuln/detail/cve-2016-2177 adresinden 28 Temmuz 2025 tarihinde alınmıştır

NIST. (2016b). CVE-2016-2178 Detail. NVD. https://nvd.nist.gov/vuln/detail/cve-2016-2178 adresinden 28 Temmuz 2025 tarihinde alınmıştır.

NIST. (2016c). CVE-2016-2182 Detail. NVD. https://nvd.nist.gov/vuln/detail/cve-2016-2182 adresinden 28 Temmuz 2025 tarihinde alınmıştır.

NIST. (2016d). CVE-2016-2183 Detail. NVD. https://nvd.nist.gov/vuln/detail/cve-2016-2183 adresinden 28 Temmuz 2025 tarihinde alınmıştır.

NIST. (2016e). CVE-2016-6304 Detail. NVD. https://nvd.nist.gov/vuln/detail/cve-2016-6304 adresinden 28 Temmuz 2025 tarihinde alınmıştır.

NIST. (2016f). CVE-2016-6306 Detail. NVD. https://nvd.nist.gov/vuln/detail/cve-2016-6306 adresinden 28 Temmuz 2025 tarihinde alınmıştır.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. https://doi.org/10.6028/NIST.CSWP.04162018

NIST. (2020). CVE-2020-11907 Detail. NVD. https://nvd.nist.gov/vuln/detail/CVE-2020-11907 adresinden 07 Mayıs 2024 tarihinde alınmıştır.

NIST. (2022). CVE-2019-12256 Detail. NVD. https://nvd.nist.gov/vuln/detail/CVE-2019-12256 adresinden 15 Mayıs 2024 tarihinde alınmıştır.

NIST. (2025a). National Vulnerability Database (NVD). NVD. https://nvd.nist.gov/ adresinden 21 Haziran 2025 tarihinde alınmıştır.

NIST. (2025b). NVD Dashboard. NVD. https://nvd.nist.gov/general/nvd-dashboard 17 Temmuz 2025 tarihinde alınmıştır.

NIST SP800-53. (2020). *Security and Privacy Controls for Information Systems and Organizations* (NIST Special Publication). Erişim adresi https://doi.org/10.6028/NIST.SP.800-53r5

NISTIR 7628. (2014). *Guidelines for smart grid cybersecurity* (C. 3). Erişim adresi https://doi.org/10.6028/NIST.IR.7628r1

Nmap. (1997). Nmap. https://nmap.org/ adresinden 29 Temmuz 2025 tarihinde alınmıştır.

Nozomi Networks. (2025). Nozomi Networks. https://www.nozominetworks.com/ adresinden 25 Temmuz 2025 tarihinde alınmıştır.

Omicron. (2024). IEDScout: Versatile software tool for working with IEC 61850 devices. Omicron. https://www.omicronenergy.com/en/products/iedscout/ adresinden 10 Temmuz 2025 tarihinde alınmıştır.

Ozcelik, I., Iskefiyeli, M., Balta, M., Ovaz Akpinar, K. ve Toker, F. S. (2021). CENTER Energy: A Secure Testbed Infrastructure Proposal for Electricity Power Grid. *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*, *December*, 149–154. https://doi.org/10.1109/ISCTURKEY53027.2021.9654352

Parsons, D. (2018). Know Thyself Better Than The Adversary - ICS Asset Identification and Tracking. SANS. https://www.sans.org/blog/know-thyself-better-than-the-adversary-ics-asset-identification-and-tracking/ adresinden 15 Temmuz 2025 tarihinde alınmıştır.

Pinto, A., Herrera, L.-C., Donoso, Y. ve Gutierrez, J. A. (2023). Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. *Sensors*, *23*(5), 2415. https://doi.org/10.3390/s23052415

Pöhler, L., Schuba, M., Höner, T., Hack, S. ve Neugebauer, G. (2024). An Open-Source Approach to OT Asset Management in Industrial Environments. *Proceedings of the 10th International Conference on Information Systems Security and Privacy*, *1*(Icissp), 128–136. https://doi.org/10.5220/0012362200003648

Qassim, Q. S., Jamil, N., Daud, M., Patel, A. ve Ja'affar, N. (2019). A review of security assessment methodologies in industrial control systems. *Information and Computer Security*, *27*(1), 47–61. https://doi.org/10.1108/ICS-04-2018-0048

Radiflow. (2024). *Ukrainian BlackJack APT Attack on Moscow OT Infrastructure (Fuxnet)* (Nisan 2027). Erişim adresi https://www.radiflow.com/wp-content/uploads/Fuxnet-attack-on-Russian-infrastructure-1-1.pdf

Rahman, M. S., Pota, H. R. ve Hossain, M. J. (2014). Cyber vulnerabilities on agent-based smart grid protection system. *2014 IEEE PES General Meeting | Conference & Exposition*, *2014-Octob*(October), 1–5. https://doi.org/10.1109/PESGM.2014.6939298

Rajkumar, V. S., Ştefanov, A., Presekal, A., Palensky, P. ve Torres, J. L. R. (2023). Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures. *IEEE Access*, *11*(July), 103154–103176. https://doi.org/10.1109/ACCESS.2023.3317695

Rajkumar, V. S., Tealane, M., Stefanov, A. ve Palensky, P. (2020). Cyber attacks on protective relays in digital substations and impact analysis. *8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2020 - Proceedings*. https://doi.org/10.1109/MSCPES49613.2020.9133698

Reilly, S. (2015). Records: Energy Department Struck by Cyber Attacks. USA Today. http://www.usatoday.com/story/ news/2015/09/09/cyber-attacks-doe-energy/71929786/ adresinden 14 Temmuz 2025 tarihinde alınmıştır.

Rockwell Automation. (2025a). Rockwell Automation Security Advisories. Security Advisories. https://www.rockwellautomation.com/en-tr/trust-center/security-advisories.html adresinden 18 Temmuz 2025 tarihinde alınmıştır.

Rockwell Automation. (2025b). Verve. Verve. https://verveindustrial.com/ adresinden 25 Temmuz 2025 tarihinde alınmıştır.

Sakarya Üniversitesi. (2023). Kritik Altyapılar Ulusal Test Yatağı Merkezi. CENTER-SAÜ. https://center.sakarya.edu.tr/ adresinden 20 Temmuz 2025 tarihinde alınmıştır.

Salmon, D., Zeller, M., Guzman, A., Mynam, V. ve Donolo, M. (2009). Mitigating the Aurora Vulnerability With Existing Technology. *36th Annual Western Protective Relay Conference*, *Ekim 2009*, 1–7. https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6392_MitigatingAurora_MZ_20090918_Web.pdf

Samanis, E., Gardiner, J. ve Rashid, A. (2022). SoK: A Taxonomy for Contrasting Industrial Control Systems Asset Discovery Tools. *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–12. https://doi.org/10.1145/3538969.3538979

Samtani, S., Yu, S., Zhu, H., Patton, M. ve Chen, H. (2016). Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques. *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 25–30. https://doi.org/10.1109/ISI.2016.7745438

Sanguino, L. A. B. ve Uetz, R. (2017). Software Vulnerability Analysis Using CPE and CVE. *Computers & Security*. http://arxiv.org/abs/1705.05347

Shang, W., Gong, T., Hou, J., Lu, J. ve Cao, Z. (2023). Quantitative Evaluation Method for Industrial Control System Vulnerability Based on Improved Expert Elicitation and Fuzzy Set Method. *IEEE Access*, *11*(August), 101007–101019. https://doi.org/10.1109/ACCESS.2023.3314629

Shirani, P., Collard, L., Agba, B. L., Lebel, B., Debbabi, M., Wang, L. ve Hanna, A. (2018). BINARM: Scalable and Efficient Detection of Vulnerabilities in Firmware Images of Intelligent Electronic Devices. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): C. 10885 LNCS* (ss. 114–138) içinde. https://doi.org/10.1007/978-3-319-93411-2_6

Siemens. (2024). *SIPROTEC 5 Transformer Differential Protection 7UT82, 7UT85, 7UT86, 7UT87 V9.90 and Higher Manual* (11.2024).

Siemens ProductCERT. (2025). Siemens Security Advisories. https://www.siemens.com/global/en/products/services/cert.html adresinden 18 Temmuz 2025 tarihinde alınmıştır.

Smith, K. ve Wilson, I. D. (2023). Critical infrastructures: a comparison of definitions. *International Journal of Critical Infrastructures*, *19*(4), 323–339. https://doi.org/10.1504/IJCIS.2023.132213

Sridhar, S. ve Govindarasu, M. (2014). Model-Based Attack Detection and Mitigation for Automatic Generation Control. *IEEE Transactions on Smart Grid*, *5*(2), 580–591. https://doi.org/10.1109/TSG.2014.2298195

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A. ve Thompson, M. (2023). *Guide to Operational Technology (OT) security* (NIST Special Publication). Erişim adresi https://doi.org/10.6028/NIST.SP.800-82r3

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. ve Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security* (NIST Special Publication 800-82 rev 2). Erişim adresi https://doi.org/10.6028/NIST.SP.800-82r2

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 1 (2013). https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf

TEDAŞ. (2024). *2023 Yılı Türkiye Elektrik Dağıtımı Sektör Raporu*. Erişim adresi https://www.tedas.gov.tr/FileUpload/MediaFolder/25819eac-d024-4308-891a-d248db8c1e0a.pdf

TEİAŞ. (2024a). *GRAFİK VI.I- TÜRKİYE İLETİM HAT UZUNLUKLARININ GELİŞİMİ (2013-2023)*. Erişim adresi https://www.teias.gov.tr/turkiye-elektrik-uretim-iletim-istatistikleri

TEİAŞ. (2024b). *GRAFİK VI.III- TÜRKİYE TRAFO ADETLERİNİN GELİŞİMİ (2013-2023)*. Erişim adresi https://www.teias.gov.tr/turkiye-elektrik-uretim-iletim-istatistikleri

Tenable® Inc. (2025). *Plugins*. https://www.tenable.com/plugins adresinden 17 Temmuz 2025 tarihinde alınmıştır.

Thomas, A. M., Marali, M. ve Reddy, L. (2022). Identification of Assets in Industrial Control Systems Using Passive Scanning. A. P. Pandian, X. Fernando ve W. Haoxiang (Ed.), *Lecture Notes on Data Engineering and Communications Technologies Computer Networks, Big Data and IoT* (ss. 269–283). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-0898-9_21

Thomas, R. J., Gardiner, J., Chothia, T., Samanis, E., Perrett, J. ve Rashid, A. (2020). Catch Me If You Can: An In-Depth Study of CVE Discovery Time and Inconsistencies for Managing Risks in Critical Infrastructures. *Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy*, 49–60. https://doi.org/10.1145/3411498.3419970

Tidy, J. (2022). European oil facilities hit by cyber-attacks. BBC. https://www.bbc.com/news/technology-60250956 adresinden 15 Temmuz 2025 tarihinde alınmıştır.

Timcke, S., Gaffley, M. ve Rens, A. (2023). The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa's Transnet. *The African Journal of Information and Communication (AJIC)*, *32*, 1–28. https://doi.org/10.23962/ajic.i32.16949

Tran, T.-T., Shin, O.-S. ve Lee, J.-H. (2013). Detection of replay attacks in smart grid systems. *2013 International Conference on Computing, Management and Telecommunications (ComManTel)*, 298–302. https://doi.org/10.1109/ComManTel.2013.6482409

UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001, PUBLIC LAW 107-56-OCT.26,2001 401 (2001). Erişim adresi https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

Wallace, N. ve Proctor, B. (2018). Passive Real-Time Asset Inventory Tracking and Security Monitoring of Grid-Edge Devices. *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, *2018-April*. https://doi.org/10.1109/TDC.2018.8440434

Wang, J. ve Shi, D. (2018). Cyber-Attacks Related to Intelligent Electronic Devices and Their Countermeasures: A Review. *2018 53rd International Universities Power Engineering Conference (UPEC)*, 1–6. https://doi.org/10.1109/UPEC.2018.8542059

Wedgbury, A. ve Jones, K. (2015). *Automated Asset Discovery in Industrial Control Systems - Exploring the Problem*. 73–83. https://doi.org/10.14236/ewic/ICS2015.8

Weerathunga, P. E. ve Cioraca, A. (2017a). The importance of testing Smart Grid IEDs against security vulnerabilities. *69th Annual Conference for Protective Relay Engineers, CPRE 2016*, 1–21. https://doi.org/10.1109/CPRE.2016.7914920

Weerathunga, P. E. ve Cioraca, A. (2017b). Securing IEDs against cyber threats in critical substation automation and industrial control systems. *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, 1–20. https://doi.org/10.1109/CPRE.2017.8090048

Wen, H. (2023). Vulnerability Assessment of Industrial Control System with an Improved CVSS. *ArXiv Preprint*. http://arxiv.org/abs/2306.08631

Wiberg, K. C. (2006). *Identifying Supervisory Control and Data Acquisition (SCADA) Systems on a Network via Remote Reconnaissance* [Yüksek lisans tezi]. Naval Postgraduate School.

Xia, Y., Wang, J., Liu, C. ve Yu, K. (2020). Design and Implementation of Vulnerability Scanning Tools for Intelligent Substation Industrial Control System Based on Openvas. *IOP Conference Series: Earth and Environmental Science*, *440*(4), 042031. https://doi.org/10.1088/1755-1315/440/4/042031

Youssef, E.-N. S. ve Labeau, F. (2018). False Data Injection Attacks Against State Estimation in Smart Grids: Challenges and Opportunities. *2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE)*, *2018-May*(1), 1–5. https://doi.org/10.1109/CCECE.2018.8447683

Zhang, J. ve Dong, Y. (2017). Cyber attacks on remote relays in smart grid. *2017 IEEE Conference on Communications and Network Security (CNS)*, *2017-Janua*, 1–9. https://doi.org/10.1109/CNS.2017.8228637

Zhang, Z., Gong, S., Dimitrovski, A. D. ve Li, H. (2013). Time Synchronization Attack in Smart Grid: Impact and Analysis. *IEEE Transactions on Smart Grid*, *4*(1), 87–98. https://doi.org/10.1109/TSG.2012.2227342

ÖZGEÇMİŞ

Ad-Soyadı: Khouloud GARGOURI

ÖĞRENİM DURUMU:

- **Lisans :** 2021, Sakarya Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği
- **Yüksek Lisans :** 2025, Sakarya Üniversitesi, Bilgisayar Mühendisliği, Siber Güvenlik

TEZDEN TÜRETİLEN ESERLER:

Gargouri K. ve İskefiyeli M. 2025. Firmware Analyzer Of Intelligent Electronic Devices In Substations Based On Vulnerability Databases. *Sakarya University Journal of Computer and Information Sciences*.