



**T.C.
İSTANBUL ÜNİVERSİTESİ-CERRAHPAŞA
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**



[DOKTORA TEZİ]

**[AKILLI DOĞAL GAZ ŞEBEKELERİNDE SİBER GÜVENLİK
AÇIKLARININ ARAŞTIRILMASI ve OLGUNLUK MODELİ
GELİŞTİRİLMESİ]**

[İsa AVCI]

[DANIŞMAN]

Doç. Dr. Muhammed Ali AYDIN

[II. DANIŞMAN]

Dr. Öğr. Üyesi Cevat ÖZARPA

[Bilgisayar Mühendisliği Anabilim Dalı]

[Bilgisayar Mühendisliği Programı]

[İSTANBUL-2021]

Bu çalışma, 11.01.2021 tarihinde ařağıdaki jüri tarafından Bilgisayar Mühendisliğı Anabilim Dalı, Bilgisayar Mühendisliğı Programında Doktora tezi olarak kabul edilmiştir.

Tez Jürisi

Doç. Dr. Muhammed Ali AYDIN (Danışman)
İstanbul Üniversitesi-Cerrahpařa
Mühendislik Fakültesi

Prof. Dr. Ahmet SERTBAŞ
İstanbul Üniversitesi-Cerrahpařa
Mühendislik Fakültesi

Doç. Dr. Şerif BAHTİYAR
İstanbul Teknik Üniversitesi
Bilgisayar ve Biliřim Fakültesi

Prof. Dr. Selim AKYOKUŞ
İstanbul Medipol Üniversitesi
Mühendislik ve Doğı Bilimleri Fakültesi

Doç. Dr. Atakan KURT
İstanbul Üniversitesi-Cerrahpařa
Mühendislik Fakültesi



|20.04.2016 tarihli Resmi Gazete’de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, İstanbul Üniversitesi-Cerrahpaşa’nın abonesi olduğu intihal yazılım programı kullanılarak Lisansüstü Eğitim Enstitüsü’nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır.|

ÖNSÖZ

Tez danışmanım kıymetli hocam Doç. Dr. Muhammed Ali AYDIN' a değerli rehberliği ve katkıları için teşekkür etmek isterim. Ayrıca ikinci tez danışmanım kıymetli hocam Dr. Öğr. Üyesi Cevat ÖZARPA' ya tezime değerli katkılarından dolayı teşekkür ederim. Değerli yönlendirmeleri ile tezime katkı sunan ve tez komitesinde bulunan değerli hocalarım Prof. Dr. Ahmet SERTBAŞ ve Doç. Dr. Şerif BAHTİYAR' a teşekkür ederim.

Son olarak 4 yıllık çalışmalarım boyunca manevi desteği ile beni daha da güçlendiren, desteğini esirgemeyen, yüksek anlayışla ve sabırla arkamda olan eşim Mihriban Sultan AVCI' ya ve bana her konuda destek olan çok değerli çocuklarıma en içten teşekkürlerimi ifade etmek isterim.

Ocak 2021

İsa AVCI

İÇİNDEKİLER

Sayfa No

ÖNSÖZ	iv
İÇİNDEKİLER.....	v
ŞEKİL LİSTESİ	xiii
TABLO LİSTESİ.....	xvii
SİMGE VE KISALTMA LİSTESİ	xix
ÖZET	xxii
SUMMARY	xxiv
1. GİRİŞ	1
2. GENEL KISIMLAR.....	4
2.1. GENEL TANIMLAR.....	4
2.2. BİLGİ GÜVENLİĞİ	10
2.2.1. Bilgi Güvenliğinin Bileşenleri.....	11
2.2.2. Bilgi Sistemleri Katmanları	12
2.3. VERİ İLETİM GÜVENLİK PROTOKOLLERİ	13
2.3.1. Pretty Good Privacy-PGP	13
2.3.2. SSL/TSL	14
2.3.3. SSH (Secure SHell)	14
2.3.4. S/MIME (Secure/Multipurpose Internet Mail Extensions)	14
2.3.5. IPsec (Internet Protocol Security)	14
2.3.6. Kerberos	15
2.4. SİBER GÜVENLİK.....	15
2.4.1. Siber Güvenlik Yaşam Döngüsü	16
2.4.2. Siber Saldırı Yaşam Döngüsü	16
2.4.3. Temel Siber Güvenlik Gereksinimleri.....	18
2.5. SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİ ARASINDAKİ FARK	18
2.6. AKILLI ŞEHİR	19
2.7. AKILLI ŞEBEKE	23
2.7.1. Akıllı Şebeke Güvenlik Ekosistemi.....	26
2.7.2. Akıllı Şebeke İletişim Teknolojileri	26
2.8. AKILLI DOĞAL GAZ ŞEBEKESİ.....	27

2.9. AKILLI ŞEBEKELERDE EN SIK KARŞILAŞILAN SİBER SALDIRI YÖNTEMLERİ	31
2.9.1. Dağıtık Hizmet Dışı Bırakma (Distributed Denial of Service-DDoS-DoS)	33
2.9.2. Köle Bilgisayarlar (Botnet, Zombie)	34
2.9.3. Sıfırcı Gün Açıkları (Zero-Day Exploits)	34
2.9.4. Gelişmiş Siber Tehditler (Advanced Persistent Threats – APT).....	34
2.9.5. Saldırı Kitleri (Attack Kits)	35
2.9.6. İstem Dışı Yığın E-Posta Gönderme (Spam, Bulk, Junk)	35
2.9.7. Ağ Trafiğinin Dinlenmesi (Sniffing - Monitoring)	35
2.9.8. Zararlı Yazılım Kullanımı (Malware)	36
2.9.9. Kriptografik Saldırıları	39
2.9.10. IP Aldatmacası - Gizlenmesi (IP Spoofing)	40
2.9.11. Dijital Manipülasyon (Digital Manipulation).....	40
2.9.12. Kabloya Saplama Yapma (Wire Tapping)	40
2.9.13. İnternet Servis Sağlayıcı Saldırıları (ISP Attacks)	40
2.9.14. SQL Enjeksiyonu.....	41
2.9.15. Mantık Bombası (Logic Bomb).....	41
2.9.16. Yemleme - Oltalama (Phishing) Saldırıları	41
2.9.17. Yerine Geçme (Masquerading)	41
2.9.18. Sosyal Mühendislik (Social Engineering)	41
2.9.19. Çöpe Dalma (Scavenging).....	42
2.9.21. XXE Dış Varlık Güvenlik Zafiyeti (XML External Entity).....	43
2.9.22. Araya Girme Saldırısı (MITM)	43
2.9.23. Replay Saldırısı	44
2.9.24. MODBUS/TCP Protocol Attack	44
2.9.25. DNP3 Protocol Attack.....	44
2.9.26. Malicious Command and Software Injection	44
2.9.27. Arabellek Taşması (Buffer Overflow).....	45
2.9.28. Fiziksel Saldırı (Sensör, Actuator, Kamera).....	45
2.9.29. Yetkisiz Erişim Faaliyetleri (Unauthorized Access Activities).....	45
2.9.30. İç ve Dış Ataklar (Insider-Outsider Attacks).....	45
2.9.31. Ağ Trafiği Anomalisi	46
2.9.32. Keşif Saldırıları (Reconnaissance Attacks)	46
2.9.33. Ağda Kötü Amaçlı Yazılımlar (Process Network Malware Injection)	46
2.9.34. Gereksiz Port ve Servisleri Tarama.....	46

2.9.35. PROFIBUS Protokol Atağı (PROFIBUS Protocol Attack)	46
2.9.36. Firmware Değişiklik Saldırısı (Firmware Modification Attack).....	47
2.9.37. Yanlış Veri Enjeksiyonu (False Data Injection).....	47
2.9.38. Zehirleme (Poisoning-ARP, DNS).....	47
2.9.39. Gizli Dinleme (Eavesdropping).....	48
2.9.40. Cevap ve Ölçüm Enjeksiyon Saldırısı (Response and Measurement Injection).....	48
2.9.42. Çerçeve (Fragmentation) Saldırısı.....	48
2.9.43. Yanlış Alarm Üretilmesi.....	48
2.9.45. Reverse-Engineering Attack.....	48
2.10. ÇEŞİTLİ SİBER GÜVENLİK RAPOR ÖRNEKLERİ.....	49
2.10.1. Dünyada Ekim 2020 Tarihinde Yaşanan Siber Olaylar	49
2.10.2. 2018 Yılı Veri İhlalinin Ülke veya Bölgeye Göre Kişi Başına Düşen Maliyeti ve Kök Nedenlerine Göre Dağılımı	49
2.10.3. Dünya Geneline Ekim Ayında Yaşanılan Siber Saldırı Yöntemleri	52
2.10.4. Dünya Geneline 2019 Yılında Gerçekleşen Siber Atakların Yüzdesel Dağılımı	52
2.10.5. En Yaygın Kullanılan Standartlar, Regülasyonlar ve En İyi Kullanım Örnekleri	53
2.11 DÜNYADA VE TÜRKİYE’ DE GERÇEKLEŞEN SİBER SALDIRILAR	54
2.11.1. Dünya Geneline Yaşanan En Önemli Siber Saldırıları	54
2.11.1.1. Rusya (Sibirya) Doğal Gaz Boru Hattı Patlaması-1982	54
2.11.1.2. ABD’ nin Irak Hava Savunma Radar ve Füze Üssü Sistemlerine Saldırısı-1990.....	55
2.11.1.3. Ay Işığı Labirenti-1998.....	55
2.11.1.4. NATO ile Kosova Krizi -1999.....	55
2.11.1.5. Avustralya’da Atık Kontrol Sistemine Siber Saldırı-2000.....	56
2.11.1.6. Dünya Geneline Slammer Adlı Solucan Siber Saldırısı-2003	56
2.11.1.7. Estonya Siber Saldırısı - 2007	56
2.11.1.8. İsrail Tarafından Suriye Nükleer Santraline Siber Saldırı - 2007	57
2.11.1.9. Rusya’ dan Gürcistan’a Karşı Siber Savaş - 2008.....	57
2.11.1.10. Çin’de Bir Siber Casusluk Şebekesi (GhostNet) - 2009	58
2.11.1.11. Filistinden İsraile Siber Saldırı - 2008/2009.....	58
2.11.1.12. Mavi Marmara Saldırısı - 2010.....	58
2.11.1.13. Stuxnet Siber Saldırısı - 2010	59
2.11.1.14. Night Dragon Siber Saldırısı – 2011	60

2.11.1.15. Duqu Adlı Virüs İle Siber Saldırı - 2011	60
2.11.1.16. Flame Adlı Virüs İle Siber Saldırı - 2012	61
2.11.1.17. Kanada Telvent Firmasına Siber Saldırı - 2012.....	61
2.11.1.18. Regin Adlı Bir Virüs İle Siber Saldırı - 2014.....	61
2.11.1.19. Equation Grubu Adlı Siber Saldırı - 2014.....	62
2.11.1.20. Almanya Demir Çelik Tesislerine Yapılan Siber Saldırı - 2014.....	62
2.11.1.21. Ukrayna' da Elektrik Şebekesine Siber Saldırı - 2015	62
2.11.1.22. Duqu 2.0 Adlı Siber Saldırı - 2015	63
2.11.1.23. İngiltere' deki WannaCry Siber Saldırısı - 2016.....	63
2.11.1.24. ABD DDoS Mirai Saldırısı - 2016.....	63
2.11.1.25. Schneider Elektiriğe Ait Elektrik Üretim Santraline Yapılan Siber Saldırı - 2017	63
2.11.1.26. Uber Firmasına Yapılan Siber Saldırı - 2017	64
2.11.1.27. NotPetya Siber Saldırısı - 2017	64
2.11.1.28. Amadeus Uçuş Rezervasyon Sisteminde Bulunan Güvenlik Zafiyeti - 2019.....	64
2.11.2. Türkiye' de Yaşanan En Önemli Siber Saldırıları	65
2.11.2.1. Batman Hidroelektrik Santrali Vakası - 2003	65
2.11.2.2. İMKB Fiber Optik Kablo Vakası - 2007.....	65
2.11.2.3. Bakü-Tiflis-Ceyhan Petrol Boru Hattına Siber Saldırı - 2008	65
2.11.2.4. Atatürk Havalimanı Bilgisayarlarına Yapılan Siber Saldırı - 2009.....	65
2.11.2.5. Telekomünikasyon İletişim Başkanlığı Web Sayfasına Yapılan Siber Saldırı - 2011.....	66
2.11.2.6. 155 Polis İhbar Hattı Vakası - 2012.....	66
2.11.2.7. Türkiyede Yaşanan Elektrik Kesintisi Siber Saldırısı - 2015.....	66
2.11.2.8. Devlet Kurumlarına ve Bankalara Yapılan Siber Saldırıları - 2015.....	66
2.11.2.9. Sağlık Bakanlığı Hastanelerine Yönelik Siber Saldırıları - 2016.....	67
2.12. OLGUNLUK MODELLERİNİN ARAŞTIRILMASI VE MODEL KURULUMU	67
2.12.1.Olgunluk Modeli	67
2.12.2. Uluslararası Siber Güvenlik Olgunluk Modelleri.....	68
2.12.2.1. NISTIR 7628 (National Institute of Standards and Technology Interagency Report) Akıllı Şebeke Siber Güvenlik Kılavuzu (2010).....	68
2.12.2.2. ONG-C2M2 (Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model) Petrol ve Doğal Gaz Alt Siber Güvenlik Yeteneği Olgunluk Modeli (2014).....	69

2.12.2.3. ES-C2M2 (Electricity Subsector Cybersecurity Capability Maturity Model) Elektrik Alt Siber Güvenlik Yetenek Olgunluk Modeli (2014)	69
2.12.2.4. C2M2 (Cybersecurity Capability Maturity Model) Siber Güvenlik Yetenek Olgunluk Modeli (2014)	70
2.12.2.5. Enerji Sektörü Siber Güvenlik Çerçevesi Uygulama Rehberi (Energy Sector Cybersecurity Framework Implementation Guidance-2015)	70
2.12.2.6. Uluslar İçin Siber Güvenlik Kapasitesi Olgunluk Modeli (CMM-Cybersecurity Capacity Maturity Model) (2016)	71
3. MALZEME VE YÖNTEM	72
3.1. OLGUNLUK MODELİ KURULMASI	72
3.1.1. Analitik Hiyerarşi Proses (AHP)	73
3.1.2. Olgunluk Modeli Kurulum Adımları	73
3.2 AKILLI DOĞAL GAZ ŞEBEKELERİNDE SİBER GÜVENLİK AÇIKLARININ ARAŞTIRILMASI VE OLGUNLUK MODELİNİN GELİŞTİRİLMESİ	78
3.2.1. Yeni Siber Güvenlik Olgunluk Modelinin Kurulumu	81
3.2.1.1. Problem Tanımı ve Bilgi Toplama	82
3.2.1.2. KPI Belirleme Süreci	83
3.2.1.3. Model Süreç Performans Değerlendirme Döngüsü	84
3.2.1.4. AHP Yöntemi ve Ağırlıklandırma	84
3.3. AKIŞ YÖNETİMİ	91
3.3.1. Akıllı Doğal Gaz Şebekesinde SCADA	92
3.3.1.1. SCADA Çalışma Prensipleri	93
3.3.1.2. SCADA Ekipmanları	95
3.3.1.3. SCADA Üzerinden İzlenen Sistemler	98
3.3.1.4. SCADA Sistemi İle Haberleşen Sistemler	107
3.3.1.5. SCADA Sistemi Ağ Mimarisi	108
3.3.1.6. SCADA Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi	109
3.3.2. Akıllı Doğal Gaz Şebekesinde Elektronik Bülten Tablosu (EBT)	112
3.3.2.1. EBT Sistemi İle Haberleşen Sistemler	113
3.3.2.2. EBT Sistemi Ağ Mimarisi	114
3.3.2.3. EBT Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi	115
3.3.3. Akıllı Doğal Gaz Şebekesinde Ölçme ve Raporlama Sistemi (ÖRS-AVE)	117
3.3.3.1. ÖRS-AVE Sistemi İle Haberleşen Sistemler	118
3.3.3.2. ÖRS-AVE Sistemi Ağ Mimarisi	119
3.3.3.3. ÖRS-AVE Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi	120
3.3.4. Akıllı Doğal Gaz Şebekesinde Akıllı Sayaç (AMI/AMR)	121

3.3.4.1. AMI/AMR Sistemi İle Haberleşen Sistemler.....	122
3.3.4.2. AMI/AMR Sistemi Ağ Mimarisi	123
3.3.4.3. AMI/AMR Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi.....	125
3.4. VERİ YÖNETİMİ.....	126
3.4.1. Akıllı Doğal Gaz Şebekesinde Kurumsal Kaynak Planlama (ERP)	126
3.4.1.1. ERP Sistemi İle Haberleşen Sistemler	127
3.4.1.2. ERP Sistemi Ağ Mimarisi	127
3.4.1.3. ERP Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi.....	129
3.4.2. Akıllı Doğal Gaz Şebekesinde Çağrı Merkezi (CRM).....	130
3.4.2.1. CRM Sistemi İle Haberleşen Sistemler	130
3.4.2.2. CRM Sistemi Ağ Mimarisi	131
3.4.2.3. CRM Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi.....	132
3.4.3. Akıllı Doğal Gaz Şebekesinde Siber Güvenlik Sistemi (SGS)	133
3.4.3.1. SGS Sistemi İle Haberleşen Sistemler	134
3.4.3.2. SGS Sistemi Ağ Mimarisi.....	135
3.4.3.3. SGS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi	136
3.5. İŞGÜCÜ YÖNETİMİ	138
3.5.1. Akıllı Doğal Gaz Şebekesinde İşletme Otomasyon Sistemi (İOS)	138
3.5.1.1. İOS Sistemi İle Haberleşen Sistemler	139
3.5.1.2. İOS Sistemi Ağ Mimarisi	139
3.5.1.3. İOS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi	141
3.5.2. Akıllı Doğal Gaz Şebekesinde Araç Takip Sistemi (ATS)	142
3.5.2.1. ATS Sistemi İle Haberleşen Sistemler.....	142
3.5.2.2. ATS Sistemi Ağ Mimarisi	143
3.5.2.3. ATS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi.....	145
3.5.3. Akıllı Doğal Gaz Şebekesinde Bina Enerji Yönetim Sistemi (EYS).....	146
3.5.3.1. EYS Sistemi İle Haberleşen Sistemler.....	146
3.5.3.2. EYS Sistemi Ağ Mimarisi	147
3.5.3.3. EYS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi.....	148
3.6. BORU HATTI BÜTÜNSEL YÖNETİMİ	150
3.6.1. Akıllı Doğal Gaz Şebekesinde Katodik Koruma Sistemi (KKS).....	151
3.6.1.1. KKS Sistemi İle Haberleşen Sistemler	152
3.6.1.2. KKS Sistemi Ağ Mimarisi	152
3.6.1.3. KKS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi.....	153

3.6.2. Akıllı Doğal Gaz Şebekesinde Boru İçi Denetleme Robotu (BİDR)	155
3.6.2.1. BİDR Sistemi İle Haberleşen Sistemler	156
3.6.2.2. BİDR Sistemi Ağ Mimarisi.....	156
3.6.2.3. BİDR Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi	157
3.6.3. Akıllı Doğal Gaz Şebekesinde Boru Hattı Risk Yönetim Sistemi (BHRYIS)	158
3.6.3.1. BHRYIS Sistemi İle Haberleşen Sistemler	159
3.6.3.2. BHRYIS Sistemi Ağ Mimarisi.....	160
3.6.3.3. BHRYIS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi	160
3.7. AFET YÖNETİMİ	162
3.7.1. Akıllı Doğal Gaz Şebekesinde Deprem Risk Azaltım Sistemi (DRAS-SI)	162
3.7.1.1. DRAS-SI Sistemi İle Haberleşen Sistemler	163
3.7.1.2. DRAS-SI Sistemi Ağ Mimarisi	164
3.7.1.3. DRAS-SI Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi.....	165
3.7.2 Akıllı Doğal Gaz Şebekesinde İhbar Yönetim Sistemi (İYS)	167
3.7.2.1. İYS Sistemi İle Haberleşen Sistemler.....	168
3.7.2.2. İYS Sistemi Ağ Mimarisi	169
3.7.2.3. İYS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi.....	169
3.8. TESİSAT YÖNETİMİ	171
3.8.1. Akıllı Doğal Gaz Şebekesinde Coğrafi Bilgi Sistemi (CBS)	171
3.8.1.1. CBS Sistemi İle Haberleşen Sistemler	172
3.8.1.2. CBS Sistemi Ağ Mimarisi.....	172
3.8.1.3. CBS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi	173
3.8.2. Akıllı Doğal Gaz Şebekesinde DPOS & DGAS	175
3.8.2.1. DPOS & DGAS Sistemi İle Haberleşen Sistemler.....	175
3.8.2.2. DPOS & DGAS Sistemi Ağ Mimarisi	176
3.8.2.3. DPOS & DGAS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi.....	178
3.8.3. Akıllı Doğal Gaz Şebekesinde Şebeke Yük Optimizasyon Sistemi (ŞYOS).....	179
3.8.3.1. ŞYOS İle Haberleşen Sistemler.....	180
3.8.3.2. ŞYOS Sistemi Ağ Mimarisi.....	181
3.8.3.3. ŞYOS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi	182
3.9. AKILLI DOĞAL GAZ ŞEBEKELERİNDE EN SIK YAŞANAN SİBER SALDIRI YÖNTEMLERİ	183
4. BULGULAR	186
4.1. AKILLI DOĞAL GAZ ŞEBEKESİ SİBER GÜVENLİK OLGUNLUK MODELİ ÖNEM AĞIRLIK SONUÇLARI	186

4.1.1.KURUM-A Ana Bileşenlerin Önem Ağırlık Sonuçları	186
4.1.2. KURUM-A Alt Bileşenlerin Önem Ağırlık Sonuçları	187
4.1.3. KURUM-A KPI Parametrelerinin Önem Ağırlık Sonuçları	188
4.2. İNCELENEN KURUMLARIN AKILLI DOĞAL GAZ ŞEBEKELERİ SİBER GÜVENLİK OLGUNLUK SEVİYELERİ	189
4.2.1.KURUM-A Siber Güvenlik Olgunluk Seviyesi	189
4.2.2. KURUM-B Siber Güvenlik Olgunluk Seviyesi	190
4.2.3. KURUM-C Siber Güvenlik Olgunluk Seviyesi	191
4.3. İNCELENEN KURUMLARIN SİBER GÜVENLİK AÇISINDAN OLGUNLUK SEVİYELERİNİN KARŞILAŞTIRILMASI	192
4.4. KURUM-A AKILLI DOĞAL GAZ ŞEBEKESİ SCADA KPI SİBER GÜVENLİK OLGUNLUK SEVİYESİ	194
4.5. ÖNERİLEN AĞ KATMANI VE MİMARİSİ	195
4.5.1. Önerilen Akıllı Doğal Gaz Şebekesi Yeni Ağ Mimarisi Katmanı	195
4.5.2. Önerilen Akıllı Doğal Gaz Şebekesi Yeni Katmanlı Ağ Mimarisi	196
5. TARTIŞMA VE SONUÇ	198
KAYNAKLAR	201
EKLER	208
KPI PARAMETRELERİNE AİT ÖRNEK SORU SETLERİ	208
ÖZGEÇMİŞ	211

ŞEKİL LİSTESİ

	Sayfa No
Şekil 1.1 Kritik altyapılar (BG Derneği, 2012).	2
Şekil 2.1: Bilgi güvenliği kavramları (Baykara ve diğerleri, 2013).	11
Şekil 2.2: Bilgi güvenliğinin temel bileşenleri (Baykara ve diğerleri, 2013).	12
Şekil 2.3: Bilgi sistemleri katmanları.	13
Şekil 2.4: Siber güvenlik yaşam döngüsü (NIST, 2018).	16
Şekil 2.5: Siber saldırı yaşam döngüsü (Erol, 2015).	17
Şekil 2.6: Temel siber güvenlik gereksinimleri (BİLGEM, 2017).	18
Şekil 2.7: Akıllı şehirlerin 3 temel aktörü (Nam & Pardo, 2011).	20
Şekil 2.8: Akıllı şehirlere genel bakış (Channelpostmea, 2017).	22
Şekil 2.9: Akıllı şebekelere genel bakış (Feroze and Javaid, 2017).	23
Şekil 2.10: Akıllı şebeke temel yapı taşları (Goel, 2017).	25
Şekil 2.11: Akıllı şebeke güvenlik ekosistemi (Yan vd., 2012).	26
Şekil 2.12: Genel doğal gaz iletim ve dağıtım sistemi (GAZBİR, 2017).	28
Şekil 2.13: Akıllı doğal gaz şebekelerinin faydaları (GAZBİR, 2017).	30
Şekil 2.14: Siber saldırı yöntemleri.	33
Şekil 2.15: İstem dışı örnek bir mail.	35
Şekil 2.16: En genel zararlı yazılım (Malware) türleri.	37
Şekil 2.17: XSS örnekleme (Siber Güvenlik Danışmanlığı, 2019).	42
Şekil 2.18: XXE dış varlık güvenlik zafiyeti (Bgasecurity, 2019).	43
Şekil 2.19: MITM atak örneği (Mishra, 2013).	Error! Bookmark not defined. 44
Şekil 2.20: Ekim ayında gerçekleşen siber olaylar (Hackmaggeddon, 2020).	49
Şekil 2.21: Ülke veya bölgeye göre kişi başına düşen 2018 yılı veri ihlal maliyeti (IBM, 2018).	50

Şekil 2.22: Ülke veya bölge başına veri ihlal kök neden yüzdesi (IBM, 2018).....	51
Şekil 2.23: Kıyaslama örneğinin veri ihlalinin kök nedenine göre dağılımı (IBM, 2018).	51
Şekil 2.24: Dünya genelinde Ekim ayında gerçekleşen siber atakların yüzdesel dağılımı (Hackmaggeddon, 2020).	52
Şekil 2.25: Dünya genelinde 2019 yılında gerçekleşen siber atakların yüzdesel dağılımı (Hackmaggeddon, 2020).	53
Şekil 3.1: 2015-2019 Yılları arası abone sayısı (EPDK, 2020).	78
Şekil 3.2: Ekim 2019 Yılında sektörel bazda doğal gaz tüketimini dağılımı (EPDK, 2020).....	79
Şekil 3.3: Akıllı doğal gaz şebekesinin bileşenleri.	80
Şekil 3.4: Anahtar performans göstergesi (KPI) belirleme süreci.	83
Şekil 3.5: Modelin süreç performans değerlendirme döngüsü.....	84
Şekil 3.6: Önerilen AHP yöntemi ile oluşturulan olgunluk modeli.	86
Şekil 3.7: İkili karşılaştırma matrisi.	86
Şekil 3.8: Örnek bir SCADA sistemi.	94
Şekil 3.9: SCADA sistemi saha örneği.	94
Şekil 3.10: Örnek bir SCADA RTU.	96
Şekil 3.11: Örnek bir HMI arayüzü.	96
Şekil 3.12: Basınç sensörü.	97
Şekil 3.13: Sıcaklık sensörü.	97
Şekil 3.14: Kapı sensörü.	97
Şekil 3.15: GPRS modem.	98
Şekil 3.16: Örnek bir RMS A istasyonu.	99
Şekil 3.17: Örnek bir RMS A istasyonunun iç görünüşü.....	99
Şekil 3.18: Örnek bir bölge ve müşteri istasyonu.	100
Şekil 3.19: Bölge regülatörünün SCADA üzerinden izlenmesi.	101
Şekil 3.20: Örnek bir aktuatörlü vana odası.	102

Şekil 3.21: SCADA sisteminde izlenen örnek bir vana odası.....	103
Şekil 3.22: Örnek bir kromatograf cihazı.....	104
Şekil 3.23: Örnek bir kokulandırma ünitesi (Dağgaz, 2020).	105
Şekil 3.24: Örnek bir uç nokta koku ölçüm cihazı.....	106
Şekil 3.25: SCADA sistemi ile haberleşen sistemler.	107
Şekil 3.26: SCADA sistemi ağ mimarisi.	108
Şekil 3.27: EBT giriş ekranı (BOTAŞ, 2020).	113
Şekil 3.28: EBT sistemi ile haberleşen sistemler.	114
Şekil 3.29: EBT sistemi ağ mimarisi.	115
Şekil 3.30: Örnek ÖRS-AVE sistem mimarisi.....	118
Şekil 3.31: ÖRS-AVE sistemi ile haberleşen sistemler.	118
Şekil 3.32: ÖRS-AVE sistemi ağ mimarisi.....	119
Şekil 3.33: AMI/AMR sistemi ile haberleşen sistemler.....	123
Şekil 3.34: AMI/AMR sistemi ağ mimarisi.	124
Şekil 3.35: ERP sistemi ile haberleşen sistemler.	127
Şekil 3.36: ERP sistemi ağ mimarisi.....	128
Şekil 3.37: CRM sistemi ile haberleşen sistemler.....	131
Şekil 3.38: CRM sistemi ağ mimarisi.	132
Şekil 3.39: SGS sistemi ile haberleşen sistemler.	135
Şekil 3.40: SGS sistemi ağ mimarisi.....	136
Şekil 3.41: İOS sistemi ile haberleşen sistemler.	139
Şekil 3.42: İOS sistemi ağ mimarisi.....	140
Şekil 3.43: ATS sistemi ile haberleşen sistemler.	143
Şekil 3.44: ATS sistemi ağ mimarisi.	144
Şekil 3.45: EYS sistemi ile haberleşen sistemler.	147
Şekil 3.46: EYS sistemi ağ mimarisi.	148
Şekil 3.47: KKS sistemi ile haberleşen sistemler.	152

Şekil 3.48: KKS sistemi ağ mimarisi.	153
Şekil 3.49: BİDR sistemi ile haberleşen sistemler.	156
Şekil 3.50: BİDR sistemi ağ mimarisi.	157
Şekil 3.51: BHRYs sistemi ile haberleşen sistemler.	159
Şekil 3.52: BHRYs sistemi ağ mimarisi.	160
Şekil 3.53: DRAS-SI sistemi ile haberleşen sistemler.	164
Şekil 3.54: DRAS-SI sistemi ağ mimarisi.	165
Şekil 3.55: Örnek İYS çalışma mimarisi.	167
Şekil 3.56: İYS sistemi ile haberleşen sistemler.	168
Şekil 3.57: İYS sistemi ağ mimarisi.	169
Şekil 3.58: CBS sistemi ile haberleşen sistemler.	172
Şekil 3.59: CBS sistemi ağ mimarisi.	173
Şekil 3.60: DPOS & DGAS sistemi ile haberleşen sistemler.	176
Şekil 3.61: DPOS & DGAS sistemi ağ mimarisi.	177
Şekil 3.62: Örnek ŞYOS sistemi.	180
Şekil 3.63: ŞYOS sistemi ile haberleşen sistemler.	180
Şekil 3.64: ŞYOS sistemi ağ mimarisi.	181
Şekil 3.65: Akıllı doğal gaz şebekelerinde en sık yaşanan ilk 6 siber saldırı yöntemleri.	183
Şekil 4.1: KURUM-A Akıllı doğal gaz şebekesi siber güvenlik olgunluk seviyesi.	186
Şekil 4.2: KURUM-B Akıllı doğal gaz şebekesi siber güvenlik olgunluk seviyesi.	190
Şekil 4.3: KURUM-C Akıllı doğal gaz şebekesi siber güvenlik olgunluk seviyesi.	191
Şekil 4.4: 3 farklı kurumun akıllı doğal gaz alt bileşenlerinin siber güvenlik olgunluk seviyelerinin karşılaştırılması.	193
Şekil 4.5: KURUM-A Akıllı doğal gaz şebekesi SCADA KPI siber güvenlik olgunluk seviyesi.	194
Şekil 4.6: Önerilen akıllı doğal gaz şebekesi yeni ağ mimarisi katmanları.	195
Şekil 4.7: Önerilen akıllı doğal gaz şebekesi yeni katmanlı ağ mimarisi.	197

TABLO LİSTESİ

Sayfa No

Tablo 2.1: Akıllı şebeke iletişim teknolojilerinin karşılaştırma tablosu (Goel and Jindal, 2017).....	27
Tablo 2.2 Kullanıcılar tarafından kullanılan en iyi 10 standartlar, yönetmelikler ve iyi uygulama kullanım örnekleri (Radiflow, 2019).	54
Tablo 3.1: AHP Önem Skalası	75
Tablo 3.2: Akıllı doğal gaz şebekesi bileşenleri.....	81
Tablo 3.3: AHP yöntemi önem seviyeleri.	87
Tablo 3.4: Yönetim sistemlerinin önem ağırlıklarının hesaplanması.	88
Tablo 3.5: Yönetim sistemlerinin normalize edilmiş önem ağırlıklarının hesaplanması.	89
Tablo 3.6: Yönetim sistemlerinin önem ağırlıkları.....	89
Tablo 3.7: Akış yönetimi sistemine ait alt katagorilerinin ikili mukayesesi.	90
Tablo 3.8: Akış yönetimi sistemine ait alt katagorilerinin normalize edilmiş önem ağırlıkları.	90
Tablo 3.9: Akıllı doğal gaz şebekesi alt bileşenlerinin önem ağırlıkları.	91
Tablo 3.10: SCADA siber güvenlik olgunluk seviyesi ve KPI örnek listesi.....	109
Tablo 3.11: EBT siber güvenlik olgunluk seviyesi ve KPI listesi.....	116
Tablo 3.12: ÖRS-AVE siber güvenlik olgunluk seviyesi ve KPI listesi.	120
Tablo 3.13: AMI/AMR siber güvenlik olgunluk seviyesi ve KPI listesi.	125
Tablo 3.14: ERP siber güvenlik olgunluk seviyesi ve KPI listesi.	129
Tablo 3.15: CRM siber güvenlik olgunluk seviyesi ve KPI listesi.	132
Tablo 3.16: SGS siber güvenlik olgunluk seviyesi ve KPI listesi.	137
Tablo 3.17: İOS siber güvenlik olgunluk seviyesi ve KPI listesi.	141
Tablo 3.18: ATS siber güvenlik olgunluk seviyesi ve KPI listesi.....	145
Tablo 3.19: EYS siber güvenlik olgunluk seviyesi ve KPI listesi.....	149

Tablo 3.20: Doğal gazın temel bileşenleri.	150
Tablo 3.21: KKS siber güvenlik olgunluk seviyesi ve KPI listesi.	154
Tablo 3.22: BİDR siber güvenlik olgunluk seviyesi ve KPI listesi.	157
Tablo 3.23: BHRYs siber güvenlik olgunluk seviyesi ve KPI listesi.	161
Tablo 3.24: DRAS-SI siber güvenlik olgunluk seviyesi ve KPI listesi.	166
Tablo 3.25: İYS siber güvenlik olgunluk seviyesi ve KPI listesi.	170
Tablo 3.26: CBS siber güvenlik olgunluk seviyesi ve KPI listesi.	174
Tablo 3.27: DPOS & DGAS siber güvenlik olgunluk seviyesi ve KPI listesi.	178
Tablo 3.28: ŞYOS siber güvenlik olgunluk seviyesi ve KPI listesi.	182
Tablo 3.29: Akıllı doğal gaz şebekelerinde en sık yaşanan siber saldırı yöntemleri.	184
Tablo 4.1: KURUM-A Ana bileşenlerin önem ağırlıkları.	186
Tablo 4.2: KURUM-A alt bileşenlerin önem ağırlıkları.	187
Tablo 4.3: KURUM-A KPI parametrelerinin önem ağırlıkları.	188
Tablo 4.4: 3 farklı kurumun akıllı doğal gaz alt bileşenlerinin olgunluk seviyelerinin karşılaştırılması.	192

SİMGE VE KISALTMA LİSTESİ

Simgeler	Açıklama
----------	----------

w_i	: Sütun vektörü önem ağırlığı
m	: Karar noktası sayısı
n	: Noktaları etkileyen faktör
B	: Sütun vektörü
A	: Karşılaştırma matrisi
C	: Karşılaştırma matrisi

Kısaltmalar	Açıklama
-------------	----------

CaaS (Crime as a Service)	: Hizmet Olarak Suç İşleme
AES (Advanced Encrytion Standard)	: Gelişmiş Şifreleme Standartı
AHP (Analytic Hierarchy Process)	: Analitik Hiyerarşi Proses
AMI (Advance Metering Infrastructure)	: Gelişmiş Ölçüm Altyapısı
AMR (Automatic Meter Reading)	: Otomatik Sayaç Okuma
APN (Access Point Name)	: Erişim Noktası Adı
ARP (Adress Resolution Protocol Poisoning)	: ARP Zehirlenmesi
C2M2 (Cybersecurity Capability Maturity Model)	: Siber Güvenlik Kapasite Olgunluk Modeli
CAM (Content Addressable Memory)	: İçerik Adreslenebilir Bellek
CBS	: Coğrafi Bilgi Sistemleri
CERT (Computer Emergency Response Team)	: Bilgisayar Acil Müdahale Ekibi
CIS (Central of Information Security)	: Bilgi Güvenliği Merkezi
CMM (Cybersecurity Capacity Maturity Model)	: Siber Güvenlik Kapasitesi Olgunluk Modeli
CRM (Customer Relation Management)	: Müşteri İlişki Yönetimi
BİT	: Bilgi ve İletişim Teknolojileri
BTK	: Bilgi Teknolojileri Kurumu
DCS (Distributed Control System)	: Dağınık Kontrol Sistemleri
DDOS (Distributed Denial of Service)	: Dağıtık Hizmet Engelleme
DES (Data Encrytion Standard)	: Veri Şifreleme Standartı
DHCP (Dynamic Host Configuration Protocol)	: Dinamik İstemci Ayarlama Protokolü

DNS (Domain Name System) : Alan Adı Sistemi

DOS (Denial of Service) : Hizmet Engelleme

DSA (Digital Signature Algorithm) : Dijital İmza Algoritması

EBT : Elektronik Bülten Tablosu

EKS : Endüstriyel Kontrol Sistemi

ERP (Enterprise Resources Planning) : Kurumsal Kaynak Planlama

EPDK : Enerji Piyasası Düzenleme Kurumu

GDPR (General Data Protection Regulation) : AB Genel Veri Koruma Regülasyonu

GKM : Gaz Kontrol Merkezi

GPRS (General Packet Radio Service): Genel Paket Radyo Servisi

HIPAA (Health Insurance Portability and Accountability Act) : Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası

IAEA (The International Atomic Energy Agency): Uluslararası Atom Enerjisi Kurumu

IETF (Internet Engineering Task Force): İnternet Mühendisliği Görev Grubu

IoT (Internet of Thing) : Nesnelerin İnterneti

IIoT (Industrial Internet of Thing) : Endüstriyel Nesnelerin İnterneti

IP (Internet Protocol) : İnternet Protokolü

ISO (International Organization for Standardization) : Uluslararası Standardizasyon Örgütü

IT (Information Technology) : Bilgi Teknolojisi

ITU (International Telecommunication Union) : Uluslararası Telekomünikasyon Birliği

İMKB : İstanbul Menkul Kıymetler Borsası

İYS : İhbar Yönetim Sistemi

KPI (Key Performance Indicator) : Anahtar Performans Göstergesi

KVKK : Kişisel Verileri Koruma Kanunu

LAN (Local Area Network) : Yerel Alan Ağ

MD 2-4-5 (Message-Digest Algorithm 2-4-5) : 5-Mesaj Özümleme Algoritması

MIME (Multipurpose Internet Mail Extensions) : Çok Amaçlı İnternet Posta Uzantıları

S/MIME (Secure/Multipurpose Internet Mail Extensions) : Güvenli Çok Amaçlı İnternet Posta Uzantıları

NIST (National Institute of Standards and Technology) : Ulusal Standartlar ve Teknoloji Enstitüsü

NMAP (Network Mapper) : Ağ Eşleştirme

ONG (Oil and Natural Gas) : Petrol ve Doğal Gaz

OT (Operational Technology) : Operasyonel Teknoloji

ÖRS : Ölçüm ve Raporlama Sistemi

PCI DSS (Payment Card Data Security Standard) : Ödeme Kart Veri Güvenlik Satandartı

PCKS#7 (Public Key Cryptography Standards) : Ortak Anahtar Şifreleme Standartı

PGP (Pretty Good Privacy) : Kapsamlı Gizlilik

PLC (Programmable Logic Controller) : Programlanabilir Mantıksal Denetleyici

RFID (Radio Frequency Identification) : Radyo Frekans İle Tanımlama

RMS (Regulation and Measurement Station) : Basınç Düşürme ve Ölçüm İstasyonu

RSA (Rivest-Shamir-Adleman) : Rivest-Shamir-Adleman Şifreleme Algoritması

SCADA (Supervisory Control and Data Acquisition) : Merkezi Denetleme Kontrol ve Veri Toplama

SHA-1 (Secure Hash Algorithm-1) : Güvenli Özetleme Algoritması

SFM : Siber Füzyon Merkezi

SIC (Cyber Intelligence Center) : Siber İstihbarat Merkezi

SOC (Cyber Operation Center) : Siber Operasyon Merkezi

SOME : Siber Olaylara Müdahale Ekibi

SOX (Sarbanes-Oxley) : Sarbanes-Oxley Yasası

SSH (Secure SHell) : Güvenli Kabuk

SSL (Secure Socket Layer) : Güvenli Soket Katmanı

TCP (Transmission Control Protocol) : İletim Kontrol Protokolü

TEİAŞ : Türkiye Elektrik İletim Anonim Şirketi

TLS (Transport Layer Security): Taşıma Katman Güvenliği

USOM : Ulusal Siber Olaylara Müdahale

|

ÖZET

[DOKTORA TEZİ]

[AKILLI DOĞAL GAZ ŞEBEKELERİNDE SİBER GÜVENLİK AÇIKLARININ ARAŞTIRILMASI ve OLGUNLUK MODELİ GELİŞTİRİLMESİ]

[İsa AVCI]

İstanbul Üniversitesi-Cerrahpaşa

Lisansüstü Eğitim Enstitüsü

[Bilgisayar Mühendisliği Anabilim Dalı]

[Danışman : Doç. Dr. Muhammed Ali AYDIN

II. Danışman : Dr. Öğr. Üyesi Cevat ÖZARPA]

[Bu çalışmada, akıllı doğal gaz şebekelerinde siber güvenlik açıklarının araştırılması için bir olgunluk modeli geliştirilmiştir. Bu geliştirilen model akıllı doğal gaz şebekesine sahip enerji kurumlarının siber güvenlik açısından sistemlerinin güvenliği ölçer. Bu model sistemlerin siber güvenlik açısından olgunluk seviyelerini gösterir. Bu değerlerin kurumun siber saldırılara karşı olan dayanıklılığının ölçülmesinde katkı sunar. Olgunluk modeli uzman görüşü ve AHP metodu kullanılarak oluşturulmuştur. Bu modelde akıllı doğal gaz şebekelerine ait ana ve alt bileşenler belirlenerek AHP metodu kullanılarak sistemlerin önem ağırlıkları hesaplanmıştır. Doğal gaz dağıtımını yapan şirketlerin sayısal bir değer ile ifade edilebilen olgunluk modeli seviyeleri belirlenerek olgunlaşmaları için bir yol haritası çıkarılmıştır. Bu oluşturulan model ile doğal gaz şirketlerinden örnekleme yapılarak siber güvenlik açısından açıklıklar araştırıldı ve olgunluk seviyeleri hesaplandı. Bu olgunluk modeli 3 farklı kurum ve 5 farklı uzman görüşü alınarak geliştirilmiştir.]

Ocak 2021, 236 sayfa.

Anahtar kelimeler: Akıllı Doğal Gaz Şebeke, Siber Güvenlik, Siber Güvenlik Olgunluk Modeli, Kritik Altyapılar



SUMMARY

Ph.D. THESIS

INVESTIGATION OF CYBER SECURITY VULNERABILITIES AND DEVELOPMENT OF MATURITY MODEL IN SMART NATURAL GAS NETWORKS

İsa AVCI

Istanbul University-Cerrahpasa

Institute of Graduate Studies

Department of Computer Engineering

Supervisor : Assoc. Prof. Dr. Muhammed Ali AYDIN

Co-Supervisor : Assist. Prof. Dr. Cevat ÖZARPA

In this study, a maturity model has been developed to investigate cybersecurity vulnerabilities in smart natural gas networks. This developed model measures the security of the systems of energy institutions with smart natural gas networks in terms of cybersecurity. This model shows the mature levels of systems in terms of cybersecurity. These values contribute to measuring the resilience of the institution against cyber attacks. The maturity model was created using expert opinion and the AHP method. In this model, the main and sub-components of the smart natural gas networks are determined and the importance weights of the systems are calculated using the AHP method. A roadmap has been drawn for the companies that distribute natural gas to mature by determining their maturity model levels that can be expressed with a numerical value. With this model, sampling from natural gas companies was made, vulnerabilities in terms of cybersecurity were investigated and maturity levels were calculated. This maturity model has been developed by taking the opinions of 3 different institutions and 5 different experts.

January 2021, 236 pages.

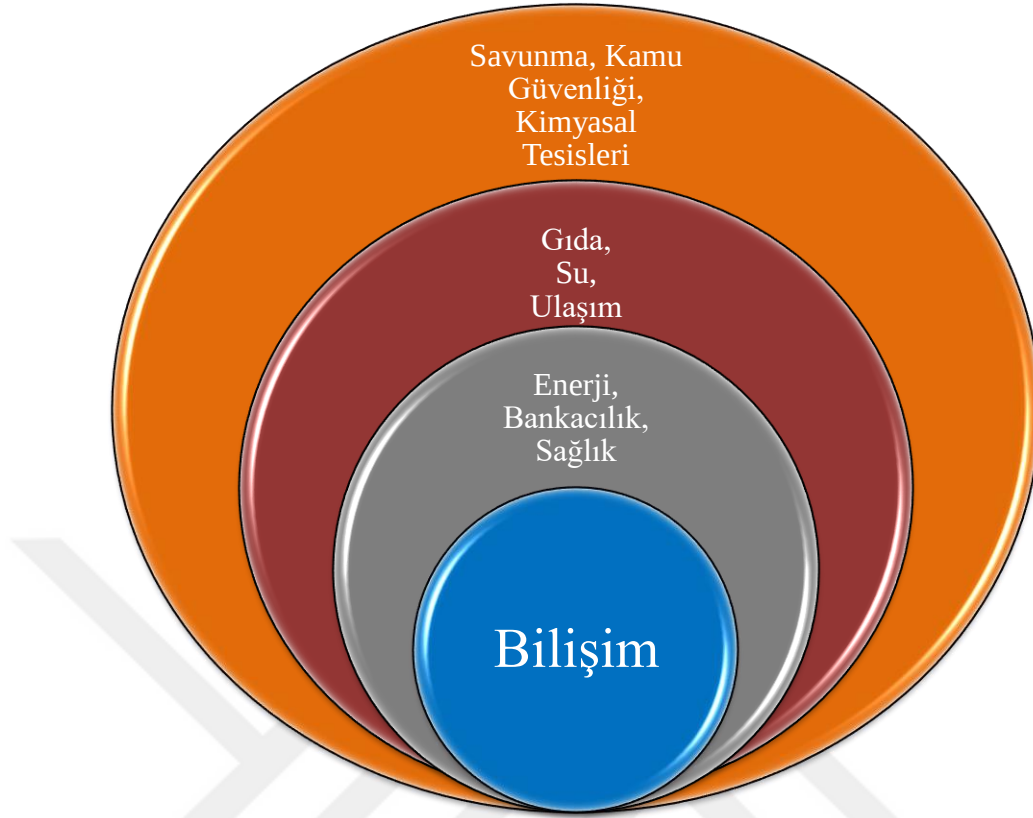
Keywords: Smart Natural Gas Grid, Cyber Security, Cyber Security Maturity Model, Critical Infrastructure

1. GİRİŞ

Bilgi ve iletişim teknolojileri toplumun ve ekonominin ayrılmaz bileşenleri olmuştur ve kalkınmaya önemli katkı sağlamaktadır. Ülkemizde bilgi ve iletişim sistemlerinin kullanımı kamu kurumlarında, özel sektörde ve vatandaşlara ilave olarak; enerji, su kaynakları, sağlık, kara, hava ve deniz ulaşımı, haberleşme ve finansal hizmetler gibi kritik altyapı sektörlerinde faaliyet gösteren kurum ve kuruluşlarda da hızla yaygınlaşmaktadır. Bilgi ve iletişim teknolojileri, özellikle de internet kullanımı siber uzaydaki tüm IT, OT, IoT veya IIoT sistemlerinin birbiriyle bağlantılı olmasını, bununla birlikte sistemlerdeki belirsizlikleri ve siber güvenlik risklerini beraberinde getirmektedir.

Milli Güvenlik açısından korunması gereken kritik altyapılar Şekil 1.1’ de belirtilmiş olsa da her bir kritik altyapı sistemi kendi içerisinde hayati bir öneme sahiptirler. Başlıca bilişim sistemleri gelişen teknoloji ile kritik altyapıların temelini oluşturmaktadır. Ülkeler kritik altyapı sistemlerinde haberleşme ve iletişimi sağlayan bilişim teknolojilerini temelinde olan internet ortamlarını korumalıdır. Enerji sektöründe bulunan su, elektrik ve doğal gaz kurumları hizmet ve dağıtım anlamında bir devletin ana omurgalarından biridir. Bu sistemlerin korunması milli güvenlik açısından kritik seviyede bir güvenlik önlemlerinin alınmasına ihtiyaç duyulmaktadır.

Gelişen bilgi ve iletişim teknolojilerine ilave olarak büyük şehirlerde artan nüfus, yapılaşma ve mega yatırımlar sebebiyle şehirlerde enerji ihtiyacının artması, yönetilebilirlik, sürdürülebilirlik, olası olumsuzlukların önceden tespit edilebilme imkanı ve uzaktan müdahale şansı, maliyetlerin düşürülmesi ve enerji verimliliği gibi hususlar akıllı şebekelere olan ihtiyacı ön plana çıkarmıştır. Ülkemizde 2019 yılında üretilen elektriğin % 25’ i doğal gazdan üretiliyor olması doğal gaz şebekesinin optimum işletilmesi hususu önemli bir hedef olmuştur (GAZBİR, 2020). Bu hedefin sadece akıllı şebekeler konseptiyle yapılabilecek olması, yeni yatırımların akıllı şebeke konseptiyle kurulması gerekliliğini ön plana çıkarmaktadır.



Şekil 1.1: Kritik altyapılar (BG Derneği, 2012).

Akıllı şebekeler son yıllarda teknolojinin gelişmesi ile birlikte yaygın hale gelmiş olup gelişen teknoloji ile birlikte öngörülemedi riskler ve güvenlik açıklıkları gündeme oturmuş ve çözülmesi gereken bir problem haline gelmiştir. Akıllı şebekeler özellikle elektrik, su ve doğal gaz iletim ve dağıtım hizmetleri gibi kamu hizmetleri ve kullanım alanlarını kapsamaktadır.

Akıllı doğal gaz şebekelerinde kullanılan bilgi ve iletişim sistemlerinde bulunan güvenlik zafiyetleri, bu sistemlerin hizmet dışı kalmasına veya kötüye kullanılmasına, can kaybına, büyük ölçekli ekonomik zarara, kamu düzeninin bozulmasına ve/veya ulusal güvenlik risklerine neden olabilir. Siber saldırı sebebi ile ortaya çıkan maddi zarar olağanüstü boyutlara ulaşmıştır. Son yıllarda artan siber olaylar ve güvenlik firmalarının yapmış olduğu çalışmalar bu gerçeği açıkça ortaya koymaktadır.

Hali hazırda kimlik gizleme (anonimlik) ve inkâr edilebilirlik açısından saldırganlara siber saldırı fırsatı sunduğu bir gerçektir. Ayrıca bu saldırıların kimin ve kimlerin tarafından finanse edildiği ve hangi ülkelerin bu saldırıların arkasında olduğunu tespit etmek de zordur. Bu nedenle siber uzaydaki risk ve tehditleri belirlemek, bunlara karşı önlem almak oldukça güçtür. Böyle bir ortamda artık siber güvenliğin mutlak olarak sağlanmasından bahsedilmemekte,

bunun yerine siber güvenlik risklerinin yönetilebilir ve kabul edilebilir düzeylerde tutulması hedeflenmektedir. İnternet gibi açık ve bağlantılı bir ortamda bulunmanın artan erişilebilirlikle birlikte bazı riskleri de getireceği kabul edilmektedir. Bu risklerin tüm paydaşları içeren bütüncül bir yaklaşımla yönetilerek siber olaylara karşı hazırlıklı olunması ve bu olaylardan en az zararla çıkılarak sürekliliğin sağlanması esas alınmalıdır.

Bu tez çalışmasının amacı, şehirlerde doğal gaz dağıtımı yapan şirketlerin kullandığı akıllı doğal gaz şebekelerinde siber güvenlik açıklarını araştırmak, olgunluk modeli geliştirmek ve iyileştirilmeye açık alanları tespit etmektir. Bu çerçevede IT, OT, IoT, IIoT ve EKS/SCADA sistemleri incelenecek, siber güvenlik açıkları tespit edilecek ve uzmanlardan alınan görüşler ile puanlama yapılarak önceliklendirilecektir. Doğal gaz dağıtımı yapan şirketlerin sayısal bir değer ile ifade edilebilen olgunluk modeli seviyeleri belirlenerek olgunlaşmaları için bir yol haritası çıkarılacaktır. Bu oluşturulacak model ile doğal gaz şirketlerinden örnekleme yapılarak siber güvenlik açısından açıklıklar tespit edilerek olgunluk seviyesi hesaplamaları yapılacaktır. |

2. GENEL KISIMLAR

Bu bölümde akıllı şehir ve şebeke, akıllı doğal gaz şebekesi bilgi güvenliği, siber güvenlik, en çok kullanılan siber saldırı yöntemleri ve siber güvenlik raporlarından örnekler tezin amacına uygun olarak verilmiştir. Ayrıca tezin içerisinde geçen genel kavramların tanımları kısaca yapılmaya çalışılmıştır ve kavramlar arasındaki ilişkilerin tanım olarak verilmesi hedeflenmiştir.

2.1. GENEL TANIMLAR

Akıllı Şehir: “Kritik altyapı bileşenlerinin ve kentsel yönetim, eğitim, sağlık, kamu güvenliği, gayrimenkul, ulaşım gibi kamu hizmetlerinin akıllı bilgi işlem teknolojileri kullanılarak, birbirine bağlı olarak daha akıllı ve daha verimli hale getirildiği şehirlerdir.” (Washburn, et al., 2010)

Akıllı Şebeke: Akıllı şebekeler konsepti, bilgi teknolojisi ve iletişim sistemlerinin kullanılması yoluyla verimli ve güvenilir enerji tedariki, depolama, tüketim için dağıtım ve iletim sisteminin esnek kontrolünü hedefleyen sistemler bütünüdür.

Akıllı Doğal Gaz Şebekesi: Akıllı doğalgaz şebekesi, doğal gazın basıncı, ısı değeri, deprem olma riskleri, altyapı varlık bilgileri, ticari ve bireysel abonelerin tüketim miktarı gibi birçok parametre anlık olarak bir kontrol merkezinden takip edilebilmesini sağlayan ve gelişmiş bilişim teknolojilerini kullanan sistemlerin bütünüdür.

Bilgi Güvenliği : Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunu garanti etme, bilginin ve işleme yöntemlerinin doğruluğunu ve bütünlüğünü temin etme ve yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara erişebileceklerini garanti etme olarak tanımlanmaktadır (Baykara ve diğerleri, 2013).

Bilişim Sistemleri: Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin, işlemin ve bilgi/verinin sunumunda yer alan sistemlerin bütünü olarak tanımlanmaktadır (T.C. UDHB, 2016).

Bilgi Teknolojileri (IT) : Herhangi bir bilgisayar, depolama aracı, ağ ve diğer fiziksel aygıtların kullanılmasıyla dijital verilerin yapılandırılması, işlenmesi, oluşturulması, korunması ve değiştirilmesini kapsayan alandır.

Bilgi: “Verinin bir üst formu olup, verinin değerlendirilmiş, analiz edilmiş, düzenlenmiş ve verinin belirli bir anlam ifade edecek forma dönüştürülmüş hali olarak tanımlanmaktadır” (BGD, 2018).

Dağıtık Kontrol Sistemleri (DKS/DCS): Bir tesisin veya endüstriyel prosesin otomatik olarak kontrol edilmesi olarak tanımlanmaktadır. Tek bir kontrol fonksiyonu yerine her bir proses veya makine grubuna özel bir kontrol mekanizması kullanılır. Kontrol mekanizmasının çok sayıda denetleyiciden oluşmaktadır. Dağıtık kontrol sisteminde, veri toplama ve kontrol fonksiyonları için mikrodenetleyici tabanlı işlemciler ve PLC’ler kullanılır.

Endüstriyel Kontrol Sistemleri (EKS/ICS): Geleneksel bilişim teknolojileri dışında, programlanabilir mantıksal denetleyiciler aracılığı ile üretim, ürün işleme ve dağıtım kontrolleri gibi endüstriyel işlemler için kullanılan, SCADA (Supervisory Control and Data Acquisition) ve DCS (Dağıtık Kontrol Sistemleri) şeklinde gruplanan bilgi sistemleri olarak tanımlanmaktadır (T.C. UDHB, 2016).

Gerçek ve Tüzel Kişilere Ait Bilişim Sistemleri: Türkiye Cumhuriyeti kanunlarına tabi olarak gerçek ve tüzel kişilere ait olan ve/veya gerçek ve tüzel kişilerce işletilen/yönetilen bilişim sistemleri olarak tanımlanmaktadır (T.C. UDHB, 2016).

Güvenlik Zaafiyeti: Kullanılan sistemler üzerindeki zayıflıklar olarak tanımlanmaktadır. Zaafiyetler teknik, operasyonel, fiziksel ve bireysel zaafiyet olarak gerçekleşebilir (T.C. UDHB, 2016).

Hacker: “Hacker, şahsi bilgisayarlara veya çeşitli kurum ve kuruluşlara ait bilgisayarlara ve ağlara izinsiz olarak giriş yapan kişidir.” Hacker diğer anlamı ise saldırgan veya Bilgisayar korsanı olarak bilinmektedir. Bunlar siyah, beyaz, gri ve kırmızı olarak 4 çeşittir. Siyah kötülüğü, beyaz masumiyeti, gri net olmayan ve kırmızı ise kendini diğerlerden farklı olarak tanıtan gruplardır (Kara, 2013).

Hacking: Bir sistem üzerindeki gizli ve ulaşılamayan bilgileri ele geçirmektir (Kara, 2013).

Hacktivizm: Hacktivist, amaçları için siber ortamı kullanmayı tercih eden, sanal protestocularıdır. Bu protestocuların yapmış oldukları siyasi ve toplumsal eylemlere Hacktivizm denilmektedir (Kara, 2013).

Kamu Bilişim Sistemleri: Türkiye Cumhuriyeti kamu kurum ve kuruluşlarına ait olan ve/ veya kamu kurum ve kuruluşları tarafından işletilen/yönetilen bilişim sistemleri olarak tanımlanmaktadır (T.C. UDHB, 2016).

Kritik Hizmet: Kritik hizmetler verilmediği durumlarda can kaybına, büyük ölçekli ekonomik zarara ve Ulusal Güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek hizmetler olarak tanımlanmaktadır (T.C. UDHB, 2016).

Kritik Ürün: Kritik hizmetlerin gizlilik, bütünlük ve erişilebilirliğini sağlayan bilgi teknolojisi ürünleri olarak tanımlanmaktadır (T.C. UDHB, 2016).

Kritik Altyapılar: İşlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliğinin olmadığı durumlarda can kaybına, büyük ölçekli ekonomik zarara, Ulusal Güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar olarak tanımlanmaktadır (T.C. UDHB, 2016).

Kritik Altyapı Sektörleri: 20/06/2013 tarih, 2 sayılı Siber Güvenlik Kurulu kararı uyarınca kritik altyapıları barındırmakta olan “Elektronik Haberleşme”, “Enerji”, “Su Yönetimi”, “Kritik Kamu Hizmetleri”, “Ulaştırma” ve “Bankacılık ve Finans” sektörlerini tanımlamaktadır (T.C. UDHB, 2016).

Kurum: Kamu kurumları ve kritik altyapı işleten kamu ya da özel sektör kuruluşlarına verilen ad olarak tanımlanmaktadır (T.C. UDHB, 2016).

Operasyonel Teknolojiler (OT) : Fiziksel cihazların performansını izleyen ve kontrol eden bir donanım ve yazılım kategorisidir. Özellikle IT’ den ayıran nokta ise EKS sistemlerinde operasyonel teknoloji altyapısının oluşturulması ile kurumsal IT sistemlerinden ayrı olarak yönetilmesi ve kontrol edilmesidir.

Risk: Tehditlerin bir veya birden çok bilgi varlığındaki açıklığı kullanarak zarar meydana getirme potansiyeli olarak tanımlanmaktadır (T.C. UDHB, 2016).

SCADA-Denetleme Kontrol ve Veri Toplama (Supervisory Control And Data Acquisition): Sistemleri geniş alana yayılmış üretim, dağıtım vb. kritik altyapı tesislerinin bir merkezden bilgisayar aracılığı ile izlenmesi ve kontrol edilmesi olarak tanımlanmaktadır (T.C. UDHB, 2016).

Sınır Güvenliği: Bilişim sistemlerinin güvenlik duvarı ve saldırı engelleme sistemleri gibi erişim kontrolü sağlayan sistemler aracılığı ile dış ağlardan gelebilecek saldırılardan korunması ve ele geçirilmesinin önlenmesi olarak tanımlanmaktadır (T.C. UDHB, 2016).

Siber Uzay: Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam olarak tanımlanmaktadır (T.C. UDHB, 2016).

Siber Olay: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilgi/verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulması olarak tanımlanmaktadır.

Siber Savaş: Düşman devletlere ait sistemlere gizli, görünmez ve izinsiz olarak internet üzerinden erişerek düşmanı psikolojik olarak çökertmek olarak tanımlanmaktadır. Sistemlerin kontrolü ele geçirilerek bilgilere ulaşmak, çalmak, çökertmek ve yanlış yönlendirmek gibi faaliyetleri kapsamaktadır. Diğer bir tanımla bir devletin başka bir devletin bilgisayar sistemlerine ve ağlarına sızarak hasar veya kesinti oluşturmak için yapılan hareketler bütünüdür (Kara, 2013).

Siber Varlık: “Siber ortamlarda bulunan, araçlar, işlemler, dokümanlar, planlar, dokümante edilmiş düşünceler, veriler veya bilgilerdir” (BGD, 2018).

Siber Casusluk: “Çoğunlukla elektronik ortamları kullanarak yapılan casusluğa verilen isimdir” (BGD, 2018). Ulusal güvenlik veya ticari istihbarat toplama amacıyla e-mail trafiği, metin mesajları ile diğer elektronik haberleşmelerin ve kurumsal verinin gizlice ele geçirilmesi olarak tanımlanmaktadır.

Siber Suç: Bir bilişim sisteminin güvenliğini ve / veya buna bağlı verileri ve / veya kullanıcılarını hedef alan ve bilişim sistemi kullanılarak işlenen suçlardır. Diğer bir ifade ile siber uzayda hizmetlerin ve uygulamaların bir suç için kullanıldığı veya siber uzayın bir suçun kaynağı,

hedefi, yöntemi ve aracı olduğu suç faaliyetidir. Bu suç türü bilgisayar ve internete özgü suçlar olarak da adlandırılmaktadır (Kaya Kurt, 2017).

Siber Silah: “Elektronik ortamda saldırı ve savunma amaçlı olarak kullanılabilecek her türlü araçtır. “Kötücül amaçlı yazılım veya kod parçaları” olarak ifade edilmektedir “(BGD, 2018).

Siber Saldırı: Ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi, topluluk, kurum ve/ veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler olarak tanımlanmaktadır (T.C. UDHB, 2016).

Siber Güvenlik: Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi olarak tanımlanmaktadır (T.C. UDHB, 2016).

Siber Olaylar Müdahale Ekibi (SOME): USOM ile işbirliği içinde çalışan kurum ve kuruluşların görevlerini yapan birim ve ekip olarak tanımlanmaktadır (BGD, 2018).

Siber Operasyon Merkezi (SOC): “Bilinen zafiyet veri tabanlarının kontrol edildiği, zafiyetlerin istismar edilebileceği alanların kıymetlendirildiği ve ardından bu zafiyetlerin sistemlerde olup olmadığının kontrol edildiği, gerekli tedbirler alındığı veya alınıldığı merkezdir” (STM, 2019).

Siber İstihbarat Merkezi (SIC): “Klasik SOM görevlerinin yanında, siber ortam olaylarını değerlendirerek siber tehdit istihbaratının oluşturulduğu; siber olaylar olmadan önce tehditlerin öngörüldüğü, siber tehdit istihbaratını bilgi güvenliği teknolojileri ile entegre edildiği ve karar vericilere üzerinde işlem yapılabilir bilgi sunulduğu merkezdir” (STM, 2019).

Siber Risk: Siber saldırı olasılığı ile saldırının olası etkisi olarak tanımlanmaktadır ve her iki terim ile doğru orantılıdır. Siber saldırı olasılığı alınan önlemler, zaafiyetler ve tehditlere bağlı olarak değişmektedir, ancak saldırının olası etkisi ise potansiyel kayıplara bağlı olarak değişmektedir (T.C. UDHB, 2016).

Pentest/Penetration: Belirlenen bilişim sistemlerindeki mantık hataları ve zafiyetleri tespit ederek, söz konusu güvenlik açıklıklarının kötü niyetli kişiler tarafından istismar edilmesini önlemek ve sistemleri daha güvenli hale getirmek amacıyla, “yetkili” kişiler tarafından ve “yasal” olarak gerçekleştirilen güvenlik testleridir. Pentest çalışmalarındaki asıl amaç, zafiyeti tespit etmekten öte ilgili zafiyeti sisteme zarar vermeyecek şekilde istismar etmek ve yetkili erişimler elde etmektir. Whitebox, Blackbox, Graybox olmak üzere genel kabul görmüş üç çeşidi vardır. Zaafiyet taramasında genellikle açık kaynak kodlu otomatize pentest araçlar (Nmap, Nessus, Qualys, Metasploit, Inguma, hping, WebScarab, jtr, W3af vb.) kullanılmaktadır. Bunların yanı sıra ticari pentest araçlar (Immunity Canvas, Core Impact, HP Webinspect, SAINT Ssecurity Scanner) vardır. Ayrıca pentest araçlarını bilmek kadar metodolojilerininide (OWASP Guide, NIST, ISSAF, OSTTM) bilmek önemlidir.

Siber Füzyon Merkezi (SFM): “Siber Füzyon Merkezi, kritik teknoloji ve bilgi varlıklarının güvenliğine yönelik proaktif ve koruyucu faaliyetleri içerir. SFM, bilgi teknolojileri operasyonları ile tehdit istihbaratından gelen bilgi akışını ve güvenlik fonksiyonlarını yönetir ve koordine eder. Bu sayede, harekât etkinliğini artırır, siber tehdit istihbaratının zamanında dağıtılmasıyla saldırıları önleyerek veya etkisini azaltarak güvenlik seviyesini artırır” (STM, 2019).

Tehdit: Bir şirketin veya sisteminin zarar görmesi ile sonuçlanabilecek istenmeyen bir olayın potansiyel nedeni olarak tanımlanmaktadır (T.C. UDHB, 2016).

Ulusal Siber Uzay: Kamu bilişim sistemleri ile gerçek ve tüzel kişilerce işletilen/kullanılan bilişim sistemlerinden oluşan ortam olarak tanımlanmaktadır (T.C. UDHB, 2016).

Ulusal Siber Güvenlik: Ulusal siber uzayı oluşturan bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem, bilgi/verinin ve bunların sunumunda yer alan donanım ve yazılım sistemlerinin ulusal ölçekte sağlanan siber güvenlik olarak tanımlanmaktadır (T.C. UDHB, 2016).

Ulusal Siber Olaylara Müdahale (USOM): USOM, 2013-2014 yıllarında Ulusal Siber Güvenlik Stratejisi ve Eylem Planı kapsamında, ulusal ve uluslararası koordinasyonun sağlanması için kurulmuştur. Ayrıca, hem ulusal ve uluslararası koordinasyon görevini yürütmekte hem de internet aktörleri, kolluk güçleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişimi sağlamaktadır. Aynı zamanda, ülkemize karşı

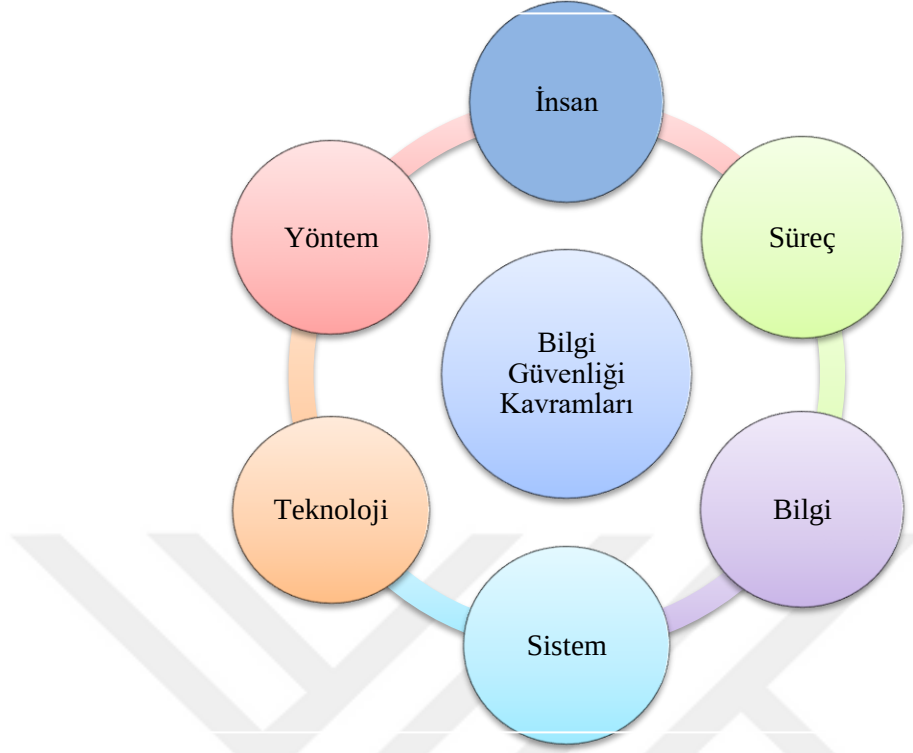
yapılan saldırıları yakinen takip etmekte, önlemler almakta ve 2000' e yakın kurumsal SOME ile bu görevi başarıyla yürütmektedir.

Veri (Data): “Olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi olarak tanımlanmaktadır” (BGD, 2018).

Zafiyet/Açıklık Tarama (Vulnerability Assessment): Zafiyet taraması bir sistemdeki muhtemel tüm açıklıkların belirlenmesine yönelik tasarlanmış bir testtir. Bu yöntem için genellikle otomatize araçlar (Nessus, Nmap, Qualys vb) kullanılır. Zafiyet taramasında asıl amacı taranan sistemin anlık olarak genel güvenlik durumunu görmektir. Bu yöntemde denetlenen diğer şey ise uyumluluk süreçleridir. Firmaların bu yöntemler sayesinde HIPAA, PCI DSS, SOX, CIS vb. gibi dünyaca kabul edilmiş birçok uyumluluk standartlarına göre uyumluluk durumunu belirlenir ve rapor olarak sunulur.

2.2. BİLGİ GÜVENLİĞİ

Bilgi güvenliği, bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunu garanti etme, bilginin ve işleme yöntemlerinin doğruluğunu ve bütünlüğünü temin etme ve yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara erişebileceklerini garanti etme olarak tanımlanmaktadır (Baykara ve diğerleri, 2013). Bilgi güvenliği aşağıdaki Şekil 2.1' de görüleceği gibi bir çok kavramla ilişkilendirilmiştir ve her bir kavram doğrudan bilginin güvenirliliğini etkilemektedir. Her bir kavram bilgi güvenliğinin temelini oluşturmaktadır ve her biri birbirine bağlı olarak kendi içerisinde belirli yöntem ve yaşam döngüsüne sahiptirler.



Şekil 2.1: Bilgi güvenliği kavramları (Baykara ve diğerleri, 2013).

Bilgi güvenliği, yukarıda şekilde gösterildiği gibi içerisinde teknoloji (yazılım ve donanım), insan, süreç, yöntem ve metodoloji gibi bir çok terimi içeren ve bilgi teknolojileri dünyasında oldukça yüksek değere sahip bir olgudur. Bütün bu temel kavramlar bilgi ve bilişim güvenliğinde iç içe geçmiş halkalar gibi birbirleriyle ilişkilidirler.

2.2.1. Bilgi Güvenliğinin Bileşenleri

Gizlilik, bütünlük, erişilebilirlik, doğrulama, yetkilendirme ve hesap bilişim güvenliğinin temel bileşenlerini oluşturur (Baykara ve diğerleri, 2013). Aşağıda temel kavramlar kısaca anlatılmaya çalışılmıştır ve Şekil 2.2’ de gösterim olarak verilmiştir.

Gizlilik (Confidentially): Bilginin üçüncü şahıslar tarafından ağ dinleme gibi yöntemlerle ele geçirilmesinin engellenmesi için şifrelenmesi ve yetkisiz kişilerin de anlamaması için yapılması gereken bir uygulamadır.

Bütünlük (Integrity): Bilginin aktarımı sırasında herhangi bir değişikliğe uğramasının engellenmesi bilginin bütünlüğü sağlar. Parity bitleri ile yapılan kontroller bu bileşenin örnek uygulaması olarak verilebilir.

Erişilebilirlik (Availability): Sistemin sürekli erişilebilir olmasını esas alır. Hizmet veremeyen sistemler maddi kayıplar ile müşteri kayıplarına neden olabilirler. Bu bağlamda erişilebilirlik çok önemlidir.

Doğrulama (Authentication): Kullanıcının kim olduğu sorgulanır. Şifre ve kullanıcı isim tanımlanması gerekmektedir.

Yetkilendirme (Authorization): Kullanıcılara yetkilerin atanması ve hangi kullanıcının ne kadar yetkili olduğunun belirlenmesi işleminin yapılmasıdır.

Hesap (Account): Hangi kullanıcı hangi noktada ve hangi alanlarda neler yaptığının kontrol edilebilmesi için kullanılmaktadır.

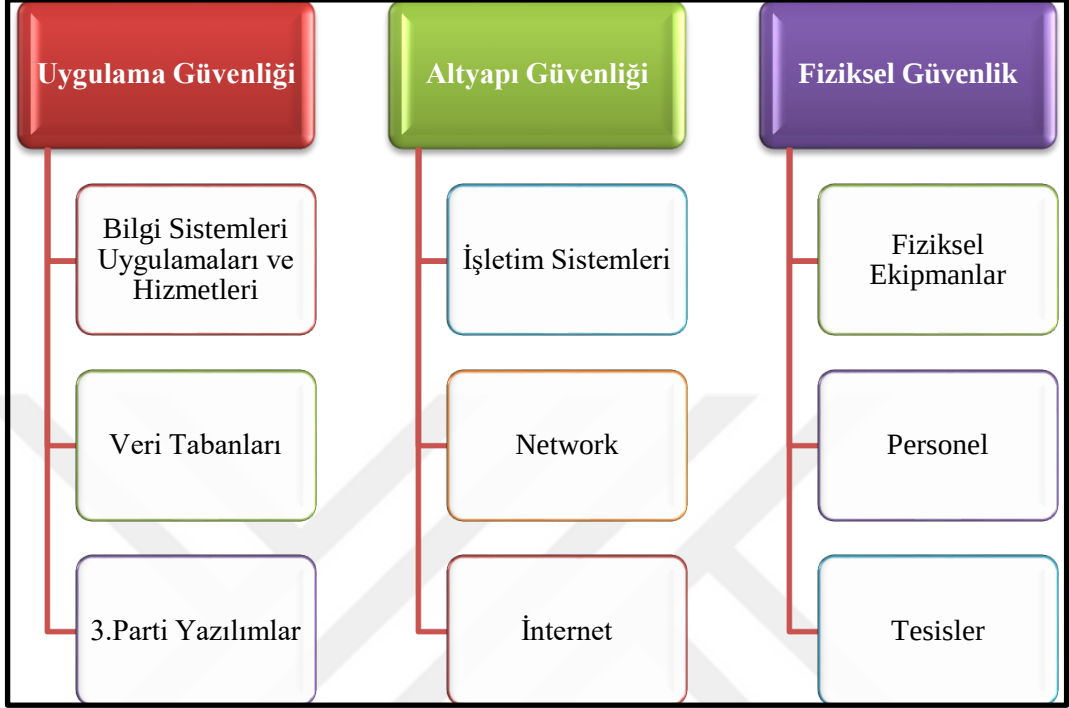


Şekil 2.2: Bilgi güvenliğinin temel bileşenleri (Baykara ve diğerleri, 2013).

2.2.2. Bilgi Sistemleri Katmanları

Bilgi sistemleri güvenlik açısından belirli katmanlarda tanımlanabilmektedir ve her katman kendi arasında bir alt kısıtlımlara sahiptir. Bu sistemlerin en önemli özelliği bilginin

güvenliğinin ön plana çıkarılmasıdır. Bilgi sistemlerinin katmanlarıda güvenlik açısından uygulama, altyapı ve fiziksel güvenlik olmak üzere 3 ana başlık altında belirtilmektedir.



Şekil 2.3: Bilgi sistemleri katmanları.

Bilgi sistemleri katmanları Şekil 2.3’ de uygulama katmanında bilgi sistemleri uygulamaları ve servisleri, veri tabanları, 3.parti uygulamalar olmak üzere 3 alt başlıkta belirtilebilir. Altyapı güvenliği katmanının altında ise işletim sistemleri, network, internet olarak alt sınıflandırma yapılırken, fiziksel güvenlik açısından fiziksel ekipmanlar, personel ve tesisler olarak alt sınıflara ayrılabilir. Şekil 2.3’ de uygulama katmanında bilgi sistemleri uygulamaları ve servisleri, veri tabanları, 3.parti uygulamalar olmak üzere 3 alt başlıkta belirtilebilir. Altyapı güvenliği katmanının altında ise işletim sistemleri, network, internet olarak alt sınıflandırma yapılırken, fiziksel güvenlik açısından fiziksel ekipmanlar, personel ve tesisler olarak alt sınıflara ayrılabilir.

2.3. VERİ İLETİM GÜVENLİK PROTOKOLLERİ

Güvenlik protokolleri arasında en sık kullanılanlar SSL/TSL (Secure Socket Layer/Transport Layer Security), PGP (Pretty Good Privacy) ve genellikle sertifika gerektirmeyen SSH (Secure SHell) olarak belirtilmektedir. Aşağıda bu protokoller tanımlanmaktadır (BGA, 2018).

2.3.1. Pretty Good Privacy-PGP

Bu protokol bir e-posta yazılımı olup ücretsiz ve açık kaynak kodludur. Ayrıca güçlü şifreleme algoritması olması, kendine has karmaşık bir güvenlik sertifika modeli ve kullanımı kolay olması avantajları arasındadır.

2.3.2. SSL/TSL

Bu protokol genel amaçlı geliştirilmiş olması, güvenli HTTP bağlantısı sağlaması ve yaygın olarak tarayıcı (browser) programlar tarafından desteklenmesiyle birçok kullanıcı tarafından kullanılmaktadır. SSL ve TSL protokolleri, genel olarak TCP/ IP protokolleri güvenlik katmak amacıyla geliştirilmiştir.

SSL' in en basit hali, iletişim hattının şifrelenmesi durumudur ve bu protokol sayesinde bağlantı kuran iki uç arasındaki kimlik doğrulamayı, doğrulama işlemini şifrelemeden ayırmayı ve daha önceki bağlantının kaldığı yerden devam etmesini sağlamaktadır. SSL protokolü, bir birlerine gönderilen ya da gönderilmeyen bir dizi mesaj kümesinden oluşur.

SSL protokolü Netscape tarafından geliştirilmiş olmasına rağmen, bu protokolün internette yaygın kullanımından dolayı, IETF (İnternet Mühendisliği Görev Grubu-Internet Engineering Task Force) için çok kritik bir hale gelmiştir. Bu grup bu protokolü biraz daha geliştirerek TSL (Ulaşım Güvenlik Katı-Transport Security Layer) olarak değiştirmiştir. TSL protokolü SSL'e göre çok az değiştirilmiş, güvenliği daha da arttırılmıştır.

2.3.3. SSH (Secure SHell)

Bu protokol telnet ve ftp gibi uzak erişim protokollerine alternatif olarak kullanılan ve sunucu ile istemci arasında iletişimi şifreleyen bir protokoldür.

2.3.4. S/MIME (Secure/Multipurpose Internet Mail Extensions)

Bu protokol, güvenli e-posta ortamı oluşturmak için kullanılan bir standart olup PKCS#7 yapısı üzerine kurulmuştur ve DSA ve MIME standartlarını içermektedir. Bu protokolde mesaj içeriği açıktır, fakat tüm yapı şifrelenmiştir. Mesaj alındı teyidi, güvenlik etiketleri, posta listeleri, anahtar belirleme gibi işlemleri destekler. MD2, MD4, DES, 3DES, SHA-1, MD5, RSA, DSA, Diffie-Hellman gibi özetleme, imzalama, şifreleme ve anahtar şifreleme algoritmaları bu yapı içerisinde kullanılır.

2.3.5. IPSec (Internet Protocol Security)

Bu protokol iki istemci arasındaki haberleşmeden, IP paketlerinin şifrelenmesi, online anahtar dağıtımı, sanal özel ağ (VPN) haberleşmesi, bilgisayar ile şifreleme cihazlarının

haberleşmesine kadar, internet tabanlı tüm haberleşmelerde güvenliği sağlamak veya güvenli bir ortam oluşturabilmek için kullanılmaktadır. Ayrıca bu protokol IPv4 ve IPv6' da kullanılmaktadır. IP doğrulama başlığı ve IP zarflama modları olmak üzere iki farklı türde gerçekleştirilmektedir. IP doğrulama başlığı modu, değiştirilmiş veriyi ve taklit edilen IP adreslerini anlama, tüm paketlerin bütünlüğünün ve kimlik doğrulamasının yapılması işlemlerini yapmaktadır. IP zarflama modu ise, izlemeyi önlemek için şifreleme, paketteki verinin bütünlüğü ve kimlik doğrulama işlemlerini yapmaktadır.

2.3.6. Kerberos

Needham ve Shroeder tarafından 1978 geliştirilmiştir bir protokoldür. Bir anahtar sunucusu tarafından simetrik anahtarların dağıtılması için kullanılır ve anahtar dağıtım merkezinden bir bilet alma işlemi ile süreç başlamaktadır ve anahtar dağıtım merkezi her zaman aktif tutulması gerekmektedir.

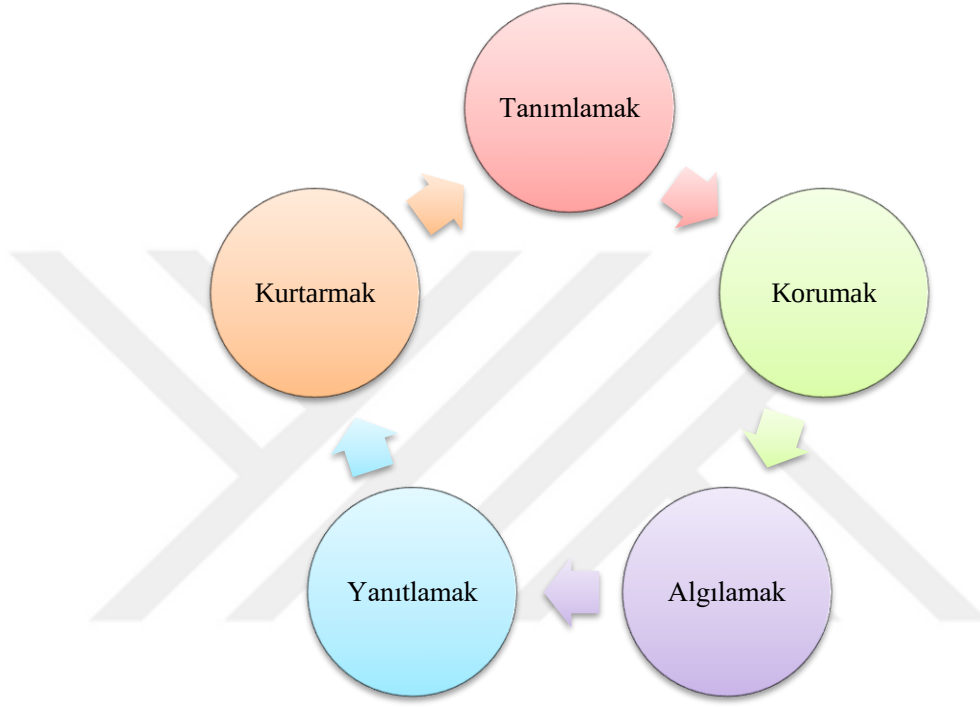
2.4. SİBER GÜVENLİK

Gelişen bilgi teknolojiler ile birlikte son yıllarda siber güvenlik tehditlerinin sürekli bir artış trendinde olduğu gözlemlenmektedir. Bu açıdan kurumlar kendi iç bilgi güvenliği dinamiklerini güçlendirmek ve siber güvenlik konusunda stratejik hedeflerini ilk sırasına koydukları açıkça görülmektedir. Siber güvenlik alanında ülkeler uluslararası standartları takip ederek ve kendilerine uyarlayarak kamu ve özel sektördeki bilgisayar ağlarını korumayı hedeflemektedir.

Siber güvenlik açısından hiçbir yazılım uygulaması kurumlara yüzde yüz güvenlik konusunda garanti verememektedir. Bu sebepten dolayı her kurum kendi güvenlik önlemlerini almalı, bu önlemler teknolojik, yönetsel ve eğitimidir. Belli başlı önemli önlemler belirtmek gerekirse; çalışan bilgi güvenliği farkındalık eğitimlerini her yıl yapmalı, kurum içerisinde yetkin ve kıdemli uzmanlara sahip olmalı, siber güvenlik uzmanı olarak çalışacak personellerin eğitimlerine yatırım yapmalı, kullanıcı ve sistem erişim logları tutulmalı, SOME, SOC, SIC, yazılım güvenlik test laboratuvarı (Pentest Lab.) ile birlikte siber olaylara karşı hemen müdahale edebilmek için bir Siber Füzyon Merkezi (SFM) kurulmalı, kurumsal bir siber güvenlik politikası oluşturulmalı ve bunları uygulamak için kurum üst yönetiminin desteği alınmalıdır.

2.4.1. Siber Güvenlik Yaşam Döngüsü

Siber güvenlik bakış açısından 5 farklı aşamadaki yaşam döngüsünden oluşmaktadır. Bu yaşam döngüsü NIST standartlarında belirlenen ana çerçevenin ana unsurların temelini oluşturmaktadırlar. Her bir ana çerçevedeki unsur alt katagorilere sahiptir.



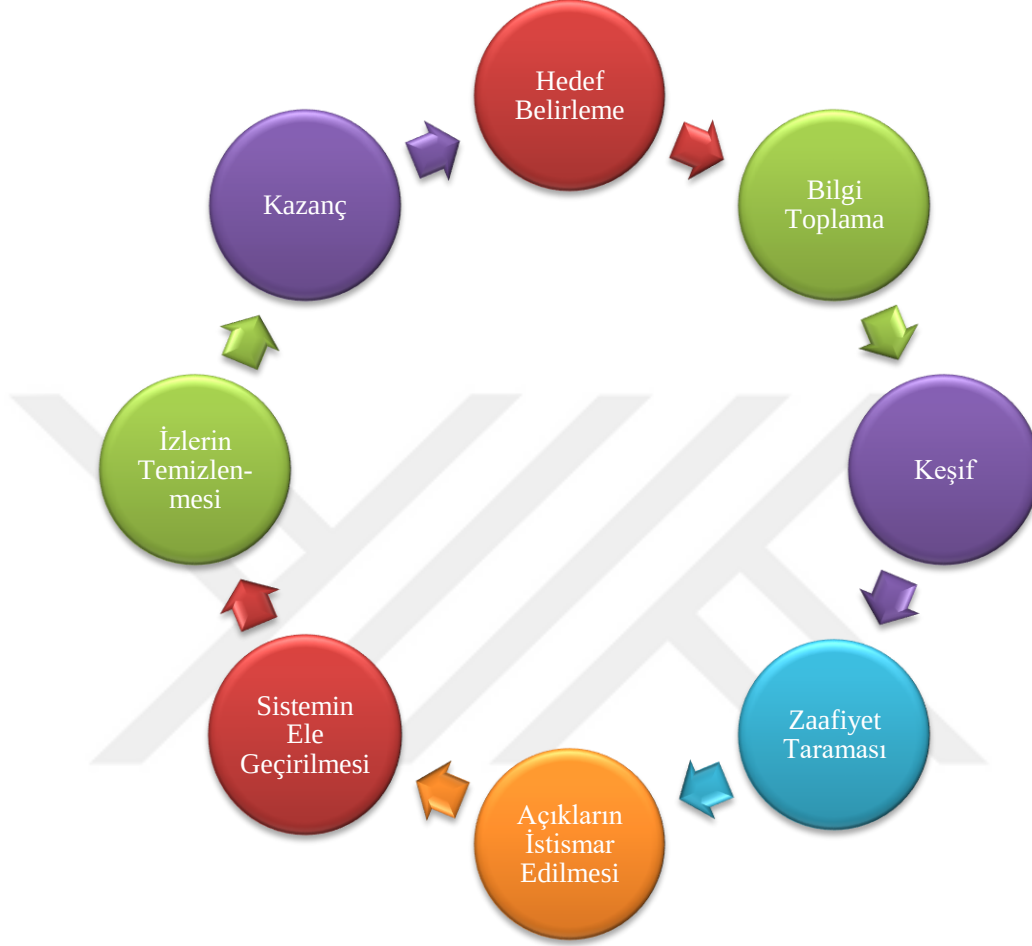
Şekil 2.4: Siber güvenlik yaşam döngüsü (NIST, 2018).

Siber güvenlik temel yaşam döngüsü “Tanımlamak (Identify)”, “Korumak (Protect)”, “Algılamak (Detect)”, “Yanıtlamak (Respond)”, “Kurtarmak (Recover)” olmak üzere tanımlanmaktadır. Bunlara ilave olarak bu temel aksiyonlarını destekleyen ve besleyen “Teknoloji”, “İnsan” ve “Prosedürler” bulunmaktadır.

2.4.2. Siber Saldırı Yaşam Döngüsü

Siber saldırı yaşam döngüsü Şekil 2.5’ de görülen dinamik bir döngüye dönüşmekte bu da saldırıların sürekli olarak kendini yenilemesini ve geliştirmesini sağlamaktadır. Günümüzde siber saldırıları gerçekleştirebilen bir çok araç bulunmaktadır. Genellikle siber saldırılarının yaşam döngüsünü hedefe ait bilgilerin toplanması ve keşif adımıdır. Saldırganlar sistemlere sızmak veya saldırmak için Host Sweep ve Port Tarama yöntemlerini kullanmaktadırlar. NMAP uygulaması ile port tarama çok kolay yapılabilinmektedir. Buna ek olarak sosyal

mühendislik, whois sorgusu, pasif saldırılar, ping okuma, google hacking, shodan gibi arama motorları bilgi toplama ve keşif için saldırganlar tarafından etkin kullanılmaktadır (Erol, 2015).

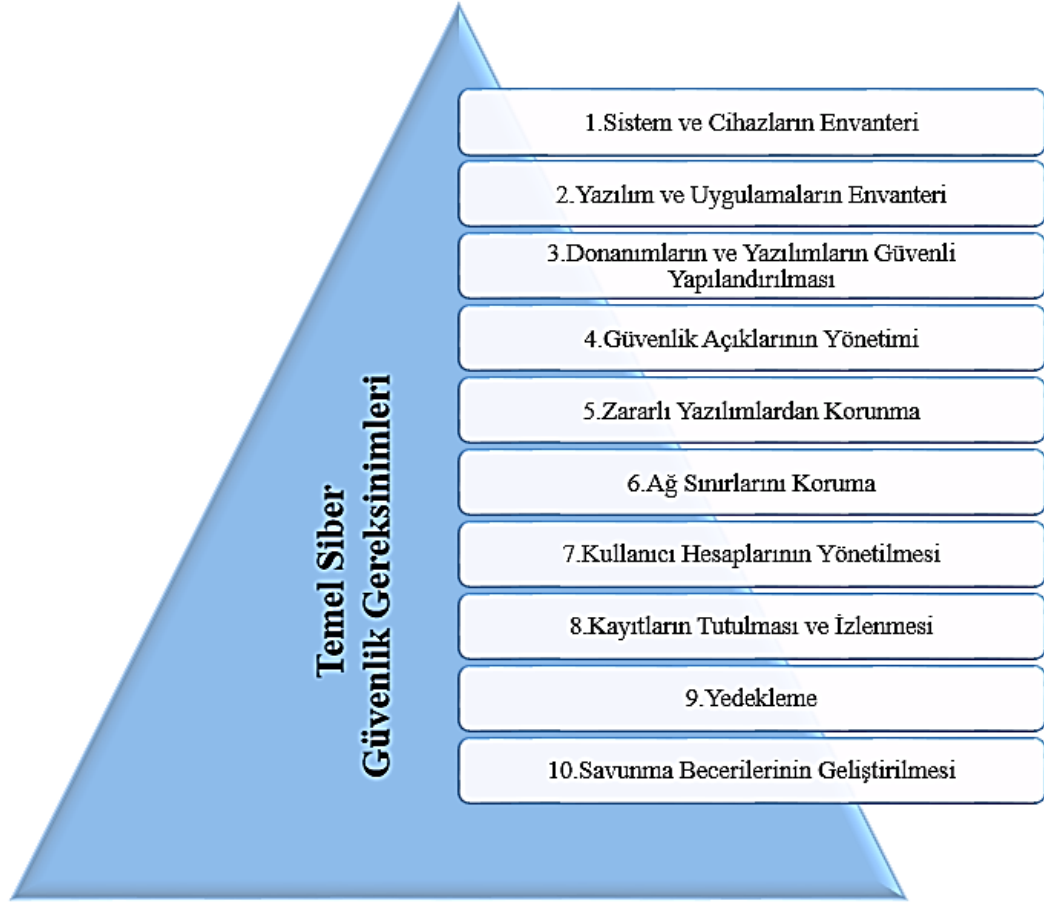


Şekil 2.5: Siber saldırı yaşam döngüsü (Erol, 2015).

Siber saldırı yaşama döngüsü Şekil 2.5’ de belirlenen özelliklerde gerçekleşeceği gibi bu özelliklerinde Uygulama alanlarına göre değişiklikler gösterebileceği belirtilmektedir. Genelde saldırı yapacak gruplar veya kişiler hedefte bulunan kurum, şirket veya şahıslar belirlenir ve bu hedef üzerinde bilgilerin toplanması, keşif yapılması ve zaafiyet taraması ilk adım olarak gerçekleştirilir. Elde edilen sonuçlar üzerinde analizler yapılarak bulunan açıklar üzerinden istirmarin başlaması ve sistemin ele geçirilmesi mümkün olmaktadır. Ele geçirilen system üzerinde saldırganlar iz bırakmak istemezler ve bunların silinmesi için çalışma yaparak sistemden elde edilen kazançlar ile birlikte olayı sonlandırırlar. Bütün siber olaylar incelendiğinde yaşam döngüsünün birebir uygulandığı görülmektedir.

2.4.3. Temel Siber Güvenlik Gereksinimleri

TÜBİTAK BİLGEM tarafından 2017 yılında taslak olarak aşağıdaki Şekil 2.6’ da belirtilen 10 adet siber güvenlik temel gereksinimleri tanımlanmıştır. Ancak bu gereksinimler kurumlara tavsiye ve uygulama amaçlı olarak hazırlanmıştır.



Şekil 2.6: Temel siber güvenlik gereksinimleri (BİLGEM, 2017).

2.5. SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİ ARASINDAKİ FARK

Bilgi güvenliği sistemlerin, sağlanan servislerin ve verinin korunmasını sağlar. Kişisel olarak bilgi güvenliğine bakıldığında ise günlük hayatta kullanılan bilgisayarların veya kullanılan sosyal hesapların güvenliğinin sağlanması olarak tanımlanmaktadır. Siber güvenlik kavramı hayatımıza son yıllarda girmesi ile popüler bir hale gelmiştir ve bilgi güvenliği ile karşılaştırıldığında birbirini kapsayan ve ayrışan yönleri bulunmaktadır. “Bilgi güvenliği, fiziksel ve sayısal olarak tutulan verinin, yetkisiz erişimlerden, kullanımlardan, bozulmalardan

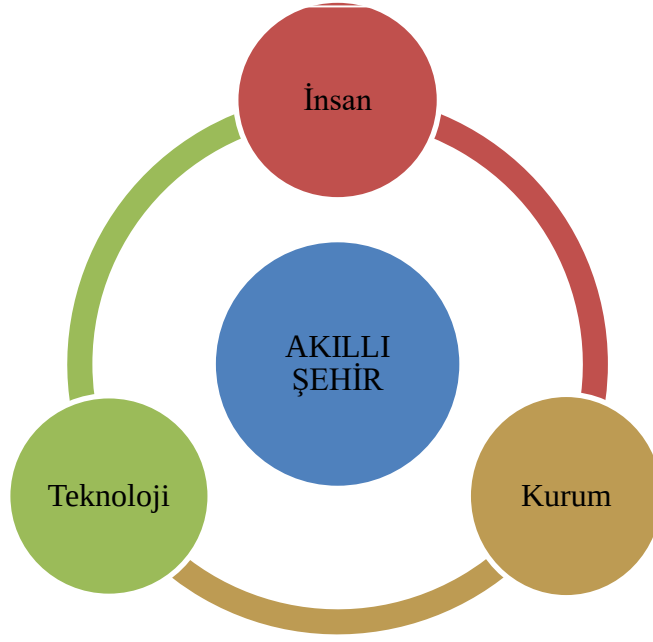
veya değiştirilmelerden korunması” olarak tanımlanmaktadır. Siber güvenlik ise, “bilgisayarların, verinin ve ağların yetkisiz sayısal ataklardan, erişimden veya tahripten, çeşitli yöntem ve teknolojilerin kullanımı ile korunması” olarak tanımlanmaktadır.

Özetlemek gerekirse, her iki terim birbiri yerine kullanılmakta ancak siber güvenlik kavramı bilgi güvenliği kavramının altında bulunmaktadır ve “Siber Güvenlik” ağların, bilgisayarların ve verinin izinsiz elektronik erişiminden korunması ile ilgilenirken, “Bilgi Güvenliği” verinin sayısal veya fiziksel biçimde tutulmasına bakılmaksızın tüm veri varlıklarının korunmasını hedeflemektedir.

2.6. AKILLI ŞEHİR

Akıllı şehirler, şehirlerin içinde bulundukları karmaşıklıklar azaltılarak insan ve doğa odaklı maksimum verimlilik sağlayacak şekilde yeniden yapılandırılması düşüncesine dayanır. Ayrıca akıllı şehirler insan odaklı, stratejik, gelişim, değişim, ortam yaratan ve destekleyen bir yönetim anlayışına sahiptirler. Bu nedenlere bağlı olarak bu şehirler hizmet alanları ve yaşam standartları gelişmiş bir şehir yapılarıdır. Bu yapılar, yenilikçi ve sürdürülebilir yöntemleri kullanarak kaynakların etkin ve akıllıca tüketildiği, doğaya saygılı, çevre sorunlarının minimuma indirildiği, konforlu, sağlıklı, insan odaklı, kendi kendine yetebilen yeni yaşam alanları oluşturabilmeyi temel almaktadır.

Nam ve Pardo, akıllı şehirlerin modellenmesinde 3 temel aktör bulunmaktadır ve bu aktörler sırası ile insan, teknoloji ve kurum olarak belirtilmektedir. Bu akıllı şehirleri oluşturan temel aktörler etkili bir şehir yönetimi için uyum içerisinde çalışıyor olması gerekmektedir. Teknoloji, insan ve kurum aktörlerinin birbirine bağlı olması ve birlikte çalışma stratejisine dayalı olması şehirlere akıllı şehir olma yolunda çok büyük katkı sağlayacaktır (Nam & Pardo, 2011).



Şekil 2.7: Akıllı şehirlerin 3 temel aktörü (Nam & Pardo, 2011).

Gelişen teknolojilere bağlı olarak içinde bulunduğumuz çağın en belirgin özelliği hızlı değişimdir. Çağın gereksinimlerine ve hızlı değişimine ayak uydurabilecek toplumların oluşumu ise sürdürülebilir ve refah seviyesi yüksek yaşam ortamları ile doğrudan ilişkilidir. Toplumların refah seviyesini yükseltme ve sürdürülebilir bir yöntemle büyüme ve kalkınmayı yönetme hususunda son yıllarda birçok ülke, şehir altyapı ve hizmetlerini yapılandırma yoluna gitmiştir. Tüm ülkelerde olduğu gibi Türkiye’de de yaşanan hızlı nüfus artışı, kentleşme oranı, küresel iklim değişikliği, artan karbon ayak izi ve tüketim unsurları şehirlerde, insan doğasına aykırı yaşam alanlarını ve çevresel deformasyonu beraberinde getirmiştir. Bu noktada akıllı şehirler, kentsel problemlerin akılcı bir şekilde çözülmesinde önemli bir potansiyele sahip bir yaklaşım olarak ülkelerin ve uluslararası örgütlerin politikaların belirlenmesinde ön plana çıkmaya başlamıştır. Temel olarak, başta ulaştırma ve enerji olmak üzere, kentsel altyapıların ve şebekelerin insan müdahalesine gerek duyulmadan kendi kendine yönetilebilmesi mantığına dayanan bu yaklaşımla, insanların yaşam standartlarında önemli ölçüde iyileşme sağlanması ve daha yaşanılabilir bir şehirlerin oluşması amaçlanmaktadır. Bu konuda dikkat edilmesi gereken en önemli husus, bu yaklaşımın temel felsefesinin “dönüşüm” mantığına dayanması gerektiğidir. Ancak, bu dönüşümün kentin dokusuna uygun bir şekilde ve kentin sahip olduğu mevcut sistem ve altyapıları aksatmadan adım adım yapılması esastır. Bu açıdan bakıldığında, bu dönüşüm hamlesinin kentlerin kendi içinden başlatılması ve kendi ihtiyaçlarına göre kurgulanması çok önemli bir husustur.

Akıllı şehir kavramı enerji altyapısı, trafik yönetimi, atık yönetimi, sağlık, ulaşım, su ve diğer hizmetleri içerir. Bu nedenle, hizmet sağlayıcı ve vatandaşın akıllı bir şehirde karşılıklı etkileşimi vardır. Akıllı kentte Bilgi ve İletişim Teknolojileri (BİT), kentsel hizmetin kalitesini, performansını ve uyumunu arttırmak için kullanılmaktadır. Ek olarak, akıllı şehirler maliyetleri ve kaynak tüketimini azaltmayı ve vatandaşlar ve devlet arasındaki iletişimi geliştirmeyi amaçlıyor. Akıllı şehir çalışmaları 2000' li yıllarda başlamış olup akıllı şehir için birçok tanım vardır. Örneğin, akıllı bir şehir, sağlam altyapının ve veri iletişiminin ve kurumsal altyapının kalitesinin bir birleşimi olarak tanımlanabilir. İnsan ve sosyal sermaye ve klasik (ulaştırma) ve çağdaş (BİT) iletişim altyapısındaki işletmeler, sürdürülebilir ekonomik destek ve yüksek bir yaşam değeri sağlamalıdır. Dahası, doğal kaynaklar, yönetim yoluyla akıllı bir yönetim ile yönetilmelidir (Caragliu vd., 2009).

Öte yandan, akıllı şehir çözümleri, Şehir Bilgi Sistemi (CIS) ve Coğrafi Bilgi Sistemi (CBS) gibi diğer altyapı sistemlerinin bilişim teknolojilerinden (IT) gelen entegre ve gerçek zamanlı bilgiler yoluyla kesin karar vermeyi mümkün kılmaktadır (Kalkınma Bakanlığı, 2013). Uluslararası Standardizasyon Örgütü (ISO) şu hususları rapor etmiştir: Dünyada kullanımda olan Akıllı Şehirler için birçok tanım vardır. Örneğin; Akıllı Şehirler, şehirlerin planlaması, inşası, yönetimi ve akıllı hizmetlerini mümkün kılmak için, BT' nin yükselen üretimini, nesnelerin interneti, bulut teknolojisi, büyük bilgi ve coğrafi bilgi entegrasyonunu uygulayan yeni bir kavramdır.

Akıllı şehirlerin geliştirilmesinin ve yaygınlaştırılmasının temel amacı;

- Kentsel araçların uygunluğu,
- Şehir yönetiminin zarafeti,
- Yaşam alanının yaşanabilirliği,
- Altyapıların akıllılığı,
- Uzun süreli şebeke güvenliği etkinliği (ISO-IEC, 2015).



Şekil 2.8: Akıllı şehirlere genel bakış (Channelpostmea, 2017).

Uluslararası Telekomünikasyon Birliği (ITU) Akıllı Dayanıklı Şehirler için Merkez Grubu, yaklaşık 100 ifadeyi incelemiş olup bunları aşağıdaki yenilikleri geliştirmek için kullanmıştır. Akıllı, sürdürülebilir bir metropol şehirler, kentsel çalışmaların, kamu hizmetlerinin ve rekabetçiliğinin canlı, etkili olma niteliğini geliştirmek için Bilgi İletişim Teknolojilerini ve diğer düzenlemeleri kullanan modern şehirlerdir. Ek olarak, mevcut ve gelecek nesillerin ekonomik, kamusal ve çevresel açılara karşılık gelen ihtiyaçlarını karşılamaktadır (Sang vd., 2015).

Akıllı şehirle ilgili olan İngiliz Standardı, Halka Açık Mevcut Şartname (PAS 181), yerli halk için akıllı bir şehrin sürdürülebilir, rahat ve kapsamlı bir yarın sunmak için kurulmuş bir ortamda dijital, somut ve insani sistemlerin işlevsel bir entegrasyonu olduğunu göstermektedir (British-Standard-Institution, 2014).

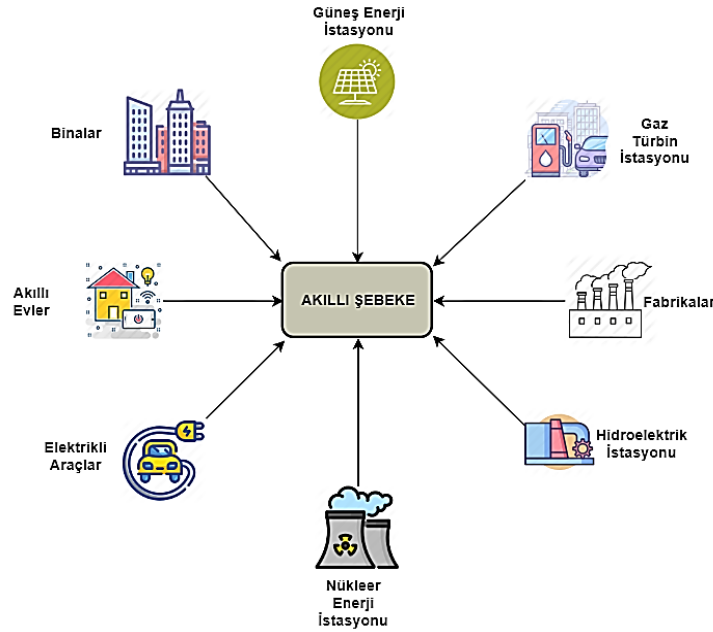
Akıllı şehir; bütünsel bir bakış açısıyla şehrin daha yaşanabilir, daha sürdürülebilir, daha verimli olması amacıyla bilgi iletişim teknolojilerinin sağladığı çözümler ile aşağıdaki noktalara odaklanmaktadır:

- Odağına insanı alarak,
- İlgili tüm paydaşların ve kurumların sahipliğinde,
- Kişisel verinin gizliliği ve diğer etik kuralları ihlal etmeden,
- Katılımcı ve şeffaf bir şekilde uygulayabilen,
- Kendini sürekli geliştiren ve öğrenen.

2.7. AKILLI ŞEBEKE

Altyapı hizmetleri, şehir hayatı için vazgeçilmez bir unsur olarak çok önemli bir konuma sahiptir. Şehir nüfusunun artması nedeniyle, bu altyapı hizmetlerinin kontrolü hayati önem kazanmıştır. Artan nüfus, Bilgi Teknolojileri (BT) uygulamaları olmadan altyapı kullanımını ve kontrolünü imkânsız kılmıştır.

ISO, fiziksel varlıkların optimal yönetimiyle ilgili olarak altyapı yönetiminin bütünsel, sistemli, risk temelli, optimum ve sürdürülebilir olması gerektiğini göstermektedir. Sistematik ve birbirine bağlı hareketler ile varlıkları ve varlık sistemlerini en uygun ve sürekli kontrol eden, kuruluşunu başarmak amacıyla maruz kalma süreleri boyunca yürütme, risk ve harcamaları gerçekleştiren bir temelde egzersiz yapmak için hayati planlar gereklidir (Minnaar vd., 2013). Bu sistematik kontrollerin zorunluluğu akıllı şebekelerin ortaya çıkmasına neden olmaktadır.



Şekil 2.9: Akıllı şebekelere genel bakış (Feroze and Javaid, 2017).

Akıllı şebeke iletişimi ağı IEC 61850 standardına dayanmaktadır. Alt istasyon için IEC 61850 protokol standardı, tüm koruma, hesaplama, test ve izleme işlemlerinin tek bir standart protokolle birleştirilmesine izin verir (Baigent vd., 2004). Aksi taktirde, farklı üreticilere ait cihazlar, birbirleriyle karşılıklı uyum sağlamayan veya birbirine paralel olmayan çok sayıda protokol ve arabirimleri çok fazla kullanamayacaktır. Teknik alanda ekipman standardizasyonu ve birlikte çalışabilirliği uzun bir süredir uygulanmaktadır (Dönmez, 2013).

Aşırı yük, daralma ve elektrik kesintileri yerine akıllı şebekeler, enerji kaynaklarının istikrarını, sürdürülebilirliğini ve verimliliğini garanti etmektedir. Şebekenin içindeki iletişim ve bilgi sistemleri sürekli olarak büyüyecek ve homojenleştirilecektir (Siemens, 2014). Ayrıca, Bilgi ve İletişim Teknolojileri (BİT) enerji üretimi, iletimi, dağıtımı ve tüketimi arasındaki hayati bağları oluşturmaktadır.

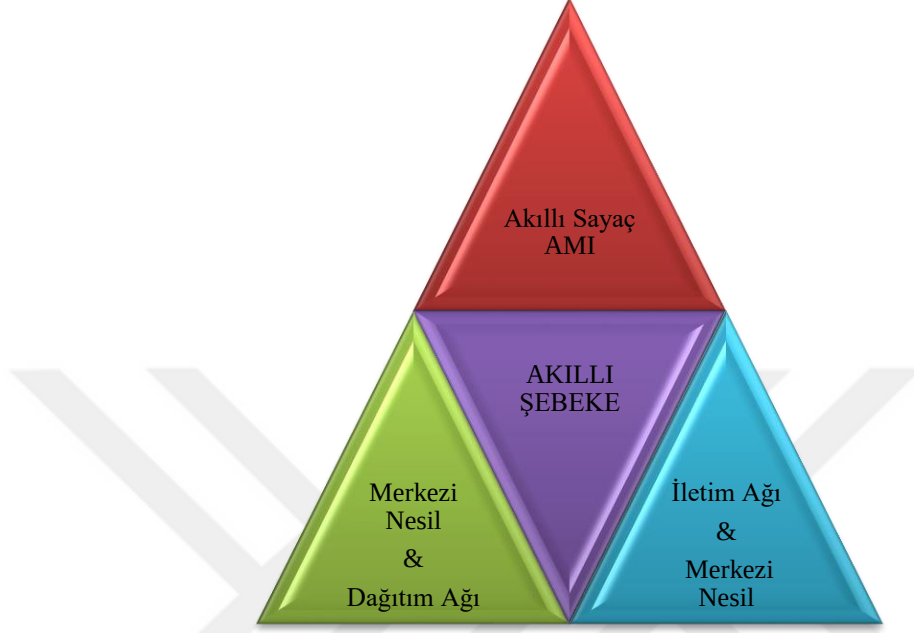
Alt istasyonların mekanizasyonu ve güvenliği, daha fazla akıllı şebekelerin genişletilmiş ihtiyaçlarını güvenli bir şekilde karşılayacak şekilde yükseltilmelidir. Alt istasyon, dağıtıcıdan müşteriye tüm veriler için kamu yararı bilgi teknolojisi şebekesi üzerinde bir ortaklığın geliştirilmesi sürecindedir. Örneğin sistemi geliştirmek için; Besleyici mekanizasyon birimleri, güç özellikleri, sayaçlar, eksantrik enerji kaynakları ve ev otomasyon sistemleri üzerinden gelen bilgiler toplanmalı ve incelenmelidir. Ek olarak, modern akıllı şebeke problemleri, güvenlik, komuta ve mekanizasyonun bilinen görevleri, her zamanki gibi güvenli ve verimli kalmalıdır.

Akıllı şebekeler konsepti, bilgi teknolojisi ve iletişim sistemlerinin kullanılması yoluyla verimli ve güvenilir enerji tedariki, depolama, tüketim için dağıtım ve iletim sisteminin esnek kontrolünü hedeflemektedir. Ayrıca, bu sektörde bilgi teknolojisi ve elektrik dağıtımına benzer süreçler için geliştirilen işletme şirketindeki doğal gaz dağıtım ve su atıksu şebekeleri ve sistemleri süreçleri mevcuttur (Dönmez, 2013).

Akıllı şebekeleri gerçekleştirmenin tam olarak değerini ortaya koyan ana unsur, mühendislik bilimi ile bağlı bütünleştirilmiş, ölçeklenebilir ve birlikte çalışabilir cevapları yerine getirme performans ve kapasitesine sahip olmasıdır. Bu yeni, daha akıllı dünyada, müşteriler, enerji kullanımını mobil cihazlar, internet veya özel ev monitörleri aracılığıyla görebilecekler ve bu hizmet, bir akıllı sayaç veri yönetim sistemi aracılığıyla da benzer sistemi yapacaktır. Bu sayaç sistemi aynı zamanda güç dalgalanmalarını ve kesintileri tespit etmeye ve servisi uzaktan bağlamak veya bağlantıyı kesmek için kullanılabilir bir akıllı sensör olarak da hizmet verecektir (Borlase, 2016).

Akıllı şebekenin dayanağı ve gücü, gelişmiş ölçüm altyapısı (AMI) veya “akıllı sayaçlar” aracılığıyla kamu hizmetleri ve tüketiciler arasında iki yönlü iletişimin bütünleşmesidir. Böylece AMI, gerçek zamanlı veya gerçek zamanlı olarak fiyatlandırma, talep, güç ve kalite gibi enerji parametrelerini bilmek için tasarlanmıştır. Böyle bir durumda, halihazırda konuşlandırılmış olan teknoloji için yatırımın geri dönüşü için doğru bir yönlendirme yapmak,

yardımcı program için şaşırtıcı olacaktır. Enerji verimliliği alanında gerçekleşen tüm teknolojik gelişmeler gibi, akıllı şebekenin aşağıdaki hususlara dikkat etmesi gereken önemli bir faydası vardır ve bunlar Şekil 2.10’ da vurgulanmıştır (Goel, 2017).



Şekil 2.10: Akıllı şebeke temel yapı taşları (Goel, 2017).

Akıllı bir şebekeyi dağıtmanın kritik bir zorluğu, tüm uygulamalarda tutarlı bir siber güvenlik görüşüne sahip olmasıdır. Harici arayüzler izinsiz girişlere karşı çoklu savunma katmanları sağlayan gelişmiş sınır savunmalarıyla korunmalıdır.

Ayrıca, operasyonel uygulamaların ve şebeke mimarilerinin incelenmesi, Cisco EnergyWise adı verilen bir enerji yönetim aracı olarak enerji verimliliğinin artırılması ve önemli maliyet azaltımı sağlamaktadır (Cisco, 2013).

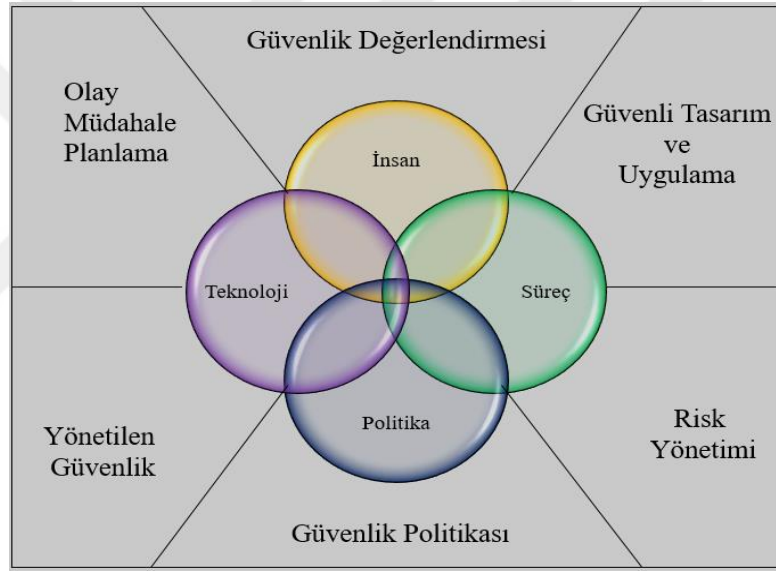
Akıllı bir şebeke sistemi temel olarak aşağıdaki özelliklere sahip olmalıdır;

- Dijitalleşme,
- Zeka,
- Dayanıklılık,
- Kişiselleştirme,
- Esneklik.

Dijitalleşme, sistemi hızlı ve güvenilir kılan dijital bir platforma sahip olmak demektir. Zeka, akıllı bir teknolojiyi kullanmak anlamına gelmektedir. Dayanıklılık, sistemin herhangi bir saldırıdan etkilenmemesi gerektiği anlamına gelmektedir. Kişiselleştirme, sistemin müşteriye özel olması gerektiği anlamına gelmektedir. Son olarak esneklik, akıllı şebekenin uyumlu, genişletilebilir ve uyarlanabilir olması gerektiği anlamına gelmektedir (Iyer, 2011).

2.7.1. Akıllı Şebeke Güvenlik Ekosistemi

Akıllı şebeke iletişimde aşağıdaki Şekil 2.11' de tipik bir güvenlik hizmetleri ekosistem kümesini göstermektedir. Bu kümede siber güvenlik açısından her kurumun çalışanları, süreci, politikası ve teknoloji temelleri arasında işleyen bir sistematik süreç olduğunu göstermektedir.



Şekil 2.11: Akıllı şebeke güvenlik ekosistemi (Yan vd., 2012).

2.7.2. Akıllı Şebeke İletişim Teknolojileri

Akıllı şebekelerde kullanılan iletişim teknolojileri aşağıdaki tabloda özet olarak verilmiştir. Kullanılan teknolojiler kapsamında kablolu, kablosuz ve uydu haberleşme ve iletişim teknolojileri bulunmaktadır. Her bir teknolojinin maksimum veri taşıma band genişliği ve verinin taşınabileceği maksimum uzaklıklar detaylı olarak verilmiştir.

Tablo 2.1: Akıllı şebeke iletişim teknolojilerinin karşılaştırma tablosu (Goel and Jindal, 2017).

Teknoloji	Standart/Protokol	Maks. Teorik Veri Hızı	Kapsam Alanı
Kablolu İletişim Teknolojileri			
Fiber Optik	PON	155 Mbps-2.5 Gbps	60 Km Kadar
	WDM	40 Gbps	100 Km Kadar
	SONET/SDH	10 Gbps	100 Km Kadar
DSL	ADSL	1-8 Mbps	5 Km Kadar
	HDSL	2 Mbps	3.6 Km Kadar
	VDSL	15-100 Mbps	1.5 Km Kadar
Koaksiyel Kablo		172 Mbps	28 Km Kadar
PLC	Home Plug	14-200 Mbps	200 m Kadar
	Dar Bant	10-500 kbps	3 Km Kadar
Ethernet	802.3x	10 Mbps-10 Gbps	100 Km Kadar
Kablosuz İletişim Teknolojileri			
Z-Wave	Z-Wave	40 kbps	30 m Kadar
Bluetooth	802.15.1	721 kbps	100 m Kadar
ZigBee	ZigBee	250 kbps	100 m Kadar
	ZigBee Pro	250 kbps	1600 m Kadar
Wi-Fi	802.11x	2-600 Mbps	100 m Kadar
WiMAX	802.16	75 Mbps	50 Km Kadar
Wireless	RFMesh802.11,15,16		
Hücresel Mobil	2 G	14.4 kbps	50 Km Kadar
	2.5 G	144 kbps	
	3 G	2 Mbps	
	3.5 G	14 Mbps	
	4 G	100 Mbps	
Uydu	Uydu İnternet	1 Mbps	100-6000 Km

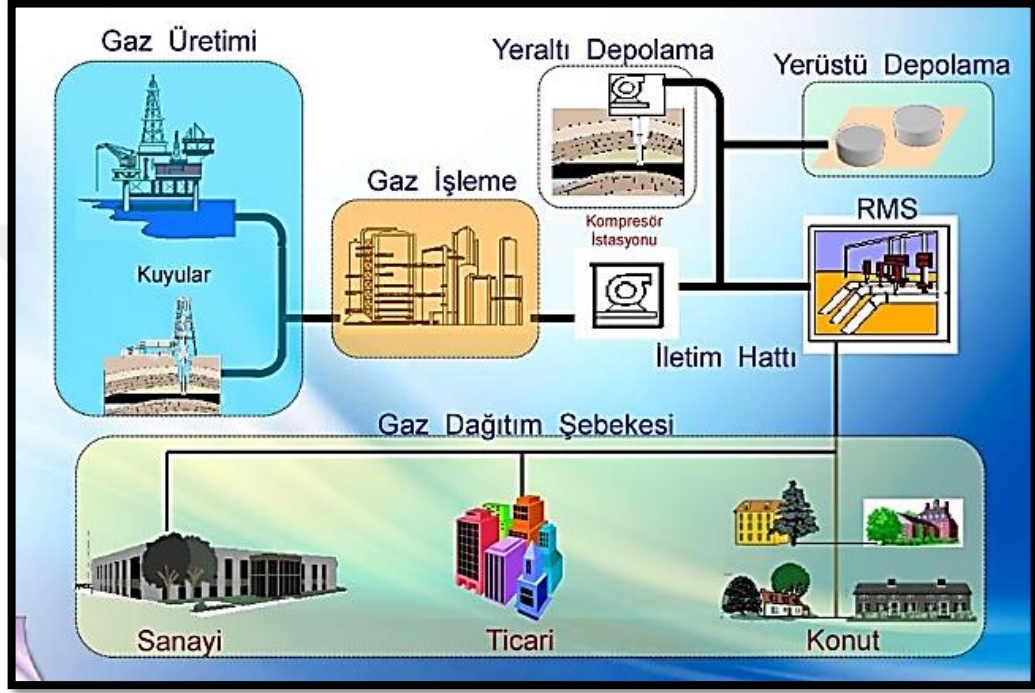
2.8. AKILLI DOĞAL GAZ ŞEBEKESİ

Akıllı doğal gaz dağıtım şebekesi, farklı çaplardaki borulardan oluşan bir sistem olarak tanımlanmakta ve yüksek basınçlı iletim hattı ile şehirlere taşınan gaz basıncını düşürerek, doğal gazın tüketiciye dağıtımını sağlamaktadır.

Dağıtım şebekeleri, düşük basınçlı gazı şehir giriş istasyonlarından endüstriyel, ticari ve konut binalarına farklı basınç sınıflarına sahip olan ve çelik ve polietilen (PE) borulardan oluşan hatlar üzerinden iletilmesini sağlayan sistemdir.

Dağıtım ağları aşağıdaki bölümlerden oluşmaktadır;

- Düzenleme ve Ölçme İstasyonları (RMS-A) istasyonları,
- Ana taşıyıcı (çelik) hatları,
- Bölgesel istasyon dağıtım hatları, servis hatları ve servis kutuları.



Şekil 2.12: Genel doğal gaz iletim ve dağıtım sistemi (GAZBİR, 2017).

Doğal gaz iletim ve dağıtım şebekesi modellerinin tasarımı ve hesaplanması, mevcut ağların revizyonu, ağların simülasyonu ve izlenmesi, Coğrafi Bilgi Sisteminin (CBS) ve Denetleyici Kontrol ve Verilerin entegrasyonu (SCADA) için çeşitli şebeke simülasyonu ve hesaplama programları kullanılmaktadır. Şebekenin mevcut ve gelecekteki durumunu ölçmek ve ağları türlerine ve yüklerine göre analiz etmek için kullanılan bu otomasyon programlarının birçok avantajı vardır.

Doğal gaz, ekonomiye ve gündelik yaşama çevresel, sağlık ve diğer sosyal faydalar gibi hizmetler ile hayati önem taşımaktadır. İyi tasarlanmış akıllı şebekeler, minimum kayıplar, daha düşük maliyetler ve daha yüksek verimlilik gibi önemli ek avantajlar sağlayabilir.

Klasik sıkıştırma ünitelerine, çelik borulara ve regülasyon istasyonuna ek olarak, bu kontrolün sağlanması için bir dizi BT sistemi gerekli hale gelmiştir. Bu gelişmekte olan akıllı şebeke,

altyapı sistemi ve bilgi teknolojilerinin bir araya gelmesi olarak tanımlanmıştır. Akıllı şebeke, hem servisler hem de son kullanıcılar için geniş kapsamlı avantajlar sunan, çaba genişliğindeki kararları garantilemektedir. Akıllı şebeke teknolojilerini kabul eden hizmetler, azalan sermaye ve çalışma maliyeti, gelişmiş güç kalitesi, gelişmiş müşteri memnuniyeti ve olumlu çevresel etkiler açısından önemli avantajlar sağlamaktadır. Akıllı şebekeler sadece etkinleştirilmiş çözümleri değil, aynı zamanda iş ve çalışma endişelerini ifade eden ve hizmet, kullanıcı, tasarruf ve çevre için anlamlı, sayılabilir ve sürdürülebilir avantajlar sunan birleştirilmiş çözümleri de geliştirir (Borlase, 2016).

Büyük şehirlerde doğal gazın, sanayi ve konut kullanımında müşteriye belli sıcaklık ve basınçta ulaştırılması gerekmektedir. Mevsimsel olarak değişen tüketim değerleri, hava sıcaklıkları, arıza, iş süreçleri, saha ekipmanları vb. parametreleri bütünsel olarak değerlendirip kesintisiz ve verimli bir şekilde gaz arzının sağlanması arayışı akıllı şebeke sistemlerini zorunlu kılmıştır. Şehirde doğal gaz gibi yaşamsal öneme sahip bir enerji kaynağının alt yapısının varlık yönetimi en kusursuz biçimde yapılmalıdır.

Şebeke güvenilirliğini ve işletim verimliliğini artırmak, dağıtım şebekesinde gaz akışını gerçek zamanlı olarak izlemek ve optimum basıncı artırmak için daha akıllıca kullanmak mümkündür. Akıllı şebekenin gereksinimleri oldukça farklı olduğu için mevcut şebekenin yeniden yapılandırılması gereklilik olarak değerlendirilmektedir (Borlase, 2016).

Akıllı şebekeler, ilk olarak elektrik dağıtım sistemlerine uygulanmaya başlandı ve daha sonra buradaki olumlu geri dönüşler sayesinde benzer aksiyonlar doğal gaz şebekelerinde de uygulanmaya başlanılmıştır. Akıllı doğalgaz şebekeler ile doğal gazın basıncı, ısı değeri, deprem olma riskleri, altyapı varlık bilgileri, ticari ve bireysel abonelerin tüketim miktarı gibi birçok parametre anlık olarak takip edilebilir. Bu sayede, piyasanın ve şirketlerin karşılaşılabileceği bazı zorluklar giderilebilecektir.



Şekil 2.13: Akıllı doğal gaz şebekelerinin faydaları (GAZBİR, 2017).

Günümüzde kullanılan klasik şebeke sistemlerinde; enerji kesintileri, sayaç arızaları, düşük verimlilik, doğal gaz kaçakları, doğal afetlerde oluşan hasarlar, dış müdahale sonucu oluşan hasarlar ve enerji kaçakları gibi sorunlar, aboneler tarafından belirli merkezlere iletilerek veya dağıtım şirketlerinin çalışmalarıyla tespit edilebilmektedir. Akıllı şebekelerde ise bu problemler otomatik alarm sistemleri, 7/24 izleme sistemleri ve acil durum ekip ihbarları ile anında saptanarak, hizmette herhangi bir kesintiye gitmeden hızlı ve öncelikli olarak yerinde veya otomatik olarak uzaktan çözümlenmektedir. Akıllı şebekeler, gerçek zamanlı haberleşme altyapısı sayesinde aşırı yüklenmeleri tespit etmekte, enerji akış yönlerini düzenlemekte ve enerji kayıp-kaçaklarını önlemeye katkı sağlamaktadır. Aynı zamanda, enerji arz-talep dengesini ve enerji dağıtımını yöneterek, daha adil tüketim bedeli ve daha dengeli kaynak kullanımını sağlar.

2.9. AKILLI ŞEBEKELERDE EN SIK KARŞILAŞILAN SİBER SALDIRI YÖNTEMLERİ

Akıllı şebekelerin kapsamı alanına giren elektrik, su, doğalgaz gibi alanlarda ilk yapılması gereken tehditleri tanımlayabilmektir. Bu kapsamda her biri farklı motivasyonlarla, amaçlarla farklı büyüklüklerde saldırılar olan siber terörizm, siber suçlar, siber savaş, siber istihbarat gibi pek çok kavram/yöntem bulunmaktadır. Bu çalışmada bu yöntemlerin tümü için siber saldırılar ifadesi kullanılacaktır. Bu yapılara zarar vermeye yönelik amaçlanan siber güvenlik ihlallerinin tümü işlevsel olarak siber saldırı sayılabilir. Özellikle çalışmamız, akıllı doğalgaz şebekelerinde kullanan tüm sistemlerin maruz kalabileceği siber saldırıların araştırılması ve bu saldırılara karşı alınabilecek çözümler için bir olgunluk modelinin analizinin oluşturulmasına yönelik çalışmalara motivasyon olmasına çalışılmıştır.

Siber güvenlik; kişisel bilgisayarlara bulaşan virüslerden, güncellenmesi gereken antivirüs programlarından, e-postalara gelen reklamların engellenmesinden ya da kişisel bilgilerin ele geçirilmesinden çok daha kapsamlı ve hayati bileşenleri içermektedir. Bunlar ve benzeri durumlar elbette önemlidir ancak siber güvenlik denildiğinde ilk anda düşünülmesi gereken konulardan biride akıllı şehirler ve şebekeler olmalıdır. Çünkü ulusal güvenlik açısından değerlendirildiğinde; akıllı şebekelerde oluşabilecek hizmet kaybı veya hizmetlerinin aksaması halinde büyük ölçekli ekonomik zarara, can kaybına veya ulusal güvenlik zafiyetlerine neden olabilecektir. Bu nedenle bu kritik öneme sahip sistemler, siber güvenlik kapsamında korunması gereken en önemli varlıklardır. Bu çalışmada bu hususa dikkat çekilmeye çalışılmıştır.

Belli başlı siber saldırı yöntemleri aşağıda listelenmiştir (Yıldız, 2014);

- Dağıtık Hizmet Dışı Bırakma (Distributed Denial of Service-DDoS-DoS)

Ağ hedefli;

- SYN Flood
- ACK Flood
- UDP Flood

Uygulama hedefli;

- HTTP GET/POST Flood
- DNS Flood

- FIN&RST Flood
- SMTP Flood
- ICMP Flood
- SSL DoS
- Köle Bilgisayarlar (Botnet, Zombie)
- Sıfır Gün Açıkları (Zero-Day Exploits)
- Gelişmiş Siber Tehditler (Advanced Persistent Threats – APT)
- Saldırı Kitleri (Attack Kits)
- İstem Dışı Yığın İleti (E-posta) Gönderme
 - Spam
 - Bulk
 - Junk Mail
- Network Trafiğinin Dinlenmesi (Sniffing - Monitoring)
 - Aktif Sniffing
 - Pasif Sniffing
 - ARP Zehirlenmesi (Address Resolution Protocol Poisoning)
- Zararlı Yazılım Kullanımı (Malware)
 - Virüs
 - Solucan (Worm)
 - Truva Atı (Trojan Horse)
 - Fidyeye (Ransomware)
 - Reklam yazılımı (Adware)
 - Arka kapı (Backdoor-Trojan)
 - Casus yazılımlar (Spyware)
 - Klavye İşlemlerini Kaydeden Programlar (Keyloggers)
 - Görüntü Yakalama Sistemleri (Screen Logger)
 - Tarayıcı Soyma (Browser Hijacking)
 - Korunmasızlık Sömürücüleri (Exploits)
 - Kök Kullanıcı Takımları (Rootkit)
- Kriptografik Saldırıları (Cryptographic Attacks)
- IP Aldatmacası - Gizlenmesi (IP Spoofing)
- Dijital Manipülasyon (Digital Manipulation)

- Kabloya Saplama Yapma (Wire Tapping)
- İnternet Servis Sağalayıcı Saldırıları (IPS Attacks)
- SQL Enjeksiyonu (SQL Injection)
- Mantık Bombası (Logic Bomb)
- Yemleme - Oltalama Saldırıları (Phishing)
- Yerine geçme (Masquerading)
- Sosyal Mühendislik (Social Engineering)
- Çöpe dalma (Scavenging)
- Cross Site Scripting (XSS)
- XXE Dış Varlık Güvenlik Zafiyeti (XML External Entity)



Şekil 2.14: Siber saldırı yöntemleri.

2.9.1. Dağıtık Hizmet Dışı Bırakma (Distributed Denial of Service-DDoS-DoS)

DDoS saldırıları, virüsler tarafından etki altına alınmış çok sayıda bilgisayar sistemlerinin veya ağlarının tek bir bilgisayara saldırmasıdır. Böylece binlerce bilgisayar aynı anda tek bir

bilgisayara saldırarak onu etkisiz hale getirebilmektedir. Bu saldırılar en basit saldırı tipi olduğundan çok sık olarak kullanılan saldırılardandır. Saldırıların asıl amacı çalışan sistemi durdurarak prestij ve maddi kayıplar verdirmektir. Hacktivist grupların genellikle tercih ettikleri bir yöntemdir ve daha çok bankacılık faaliyetlerine yönelik olarak kullanılan saldırılardır. Bu saldırı sayesinde internet üzerinde çalışan servislerin ve servis ağlarının trafik sıkışıklıklarına sebebiyet verilmektedir. Bu saldırılar Botnet olarak bilinen yüz binlerce bilgisayar üzerinden yapılmaktadır. Botnet bir robot ağıdır ve uzaktan çalıştırılabilen zombiler olarak bilinmektedir. Bu saldırıların farkedilmesi zordur ancak sistemlerde veya web servislerinde bir yavaşlık olduğunda farkına varılabilir (Kara, 2013). DDoS saldırıları ağ ve uygulama hedefli saldırılar olmak üzere iki ana katagoriden oluşmaktadır. Ağ hedefli saldırılar SYN Flood, ACK Flood ve UDP Flood olarak saldırı türleri vardır. Uygulama hedefli ise, HTTP GET/POST Flood, DNS Flood, FIN&RST Flood, SMTP Flood, ICMP Flood ve SSL DoS olmak üzere saldırı türleri bulunmaktadır.

2.9.2. Köle Bilgisayarlar (Botnet, Zombie)

Köle bilgisayarlar zombie ya da botnetler olarak adlandırılır ve bu tehdit grubunun en tehlikeli olanları olarak kabul edilmektedir. Bu saldırı tipinde en önemli nokta ise, bilgisayar kullanıcısının hiçbir şeyden haberi olmadan cihazının birçok olayda çok ciddi suçlar işlenmesi ile karşı karşıya kalabileceğidir. Bu tür bilgisayarlara robot veya bot da denmektedir (Kaya, 2012).

2.9.3. Sıfıncı Gün Açıkları (Zero-Day Exploits)

Henüz siber güvenlik dünyası tarafından bilinmeyen, uzmanların keşfedemediği, uygulamanın veya ürünün sahibi tarafından henüz yayımlanmamış açıklıklara sıfıncı gün (zero day) açığı adı verilmektedir.

2.9.4. Gelişmiş Siber Tehditler (Advanced Persistent Threats – APT)

Bu tehditler hedefi tam olarak belirlenmiş, uzun zamana dayalı ve ileri düzeyde tehditler içermektedir. Daha çok siber savaşlarda kullanılmak üzere geliştirilmiş yazılımlardır. Bunlar özellikle ülkelerin kritik altyapı tesislerini hedef almaktadır. APT'lerin gerçekleştirilmesinde bir çok yöntem kullanılır bunlar özellikle web siteleri, oltalama, sıfıncı gün saldırıları, Microsoft

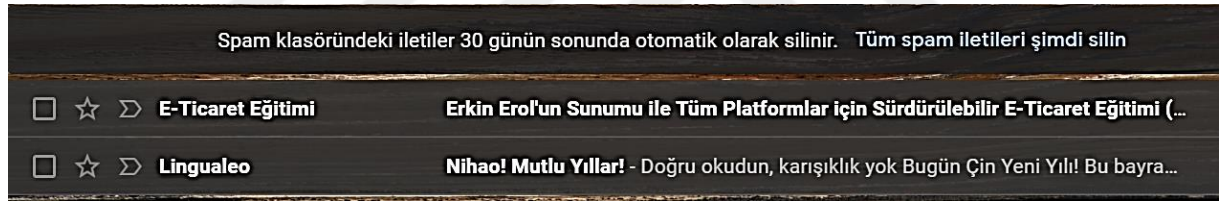
ve Adobe PDF gibi ofis programları ve USB, CD, DVD gibi donanım araçları ile yapılabilinmektedir (Kara, 2013).

2.9.5. Saldırı Kitleri (Attack Kits)

Saldırı kiti, kötü amaçlı yazılım oluşturmak, özelleştirmek ve dağıtmak için yazılım kodu yazma konusunda hiçbir deneyimi olmayan birisine izin veren bir programlama aracıdır. Exploit kitleri, enfeksiyon kiti, crimeware kiti, DIY saldırı kiti ve kötü amaçlı yazılım araç seti dahil olmak üzere diğer birçok isim tarafından bilinmektedir (Whatis, 2019).

2.9.6. İstem Dışı Yığın E-Posta Gönderme (Spam, Bulk, Junk)

Yığın iletiler istenmeyen e-postalara verilen isim olarak tanımlanmaktadır. Genelde yasa dışı (ilaç, fidye, reklam, pornografi site vb.) ürünlerin reklamı yapmak için kullanılmaktadır. İstem dışı gönderilen iletiler Spam, Bulk ve Junk e-mail olarak kullanıcılara toplu olarak gönderilen ve istenmeyen e-maillerdir.



Şekil 2.15: İstem dışı örnek bir mail.

Önemsiz e-posta sürekli bir tehdit olsa da, toplu e-posta genellikle art arda gönderilmesi muhtemel olmayan bir reklam veya pazarlama mesajından oluşur. Toplu e-posta bazı kullanıcılar tarafından aranır ve aslında bu mesajları almak için kasıtlı olarak kaydolmuş olabilirler, diğer kullanıcılar ise bu tür mesajları spam olarak kabul edebilir. Bu mailleri otomatik algılama filtresi sayesinde algılayan e-posta sağlayıcınız da bu maillerin sizi rahatsız etmemesi için otomatik olarak Spam/Gereksiz kutusu içerisine taşır.

2.9.7. Ağ Trafiğinin Dinlenmesi (Sniffing - Monitoring)

Bu yöntem ile ağ üzerindeki paketler yakalanabilir ve okunabilir. Bu yöntemin amacı şifreleri (e-mail, web, ftp, telnet, SQL), e-mail paketlerini transfer eden dosyaları (e-mail, ftp) yakalamaktır. Sniffing atakları aktif ve pasif olmak üzere iki tiptir (Yıldız, 2014).

2.9.7.1. *Aktif Sniffing*

Aktif sniffing, switch tabanlı ağı dinleme tekniğidir. Switch sahip olduğu CAM (Content Addressable Memory/İçerik Adreslenebilir Bellek) belleğini ağı ARP enjekte eder ve CAM kullanıcının bağlı olduğu portun izini tutar. Aktif sniffing teknikleri, MAC Flooding (Basma), DNS Poisoning (Zehirlenme), ARP Poisoning, DHCP Saldırıları, Switch Portu Çalma (Stealing), Kandırma (Spoofing), Ortada adam saldırısı (Man-in-the-Middle) saldırısıdır.

2.9.7.2. *Pasif Sniffing*

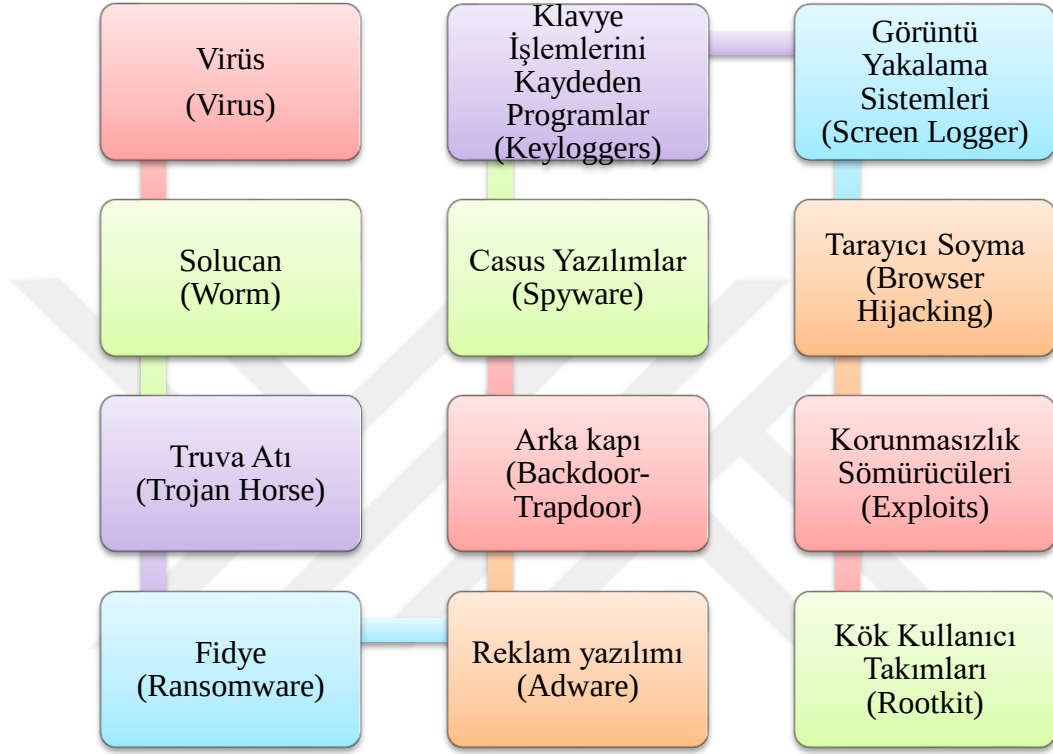
Pasif sniffing, switch ve hub' ı kokuşma işlemidir. Anahtarlanmamış veya köprülenmemiş ağı bölümünden geçen herhangi bir trafik, o bölümdeki tüm makineler tarafından görülmektedir. Sniffers, ağı veri bağlantı katmanında çalışır. LAN üzerinden gönderilen veriler aslında LAN' a bağlı her makineye gönderilir. Bu işleme pasif sniffing denir, çünkü saldırganların yerleştirdiği kokuşucular pasif olarak verilerin gönderilmesini ve yakalanmasını beklemektedir.

2.9.8. **Zararlı Yazılım Kullanımı (Malware)**

Kötücül yazılımlar bulaştığı bilgisayar sistemlerinde yazılımlara, dosyalara ve donanımlara bulaşan, bilgisayarlara izinsiz erişimlere izin veren ve verileri izinsiz olarak başkalarına gönderen zararlı yazılımlardır. En genel zararlı yazılımlar; Virüsler, solucanlar (Worm), Truva atları (Trojan Horse), arka kapılar (Backdoor), mesaj sağıanıkları (Spam), kök kullanıcı takımları (Rootkit), korunmasızlık sömürücüleri (Exploit), klavye dinleme sistemleri (Keylogger), görüntü yakalama sistemleri (Screen Logger), tarayıcı soyma (Browser Hijacking), Fidyeye (Ransomware), Reklam yazılımı (Adware) ve casus yazılımlar (Spyware) olarak belirtilebilir (Erol, 2015).

- Virüs (Virus)
- Solucan (Worm)
- Truva Atı (Trojan Horse)
- Fidyeye yazılımı (Ransomware)
- Reklam yazılımı (Adware)
- Arka kapı (Backdoor-Trojan)
- Casus yazılımlar (Spyware)
- Klavye İşlemlerini Kaydeden Programlar (Keyloggers)

- Görüntü Yakalama Sistemleri (Screen Logger)
- Tarayıcı Soyma (Browser Hijacking)
- Korunmasızlık Sömürücüleri (Exploits)
- Kök Kullanıcı Takımları (Rootkit)



Şekil 2.16: En genel zararlı yazılım (Malware) türleri.

2.9.8.1. Virüs (Virus)

Virüsler, bir bilgisayardan diğer bilgisayara bulaşmak, bu bilgisayarların çalışmasını engellemek ve verileri çalmak için yazılmış küçük boyutlu zararlı yazılımlar olarak adlandırılır.

2.9.8.2. Solucan (Worm)

Solucan, virüslerin bir alt sınıfıdır ve kullanıcı eylemi olmadan yayılır ve kendisinin tam kopyasını ağlardan ağlara yayılmasını sağlar. Bir solucan bellek veya ağ bant genişliği tüketebilir ve bu da bilgisayarın çökmesine yol açabilir.

2.9.8.3. Truva Atı (Trojen)

Truva atı, kurumların sistemlerine erişmeye çalışan saldırganlar tarafından kullanılabilir. Genellikle bir tür saldırılar kullanıcılar sosyal mühendislik tarafından kandırılarak truva atlarını sistemlerine yüklenerek çalışmasını sağlarlar. Truva atı, etkinleştirildikten sonra saldırganların sizi takip etmelerini, hassas verilerinizi çalmalarını ve sisteminize arka kapı erişimi elde etmelerini sağlamaktadır.

2.9.8.4. Fidyeye Yazılımları (Ransomware)

Fidyeye yazılımları, kullanıcıların kimlik hırsızlığı e-postalarıyla ve kötü amaçlı program içeren bir web sitesinin ziyaret edilmesi sonucunda sistemlerinin ele geçirilmesi olarak tanımlanmaktadır. Saldırganın ele geçirdiği sistemler, dosyalar ve bilgiler karşılığında para talep etmesi olayıdır.

2.9.8.5. Reklam yazılımı (Adware)

Reklam yazılımı, kullanıcıların bilgisayarlarında reklamlar görüntülemek, arama yaptıklarında reklam içeren web sitelerine yeniden yönlendirmek ve hakkınızdaki pazarlama verilerini toplamak amacıyla tasarlanmış programlara denilmektedir. Virüslü içerikli reklam siteleri bu tarz yazılımları içermektedir.

2.9.8.6. Arka kapı (Backdoor-Trapdoor)

Arka kapı (Backdoor), sistemlerin içine çeşitli yollarla yerleştirilen, sistemlerin dinlenmesine ve müdahalesine olanak tanıyan bir siber saldırı yöntemidir.

2.9.8.7. Casus yazılımlar (Spyware)

Casus yazılımlar, kullanıcıların izniyle olması veya izni olmadan yüklenen siber casus programlarıdır. Kullanıcının bilgilerinin veya sistemlere ait bilgilerin uzaktaki bir bilgisayar veya sitelere aktarılması olarak adlandırılır.

2.9.8.8. Klavye İşlemlerini Kaydeden Programlar (Keyloggers)

Klavye üzerinden işlemleri kaydeden programlar olarak tanımlanır. Kullanıcı farkına varmadan basılan her tuş kaydedilir ve salgınların belirlediği yerlerde bilgiler saklanmaktadır (Kaya, 2012).

2.9.8.9. Görüntü Yakalama Sistemleri (Screen Logger)

Ekran yakalama, keylogger saldırısı ile aynı temel mantığa dayanır. Kullanıcı fare ile bilgisayarın ekranında bir noktaya tıklaması ile beraber aynı anda ekranın bir bölümü veya o anki resmini kaydederek bunları internet ortamında sabit bir adrese iletmesidir.

2.9.8.10. Tarayıcı Soyma (Browser Hijacking)

Tarayıcı gasbı, web sayfanızı belirli bir sayfaya yönlendiren ve ana sayfanızı sürekli değiştiren küçük bir program veya registry ayarı olarak tanımlanır. Bir web arama sayfası veya ana sayfanız kendiliğinden değişiyorsa bu program bilgisayarınızda var demektir. Genelde web sayfalarının kullanıcı erişiminin artırılması amacı ile kullanılmaktadır.

2.9.8.11. Korunmasızlık Sömürücüleri (Exploits)

Sömürücüler, bilgisayarkların veya sunucuların işletim sistemlerinde ve bazı programlarda güvenlik açıklarını bulup bu açıkları kötüye kullanma yöntemi “exploit” diye adlandırılır. Sömürücüler ile sistemlere ait şifreler ve detaylı bilgiler ele geçirilebilir. Genel olarak yetkisiz erişim ve erişilen sistemleri ele geçirmek olarak sömürücülerin kullanılması saldırganlar tarafından amaçlamaktadır.

2.9.8.12. Kök kullanıcı takımı (Rootkit)

Kök kullanıcı takımı olarak adlandırılan bu saldırı türünde çalışan süreç, dosya ve sistem bilgilerini işletim sisteminden gizlenen programlardır (Yıldız, 2014).

2.9.9. Kriptografik Saldırıları

Kriptografik saldırılar sistem mekanizmalarını ve yaklaşımlarını inceleme ve veriyi çözme bilimidir. Şifrelenmiş verileri çözmek veya onları anlamlı hale getirme yaklaşımlarını içermektedir.

2.9.10. IP Aldatmacası - Gizlenmesi (IP Spoofing)

IP aldatmacası, saldırganın gerçek IP' sini gizlemesi ve gerçek kimliğini göstermemesi olarak bilinmektedir. Genellikle mail gönderme ve internet sitelerindeki sosyal ortamlarda yorum yazılması olarak karşımıza çıkmaktadır (Kaya, 2012).

2.9.11. Dijital Manipülasyon (Digital Manipulation)

Dijital manipülasyonlar, bilgisayar yardımı ile bir imajı değiştirmek ve yeni anlamlar yüklemek olarak tanımlanmaktadır. Bu tip saldırılar kamuoyu önünde yapılarak istihbarat veya güvenlik birimleri yanlış bilgilendirmeyi veya kandırmayı amaçlamaktadır. Fotoğraf, gazete, canlı video ve televizyon vb. medya araçları kullanılmaktadır.

2.9.12. Kabloya Saplama Yapma (Wire Tapping)

Kabloya saplama yapma, emniyeti alınmamış kablolardır. İki trafiğin tüm bilgileri ele geçirilebilir. Bu saldırıda ağa erişerek veri paketlerine erişim ve kişisel bilgilere ulaşılması amaçlanmaktadır. Saldırganlar, kabloya saplama saldırısı yaparak sistem üzerindeki zafiyet ve açıkları bulmayı amaçlamaktadırlar.

2.9.13. İnternet Servis Sağlayıcı Saldırıları (ISP Attacks)

ISP' lere karşı olan en tanınmış saldırı smurf saldırı veya smurfing' dir. Smurf saldırıda, saldırgan ISP' yi birçok "çöp" paketi ile tıkar, ISP nin band genişliği kullanılır ve müşterileri email kullanarak data alamaz, yollayamaz, internette dolaşamaz yada herhangi bir başka İnternet servisi kullanamaz olması durumudur.

Ping, genelde belirli bir bilgisayar yada serverin internete bağlı çalışır olup olmadığını anlamak için kullanılır. Bir bilgisayar yada sunucuya bir ping paketi gönderildiğinde, pingi yollayan kişiye bir cevap paketi yollar, özde "evet yaşıyorum ve İnternete bağlıyım" demiş olur.

Bir smurf saldırısında, hackerlar ping isteklerindeki geri dönüş adreslerini değiştirirler. Böylece bu cevap paketleri kendilerine değil de hedeflenen ISP' lerine gitmektedir. Saldırganlar, internete bağlı networkleri, ping isteklerini yeniden düzenlemek ve her basit ping isteğini birçok kere büyötmek için kullanabilirler. Bu yolla, bir saldırgan internete bağlı ağlarda, çok fazla

cevap ping pakedi yollar ve ISP' yi tıkar. Böylelikle ISP' nin gerçek müşterileri ondan hizmet alamaz. Saldırganlar basit bir smurf saldırı ile internete bağlı birden fazla ağı kullanabilirler.

2.9.14. SQL Enjeksiyonu

Bu enjekte açıkları saldırırganlar tarafından verilerin ele geçirilmesi hedeflenmekte ve web uygulamaları için ciddi bir sorun olarak ortaya çıkmaktadır. Bu açıklığı olan web uygulamaları saldırıgana uygulamaların tüm veri tabanlarına erişim imkanı sunmaktadır. Bu veri tabanlarında kullanıcılara ait çok hassas kişisel ve gizli bilgiler yer almakatadır ve güvenlik ihlallerinde bu bilgiler çalınma, ifşa edilme, satılma veya dolandırıcılık amacıyla kullanılabilmektedir (Erol, 2015).

2.9.15. Mantık Bombası (Logic Bomb)

Mantık bombası zararlı bir kod parçasının bir program içerisine yerleştirilmesidir. Genellikle hedeflenen bilgisayar ve ağlarda bilgileri yok etmek veya tamamen kullanılamaz hale getirmek için bu yöntem kullanılmaktadır (Aslay, 2018).

2.9.16. Yemleme - Oltalama (Phishing) Saldırıları

Oltalama saldırıları genellikle sahte web siteleri üzerinden gerçekleştirilmektedir. Bu saldırılarda özellikle bir banka veya alış veriş sitesinden e-posta gelmiş gibi yapılarak saldırıya uğrayan kişinin banka veya kredi kartı bilgilerinin e-postayı yanıtlayarak veya bu sahte web sayfasına girerek tuzağa düşmüş olmaktadır (Aslay, 2018).

2.9.17. Yerine Geçme (Masquerading)

Sistemde yapılacak hileler ile erişim imkanı kısıtlı ya da yetkisi hiç olmayan kullanıcıların, erişime yetkisi olan başka kullanıcıların bilgi ve yetkilerini kullanarak sisteme erişim sağlamasıdır (Aslay, 2018).

2.9.18. Sosyal Mühendislik (Social Engineering)

Yalan söyleme ve karşı tarafı ikna etme üzerine kurulan bir bilgi toplama sanatıdır. Burada kişilerin güveni kazanılarak kendilerine güvenmelerinin sağlanması amaçlanmaktadır (Aslay, 2018).

2.9.19. Çöpe Dalma (Scavenging)

Bilgisayarın sistem belleğinde bulunan ve sistem belleğinde bulunan ve artık ihtiyaç duyulmayan silinmiş bilgilerin gelişmiş yöntemlerle tekrar geri getirilmesidir (Aslay, 2018).

2.9.20. XSS-Siteler Arası Komut Dosyası (XSS- Cross Site Scripting)

XSS, siteler arası komut dosyası web uygulamalarında bulunan bir güvenlik açığıdır. .Net ve PHP gibi web programlama dillerinde meydana gelen genellikle HTML ve Javascript kodlarının arasına kod gömülmesiyle oluşmaktadır. Buradaki temel mantık, html kodlarının arasına `<script>`, `<object>`, `<embed>` gibi istemci bilgisayarında yorumlanacak kodların çalıştırılmasıdır.

Saldırı adımları olarak, ilk adım kurban web sitesinde XSS açığı aranır. Buradaki açığı kullanabilecek bir script dosyası hazırlanır, daha sonra kötü amaçlı kişiler scripti sitede, açık olan kısma eklerler ve son olarak kurbanların ağa düşmesini beklemek olarak sıralanmaktadır.

XSS saldırı türlerinden olan Reflected XSS, genelde web sitelerinde veri giriş alanlarında yapılır (login, arama gibi). Saldırı sadece saldırıyı yapan kullanıcı tarafından görünür. Yani diğer kullanıcılar bunu göremez. Stored XSS, bu saldırıda ise yapılan saldırılar veri tabanında görünmektedir ve saldırı kalıcı olmaktadır. DOM XSS ise, en tehlikeli saldırı türüdür ve Javascript kodlarıyla sitenin kodları değiştirebilir. Ayrıca bu yöntemle siteye index atılabilir.



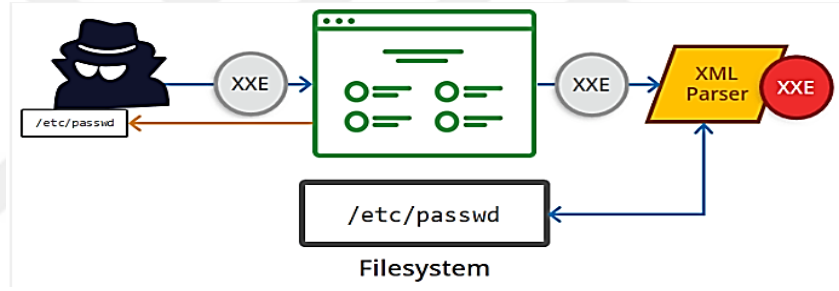
Cross Site Scripting

Şekil 2.17: XSS örnekleme (Siber Güvenlik Danışmanlığı, 2019).

2.9.21. XXE Dış Varlık Güvenlik Zafiyeti (XML External Entity)

XXE dış varlık güvenlik zafiyeti yeni olmayan ancak Facebook gibi bir sosyal medya devinin sunucularında bulunmasıyla gündeme gelen bir zafiyettir. Aslında XML' in esnekliğini arttırmak için düşünülen bir özellik olmasına karşın bu esneklik önemli güvenlik risklerini de beraberinde getirmekte, sunucudan rasgele dosya okunmasına ve bazı özel durumlarda sunucuda komut çalıştırılmasına imkan vermektedir.

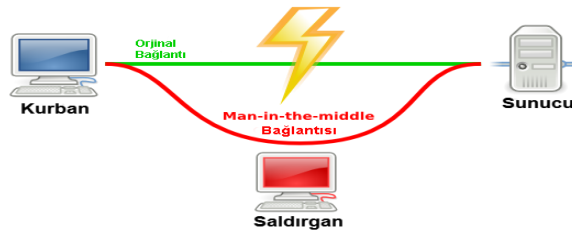
XXE zafiyeti, sunucu (sunucu tarafında çalışan yazılım) XML verisini kontrol ederken ve işlerken özel olarak tanımlanmış bir XML varlığının (entity) çağırılması sonucu tetiklenir. Bazı XML kütüphaneleri özel olarak varlık tanımlamaya ve çağırmaya varsayılan olarak izin verirken bazılarında bu özellik kapalı gelir. Saldırının başarılı olabilmesi için hedef sistemde bu özelliğin aktif olması gerekmektedir.



Şekil 2.18: XXE dış varlık güvenlik zafiyeti (Bgasecurity, 2019).

2.9.22. Araya Girme Saldırısı (MITM)

Bu saldırı tipinde, birbiri ile doğrudan iletişim halinde olan iki kişi veya sistemin arasındaki iletişimi gizlice ilettiği veya değiştirdiği saldırı türüdür. İletişim ağı üzerinde veri paketleri serbestçe dolaştığından özellikle broadcast edilen paketler, aynı ağa içerisindeki tüm cihazlar tarafından görülebilmektedir (Mishra, 2013).



Şekil 2.19: MITM atak örneği (Mishra, 2013).

2.9.23. Replay Saldırısı

Tekrar saldırıları, saldırganların bir ağ üzerinden iletilen geçerli bir verinin ele geçirip bunu tekrarlayarak gerçekleştirdiği bir siber saldırılardır. Banka hesaplarına erişimde ikinci kez mesajın tekrarlanması kurbanın hesabından doğrudan para aktarılmasına neden olabilmektedir. Şifreli mesajlar bir araya getirilerek mesajın içeriğindeki gizli bilgiler çalınabilir veya değiştirilerek kaydı ile sistemlere hatalı veri paketlerin sistemlere zarar verilmesi gibi senaryolar ile saldırılar yapılabilir.

2.9.24. MODBUS/TCP Protocol Attack

Uygulama katmanı tarafından sağlanan güvenlik açısından MODBUS, yüksek kontrollü ortamlarda kullanılmak üzere tasarlanmıştır ve bu katmanda herhangi bir güvenlik mekanizması içermez. Bu nedenle, Modbus oturumu için gerekli olan her şeyin geçerli bir adres ve işlev kodu olması için kimlik doğrulaması yoktur. Bu, bir ağ dinleyicisi kullanılarak internet üzerinden kolayca elde edilebilen bilgilerdir. Aynı şekilde, bilgilerin şifrelenmesine izin vermez. Veri paketleri clear text olarak gönderilmektedir ve tüm bu eksiklikler, DDoS saldırıları açısından zaafiyet barındırmaktadırlar. Ayrıca MODBUS' ın uzak terminal üniteleri (RTU' lar) veya PLC' ler gibi kontrol elemanlarını programlamak için tasarlanmış bir protokol olması, böylece bu elemanlara kötü amaçlı kod enjeksiyonu mümkün hale gelmektedir (Collantes, 2017).

2.9.25. DNP3 Protocol Attack

Bu protocol saldırılarının çoğu DNP3 mesajlarını yakalama, değiştirme ve / veya üretme yeteneğine dayanır. DNP3 uygulamaları tipik olarak şifreleme, kimlik doğrulama ve yetkilendirme kullanmaz. DNP3 saldırıları üç kategoriye ayrılır: DNP3 spesifikasyonlarından yararlanan saldırılar, satıcı uygulamalarından yararlanan saldırılar ve temel alt yapıyı hedef alan saldırılardır (East, 2009).

2.9.26. Malicious Command and Software Injection

Zararlı komut enjeksiyon saldırıları, yanlış kontrol ve yapılandırma komutlarını bir kontrol sistemine enjekte etmektir. Operatör kontrol sistemlerini denetler ve zaman zaman denetleyici kontrol eylemlerine müdahale etmektedir. Bilgisayar korsanları, bir kontrol sistemi ağına yanlış

denetleyici kontrol eylemleri enjekte etmeye çalışabilir. Uzak terminaller ve akıllı elektronik cihazlar genellikle fiziksel işlemi doğrudan uzak bir sitede otomatik olarak izlemek ve kontrol etmek için programlanır. Programların içerisine C kodu ile yazılmış zararlı yazılımlar enjekte edilerek sistemlerin kontrol edilmesi sağlanır. Kötü amaçlı komut enjeksiyonlarının olası etkileri, kesinti süreci kontrolü, cihaz iletişiminin kesintiye uğraması, cihaz yapılandırmalarının yetkisiz olarak değiştirilmesi ve proses ayar noktalarının yetkisiz olarak değiştirilmesini içermektedir (Morris, 2013).

2.9.27. Arabellek Taşması (Buffer Overflow)

Arabellek aşımı ya da arabellek taşkını, iki yazılım arasında veri iletişimi için ayrılmış olan bir arabelleğe boyutundan daha fazla veri konulması ile ortaya çıkan durumdur. Buffer' da dizinler (array) statik yada dinamik olarak sınıflandırılmaktadır. Diğer bir ifade ile, dinamik değişkenlerin taşıyabilecekleri veri miktarından fazlasını yükleyerek değişkenin sınırlarını aşmasıdır.

2.9.28. Fiziksel Saldırı (Sensör, Actuator, Kamera)

Fiziksel saldırılar, sistemler üzerinden veya donanım bazlı fiziksel müdahaleler sonucu belirli noktalardan sistemlere sızmak olarak tanımlanmaktadır. Bu tarz sistemlerde önlem olarak sistemleri izlemek ve anomali tespit sistemleri kullanmak gerekmektedir.

2.9.29. Yetkisiz Erişim Faaliyetleri (Unauthorized Access Activities)

Yetkisiz erişim aktiviteleri, bir bilgisayara izinsiz giriş yapmak ve veri almak, veri depolamak, veri veya yazılımla iletişim kurmak, müdahale etmek veya değiştirmek anlamına gelmektedir.

2.9.30. İç ve Dış Ataklar (Insider-Outsider Attacks)

İlk olarak iç atak, bir kuruluştaki BT sistemine ayrıcalıklı erişimi olan bir kişidir. İçeriden öğrenilen bir tehdit, 'mevcut veya eski bir çalışan, yüklenici veya kuruluşun ağına, sistemine veya verilerine erişimi olan ve bunları kasıtlı olarak kötüye kullanan veya erişimi kötüye kullanan sonuçları olan başka bir iş ortağı' olarak tanımlanabilir. Öte yandan, dış atak ise bir kişi veya grup, kuruluş dışından güvenilir bir kullanıcının içeri sızarak ve profilini alarak korunan bilgi elde etmeye çalışmasıdır.

2.9.31. Ağ Trafiği Anomalisi

Ağ trafik anomalisi, olası ataklar, ihlal ve tehditlerin ağ içerisinde gerçekleşen aktivitelerde olağan dışı olarak sistemlere sızmadır.

2.9.32. Keşif Saldırıları (Reconnaissance Attacks)

Keşif saldırıları, yetkisiz algılama, sistem haritalama ve hizmetler keşif saldırıları olarak adlandırılır. Keşif saldırıları aşağıdakilerden oluşabilir: Paket Koklayıcılar, Bağlantı Noktasını Tarama, Ping Süpürme, İnternet Bilgisine İlişkin Sorgular.

Keşif, hedef sistem hakkında bilgi bulma sürecidir. Bu işlem bir ARP, TCP senkronizasyonu veya ping taraması içerebilir, ancak SCADA sistemleri protokolü ve işlevselliği veya yapılandırması hakkında ek bilgi içerebilir. Keşif modülü, başlatılan veri nesneleri ve veri noktası değerleri hakkında bilgilerin alınmasına, bellek kayıtlarının bulunmasına veya otomasyon denetleyicilerinde depolanan diğer bilgi parçalarına izin verir (Rodofile, 2017).

2.9.33. Ağda Kötü Amaçlı Yazılımlar (Process Network Malware Injection)

İşlem ağı, kötü amaçlı yazılımların dış ağ veya iç ağ üzerinden sızmalar olarak adlandırılır. Zararlı yazılımlar iç ağda depolama cihazları (CD, DVD, disket ve USB sürücüler gibi) ile gerçekleştirilebilir. Ağ tabanlı saldırı teknikleri dış ağlar üzerinde gerçekleştirilebilir (Korkmaz, 2016).

2.9.34. Gereksiz Port ve Servisleri Tarama

Sistemlerin açık olup olmadığını ve açık olan sistemlerin portlarını durumlarını, hangi servislerin çalıştığı ve kullanılan işletim sistemi gibi birçok bilgi toplamak için kullanılan yöntemlerdir. Bu yöntemler ile servislerin güvenlik açığı barındırıp barındırmadığı ve kullanılan servisler hakkında bilgi elde edilebilir. Ayrıca içerisinde barındırmış olduğu scriptler ile hedef sisteme yönelik tarama gerçekleştirildiğinde hedef sistem hakkında detaylı bilgi ve güvenlik açığı olup olmamasına yönelik detaylı sonuçlar elde edilmektedir.

2.9.35. PROFIBUS Protokol Atağı (PROFIBUS Protocol Attack)

PROFIBUS protokolü, uygulama, bağlantı ve fiziksel katmanlarda çalışan bir protokoldür. Bu protokolde bağlantı katmanı, ortama erişimi yönetmek için bir mekanizma olarak FDL

(Fieldbus Veri Bağlantısı) kullanır. Master-slave teknolojisini kimin iletişim başlatabileceğini ve otobüsü işgal edebileceğini gösteren bir tokenin geçişiyle birleştiren hibrit bir erişim yöntemiyle çalışır. Bu önlemler, cihazların aynı anda iletişim kurmamasını sağlar, ancak herhangi bir güvenlik mekanizması oluşturmaz ve trafik enjeksiyonu veya servis reddini içeren saldırılara karşı zaafiyetler oluşturmaktadır (Collantes, 2017).

2.9.36. Firmware Değişiklik Saldırısı (Firmware Modification Attack)

Firmware değiştirme saldırısı; Bu saldırı türü, kritik kontrol altyapılarını hedeflemek için oluşturulan kötü niyetli StuxNet solucanı ile örneklendirilebilir. Bu saldırı yöntemi, kötü niyetli işlevleri uygulanıncaya kadar, solucanların iyi huylu keşif işlevleri gerçekleştiren ana bilgisayarla uyum içinde bir arada olmasını sağlayacak şekilde çalışır. Lokal SCADA aygıtlarına karşı firmware modifikasyonu saldırıları gerçekleştirilebilir, bu nedenle değiştirilebilir firmware sahip PLC' ler bu saldırılara karşı savunmasız olabilir. Pratik olarak, firmware modifikasyon saldırıları, kötü amaçlı yazılımı hedef PLC' lere enjekte ederek gerçekleştirilebilir (Korkmaz, 2016).

2.9.37. Yanlış Veri Enjeksiyonu (False Data Injection)

Yanlış veri enjeksiyon saldırıları, bir saldırganın durum tahmin edicisinin kötü ölçüm algılama algoritması tarafından algılanmadan, değişkenlerin tahmini değerinde keyfi bir değişiklik başlatmak için sensör ölçümlerini manipüle ettiği saldırılardır (Mo, 2010).

2.9.38. Zehirleme (Poisoning-ARP, DNS)

ARP Zehirlenmesi (ARP Spoofing olarak da bilinir), IP'sindeki eşleşmeleri MAC adresine değiştirmek için LAN üzerindeki varsayılan ağ geçidine kötü amaçlı ARP paketleri göndermeyi içeren bir Yerel Alan Ağı (LAN) üzerinden gerçekleştirilen bir siber saldırı türüdür. ARP Protokolü IP adreslerini MAC adreslerine çevirir. ARP protokolü yalnızca güvenlik için değil verimlilik için tasarlandığından, saldırganın hedef LAN içindeki bir makineyi kontrol ettiği veya doğrudan ona bağlı olduğu sürece ARP zehirlenmesi saldırılarının gerçekleştirilmesi son derece kolaydır.

2.9.39. Gizli Dinleme (Eavesdropping)

Gizli dinleme saldırıları, paylaşılan medya kullanımı Ethernet (hub' lı) ve Wi-Fi gibi ağlara yapılan saldırılardır. Gizli dinleme saldırısında, saldırgan ilgili ağ arabirimini karışık modda yapılandırır. Bu modda, saldırganın bilgisayarını, diğer düğümlere gönderilen paketler de dahil olmak üzere ağ üzerinde gönderilen paketleri alır. Paketler şifrelenmemişse, saldırgan muhtemelen parolalar ve diğer kimlik bilgileri de dahil olmak üzere paketlerin verilerini okuyabilmektedir (Xia, 2005).

2.9.40. Cevap ve Ölçüm Enjeksiyon Saldırısı (Response and Measurement Injection)

Bu saldırı yönteminde ise, üretim ve iletim sistemlerinde operator kontrolü dışında olağan olmayan bir durumda sistemlere ait ölçüm ve cevap sistemlerine müdahale edilerek normal değerlerin dışında bir değerlerin ölçülmesi amaçlanmaktadır. Örnek olarak, su dağıtım söz konusu olduğunda, pompa hızı artırılarak talep aslında daha düşük olduğu için su taşmalarına neden olabilir veya gaz dağıtımında ısınma sistemi pompalarını sıcaklık ayarlarının arttırılması ile gazın sıcaklığının artırılarak ölçüm sistemine müdahale edilemesi mümkündür (Morris, 2013).

2.9.42. Çerçeve (Fragmentation) Saldırısı

Çerçeve saldırıları, İnternet Protokolü'nün verilerin iletilmesini ve işlenmesini nasıl gerektirdiğine dayanan bir tür bilgisayar güvenlik saldırısıdır.

2.9.43. Yanlış Alarm Üretilmesi

Bu saldırı üzerinde, kontrol sistemleri üzerinde yanlış alarm üretilerek sistemler üzerindeki kontrolü zayıflatmak ve sistemlere zarar vermek amaçlanmaktadır.

2.9.45. Reverse-Engineering Attack

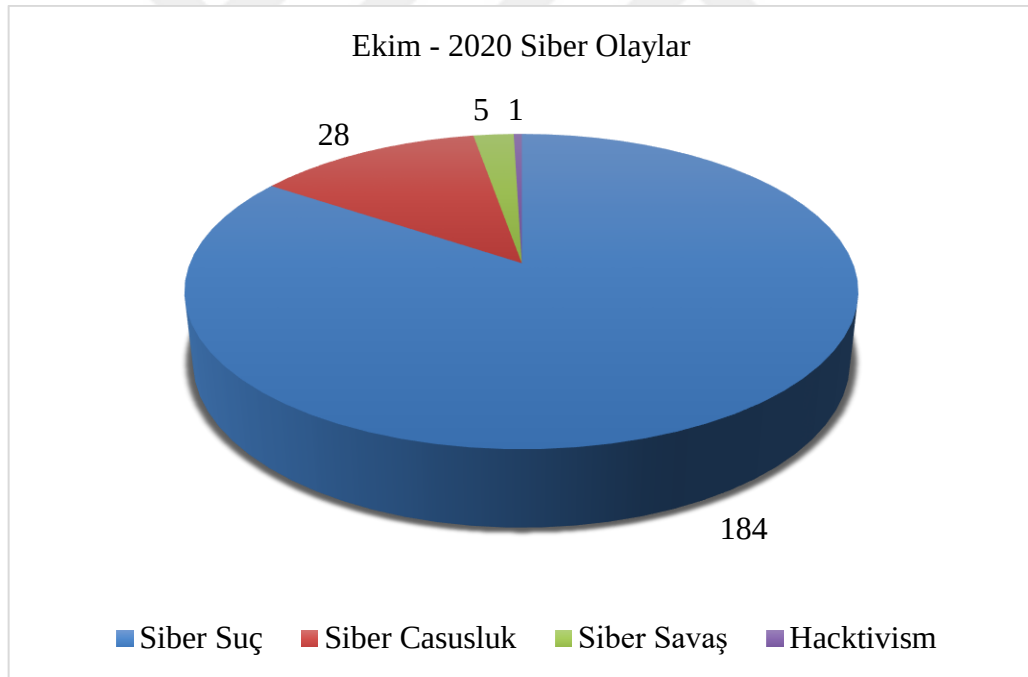
Tersine mühendislik, bir aygıtın, objenin veya sistemin yapısının, işlevinin veya çalışmasının, çıkarımcı bir akıl yürütme analiziyle keşfedilmesi işlemidir.

2.10. ÇEŞİTLİ SİBER GÜVENLİK RAPOR ÖRNEKLERİ

Buradaki çalışmamızda son yıllarda yapılmış çeşitli siber saldırı türleri, olayları, hedeflenen kurumlar ve sektörler dikkat çekilmeye çalışılmıştır. Bu araştırma çalışmalarından motive olunarak akıllı şebekeler ve enerji sektörlerinden doğal gaz alanında akıllı doğal gaz şebekelerin incelenmesi ve bir olgunluk modeli oluşturmak için bu çalışma ele alınmıştır. Aşağıda bir çok örnek çalışmalar incelenmiş, araştırılmış ve tez içerisinde verilmeye karar verilmiştir.

2.10.1. Dünyada Ekim 2020 Tarihinde Yaşanan Siber Olaylar

Saldırıların ardındaki motivasyonlar tablosuna bakıldığında siber suç her zaman % 80 civarında dalgalanan bir yüzdeyle (Eylül’ de % 82,5’ e karşı % 85,6) her zaman en üstte yer almaktadır. Siber casusluk % 28, siber savaş % 5 lik bir paya sahip ve Hacktivism ise % 1 puan olduğu görülmektedir (her ikisi de Eylül’ de % 1.5’ idi).

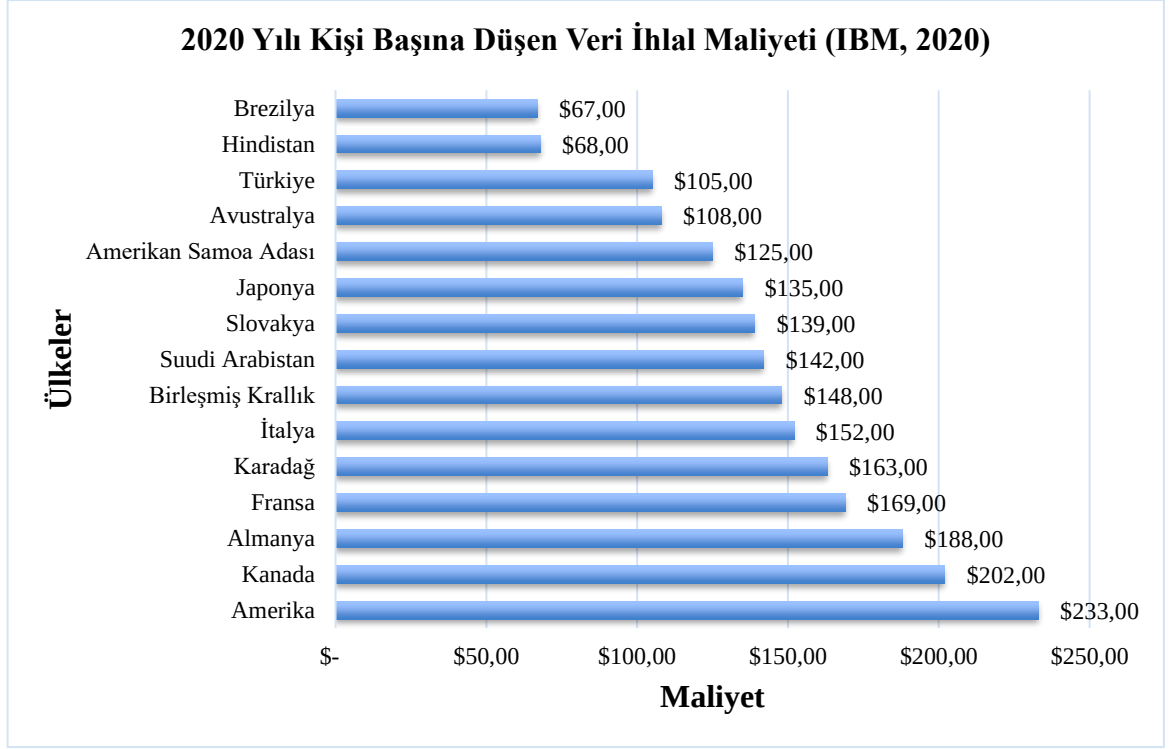


Şekil 2.20: Ekim-2020 Tarihinde gerçekleşen siber olaylar (Hackmageddon, 2020).

2.10.2. 2018 Yılı Veri İhlalinin Ülke veya Bölgeye Göre Kişi Başına Düşen Maliyeti ve Kök Nedenlerine Göre Dağılımı

Amerika Birleşik Devletleri, Kanada ve Almanya, kişi başına düşen 2018 yılındaki veri ihlal maliyetlerinde en yüksek sıralamaya sahiptir. Bu sıralama aşağıdaki şekilde görüldüğü gibi en yüksek maliyetin sırasıyla 233 \$, 202 ve 188 \$’ dır. Diğer taraftan bakıldığında Türkiye,

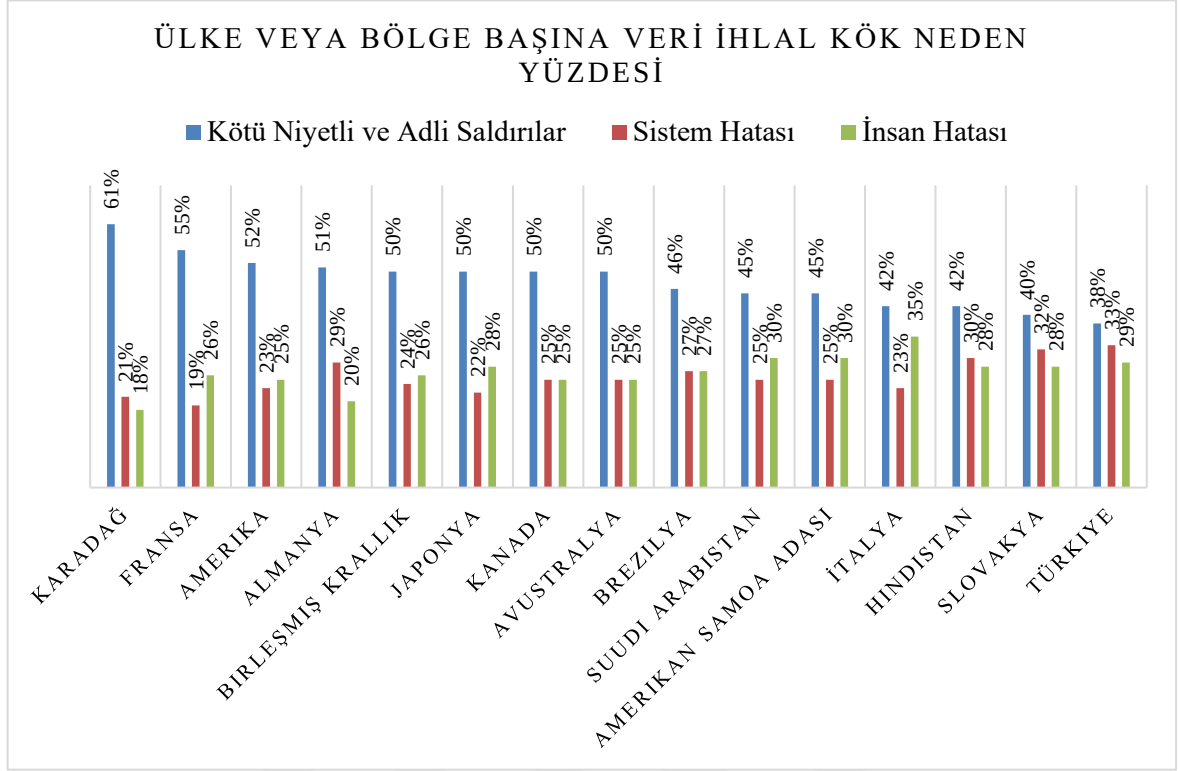
Hindistan ve Brezilya, kişi başına düşen 2019 yılındaki veri ihlal maliyetlerinde sırasıyla 105 \$, 68 \$ ve 67 \$ olduğu şekilde gösterilmektedir. 15 adet ülke kıyaslama örnekleme için ele alınmıştır.



Şekil 2.21: Ülke veya bölgeye göre kişi başına düşen 2019 yılı veri ihlal maliyeti (IBM, 2020).

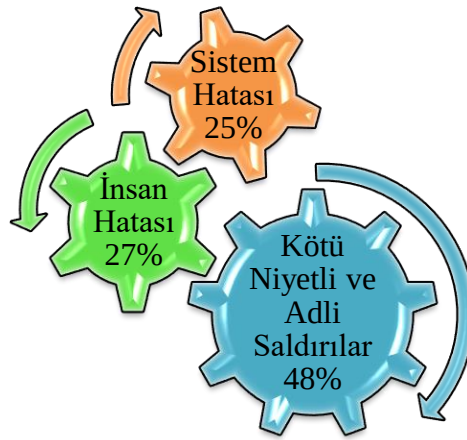
Tüm dünya genelindeki ülkeler veya bölgeler için Şekil 2.21’ de verilen örneklerde bir veri ihlalinin ana nedenlerini göstermektedir. Orta Doğu bölgesindeki şirketlerin, büyük olasılıkla, kötü niyetli veya suçlu bir saldırıya maruz kalma olasılığı yüksektir (% 61). Dünyanın bu bölgesinde faaliyet gösteren şirketler, güvenlik duruşlarını etkileyebilecek daha az düzenlemeye sahiptir. Buna ek olarak, suçlular bu şirketlerin saldırılara karşı daha savunmasız olan yüksek değerli bilgi varlıklarına ve BT altyapılarına sahip olduğunu algılamaktadırlar.

Bunun aksine, Türkiye, Güney Kore ve Hindistan’daki kuruluşlar, suçlu güdümlü veri ihlallerini yaşama ihtimalleri en düşük seviyelerdedir. İtalyan şirketleri ise en yüksek insan hatası (cezai olmayan) veri ihlallerine sahiptir. Türk şirketleri sistem aksaklığı veya iş süreçleri başarısızlığı nedeniyle veri ihlali yaşama olasılığı en yüksek olan kurumlardır.



Şekil 2.22: Ülke veya bölge başına veri ihlal kök neden yüzdesi (IBM, 2020).

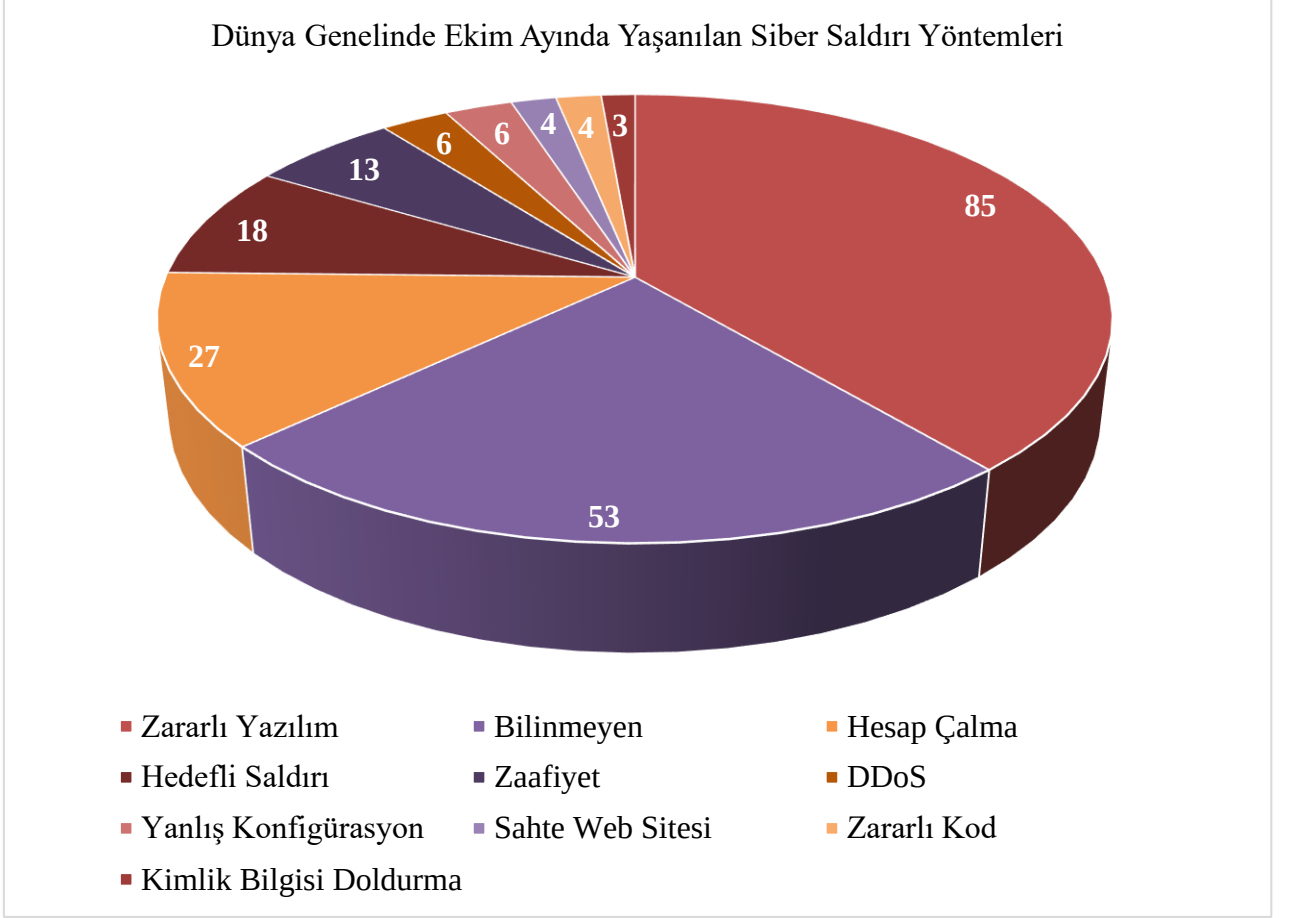
Tüm dünya genelindeki ülkeler veya bölgelere göre organizasyonlar için konsolide bazda Şekil 2.23’ de verilen örneklerde bir veri ihlalinin ana nedenlerinin özeti ve toplam oranları Şekil 2.24’ de göstermektedir. Olayların % 48’ i kötü niyetli veya suçlu saldırıya karıştığı, % 27’ si ihmalkâr çalışanlar ya da yüklenicilerden (insan faktörü) ve % 25’ i hem BT hem de iş süreçleri hataları dahil olmak üzere sistem hataları içerdiği gösterilmektedir.



Şekil 2.23: Kıyaslama örneğinin veri ihlalinin kök nedenine göre dağılımı (IBM, 2020).

2.10.3. Dünya Geneline Ekim Ayında Yaşanılan Siber Saldırı Yöntemleri

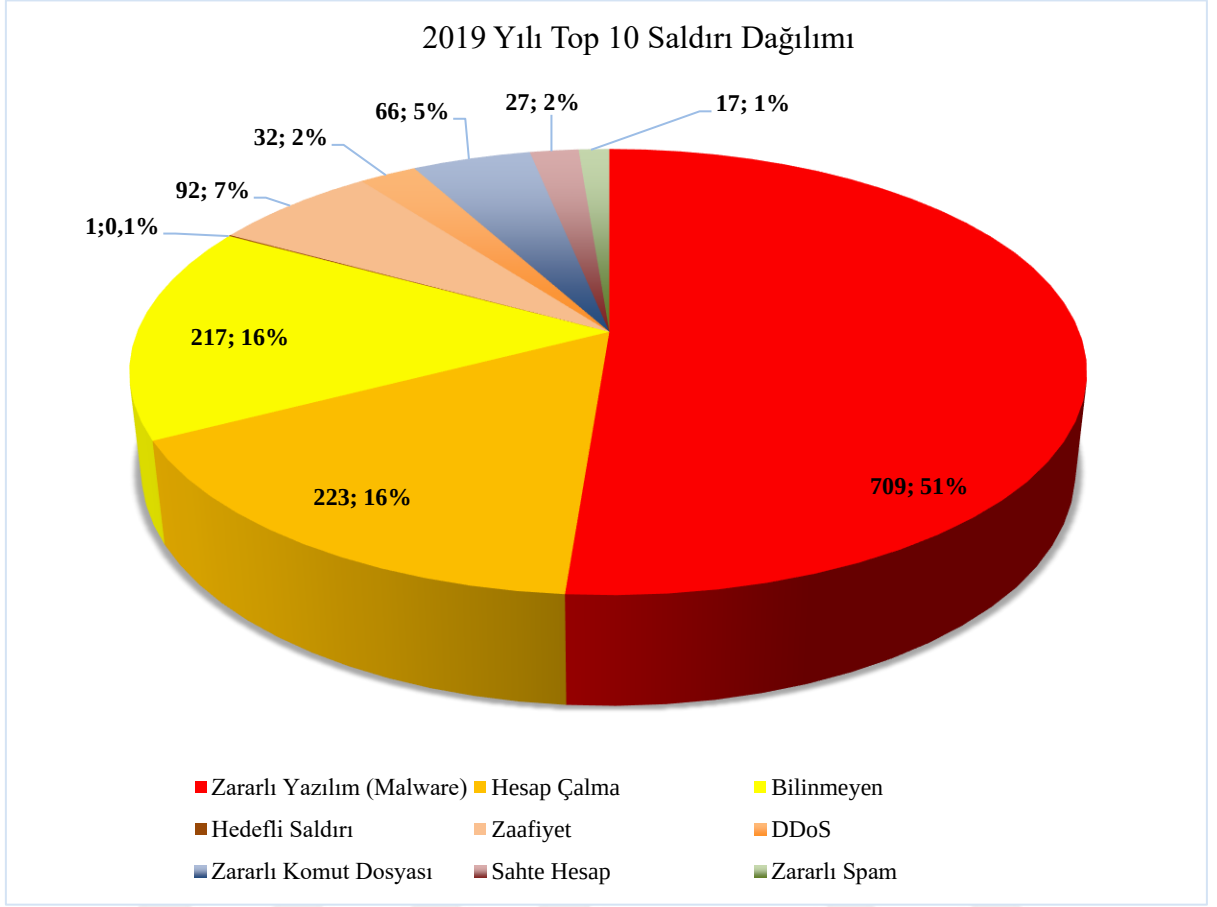
Siber saldırılar son yıllarda teknolojilerin gelişimi ile birlikte artmaktadır. Ekim ayına ait aşağıdaki Şekil 2.24’ de saldırıların türleri hakkında genel bir görüş sahibi olmamıza imkan verilmektedir. Ekim ayında dünya genelinde 219 adet saldırıdan 85 adet saldırı türü zararlı yazılımlar (Malware) birinci sırada yerini almıştır.



Şekil 2.24: Dünya genelinde Ekim ayında gerçekleşen siber atakların yüzdesel dağılımı (Hackmaggeddon, 2020).

2.10.4. Dünya Geneline 2019 Yılında Gerçekleşen Siber Atakların Yüzdesel Dağılımı

2019 yıllarında dünya genelinde yaşanan siber saldırılara bakıldığında saldırı yöntemi olarak ilk üç sıra aynı olduğu ve saldırıların adetsel olarak arttığı görülmektedir. İlk üç sırada zararlı yazılım, hesap çalma ve bilinmeyen saldırı yöntemleri olarak gerçekleşmiştir.



Şekil 2.25: Dünya genelinde 2019 yılında gerçekleşen siber atakların yüzdesel dağılımı (Hackmaggeddon, 2020).

2.10.5. En Yaygın Kullanılan Standartlar, Regülasyonlar ve En İyi Kullanım Örnekleri

2019 yılında yapılan araştırma göre kullanıcılardan aldıkları verilere göre hazırlanan raporda Tablo 2.1’ de gösterildiği gibi en çok kullanılan ilk 10 standartlar, regülasyonlar ve en iyi kullanım örnekleri gösterilmiştir.

Bu standartlar, yönetmelikler ve en iyi uygulama örnekleri dünya genelinde kullanılan ve herkez tarafından kabul görülmekte olan uluslararası uygulamalardır. Ülkemiz geneline bakıldığında GDPR yerine KVKK kullanılmaktadır. Burada önemli olan bu uygulamaların kurum ve kuruluşlarda nasıl bir uyumluluk sağlanarak kullanılabilirliğinin takibi ve yönetimidir. Bunun için yetkili kurumların bu konuda önemli aksiyonlar alması gerekmektedir.

Tablo 2.2 Kullanıcılar tarafından kullanılan en iyi 10 standartlar, yönetmelikler ve iyi uygulama kullanım örnekleri (Radiflow, 2019).

Sıra	Standartlar, Yönetmelikler ve En İyi Kullanım Örnekleri
1	NIST CSF
2	ISO 27000 Serileri
3	NIST 800-53
4	NIST 800-82
5	ISA/IEC 62443
6	CIS Kritik Güvenlik Kontrolleri
7	NERC CIP
8	GDPR
9	C2M2-Siber Güvenlik Kapasite Olgunluk Modeli
10	NIS Direktifleri(EU)

En çok kullanılan 10 yönetmeliğin, standardın veya en son değerlendirmenin yapıldığı zamana karşı en iyi uygulamaların kullanımları incelenerek Tablo 2.2' nin oluşturulmuştur.

2.11 DÜNYADA VE TÜRKİYE' DE GERÇEKLEŞEN SİBER SALDIRILAR

Dünyadaki ve Türkiye' deki siber saldırılar örnekleme alınarak gelişen teknolojilerle birlikte gelecekte hangi siber saldırıların olabileceği konusunda bizlere fikir verebilecektir. Genel olarak akıllı şebekeler kapsamında ve akıllı doğal gaz şebekelerinde gerçekleşen siber olaylar örnek olarak verilmiştir. Bu araştırmalar neticesinde bu tez çalışmasının yapılması bizlere motivasyon açısından önemini ortaya koymaktadır.

2.11.1. Dünya Geneline Yaşanan En Önemli Siber Saldırıları

Burdaki çalışmada dünya genelinde yaşanan en önemli siber saldırılar, olaylar ve saldırı türleri üzerine geniş çaplı bir araştırma yapıldı. Özellikle yapılan bu çalışmada kritik altyapılar, akıllı şebekeler ve EKS üzerinde gerçekleşen siber olaylar araştırıldı ve bu çalışmalar kronolojik sıralama yapılarak aşağıda belirtilmiştir.

2.11.1.1. Rusya (Sibirya) Doğal Gaz Boru Hattı Patlaması-1982

Soğuk savaş zamanında ABD ile Rusya sürekli casusluk faaliyetlerine devam etmişlerdir. Moskova Kanada' daki bir şirketin kullanmakta olduğu doğal gaz boru hatlarını kontrol eden yazılımı çalmaya çalışmıştır. Ancak ABD bunu fark edince operasyonu durdurduktan sonra yazılımın içerisine bir virüs yerleştirmişlerdir. Belli bir zaman sonra virüs yazılımı, kontrol

edilen doğal gaz boru hatlarındaki akışı anormal değerlere yükselterek patlamasına neden olmuştur (Karakuş, 2011).

2.11.1.2. ABD' nin Irak Hava Savunma Radar ve Füze Üssü Sistemlerine Saldırısı-1990

ABD 1990 yılında Körfez Savaşı sırasında Irak hava savunma radar ve füze üssüne karşı bir operasyon yapmıştır. Operasyon ABD siber savaşçıları tarafından yapılmıştır. Irak iletişim sistemlerine dinlemeler yapılarak telsiz sistemlerinin frekanları tespit edilerek haberleşmenin zayıfıtılması ve havadan gelecek saldırılar önlenmiş olacağı tespit edilmiştir. Sadece dinleme ile kalmayıp belli bir süre sonra iletişime geçilmiştir. İletişimin ele geçirilmesiyle Irak komuta kontrol sistemi tamamen yıkılmıştır.

2.11.1.3. Ay Işığı Labirenti-1998

Moonlight moze operasyonu olarak bilinen ve Mart 1998' de başlayan operasyon ile ABD'nin Pentagon, NASA, ABD Enerji Bakanlığı ve üniversitelere ait araştırma ve geliştirme sırları, askeri tesislerin haritaları, askeri yapılandırmaları ve askeri donanım tasarımlarını içeren birçok gizli bilgi Rus hackerlar tarafından çalındığı düşünülmektedir. Rus yetkililer bu konuyu kabul etmedikleri belirtilmiştir. Çalınan veriler çok büyük maddi değerlere eşdeğer olduğu belirtilmektedir ve ABD teknik takip sonucu verilerin Rusya' ya transfer olduğunu belirtmektedir. İnternet üzerinden sızma yapılarak gerçekleştirilmiştir (Başaran1, 2014).

2.11.1.4. NATO ile Kosova Krizi -1999

1999 yılında Yugoslavya ordusu, bağımsızlık isteyen Kosova ordusuna karşı oprasyon başlatmış ve bu nedenden dolayı NATO bu olaya Sırp odularını bombalayarak olaya el koymuştur. Ancak bu olaydan sonra NATO karargâhına ve üye ülke askeri haberleşme sistemlerine yönelik siber saldırılar başlanmıştır. NATO' ya yapılan saldırıda siber silah olarak DDoS ve binlerce zararlı bilgisayar virüsünü içeren epostalar kullanılmıştır. Saldırıları Sırp'ların yanı sıra Çinli ve Rus hacker gruplarında destek verdiği gözlemlenmiştir.

NATO' ya ait resmi web siteleri kesintiye uğramış ve e-posta hesapları günlerce kapalı kaldığı belirtilmektedir. Bazı siteler saldırganlar tarafından “Çok Yaşa Büyük Sırbistan” ve “Kara El (Black Hand) bu siteye el koydu” benzeri mesajlar bırakılmıştır. NATO, saldırılara karşı koyabilmek için kullanmış olduğu Sun Microsystem'in SPARC-20 sunucularının yerine daha

hızlı veri işleme gücü olan Ultra-SPARC'larla değiştirmiş, Pingler tarafından doldurulan bant genişliğinin de seviyesini yükseltmiştir. Bu olay karşısında NATO esir olmaktan kurtulamamıştır.

2.11.1.5. Avustralya'da Atık Kontrol Sistemine Siber Saldırı-2000

Avusturalya'da atık kontrol sistemine giren hacker bir milyon metre olan atığın deniz ve nehirlerle salınmasına neden olmuş ve dolayısı ile maddi zararlar meydana gelmiştir. Eski bir çalışan tarafından 223 kişisel bilgisayar ile SCADA sistemine girmeyi başarmışlardır. 150 adet atık istasyonu komuta ederek olaylar gerçekleşmiş ve yakalanarak 2 yıl hapis cezasına çarptırılmıştır. 224 hacker aynı sisteme girmeye çalışmışlar ve 44 başarısız erişim sonrasında sistem yöneticileri tarafından bu olaylar fark edilememiştir (Meral, 2015).

2.11.1.6. Dünya Genelinde Slammer Adlı Solucan Siber Saldırısı-2003

Dünya genelinde yapılan bu basit yapıdaki solucan saldırısı aralarında kritik altyapıların da bulunduğu pek çok sisteme zarar vermiştir. Cihazlara sızdığında başka bir cihaza sızmak için rasgele IP adreslerini deneyerek tarfiğin artmasına ve hizmetlerin yavaşlamasına sebep vermekte olduğu belirtilmiştir. Microsoft yazılımını kullanarak yayılan solucandan korunmak için ilgili yamaların 6 ay önceden yüklenmesi gerektiği belirtilmektedir. Bunlara rağmen Washington' da 911 ilk yardım servis hatlarına ulaşımın engellenmesine, Bank of America' ya ait 13000 adet ATM'nin kullanım dışı kalmasına, bazı uçak seferlerinin iptaline ve Güney Kore'nin yarım gün süreyle internet bağlantısının kesilmesine neden olabilecek kadar önemli bir etki yaratabilmiştir. Ayrıca Ohio'da bir uzmanın bilgisayarının ele geçirilmesi ile internet bağlantısı olmayan Davis-Besse Nükleer tesisinin ağına sızma olmuştur bu da SCADA sistemleri tarafından sağlanan gözlem ve kontrol işlevinin 5 saat süreyle bloke olmasına neden olduğu belirtilmiştir (Meral, 2015). Continental Airlines havayolu şirketinde etkileyen bu solucan yazılım Slammer toplam 200 bin bilgisayara bulaştığı ve 1.2 milyar dolarlık hasara yol açtığı belirtilmektedir. Saldırı kaynağı İngiltere olarak idda edilmektedir.

2.11.1.7. Estonya Siber Saldırısı - 2007

Rus hükümeti Estonya' yı 2. Dünya savaşında kaybedince ölen askerler için anıt dikilmiştir. Estonya hükümeti Tallinn şehrindeki Bronz Asker Heykeli'nin yerini değiştirmek isteyince kritik altyapılara, bankalara ve hükümetin resmi sitelerine Rus hükümetine bağlı hacker

gruplarca DDoS saldırıları yapılmıştır. Estonya yurt dışından gelen internet hatlarını kapatmış ama buna rağmen saldırılar birkaç hafta daha devam etmiştir (Başaran1, 2014). Ayrıca bu olaylar NATO bünyesinde “mükemmeliyet merkezi” (Center of Excellence) isminde uzman bir birimin kurulmasına da katkı sağlamıştır.

2.11.1.8. İsrail Tarafından Suriye Nükleer Santraline Siber Saldırı - 2007

İsrail devleti tarafından Suriye’nin Kuzey Kore işbirliğiyle yapmakta olduğu nükleer tesis 6 Eylül 2007 tarihinde bombalanmıştır. Ancak bu olayda havadan gelen bombalama saldırısının Suriye hava radar system ekranında görünmemesi şaşkınlığa neden olduğu belirtilmektedir. Bu inşaat halindeki tesis, Türkiye sınırından 75 km içeride yer almaktaydı. Richard A. Clarke yazdığı kitabında bu olay ile ilgili belirli bir ihtimallerde bulunduğu ve bunun bilişim sistemlerinden kaynaklandığı belirtilmektedir. “Birinci ihtimalde, İsrail, Suriye hava savunmasının üzerine insansız heron uçağı göndermiştir. Basit bir anlatımla, radarlardan gönderilen ışın gökyüzündeki nesneye çarpar, nesneden geri yansıtılarak alıcı radar sistemine döner ve çarpılan nesnenin hangi irtifada uçmakta olduğunu, ne hızla hareket ettiğini ve büyüklüğünü belirlemektedir. Yansıtarak dönen radar elektronik ışını, açık bir bilgisayar kapısı bulunan radar sistemine gökyüzündeki nesneyi bildirir. Ancak arıza nedeniyle heron uçağını görmemiş olabilir veya gördüğü uçağın bilgisi açık kapıdan girerken değişmiştir. İkinci bir ihtimalde, Rus yapımı bilgisayar programı ile çalışan Suriye hava savunma ağına, bilgisayar programı içine yerleştirilmiş olan truva atı virüsüdür. Heron uçağının gönderdiği sinyalle Suriye bilgisayar sisteminin ele geçirilmesi ve yetkinin elinden alınmış olmasıdır. Üçüncü ihtimal ise İsrail ajanlarının Suriye içine girip, fiber optik kabloları keserek kendi kablolarını yerleştirmesi ve sistem on-line olduktan sonra da tuzak kapısının açılmasıdır.” Bu olay hala gizliliğini korumaya devam etmekte olduğu belirtilmektedir (Kenandabirkuyu, 2019).

2.11.1.9. Rusya’ dan Gürcistan’a Karşı Siber Savaş - 2008

2008 yılında Gürcistan ordusu tarafından Güney Osetya topraklarına yönelik düzenlenen operasyon karşısında Rusya Gürcistan’ a karşı hem fiziksel hem de siber savaş başlatmıştır. Bu saldırılarda Gürcistan’ ın dünya ile bağlantılarını kesmek için medyaya ve devletin resmi sitelerine karşı olmuştur. Saldırı türü olarak internet trafiğini destekleyen tüm yönlendiricileri DDoS ile yapılmıştır. En basit banka işlemleri, kredi kartları ve cep telefonları dahi

kullanılamaz hale geldiği ve dış dünyadan haber almayan Gürcistan, dışarıya e-posta bile gönderememiş bunun üzerine Rusya'dan gelen tüm trafiği bloke etmiştir. Ancak Rusya Çin üzerinden siber saldırıya devam ettiği belirtilmektedir (Bookmark, 2019).

2.11.1.10. Çin'de Bir Siber Casusluk Şebekesi (GhostNet) - 2009

Bu saldırı özellikle devlet kurumları, büyükelçilikleri, dışişleri bakanlıkları gibi devletlerarası ilişkilerin yönetildiği makamları hedef alan bir siber casusluk olayıdır. Çin merkezli olduğu belirtilen bu siber olay bu güne kadar İran, Bangladeş, Letonya, Endonezya, Filipinler, Brunei, Barbados ve Bhutan gibi dünyanın 103 farklı ülkesindeki sistemleri hedef aldığı belirtilmektedir. Bu olay 10 aylık bir çalışmanın sonucunda, Tibet' in ruhani lideri Dalay Lama'nın çalışma ofisine yönelik yapılan saldırılarla açığa çıkarıldığı belirtilmektedir (Bookmark, 2019).

2.11.1.11. Filistinden İsraile Siber Saldırı - 2008/2009

27 Aralık 2008 tarihinde İsrail' in Gazze' de başlattığı “Dökme Kurşun” operasyonuna karşılık olarak Müslüman ve Arap Hackerlar tarafından siber saldırılar yapılmıştır. Ortalama 10.000' den fazla web sitesinin etkilendiği belirtilmektedir. Saldırılarda tepki amaçlı ekranlarda mesajlar bırakılmıştır. 27 Aralık 2008 ile 15 Şubat 2009 tarihlerinde “Defacement” olarak bilinen saldırılar özellikle ses getirecek şekilde planlanmıştır. Saldırı yapılan siteler özellikle haber siteleri, siyasi parti siteleri, Savunma Bakanlığı ve Başbakan Yardımcısı Ehud Barak'ın sitesi de dâhil olmak üzere pek çok siteye mesajlar ve görseller eklenerek gerçekleştirilmiştir (Başaran2, 2014).

2.11.1.12. Mavi Marmara Saldırısı - 2010

31 Mayıs 2010 tarihinde İsrail' in ambargo uyguladığı Gazze' ye yardım malzemesi götürmek için, değişik milletlere ve değişik dinlere mensup gönüllüleri ve insani yardım taşıyan gemiler uluslararası sularda olmalarına rağmen İsrail askerlerinin saldırısına uğramıştır. Bu saldırı neticesinde sürekli olarak gemi ile irtibat kurulmuştur ve saldırı öncesinde İsrail tarafından gemiden dünya medyasına yayın yapan uydu frekansı ve uydu telefonlarının iletişimi kesilmiştir. Gönüllülerden 9' u İsrail askerlerin silahlı saldırısı sonucu hayatını kaybetmiştir. İsrail' in, Gazze' ye yardım götüren gemilere saldırmasına tepki göstermek amacıyla değişik haktivist gruplar çok sayıda devlet, şirket ve banka web

sitesine saldırı yapmıştır. İsrail' in özür dilememek için direnmesine tepki olarak, değişik zamanlarda değişik haktivist gruplar tarafından İsrail web sitelerine saldırılar yinelenmiştir (Kenandabirkuyu, 2019).

2.11.1.13. Stuxnet Siber Saldırısı - 2010

Belarus' da yer alan Virusblokada adlı bir bilişim şirketi tarafından Microsoft Windows işletim sisteminde Mayıs ayında zararlı etkileri olabileceğini değerlendirdiği bir virüs tespit edilmiştir. Virüs sisteme bir USB bellek ile bulaştırıldığı tespit edilmiştir. Bu virüs Microsoft ile birlikte Kaspersky ve Symantec bilişim güvenlik ve yazılım şirketlerinin katılımıyla incelendiği ve bu Stuxnet adı verilen virüs yazılımının benzerlerinden çok daha karmaşık bir yapıda olduğu belirtilmiştir. Araştırma sonucunda bu virüs İran' ın Natanz nükleer yakıt-uranyum zenginleştirme tesislerindeki bilgisayar ağlarına Haziran ve Temmuz 2009 tarihlerinde iki adet saldırı gerçekleştirildiği ortaya çıkmıştır.

Stuxnet ilk aşamada tesisin SCADA sistemine bağlı çalışan ve uranyumun ayrıştırılması ile konsantrasyonunu yöneten programlanabilir mantıksal denetleyicileri (PLC) içerisindeki komutlara sızmıştır. Kontrol cihazları kullanılarak her 100 ms bir gönderdiği komutlarla santrifüjlere enerji sağlayan elektriksel akımlar göndermiştir ve frekanlarda dalgalanmalar meydana gelmiştir. Fakat sistem izleme merkezine uygulamada bir anormallik olmadığı bilgisini göndermeye devam etmiştir ve uç birimlerin merkeze gönderdiği verileri kullanmaya devam etmiştir. Böylece 100.000' den fazla bilgisayara sızan bu virüs anakartı hedef alacak şekilde programlandığı belirtilmiştir. Bu sızma İran üzerinde % 59 oranında olduğu belirtilmektedir. MS Windows işletim sistemini kullanan bu virüs Siemens SIMATIC S7-300 modelini kullanan PLC ve SCADA sistemlerini hedef alarak gerçekleştirilmiştir. İlk siber saldırı olarak kritik altyapılarda ele alınmakta olduğu belirtilmiştir.

Bu saldırı Natanz'daki tesisin ve kullanılan SCADA sisteminin internet bağlantısı olmadığı virüsün taşınabilir bir bilgisayar ile yapıldığı düşünülmektedir. Saldırı neticesinde maddi olarak zararların ortaya çıktığı ve bu zararların detayında 1000 adet santrifüjün zarar gördüğü ve bunların 600 adedinin yenisi ile değiştirildiği belirtilmektedir. Uluslararası Atom Enerjisi Kurumu (IAEA) tarafından yayınlanan bir raporda ise İran' ın Stuxnet sonrasında sistem ve üretim kayıplarını telafi ederek uranyum geliştirme programında saldırı öncesi seviyesine kısa

sürede ulaştığı belirtilmiştir (Meral, 2015). Stuxnet' in görevi 3 adımda tamamlanacak kadar basit olup, 1- Bulaş, 2- Sistemi Ele Geçir ve 3- Tesisi İmha Et adımlarından oluşmaktadır.

Bu zararlı kod C programlama dilinde yazıldığı ve Windows işletim sisteminde System32 dosyasının içindeki Isass.exe olarak kendini sisteme tanıtarak yayılması sağlanmıştır. Bu kod malicious olarak bilinmekte ve birçok zararlı Worm içermektedir. Bir Bilgisayar üzerinden Siemens PLC içerisine yerleşen zararlı kodlar reaktörleri besleyen sıcak soğuk su motorlarını kontrol eden frekans konvertörlere 100 ms' de bir komut gönderdiği belirtilmektedir. Belli bir sıcaklıkta olması gereken reaktörler motorları kontrol eden frekans konvertörleri yavaşlama ve hızlanma durumlarının tersi işlem yapılması halinde reaktörlerde arızalar oluşabilmektedir. Hedef reaktörler aktif olmadığı için büyük bir facia yaşanmamıştır. Devlet destekli ve politik bir olay olduğu belirtilmektedir.

2.11.1.14. Night Dragon Siber Saldırısı – 2011

McAfee güvenlik şirketi Şubat 2011' de tarihinde petrol, enerji ve petrokimya şirketlerine yönelik birbiriyle bağlantılı bir dizi siber saldırı tespit edildiğini duyurmuştur. Bu saldırının 2009 yılından beri Çin tarafından organize edildiği tespit edildiği belirtilmiştir.

'Night Dragon' adı verilen olay Stuxnet gibi faaliyetlerin sabote edilmesini sağlamamış olsa da kritik altyapı sistemlerine yönelik olması ve çalınan verilerin ilerleyen zamanlarda daha geniş çaplı ve hasar verici saldırılarda kullanılma ihtimali bulunması açısından önem arz etmektedir (Knapp, 2011). Saldırıların asıl amacı kritik seviyelerdeki verilerin çalınmasını olarak hedeflenmiştir. Hedeflere şirketlerin web sitelerindeki zaafiyetler üzerinden sistemlere giriş yapıldığı ve bilgisayarlara casus yazılımlar yüklenerek verilerin dışarıya çıkartıldığı belirtilmektedir (Çiftçi, 2013).

2.11.1.15. Duqu Adlı Virüs İle Siber Saldırı - 2011

Budapeşte Teknoloji ve Ekonomi Üniversitesi tarafından 1 Eylül 2011 tarihinde yazılımı Stuxnet'e benzeyen ve temel görevi endüstriyel kontrol sistemleri ile ilgili istihbarat toplamak olan Duqu adlı virüsün varlığı duyurulmuştur. Bu virüs bulaştığı cihazlara 'DQ' adlı dosyalar oluşturduğu için bu isimle anılmıştır. Özellikle sistemlere ağlar ve elektronik postalar yoluyla sızarak gelecekte oluşabilecek saldırılarda kullanılmak üzere veriler toplamıştır (Bıçakçı, 2012).

2.11.1.16. Flame Adlı Virüs İle Siber Saldırı - 2012

Mayıs 2012’ de bu kez İran Ulusal Bilgisayar Acil Müdahale Ekibi (CERT) tarafından yerleştiği bilgisayarlarda her türlü sesli görüşmeyi, ekran görüntüsünü ve klavye hareketlerini kaydedebilen, Arapça ve İbranice metinleri analiz edebilen bir kötücül yazılımın tespit edildiği duyurulmuştur (Bıçakçı, 2012). Flame adı verilen yazılım Stuxnetten 20 kat daha büyük ve çok daha karmaşık bir yapıdadır (Wilson, 2012). Yerleştiği bilgisayarın bluetooth özeliğini açarak bağlanabildiği cihazlardan veri toplayabilen, bu yolla ulaştığı akıllı telefonlarda da benzer bilgileri edinebilen yazılımın Orta Doğu’ da pek çok ülkeye ama özellikle İran’ın petrol ve gaz şirketlerine sızdığı tespit edilmiştir. Bu virüs, 2007 tarihinden itibaren kullanılan yazılımın faaliyette olduğu ve 2012 yılına kadar virüsün tespit edilemediği belirtilmektedir. Duqu, Windows’un açıklarından faydalanarak bir Microsoft Word dosyası olarak bilgisayara yerleşiyor ve bu word dosyası hedeflere e-posta yoluyla iletiliyor. Ağ üzerindeki herhangi bir bilgisayar, bu word dosyasını açarak Duqu’ yu içeri aldığı takdirde, saldırganlar sisteme uzaktan erişip bilgi çalabildikleri belirtilmektedir.

2.11.1.17. Kanada Telvent Firmasına Siber Saldırı - 2012

10 Eylül 2012 tarihinde, enerji sektörüne uzaktan yönetim ve izleme araçları sağlayan bir şirket olan, Telvent, Kanada’ nın iç güvenlik duvarı ve güvenlik sistemleri üzerinde bir ihlal tespit edildi. Ağa girdikten sonra, davetsiz misafirlerin, şirketlerin eski BT ekipmanlarını modern akıllı şebeke teknolojisiyle birleştirmelerine olanak tanıyan bir uzaktan yönetim aracı olan OASyS SCADA ürünü ile ilgili proje dosyalarını çaldı. Düşmanların bu yeni ürün hakkında, güvenlik açıklarını bulmak ve enerji sektöründe SCADA sistemlerine karşı gelecekteki saldırılara hazırlanmak için bilgi toplaması çok olası olduğu belirtilmektedir (Do vd., 2017).

2.11.1.18. Regin Adlı Bir Virüs İle Siber Saldırı - 2014

2014 yılı kasım ayında ise bilgisayar güvenlik şirketi Symantec tarafından en gelişmiş bilgisayar virüsünün tespit edildiği duyurulmuştur. Regin adı verilen gelişmiş siber tehdidin, yerleştiği bilgisayarlarda ekran görüntüsünü alma, şifreleri çalma ve silinen dosyaları yükleme işlemlerini yapabildiği belirtilmiştir. 2008 yılından beri aktif şekilde çalıştığı bildirilen virüsün çok katmanlı olarak tanımlanan kriptolu yazılımı henüz tam anlamıyla çözümlenememiştir. Yazılımının üst düzey teknik yapısı ve kod uzunluğu dikkate alındığında bir kuruluş ya da devlet desteğiyle tasarlandığı değerlendirilen Regin; aralarında Rusya, Suudi Arabistan,

Meksika ve İrlanda' nın olduğu pek çok ülkeye ait kamu ve özel sektör kuruluşları, enerji, telekomünikasyon, sağlık gibi altyapıları hedef aldığı belirtilmiştir (Symantec, 2014).

2.11.1.19. Equation Grubu Adlı Siber Saldırı - 2014

Bu grup çok donanımlı ve çok yönlü olma özelliği ile ve kullandıkları şifreleme algoritmaları, gizlenme yöntemleri ve saldırı esnasında kullandıkları gelişmiş tekniklerle şimdiye kadar görülen en tehlikeli grup olarak belirtilmektedir. Bu grup kötü amaçlı olan yazılımlar için GrayFish, Fanny ve EquationDrug one olarak isimlendirmeler yapmışlardır. Equation grubu saldırıları gerçekleştirirken kendini çoğaltabilen solucandan (Fanny), CD-ROM gibi fiziksel medya aygıtlarından veya web tabanlı açıklardan yararlanmaktadırlar. Kullandıkları şifreleme algoritmaları RC5, RC6 ve XOR şifreleme teknikleridir. İran, Rusya, Pakistan başta olmak üzere 30' un üzerinde ülkede faaliyet göstermektedirler. Hedeflerinde hükümet ve diplomatik kurumlar, telekomünikasyon sistemler, nükleer enerji, doğal gaz üretim ve askeri tesisler vardır (Akın, 2016).

2.11.1.20. Almanya Demir Çelik Tesislerine Yapılan Siber Saldırı - 2014

Almanya' da Aralık 2014' te demir çelik üretim tesislerine yönelik saldırılarda ele geçirilen endüstriyel kontrol sistemleri kullanılarak maden etirme sisteminin düzgün kapatılamamasına sebep olduğu ve üretimin durduğu belirtilmektedir. Saldırı sonrasında meydana gelen maddi zarar ve nasıl gerçekleştiğine dair detaylar paylaşılmazken siber saldırının doğrulandığına yönelik haberler yayınlanmıştır (Baltaş, 2014).

2.11.1.21. Ukrayna' da Elektrik Şebekesine Siber Saldırı - 2015

Ukrayna elektrik şebekesine Aralık 2015 tarihinde kritik bir siber saldırı yapıldığı belirtilmektedir. Tesisin akım kesicilerine saldırganlar tarafından ele geçirilen erişim şifreleri ile müdahale edilmiş ve 250.000 tüketici elektriksiz kaldığı belirtilmektedir (Securitynewsdesk, 2018). Yaşanan siber saldırı sonucu belirli süre şehirlere elektrik verilemedi. Bu saldırıda kullanılan atak vektörü ise çok tanıdık bir yöntem olduğu, Ukrayna parlementesundan geliyormuş gibi gösterilen bir e-posta ile makro'lu bir excelin son kullanıcı tarafından indirilmesi amaçlanmış ve makronun çalışması ile birlikte ilgili zararlı yazılımın farklı zararlı yazılımları indirilmesi sağlanmıştır. Bu atak vektöründe yeni olan nokta ise zararlı yazılım ile ICS-SCADA (Endüstriyel Kontrol Sistemleri) bileşenlerinin devre dışı bırakılmasıdır.

2.11.1.22. Duqu 2.0 Adlı Siber Saldırı - 2015

Duqu 2.0 adlı siber saldırı 2011 yılında ortaya çıkan Duqu saldırısının daha gelişmiş bir versiyonu olarak ortaya çıkmıştır. Ayrıca bu saldırıda üç adet sıfır gün açıklarından faydalanarak kötü amaçlı yazılımlar kullanıldığı belirtilmektedir. Duqu 2.0 saldırısı sızıntı yapılan bilgisayarların hafızasında kod gizleme özelliği ortaya çıkarılmıştır. Birleşmiş Milletlerin beş daimi üyesi olan Rusya, ABD, Çin, Fransa ve İngiltere' nin yanı sıra Almanya' yı kapsayan P5+1 olarak adlandırılan ülkelerin birlikte yaptığı faaliyetleri hedef almıştır (Akın, 2016).

2.11.1.23. İngiltere' deki WannaCry Siber Saldırısı - 2016

2016 yılında WannaCry fidye saldırısı dünya çapında 300.000' den fazla bilgisayara bulaşmıştır. Korkutucu olan, virüs bir e-posta olarak yayıldı. İngiltere Ulusal Sağlık Hizmetleri (NHS) saldırıya yakalandı. Sonuç olarak, ameliyatlar iptal edildi, personel işlemleri yapmakta zorlandı ve sadece acil hastalar tedavi edildiği belirtilmektedir (Securitynewsdesk, 2018).

2.11.1.24. ABD DDoS Mirai Saldırısı - 2016

20 Ekim 2016 yılında "Mirai", "Mirai Botnets" adında kullanılan zararlı yazılımın ABD hükümetine ait kurum ve kuruluşların sitelerine yönelik olup sitelerin çöktüğü belirtilmektedir. Ülkenin yüzde 78' inden fazlasının internetsiz kaldığı ve maddi zararın ise 7 milyar doları bulduğu ifade edilmektedir. Saldırı kaynağının Rusya ve Çin üzerindeki 14 milyondan fazla IP adresinden Amerika Birleşik Devletleri hedef alınarak yapıldığı belirtilmektedir. Cuma günü yapılan saldırı için yaklaşık 100.000 adet cihaz kullanıldığı ve Çarşamba gününe kadar Mirai zararlı yazılımının yaklaşık 500.000 cihaza bulaştığı ifade edilmektedir (Computerworld, 2016).

2.11.1.25. Schneider Elektiriğe Ait Elektrik Üretim Santraline Yapılan Siber Saldırı - 2017

Fransız şirketi Schneider Electric, endüstriyel kontrol sistemlerini bir malware saldırısından sonra Orta Doğu' daki bir santralin faaliyetlerini durdurmaya zorlanmıştır. Güvenlik araştırmacıları tarafından yapılan analiz, saldırının bir ulus devlet tarafından desteklendiğini göstermiştir (CSIS, 2018).

2.11.1.26. Uber Firmasına Yapılan Siber Saldırı - 2017

Uber, isim, telefon numarası, e-posta adresi ve plaka numarası da dahil olmak üzere, 57 milyon müşterisinin ve sürücüsünün çalıntı verilerini silmek için bilgisayar korsanlarına 100.000 dolar ödediğini açıklamıştır (CSIS, 2018).

2.11.1.27. NotPetya Siber Saldırısı - 2017

27 Haziran tarihinde meydana gelen bu saldırı daha önceki saldırılarda olduğu gibi tespit edilemeyen bir koordinasyonla Ukrayna' nın devlet kurumları ve Ukrayna' daki büyük şirketler birinci dalga saldırıdan etkilenmişlerdir. Bu olay daha önceden kurum ve şirketlerin ağlarına virüs sızmış ve saldırının etkisini artırmak için keşifler saldırganlar tarafından çok önceden yapıldığı belirtilmektedir. Salırganlar Ukrayna devlet kurumlarında kullanılan yazılımdaki açığı bularak gerçekleştirmişlerdir. Bu bir vergi yazılımı olup bulunduğu sistemlerde Yönetici (Administrator) ve/veya Etki Alanı Yöneticisi (Domain Administrator) yetkileriyle çalıştığı belirtilmektedir. Saldırıdan etkilenen cihazlardaki veriler kriptolandığı ve sistemlerin boot edemez hale geldiği belirtilmektedir (Biznet, 2019).

2.11.1.28. Amadeus Uçuş Rezervasyon Sisteminde Bulunan Güvenlik Zafiyeti - 2019

Bu siber saldırı 2019 yılı Ocak ayında gerçekleşmiş olup dünyadaki 141 havayolunun müşterilerini etkilediği belirtilmektedir. Uçak bileti rezervasyon sistemindeki zafiyet, bilgisayar korsanlarının, müşterilerin bilet detaylarına erişmesine ve bunları değiştirmesine izin verdiği anlaşılmıştır. Güvenlik zafiyeti, şu anda United Airlines, Lufthansa ve Air Canada dahil olmak üzere yaklaşık 141 uluslararası havayolu şirketi tarafından kullanılan Amadeus tarafından geliştirilen, çevrimiçi uçuş rezervasyon sisteminde ortaya çıkmıştır.

Potansiyel saldırganlar, Safety Detective's Noam Rotem' in bulduğu Amadeus çevrimiçi rezervasyon sistemindeki güvenlik sorunu nedeniyle milyonlarca büyük uluslararası havayolu şirketinin müşterileri tarafından yapılan uçuş rezervasyonlarındaki özel bilgileri görüntüleyebilir ve değiştirebilir.

Şu anda, Amadeus bilet rezervasyon sistemi, dünya çapındaki çevrimiçi rezervasyon pazarının % 44' ünü kontrol eden 141 uluslararası havayolu tarafından kullanılıyor ve United Airlines, Lufthansa ve Air Canada, bazı müşterilerinden biridir (Bleepingcomputer, 2019).

2.11.2. Türkiye’ de Yaşanan En Önemli Siber Saldırıları

Burada yapılan çalışmalar özellikle Türkiye’ de yaşanan siber saldırılar, olaylar ve saldırı türleri üzerine yapılmıştır. Yapılan çalışmalar kronolojik sıralama olarak verilmiştir ve yaşanmış olaylar kısaca özetlenmiştir. Bu araştırmalar yapılacak çalışmalara motivasyon olmuştur.

2.11.2.1. Batman Hidroelektrik Santrali Vakası - 2003

Almanya’ da bulunan Noel firması 2003 yılında Batman Hidroelektrik barajının yapımını üstlenmiş ve alacaklarını tahsil edemeyince şirket bilgisayarlarını kilitleyip şehri terk etmişlerdir. Bu olayın sonucu olarak 3 üniteye üretim durmuştur (Kaya, 2012).

2.11.2.2. İMKB Fiber Optik Kablo Vakası - 2007

28 Kasım 2007 tarihinde gerçekleşen bu olay bir kepçe operatörünün fiber optik kabloyu koparmasından dolayı İMKB borsasında işlemler ertesi gün 14:30’ a kadar yapılamamış ve büyük maddi zarar oluşmuştur (Kaya, 2012).

2.11.2.3. Bakü-Tiflis-Ceyhan Petrol Boru Hattına Siber Saldırı - 2008

Erzincan’ daki petrol boru hattına yapılan saldırıda 3 hafta boyunca hat kullanılamamış ve ortalama 1 milyar dolar zarar meydana gelmiştir. İlk olarak terör saldırısı olarak düşünülmüş, fakat olayın bir teknik arızadan kaynaklandığı ortaya çıkarılmıştır.

“Aralık 2014’ te Bloomberg International tarafından bu patlamanın siber saldırı olduğu iddiası ortaya atılmıştır. İddiaya göre; güvenlik kameralarını kullanarak sisteme giriş yapan bilgisayar korsanları kontrolü ele geçirdikten sonra basınç sensörlerini devre dışı bırakmış ve böylece artan basınç ile patlama gerçekleşmiştir. Aynı anda SCADA üzerindeki alarm sistemi etkisiz bırakılarak saldırının ancak 40 dakika sonra alevlerin görülmesiyle fark edilebilmesi sağlanmıştır. Enerji ve Tabii Kaynaklar Bakanı tarafından haber ile ilgili sorulara cevaben; güvenlik kameralarının olay esnasında var olmadığından dolayı, iddiaların asılsız olduğu ifade edilerek, soruşturmanın devam ettiği eklenmiştir” (Meral, 2015).

2.11.2.4. Atatürk Havalimanı Bilgisayarlarına Yapılan Siber Saldırı - 2009

30 Ocak 2009 tarihinde ‘Conficker’ adındaki bir virüsün, birçok ülkenin bilgisayar sistemine yayılabilen ve önemli zararlar verebilen özelliklerde olduğu belirtilmektedir. Bu virüs

İstanbul'da Atatürk Havalimanı' nın dış hatlar terminalinde çalışan bilgisayarları ciddi şekilde etkilediği belirtilmektedir (Şenol, 2016).

2.11.2.5. Telekomünikasyon İletişim Başkanlığı Web Sayfasına Yapılan Siber Saldırı – 2011

Anonymous adlı siber saldırı korsanları 9 Haziran 2011 tarihinde akşam saatlerinde BTK' nın internet sitesine saldırmış ve devre dışı kalan web sitesi çalışmaya gece yarısından sonra hizmet vermeye başladığı belirtilmektedir (Şenol, 2016).

2.11.2.6. 155 Polis İhbar Hattı Vakası - 2012

Kızıl Hacker grubu olarak ile bilenen saldırganlar 27 Şubat 2012 tarihinde Ankara ve Kırıkkale Emniyet Müdürlüklerinin internet üzerinden çalışan 155 polis ihbar hattının şifreleri kırılmış ve belgeler ele geçirilmiştir. Bu belgeler internet üzerinden sızdırılmıştır ve belgeler kişisel bilgiler içermektedir (Kaya, 2012).

2.11.2.7. Türkiyede Yaşanan Elektrik Kesintisi Siber Saldırısı - 2015

Van ve Hakkari illerimiz hariç 31 Mart 2015 tarihinde elektriğin İran' dan karşılandığı 79 ilde ülke genelinde elektrik kesintisi yaşanmıştır. Bu olay ile ilgili uzmanların görüşü; “Yüklü bir hattın devre dışı kalmasının tüm sistem dinamiğini bozması, ardından diğer hatların bir arıza olduğunu düşünerek kademeli olarak kendilerini kapatması...” şeklinde olmuştur. Bu olayların yaşanmasından hemen sonra ise, “TEİAŞ Siber Saldırıları Engellemek için Bilgisayar Ağları İhalesine Çıkıyor” haberi basında yer aldığı belirtilmektedir (Şenol, 2016).

2.11.2.8. Devlet Kurumlarına ve Bankalara Yapılan Siber Saldırıları - 2015

Özellikle ‘tr’ uzantılı alan adlarının yönetildiği sunucular, bankalar, noterler ve diğer devlet kurumlarına 14 Aralık 2015 tarihinde başlayıp ve yaklaşık 10 gün süren bu siber saldırılar nedeniyle erişim yapılamadığı belirtilmektedir. Ayrıca bu saldırılar sonucunda mobil uygulamalarında etkilediği ortaya çıkmıştır. Saldırıları özellikle internet trafiğini büyük ölçüde etkilediği ve bu siber saldırıların dünya genelinde yaşanan en yoğun yaşanan saldırılardan biri olduğu belirtilmektedir (Şenol, 2016).

Özellikle Garanti Bankası, İşbank, Akbank başta olmak üzere bir çok bankanın internet sitesi erişilemez duruma geldiği ve internet bankacılığı dışında POS cihazlarının da çalışmaması nedeniyle siber saldırı, günlük hayatı da etkilediği belirtilmektedir.

2.11.2.9. Sağlık Bakanlığı Hastanelerine Yönelik Siber Saldırıları - 2016

Sağlık Bakanlığı' na bağlı hastanelere 18 Mayıs 2016 günü sabah saatlerinde saldırıların başladığı ve 33 devlet hastanesinin veri tabanlarında bulunan verilerin kopyalandıktan sonra silindiği belirtilmiştir. Bu siber saldırıları 'Anonymous' adlı grubun üstlendiği ve Sağlık Bakanlığı sistemlerinin kısmen etkilendiği belirtilmiştir. Ayrıca sistemlerdeki yedekleme mekanizması sayesinde olası veri kayıplarının önüne geçildiğini belirtilmiştir (Şenol, 2016).

2.11.2.10. Garanti Bankası' na Yapılan Siber Saldırı – 2019

Garanti Bankası tarafından sitesinde yayınlanan bildiride “Dijital kanallarımızdaki hizmetlere erişimin yavaşlatılması ya da engellenmesine yönelik, DDOS (Dağıtık Hizmet Engelleme) olarak adlandırılan bir atak mevcuttur.” açıklaması yapılmıştır (Garanti, 2020).

2.11.2.11. Türk Telekom' a Yapılan Siber Saldırı - 2020

Türk Telekom'a ait DNS sunucularına siber saldırı yapılarak hizmet kesintisine sebep olmuştur. Bu saldırı tipi en yaygın olan siber saldırı yöntemlerinden biridir. Bu saldırı için botnetler kullanılmaktadır.

2.12. OLGUNLUK MODELLERİNİN ARAŞTIRILMASI VE MODEL KURULUMU

Bu bölümde olgunluk modelinin genel olarak tanımlanması ve dünya genelinde farklı sektörlerle ait olgunluk modellerinin araştırılması hedeflenmiştir. Ayrıca tezin amacına uygun olarak kurulacak olgunluk modelinin ülkemiz için öneminin belirtmesi ve özellikle ihtiyaç olduğuna katkı sağlayacaktır.

2.12.1.Olgunluk Modeli

Olgunluk modeli, kuruluşların mevcut durumlarının belirlenmesine ve aşamalı bir mimari oluşturulmasına olanak tanımalıdır. Mevcut durum tespitiyle birlikte, olgunluk modelinde ulaşılması hedeflenen seviye de adreslenmelidir. Mevcut durumdan hedeflenen seviyeye geçiş

için yapılması gerekenler bir iyileştirme planı kapsamında ele alınmalıdır. Bu noktada kritik başarı faktörleri aşağıdakiler olacaktır.

- Olgunluk modelini belirleme,
- Olgunluk modeline göre mevcut durum belirleme,
- İyileştirme planı ve aksiyonların alınması (Bu aksiyonlar eğitim ve gerekli süreçlerin oluşturulmasına ek olarak teknik önlemleri de içermelidir. Alınabilecek temel önlemler aşağıda detaylandırılmıştır.

Olgunluk modeli, belirli bir disiplinde yetenek ve ilerlemeyi temsil eden bir dizi özellik, özellik, gösterge veya modeldir. Model içeriği tipik olarak en iyi uygulamaları örneklendirir ve standartların veya mevcut süreçlerin diğer uygulama kurallarını içerebilir.

Dolayısıyla bir olgunluk modeli, bir kurumun uygulamalarının, süreçlerinin ve yöntemlerinin mevcut yetenek seviyesini değerlendirebileceği ve iyileştirme için hedef ve öncelikleri belirleyebildiğine dair bir kıyaslama sağlar.

Ayrıca, bir model belirli bir endüstride yaygın olarak kullanıldığında (ve değerlendirme sonuçları paylaşılsa), kuruluşlar performanslarını diğer kurumlarla kıyaslayabilir. Bir endüstri, üye kuruluşların yeteneklerini inceleyerek genel olarak ne kadar iyi performans gösterdiğini belirleyebilir.

2.12.2. Uluslararası Siber Güvenlik Olgunluk Modelleri

Dünya genelinde olgunluk modellerine bakıldığında bazı sektörlere yönelik genel olarak çalışmaların yapıldığı gözlemlenmiştir. Bu sektörlere yönelik hazırlanmış olan çalışmalar ve modeller incelenerek detaylar aşağıda verilmiştir.

2.12.2.1. NISTIR 7628 (National Institute of Standards and Technology Interagency Report) Akıllı Şebeke Siber Güvenlik Kılavuzu (2010)

Bu standart, akıllı şebeke teknolojilerinde riski değerlendirmek ve uygun güvenlik gereksinimlerini ve gizlilik önerilerini seçmek için çeşitli kuruluşlara rehberlik eder. Bu kılavuzun ilk versiyonu 2010 yılında ve son versiyonu ise 2014 yılında yayınlanmıştır. Günümüzde bu rapor artık yayımlayan kurum tarafından geri çekilmiştir.

2.12.2.2. ONG-C2M2 (Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model) Petrol ve Doğal Gaz Alt Siber Güvenlik Yeteneği Olgunluk Modeli (2014)

Bu model, yalnızca bilgi teknolojisi (IT) ve operasyonel teknoloji (OT) ile ilişkili siber güvenlik uygulamalarının ve içinde çalıştıkları ortamların uygulanması ve yönetimine yönelik olması amaçlanmıştır. Her tür kuruluşa tekrarlanan siber saldırı, gelişmiş siber güvenliğe ihtiyaç duyulduğunu göstermektedir. Siber tehditler büyümeye devam ediyor ve modern organizasyonların karşılaştığı en ciddi operasyonel risklerden birini temsil ediyor. Birleşik Devletlerin ulusal ve ekonomik güvenliği, Nation'un kritik altyapısının bu tür tehditler karşısında güvenilir bir şekilde işlemesine bağlıdır. Kritik altyapının ötesinde, ulusun ekonomik canlılığı her tür kuruluşun sürekli çalışmasına bağlıdır. Petrol ve Doğal Gaz Alt Siber Güvenlik Yeteneği Olgunluk Modeli (ONG-C2M2) her tür petrol ve doğal gaz (ONG) organizasyonunun siber güvenlik programlarını değerlendirmesine ve iyileştirmelerine yardımcı olabilir (Energy, 2019).

- ONG (Oil and Natural Gas) alt sektöründeki siber güvenlik yeteneklerini güçlendirmek,
- ONG organizasyonlarının siber güvenlik yeteneklerini etkin ve tutarlı bir şekilde değerlendirme ve kıyaslama yapmalarını sağlamak,
- Bilgi, en iyi uygulamalar ve alt sektördeki ilgili referansları siber güvenlik yeteneklerini geliştirmek için bir araç olarak paylaşmak,
- ONG organizasyonlarının siber güvenliği geliştirmek için eylemlere ve yatırımlara öncelik vermelerini sağlamak.

2.12.2.3. ES-C2M2 (Electricity Subsector Cybersecurity Capability Maturity Model) Elektrik Alt Sektör Siber Güvenlik Yetenek Olgunluk Modeli (2014)

Bu model her türlü elektrik alt sektör kuruluşunun siber güvenlik programlarını değerlendirmesine ve iyileştirmelerine yardımcı olabilmektedir. ES-C2M2, bir kurumun siber güvenlik programını ölçmesi ve geliştirmesi için bir öz değerlendirme metodolojisi ve araç seti ile kullanılmak üzere tasarlanmıştır. Ek olarak, model yeni bir siber güvenlik programının geliştirilmesini de bilgilendirebilmektedir (Energy, 2019).

- Elektrik alt sektöründeki siber güvenlik yeteneklerinin güçlendirmek,

- Siber güvenlik yeteneklerini etkin ve tutarlı bir şekilde değerlendirmek ve karşılaştırmak için yardımcı programları kullanmak,
- Bilgi, en iyi uygulamalar ve alt sektördeki ilgili referansları siber güvenlik yeteneklerini geliştirmek için bir araç olarak paylaşmak,
- Siber güvenliği geliştirmek için eylemlere ve yatırımlara öncelik vermek için kamu hizmetleri kurulmasını sağlamak.

2.12.2.4. C2M2 (Cybersecurity Capability Maturity Model) Siber Güvenlik Yetenek Olgunluk Modeli (2014)

Siber tehditler büyümeye ve modern organizasyonların karşılaştığı en ciddi operasyonel risklerden birini temsil etmeye devam etmektedir. Birleşik Devletlerin ulusal ve ekonomik güvenliği, ulusların kritik altyapısının bu tür tehditler karşısında güvenilir bir şekilde işlemesine bağlıdır. Kritik altyapının ötesinde, ulusun ekonomik canlılığı her tür kuruluşun sürekli çalışmasına bağlıdır. Siber Güvenlik Yetenek Olgunluk Modeli (C2M2), tüm sektörlerin, türlerin ve büyüklükteki kuruluşların siber güvenlik programlarını değerlendirmesine ve iyileştirmelerine yardımcı olabilir. C2M2, bilgi teknolojisi (IT) ve operasyonel teknoloji (OT) varlıkları ve içinde çalıştıkları ortamlar ile ilişkili siber güvenlik uygulamalarının uygulanması ve yönetimine odaklanmaktadır (Energy, 2019).

- Kuruluşların “siber güvenlik yeteneklerini” güçlendirmek,
- Kuruluşların siber güvenlik yeteneklerini etkin ve tutarlı bir şekilde değerlendirme ve karşılaştırmalarını sağlamak,
- Bilgi, en iyi uygulamalar ve siber güvenlik yeteneklerini geliştirmenin bir aracı olarak kuruluşlar arasındaki ilgili referansları paylaşmak,
- Kuruluşların siber güvenliği geliştirmek için eylemlere ve yatırımlara öncelik vermesini sağlamak.

2.12.2.5. Enerji Sektörü Siber Güvenlik Çerçevesi Uygulama Rehberi (Energy Sector Cybersecurity Framework Implementation Guidance-2015)

Enerji sektörü kuruluşları, kesintisiz hizmet sağlayan siber güvenlik standartlarını, araçlarını ve süreçlerini geliştirmek için birlikte çalışma konusunda güçlü bir geçmişe sahiptir. Enerji sektörüne özel kurum olarak ABD Enerji Bakanlığı, özellikle enerji sektörü sahipleri ve

işletmecileri için bu çerçeve uygulama rehberinin geliştirilmesi için elektrik sektöründe ve petrol ve doğal gaz altında koordinatör kurumlar ile birlikte çalışmaktadır. Enerji sektörünün risk ortamına ve kuruluşların özel bu çerçeveyi uygulamak için kullanabilecekleri siber güvenlik ve risk yönetimi araçlarına ve süreçlerine göre düzenleme yapılmıştır.

Bu çerçeve uygulama rehberi, enerji sektörü kuruluşlarına şu konularda yardımcı olmak için tasarlanmıştır:

- Mevcut ve hedef siber güvenlik duruşlarını karakterize etmek.
- Çerçeveyi bir rehber olarak kullanarak mevcut siber güvenlik risk yönetimi programlarındaki boşlukları ve mevcut uygulamaların çerçeveyi aşabileceği alanları belirlemek.
- Mevcut sektör araçlarının, standartlarının ve yönergelerinin çerçeve uygulamasını destekleyebileceğini kabul etmek.
- Risk yönetimi yaklaşımlarını ve çerçevenin kullanımını hem iç hem de dış paydaşlara etkin bir şekilde göstermek ve iletmek.

2.12.2.6. Uluslar İçin Siber Güvenlik Kapasitesi Olgunluk Modeli (CMM-Cybersecurity Capacity Maturity Model) (2016)

Küresel siber güvenlik kapasite merkezi' nin amacı, hem siber güvenlik kapasite olgunluk modeli' nin (CMM) uygulanması ile hem İngiltere' de hem de uluslararası olarak siber güvenlik kapasite geliştirmenin ölçeğini ve etkinliğini arttırmaktır. Kapasite merkezi bu bilgiyi siber güvenlik kapasitelerini arttırmaya yardımcı olmak için hükümetlere, topluluklara ve kuruluşlara açık hale getirecektir. Ulusal siber güvenlik kapasitesinin artırılmasına yardımcı olarak, kapasite merkezi herkes için refah, insan hakları ve refahın desteklenmesi için yenilikçi bir siber ortamın tanıtımına yardımcı olmayı hedeflemektedir (Afyonluoglu, 2019).

Şu anda siber güvenlik kapasitesinin beş boyuttan oluştuğunu düşünülmektedir:

1. Siber güvenlik politikası ve stratejisinin geliştirilmesi,
2. Toplum içinde sorumlu siber güvenlik kültürünün teşvik edilmesi,
3. Siber güvenlik bilgisinin geliştirilmesi,
4. Etkili yasal ve düzenleyici çerçeveler oluşturmak,
5. Standartlar, kuruluşlar ve teknolojiler aracılığıyla risklerin kontrol altına alınması. |

3. MALZEME VE YÖNTEM

3.1. OLGUNLUK MODELİ KURULMASI

Olgunluk modellerinin bir çok faydaları bulunmaktadır. Modeller bir sistemin gerçek durumunu ortaya koyan ve izin veren bir inceleme araçlardır. Sonuçlarda ortaya çıkan güçlülük ve zayıflık kavramı, uygulamalara öncelik vermek için bir taslak görevi görebilir. Ayrıca doğru olgunluk modeli sistem kullanıcıları için belirli bir stratejik süreç hakkında farkındalık yaratabilir.

Olgunluk modellerinin kullanımı süreç ve sistemlerin iyileştirilmesinde faydalar sağlamaktadır. Bu doğrultuda akıllı doğal gaz şebekelerine ait sistemlerinin siber güvenlik açıklarının belirlenmesi ve olgunluk seviyelerini ölçmek için bir kaç olgunluk modelleri karşılaştırıldı. Burada aşamalar olarak yol haritası, olgunluk değerlendirmesi ve olgunluk modeli seviyesi olarak belirlenmektedir (Volker, 2011). Süreçleri değerlendirmek için bu olgunluk seviyeleri ve bu seviyelerin oluşmasına yardımcı olacak olan soru setlerine ihtiyaç bulunmaktadır. İlave olarak, süreç iyileştirme konusunda tavsiyelerde bulunmaktadır. Kavramsal olgunluk modeli, kavramsal bir formdaki güvenlik açısından hedeflerin, düzeylerin ve süreç alanlarının kombinasyonu olarak düşünülebilir. Matris yapısı, güvenlik hedefleri değerlendirerek bir sistemi analiz etmek için kullanılabilir. Ayrıca, olgunluk modeli bir kurumun siber güvenlik açısından mevcut zayıflıklarını ve bir sistemin bunlara karşı dayanıklılığını ölçmeye yardımcı olmaktadır. Yol haritası, sistemler üzerindeki siber güvenlik açısından zayıflıkların iyileştirilmesi ve işletme sürekliliği için gereklidir.

Akıllı doğal gaz şebekelerinde dağıtım ağlarında kullanılan sistemlerin siber güvenlik açısından ve alternatifler arasında değerlendirilmesi için çok kriterli karar verme teknikleri kullanılmaktadır (Espie, 2003). Electra, promethee ve topsis vb. birçok karar verme yöntemi vardır. Fakat bu çalışmada Analitik Hiyerarşi Süreci (AHP) yöntemini tercih ettik çünkü AHP, hiyerarşik derecelendirme için kullanılabilir güçlü bir araçtır. Karmaşık kararları incelemek için yapılandırılmış bir yöntemdir. Örneğin, sürdürülebilir elektrik üretim sistemi için yenilenebilir enerji kaynaklarının seçiminde AHP' den faydalanılır (Ahmad, 2014).

Doyısıyla, söz konusu olgunluk modelleri yardımıyla akıllı şebeke siber güvenlik olgunluk modeli oluşturulur. Birçok farklı metot ve olgunluk modelleri incelenmiştir. Tüm bileşenlerin,

AHP yöntemi ile önem ağırlıklarını belirlenir. Bu sistemlere ait KPI ve soru setleri belirlenir ve sistemlerin siber güvenlik açısından olgunluk seviyeleri hesaplanır.

Örnek alınan kurumlar için bir durum çalışması yapılacak ve bu bölümde akıllı doğal gaz şebekelerinde dağıtımını kolaylaştıran tüm otomasyon sistemlerinin çalışma prensibine ve değerlendirilmesine odaklanılacaktır. Doğal gaz altyapısının tüm akıllı şebeke bileşenleri siber güvenlik açıkları açısından incelenecek ve tespitler yapılarak yol haritası sunulacaktır.

3.1.1. Analitik Hiyerarşi Proses (AHP)

Analitik Hiyerarşi Proses (AHP), ilk olarak 1968 yılında Myers ve Alpert ikilisi tarafından ortaya atılmış ve 1977 de ise Saaty tarafından bir model olarak geliştirilerek karar verme problemlerinin çözümünde kullanılabilir hale getirilmiştir. AHP, karar hiyerarşisinin tanımlanabilmesi durumunda kullanılan, kararı etkileyen faktörler açısından karar noktalarının yüzde dağılımlarını veren bir karar verme ve tahminleme yöntemi olarak açıklanabilir. AHP bir karar hiyerarşisi üzerinde, önceden tanımlanmış bir karşılaştırma skalası kullanılarak, gerek kararı etkileyen faktörler ve gerekse bu faktörler açısından karar noktalarının önem değerleri açısından, birebir karşılaştırmalara dayanmaktadır. Sonuçta önem farklılıkları, karar noktaları üzerinde yüzde dağılıma dönüşmektedir.

Bir karar verme probleminin AHP ile çözümlenebilmesi için gerçekleştirilmesi gereken aşamalar aşağıda tanımlanmıştır. Her bir aşamada, formülasyon ile birlikte ilgili açıklamalar yapılmıştır.

3.1.2. Olgunluk Modeli Kurulum Adımları

Adım 1 : Karar Verme Problemi Tanımlanır

Karar verme probleminin tanımlanması, iki aşamadan oluşturulur. Birinci aşamada karar noktaları saptanır. Diğer bir deyişle karar kaç sonuç üzerinden değerlendirilecektir sorusuna cevap aranır. İkinci aşamada ise karar noktalarını etkileyen faktörler saptanır. Bu çalışmada karar noktalarının sayısı m , karar noktalarını etkileyen faktör sayısı ise n ile sembolize edilmiştir. Özellikle sonucu etkileyecek faktörlerin sayısının doğru belirlenmesi ve her bir faktörün detaylı tanımlarının yapılması, ikili karşılaştırmaların tutarlı ve mantıklı yapılabilmesi açısından önemlidir.

Adım 2 : Faktörler Arası Karşılaştırma Matrisi Oluşturulur

Faktörler arası karşılaştırma matrisi, $n \times n$ boyutlu bir kare matristir. Bu matrisin köşegeni üzerindeki matris bileşenleri 1 değerini alır. Karşılaştırma matrisi aşağıda gösterilmiştir.

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \quad (3.1)$$

Karşılaştırma matrisinin köşegeni üzerindeki bileşenler, yani $i = j$ olduğunda, 1 değerini alır. Çünkü bu durumda ilgili faktör kendisi ile karşılaştırılmaktadır. Faktörlerin karşılaştırılması, birbirlerine göre sahip oldukları önem değerlerine göre birebir ve karşılıklı yapılır. Faktörlerin birebir karşılıklı karşılaştırılmasında önem skalası kullanılır.

Örneğin birinci faktör üçüncü faktöre göre karşılaştırmayı yapan tarafından daha önemli görünüyorsa, bu durumda karşılaştırma matrisinin birinci satır üçüncü sütun bileşeni $i = 1, j = 3$ olduğunda 3 değerini alacaktır. Aksi durumda yani birinci faktörün üçüncü faktörle karşılaştırılmasında, daha önemli tercihi üçüncü faktörden yana kullanılacaksa bu durumda karşılaştırma matrisinin birinci satır üçüncü sütun bileşeni $1/3$ değerini alacaktır. Aynı karşılaştırmada birinci faktörle üçüncü faktörün karşılaştırılmasında faktörler eşit öneme sahip oldukları yönünde tercih kullanılıyorsa bu durumda bileşen 1 değerini alacaktır.

Karşılaştırmalar, karşılaştırma matrisinin tüm değerleri 1 olan köşegeninin üstünde kalan değerler için yapılır. Köşegenin altında kalan bileşenler için ise doğal olarak (3.2) formülünü kullanmak yeterli olacaktır.

$$a_{ji} = \frac{1}{a_{ij}} \quad (3.2)$$

Yukarıda verilen örnek dikkate alınırsa karşılaştırma matrisinin birinci satır üçüncü sütun bileşeni ($i = 1, j = 3$) 3 değerini alıyorsa, karşılaştırma matrisinin üçüncü satır birinci sütun bileşeni ($i=3, j=1$), (3.2) formülünden $1/3$ değerini alacaktır.

Tablo 3.1: AHP Önem Skalası

Önem Değerleri	Değer Tanımları
1	Her iki faktörün eşit öneme sahip olması durumu
3	1. Faktörün 2. faktörden daha önemli olması durumu
5	1. Faktörün 2. faktörden çok önemli olması durumu
7	1. Faktörün 2. faktöre nazaran çok güçlü bir öneme sahip olması durumu
9	1. Faktörün 2. faktöre nazaran mutlak üstün bir öneme sahip olması durumu
2,4,6,8	Ara değerler

Adım 3 : Bileşenlerin Yüzde Önem Dağılımları Belirlenir

Karşılaştırma matrisi, faktörlerin birbirlerine göre önem seviyelerini belirli bir mantık içerisinde gösterir. Ancak bu faktörlerin bütün içerisindeki ağırlıklarını, diğer bir deyişle yüzde önem dağılımlarını belirlemek için, karşılaştırma matrisini oluşturan sütun vektörlerinden yararlanılır ve n adet ve n bileşenli B sütun vektörü oluşturulur.

Aşağıda bu vektör gösterilmiştir:

$$B_i = \begin{bmatrix} b_{11} \\ b_{21} \\ \cdot \\ \cdot \\ \cdot \\ b_{n1} \end{bmatrix} \quad (3.3)$$

B sütun vektörlerinin hesaplanmasında (3.4) formülünden yararlanılır.

$$b_{ij} = \frac{a_{ij}}{\sum_{i=1}^n a_{ij}} \quad (3.4)$$

Örneğin değerlendirme faktörlerinin birbirleriyle karşılaştırılmalarını gösteren A karşılaştırma matrisi aşağıdaki gibi tanımlanmışsa ve vektörü hesaplanmak isteniyorsa,

$$A = \begin{bmatrix} 1 & 1/3 & 5 \\ 3 & 1 & 4 \\ 1/5 & 1/4 & 1 \end{bmatrix}$$

bu durumda B_1 vektörünün b_{11} elemanı, $b_{11} = \frac{1}{1+3+0,2}$ olarak hesaplanacaktır.

Benzer şekilde B_1 vektörünün diğer elemanları hesaplandığında, vektör aşağıdaki gibi elde edilebilir ve sütun vektörünün bileşenleri toplandığında toplamın 1 olduğu görülebilir.

$$B_1 = \begin{bmatrix} 0,238 \\ 0,714 \\ 0,048 \end{bmatrix}$$

Yukarıda anlatılan adımlar diğer değerlendirme faktörleri içinde tekrarlandığında faktör sayısı kadar B sütun vektörü elde edilecektir. n adet B sütun vektörü, bir matris formatında bir araya getirildiğinde ise aşağıda gösterilen C matrisi oluşturulacaktır.

$$C = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{bmatrix} \quad (3.5)$$

Yukarıdaki örnek göz önüne alındığında C matrisi aşağıdaki gibi oluşur.

$$C = \begin{bmatrix} 0,238 & 0,210 & 0,500 \\ 0,714 & 0,632 & 0,400 \\ 0,048 & 0,158 & 0,100 \end{bmatrix}$$

C matrisinden yararlanarak, faktörlerin birbirlerine göre önem değerlerini gösteren yüzde önem dağılımları elde edilebilir. Bunun için (3.6) formülünde gösterildiği gibi C matrisini oluşturan satır bileşenlerinin aritmetik ortalaması alınır ve öncelik vektörü olarak adlandırılan W sütun vektörü elde edilir.

$$w_i = \frac{\sum_{j=1}^n c_{ij}}{n} \quad (3.6)$$

W vektörü aşağıda gösterilmiştir.

$$W = \begin{bmatrix} w_1 \\ w_2 \\ \cdot \\ \cdot \\ \cdot \\ w_n \end{bmatrix} \quad (3.7)$$

Yukarıdaki örnek çözüldüğünde öncelik vektörünün elemanları aşağıdaki gibi hesaplanabilir. Bu durumda her üç faktör birlikte değerlendirildiğinde yaklaşık değerlerle, birinci faktör % 32, ikinci faktör % 58 ve üçüncü faktör % 10 öneme sahip olacaktır.

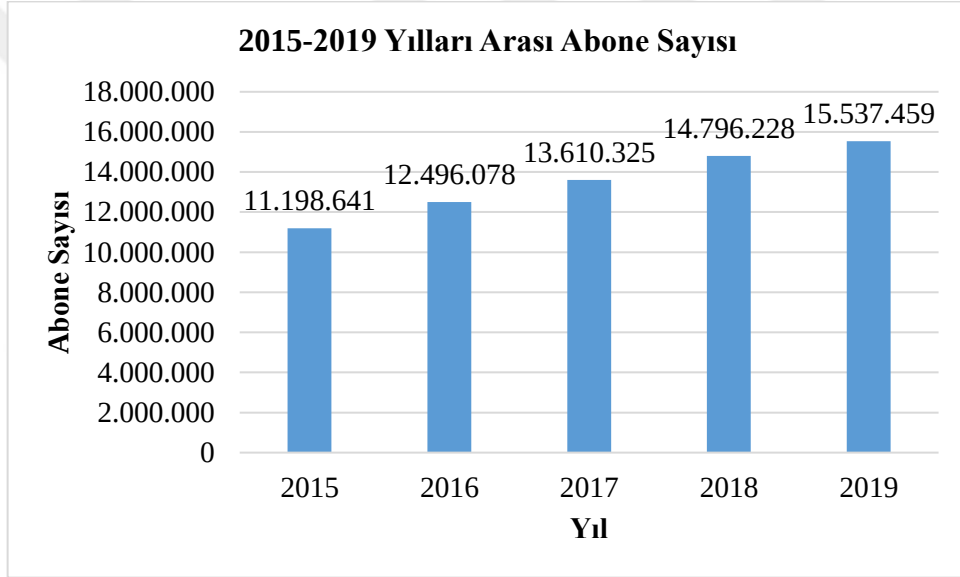
$$W = \begin{bmatrix} \frac{0,238 + 0,210 + 0,500}{3} \\ \frac{0,714 + 0,632 + 0,400}{3} \\ \frac{0,048 + 0,1580 + 0,100}{3} \end{bmatrix} \cong \begin{bmatrix} 0,32 \\ 0,58 \\ 0,10 \end{bmatrix}$$

Adım 4 : Faktör Kıyaslamalarındaki Tutarlılık Ölçülür

AHP kendi içinde ne kadar tutarlı bir sistematığe sahip olsa da sonuçların gerçekçiliği doğal olarak, karar vericinin faktörler arasında yaptığı birebir karşılaştırmadaki tutarlılığa bağlı olacaktır.

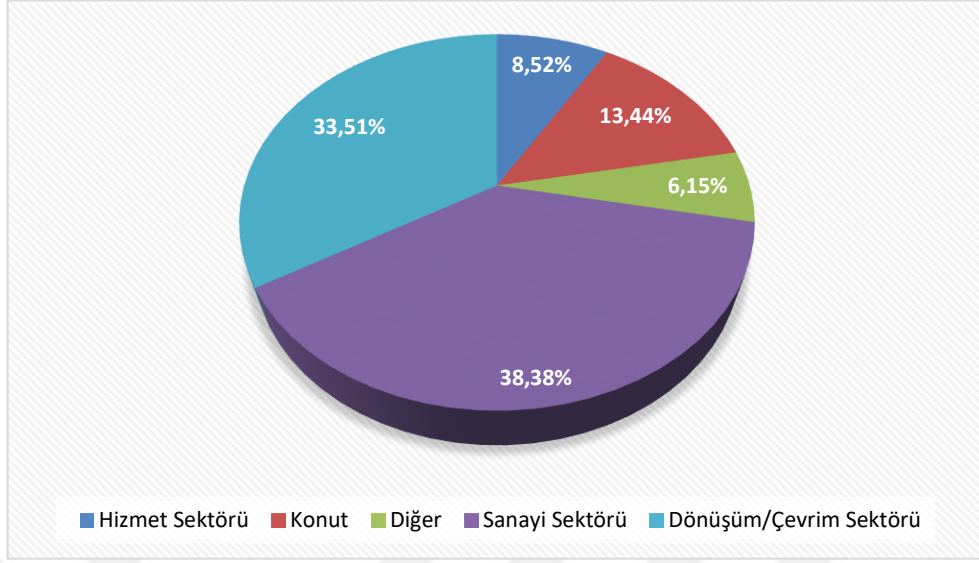
3.2 AKILLI DOĞAL GAZ ŞEBEKELERİNDE SİBER GÜVENLİK AÇIKLARININ ARAŞTIRILMASI VE OLGUNLUK MODELİNİN GELİŞTİRİLMESİ

2019 yılı Ekim ayı itibariyle Türkiye doğal gaz abone sayısı 2018 yılı Ekim ayına kıyasla 1.155.345 artarak 15.537.459' a ulaşmıştır. 2018 yılı Ekim ayında Türkiye' deki toplam doğal gaz abone sayısı 14.401.523' tür. Toplam abone sayısı 16.144.065' e ulaşmıştır ve % 96.25' ni konut aboneleri (Serbest Olmayan Tüketici Grubu) oluşturmaktadır. Serbest Tüketici sayısı 2019 yılı Ekim ayında bir önceki yılın aynı dönemine göre 19.409 artmış ve 606.606' e ulaşmıştır. 2019 yılı Türkiye toplam doğal gaz tüketimi 2018 yılına kıyasla % 16,77 azalarak 3.458,97 milyon Sm³ olarak gerçekleşmiştir (EPDK, 2020).



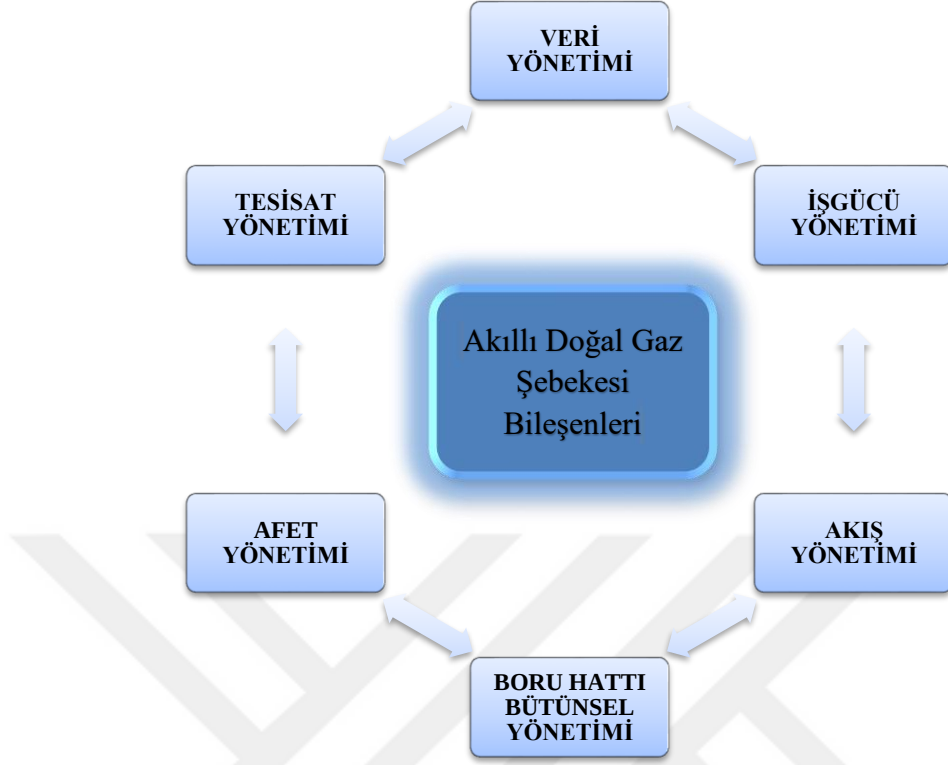
Şekil 3.1: 2015-2019 Yılları arası abone sayısı (EPDK, 2020).

2019 yılında sektörel bazda en fazla tüketim % 33,51' lik pay ile dönüşüm/çevrim santrallerinde olurken, konutlarda toplam tüketimin % 13,44' ü, sanayide ise % 38,38' i gerçekleşmiştir. Resmi dairelerin ve ticarethanelerin yer aldığı hizmet sektöründe ise toplam tüketimin % 8,52' si gerçekleşmiştir. 4 sektör toplam tüketimde % 93,85' lik paya sahiptir.



Şekil 3.2: Ekim 2019 Yılında sektörel bazda doğal gaz tüketimini dağılımı (EPDK, 2020).

İstatistiklere göre tüketilen enerji miktarları arasında en önemli artışın doğal gaz kullanımında olması beklenmektedir. Şehirlerde artan nüfus ve dolayısıyla doğal gaz talebinin artması, optimum doğal gaz dağıtımını gerektirmektedir. Doğal gaz dağıtımının optimize edilmesi açısından akıllı şebeke kaçınılmaz bir ihtiyaç haline gelmiştir. Diğer açılardan, doğal gaz dağıtımında akıllı şebeke konsepti ve siber güvenlik olgunluk modeli için herhangi bir çerçeve bulunmamaktadır. Bu çalışmada genel olarak akıllı doğal gaz şebekelerinde siber güvenlik açıklarının araştırılması ve olgunluk modeli kurulması hedeflenmektedir. Akıllı doğal gaz şebeke uygulamalarını doğalgaz dağıtım yönetiminde altı bölüm olarak sınıflandırıyoruz. Bunlar Şekil 3.3’ de gösterildiği gibi bilgi yönetimi, işgücü yönetimi, akış yönetimi, boru hattı bütünsel yönetimi, afet yönetimi ve tesisat yönetimidir.



Şekil 3.3: Akıllı doğal gaz şebekesinin bileşenleri.

Doğal gaz dağıtımında akıllı doğal gaz şebekelerinin gerekli tüm bileşenlerini belirledik. Doğal gaz dağıtımında kullanılan tüm akıllı doğal gaz şebeke bileşenleri Tablo 3.2’ de detaylandırılmıştır.

Tablo 3.2: Akıllı doğal gaz şebekesi bileşenleri.

	Ana Bileşenler		Alt Bileşenler
1	Akış Yönetimi	1	SCADA
		2	Elektronik Bülten Tablosu (EBT)
		3	Ölçme ve Raporlama Sistemi (AVE-ÖRS)
		4	Otomatik Sayaç Okuma Sistemi (AMI/AMR)
2	Veri Yönetimi	1	Kurumsal Kaynak Planlama (ERP (PM-MM-HR-CO-SD))
		2	Müşteri İlişkileri Yönetimi (CRM)
		3	Siber Güvenlik Sistemi (SGS)
3	İşgücü Yönetimi	1	İşletme Otomasyon Sistemi (İOS)
		2	Araç Takip Sistemi (ATS)
		3	Enerji Yönetim Sistemi (EYS)
4	Boru Hattı Bütünsel Yönetimi	1	Katodik Koruma Sistemi (KKS)
		2	Boru İçi Denetleme Robotu (BİDR)
		3	Boru Hattı Risk Değerlendirme Sistemi (BHRYs)
5	Afet Yönetimi	1	İhbar Yönetim Sistemi (İYS)
		2	Deprem Risk Azaltım Sistemi (DRAS-SI)
6	Tesisat Yönetimi	1	Coğrafi Bilgi Sistemi (CBS)
		2	Şebeke Yük Optimizasyon Sistemi (ŞYOS)
		3	Dijital Proje Onay ve Gaz Açma Sistemi (DPOS&DGAS)

3.2.1. Yeni Siber Güvenlik Olgunluk Modelinin Kurulumu

Prof. Peter Drucker' ın “kontrol edemediğiniz şeyleri yönetemezsiniz ve ölçemediğiniz şeyleri kontrol edemezsiniz” tespiti açık bir gerçeği ifade etmektedir (Drucker, 2012). Ülkemizde akıllı şebeke konseptinin içeriği doğal gaz dağıtım alanına siber güvenlik olgunluk modeli tam olarak tanımlanmamıştır. Akıllı doğal gaz şebekelerinin başarılı şekilde yönetilebilmesi için siber güvenlik açıklarının tespit edilmeli ve kurumun siber güvenlik açısından olgunluk modeline ihtiyaç duyulmaktadır. Bu değerlendirmeyi yapabilmek için bazı yöntemler kullanılmalıdır. Bu çalışmada, tanımlanmış adımlar takip edilmektedir. İlk olarak, tüm doğal gaz akıllı şebeke sistemleri belirlenmiştir. İkinci olarak, bu sistemlere ait alt sistemler tanımlanmıştır. Üçüncü olarak bu sistemlerin anahtar performans göstergeleri (KPI)

tanımlanmıştır. Sonrasında, akıllı doğal gaz şebekelerindeki tüm sistemlerin siber güvenlik açısından önem ağırlıklandırılması AHP (Analitik Hiyeraşi Süreci) metodu ile gerçekleştirilmiştir. Son olarak, akıllı doğal gaz şebekesi için siber güvenlik olgunluk modeli oluşturulmuştur.

3.2.1.1. Problem Tanımı ve Bilgi Toplama

Akıllı doğal gaz şebekeleri, şehirlerin enerji ihtiyacını karşılamada önemli bir yer tutmaktadır. Başka bir ifadeyle, bu akıllı şebekelerin yönetimi şehir için kritik bir konudur. Diğer teknik konularda da olduğu gibi akıllı doğal gaz dağıtım şebekeleri alt yapısının yönetimi de birçok farklı şartname ve standart ile ilişkilidir. Ancak, doğal gaz dağıtımındaki akıllı şebeke uygulama esaslarını doğrudan belirten herhangi bir standart olmaması nedeniyle, tasarlanan otomasyon sistemlerinin siber güvenlik olgunluk seviyesi konusunda ölçme ve değerlendirme tam olarak yapılamamaktadır. Bu nedenle altyapı yönetiminde kullanılan akıllı şebeke uygulamalarının siber güvenlik açıklıklarının tespitinde ve siber güvenlik olgunluk seviyesi performanslarının ölçülmesinde bu yazılım tabanlı otomasyon sistemlerinin çalışma prensiplerinin belirlenmesinde yol gösterecek bir çalışmaya ihtiyaç duyulmaktadır.

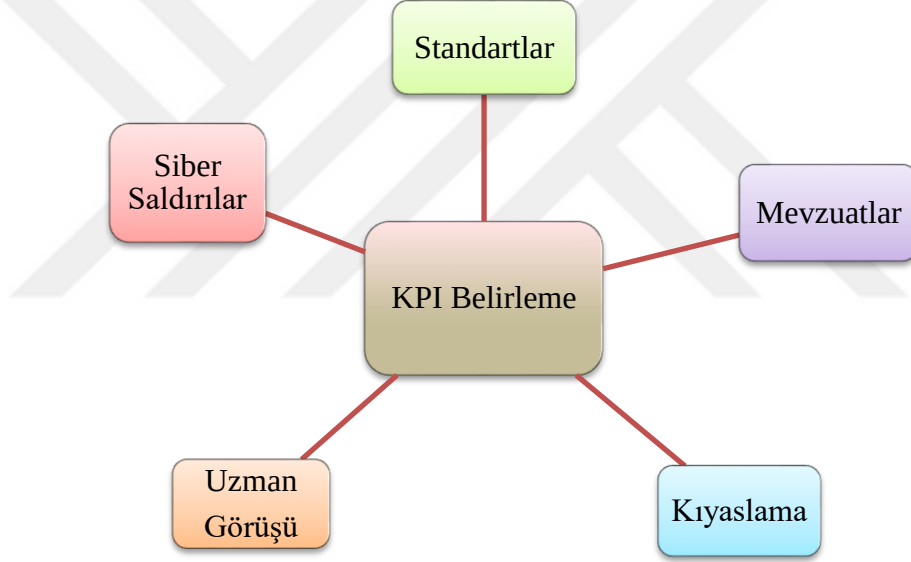
Akıllı doğal gaz şebeke yönetim prensiplerini belirlemek için doğal gaz dağıtımındaki akıllı şebeke saha uygulamaları toplanmalıdır. Bu uygulamalar bölgeye göre değişmekte olup, dolayısıyla bu farklılıklar akıllı doğal gaz şebeke yönetiminin ilkelerini belirlemeyi zorlaştırmaktadır. Bu problemin üstesinden gelmek için, akıllı doğal gaz şebeke yönetiminin ana sistemleri, alt sistemleri ve performans göstergeleri tüm akıllı doğal gaz şebeke uygulamaları için karşılaştırmalı olarak değerlendirilerek tanımlanmalıdır.

Bu karşılaştırma ve analizin amacı, doğal gaz dağıtım alanındaki akıllı doğal gaz şebeke uygulamalarının çerçevesini, siber güvenlik açıklarını belirlemek ve siber güvenlik olgunluk seviyelerini ölçmektir. Bu karşılaştırma ve analiz sonucunda, tüm doğal gaz akıllı şebeke uygulamalarını altı ana bölüm ile sınıflandırıldı. Bu bölümler; 1) Boru hattı bütünlüğü yönetimi, 2) Akış yönetimi, 3) Bilgi yönetimi, 4) Afet yönetimi, 5) Tesisat yönetimi ve 6) İşgücü yönetimi' dir. Akıllı doğal gaz şebekelerinde kullanılan tüm sistemler ve aralarındaki ilişkiler siber güvenlik açısından incelenerek temel performans göstergeleri ilgili bölümlerde tablo olarak verilmiştir.

3.2.1.2. KPI Belirleme Süreci

Akıllı doğal gaz şebekelerinde şehirlerin enerji ihtiyacının en önemli parçası güvenli ve verimli enerji arzıdır. Bu, enerji arzı sağlayan şirketler için bu büyük bir hedeftir. Bu hedef enerji sektörünün en önemli odak noktalarından biridir. Akıllı doğal gaz şebeke uygulamaları bu hedefe ulaşmak için tasarlanmıştır. Ancak, bu uygulamaların siber güvenlik açısından güvenlik zaafiyetleri araştırılmalı ve analiz edilmelidir.

Bu nedenle, doğal gaz dağıtım şirketlerinin akıllı doğal gaz şebeke bileşenlerinin Anahtar Performans Göstergelerini (KPI) siber güvenlik açısından incelemeye karar verdik. Öncelikle, Şekil 3.4' de gösterildiği gibi KPI belirleme süreci belirlenmiştir.

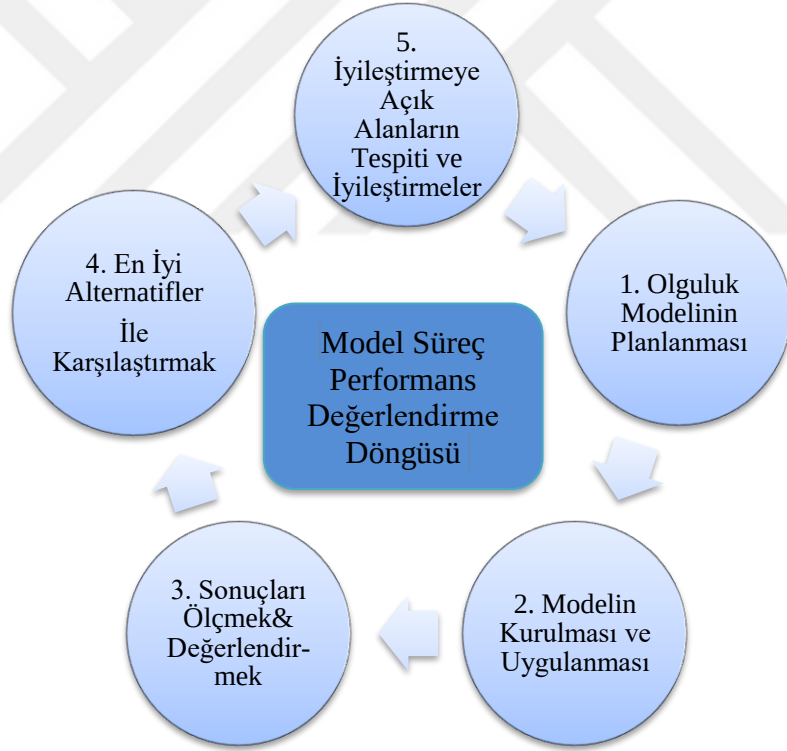


Şekil 3.4: Anahtar performans göstergesi (KPI) belirleme süreci.

Bu beş unsura dayanarak KPI parametreleri belirlenir ve bunlar ilgili standartlar, mevzuatlar, kıyaslama, gerçekleşmiş siber saldırılar ve uzman görüşü (sistem kullanıcısı) sistemine dayanarak farklı dağıtım şirketleri arasında kıyaslama yapılır. Akıllı doğal gaz şebeke bileşenleri ile ilgili tüm siber güvenlik standartları araştırıldı. Farklı gaz dağıtım şirketlerinden sistem kullanıcılarıyla görüşmeler yapıldı. Sistem uzmanları, standartlar, mevzuatlar, gerçekleşmiş siber saldırılar ve kıyaslamalardan topladığımız bilgiler ışığında siber güvenlik olgunluk modeli performans göstergeleri belirlenmiştir.

3.2.1.3. Model Süreç Performans Değerlendirme Döngüsü

Belirlenen KPI' lara göre bu seviyeler aşağıda belirteceğimiz model üzerinde performans değerlendirme süreci döngüsüne bağlı olarak kategorize edildi. Bir süreç olarak modelin performans değerlendirme döngüsü oluşturuldu. Belirlenen tüm KPI' lara göre oluşturulan soru setleri sayesinde bu süreçlere göre siber güvenlik açısından olgunluk seviyeleri belirlenir. Bu modelin tüm sistemlerdeki güvenlik süreçlerini en temelden başlayarak sistemlemlerin geliştirilmesi ve zayıf alanlarının tespiti için yönlendirme sunmaktadır. Böylece siber güvenlik olgunluk modelimiz süreçleri ve hizmetleri iyileştirmek ve siber güvenlik açıklarını tespit etmek için her bir sisteme yol haritası ve tavsiyeler sunmaktadır. Akıllı doğal gaz şebekesi siber güvenlik açısından olgunluk modeli süreç performans değerlendirme döngüsü, Şekil 3.5' de gösterildiği gibi sistemin performansını geliştirmek için bir yol haritası sunmaktadır.



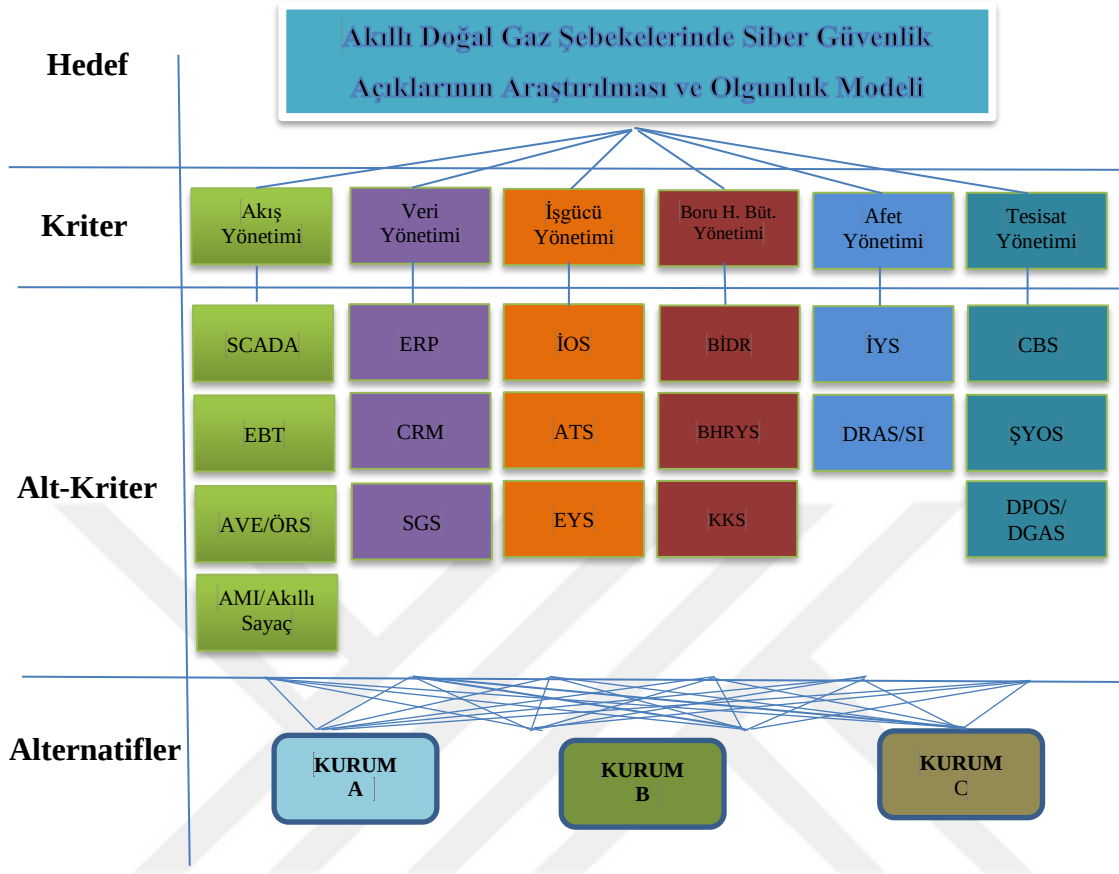
Şekil 3.5: Modelin süreç performans değerlendirme döngüsü.

3.2.1.4. AHP Yöntemi ve Ağırlıklandırma

AHP modeli, ana değerlendirme kriterlerini ve alt kriterleri belirleyerek alternatifleri önem sırasına göre sıralar. Kriterlerin ağırlıkları, her bir kriterin ve alt kriterin önemini belirtir. Her bir alternatifin karşılıklı olarak kıyaslanmasıyla oluşan puanlamalar birlikte değerlendirilir. Bu

puanlamalar veya önem ağırlıkları, sorunun kapsamlı bir şekilde değerlendirilmesini sağlar. Her katmandaki kriterlerin önemi, eşleştiği kritere göre değerlendirilir. Önem değerlendirmesi, AHP tarafından sunulan avantajlardan ve ikili karşılaştırmalardan faydalanarak sübjektif olarak belirlenir. Böylece, bu yöntem birçok durumda hataya yol açan doğrudan ağırlık değerlendirmesinden kaçınmayı sağlar (Chatzimouratidis, 2009).

AHP bir karar hiyerarşisi üzerinde, önceden tanımlanmış bir karşılaştırma skalası kullanılarak, gerek kararı etkileyen faktörler ve gerekse bu faktörler açısından karar noktalarının önem değerleri açısından, birebir karşılaştırmalara dayanmaktadır. Sonuç olarak, önem farklılıkları karar noktalarında yüzde dağılımına dönüşmektedir. AHP modelimizde doğal gaz dağıtım şirketlerini değerlendiriyoruz. Sektörel araştırmadan sonra, şu anda hizmet için kullanılan on sekiz adet alt sistemlerden oluşan akıllı doğal gaz dağıtım şebekesi altyapısının olduğunu gözlemledik. Bu sistemleri altı bölümde sınıflandırma yapıldı. Bu bölümler akış yönetimi, bilgi yönetimi, işgücü yönetimi, boru hattı bütünsel yönetimi, afet yönetimi ve tesisat yönetimidir. Gaz dağıtım şirketlerinin akıllı şebeke siber güvenlik toplam olgunluk düzeyini hesaplamak için bu otomasyon sistemlerinin önem ağırlıklarını belirledik. Bu çalışmada, model sınırlı sayıda alternatif için karar verme işlemini gerçekleştirmektedir. Bu çalışmada tanımlanan model dört katmandan oluşmaktadır. Birinci kısımda çalışmanın hedefi, ikinci kısımda kriterler, üçüncü kısımda alt mukayese kriterleri ve son kısımda ise alternatifler bulunmaktadır. Önerilen AHP Model çerçevesi Şekil 3.6' da gösterilmiştir.



Şekil 3.6: Önerilen AHP yöntemi ile oluşturulan olgunluk modeli.

Bu çalışma, akıllı doğal gaz şebekelerinde siber güvenlik açıklarının araştırılması ve olgunluk modeli oluşturularak siber güvenlik açıkları açısından çeşitli gaz dağıtım şirketleri üzerinde 6 ana bileşen altında 18 alt bileşen kullanıldı. Akış yönetimi, veri yönetimi, işgücü yönetimi, boru hattı bütünlüğü yöntemi, afet yönetimi, ve tesisat yönetimi ikili karşılaştırma yöntemi ile karşılaştırma yapıldı. Bu aşamada Şekil 3.7’ de görüldüğü gibi faktörler arası karşılaştırma matrisi oluşturulmuştur.

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

Şekil 3.7: İkili karşılaştırma matrisi.

Karşılaştırma matrisi, belirlenen katagorilerin birbirlerine göre önem seviyelerini belirli bir mantık içerisinde gösterir. Ancak bu katagoriler bütün içerisindeki ağırlıklarını, diğer bir deyişle yüzde önem dağılımlarını belirlemek için, karşılaştırma matrisini oluşturulur.

$$a_{ji} = \frac{1}{a_{ij}}$$

Yukarıda verilen örnek dikkate alınır karşılaştırma matrisinin birinci satır üçüncü sütun bileşeni ($i=1, j=3$) 3 değerini alıyorsa, karşılaştırma matrisinin üçüncü satır birinci sütun bileşeni ($i=3, j=1$), formülünden $1/3$ değerini alacaktır. İkili karşılaştırma AHP önem ölçeği ile uyumlu olarak yapılır (Belton, 1999). AHP önem seviyeleri Tablo 3.3’ de gösterilmiştir.

Tablo 3.3: AHP yöntemi önem seviyeleri.

Önem	Tanım	Açıklama
1	Eşit derece önemli	İki faktör aynı derecede önem taşır
3	Biraz daha fazla önemli	Biri diğerine göre biraz daha fazla önem taşır
5	Oldukça önemli	Biri diğerine göre oldukça önem taşır
7	Çok daha önemli	Biri diğerine göre çok daha fazla önem taşır
9	Kesinlikle daha önemli	Biri diğerine göre kesinlikle daha fazla önem taşır
2,4,6,8	Ara değerler	Tercih diğerleri birbirine yakın olduğunda kullanılır

Ayrıca, ikili karşılaştırmaları kesin subjektif değerlendirme kriterleri için yapılabilir. Tutarlılık sorgulamaları ikili karşılaştırma ile yapılan değerlendirme hükümlerine yardımcı olur. Tutarlılık hesaplarının detayları ekte sunulmuştur. Ayrıca, bu değerlendirmeler doğal gaz dağıtım sektöründeki birçok uzman tarafından yürütülmüştür. Uzman görüşlerine göre ağırlıklı ortalama değerlendirmelerini hesaplanmıştır. Yönetim kategorilerinin ikili mukayese yöntemiyle karşılaştırması Tablo 3.4’ te gösterilmiştir. Bunlar akış yönetimi, veri yönetimi, afet yönetimi, boru hattı bütünsel yönetimi, işgücü yönetimi ve tesisat yönetimidir.

Tablo 3.4: Yönetim sistemlerinin önem ağırlıklarının hesaplanması.

Ana Bileşenler	Akış Yönetimi	Veri Yönetimi	İşgücü Yönetimi	Boru Hattı Büt. Yönetimi	Afet Yönetimi	Tesisat Yönetimi
Akış Yönetimi	1	9	9	9	1	1
Veri Yönetimi	0,111	1	5	5	7	3
İşgücü Yönetimi	0,111	0,200	1	2	2	3
Boru Hattı Büt. Yönetimi	0,111	0,2	0,500	1	8	3
Afet Yönetimi	1	0,142	0,500	0,125	1	9
Tesisat Yönetimi	1	1,666	0,333	0,333	0,111	1
TOPLAM	3,333	12,210	16,333	17,458	19,111	20,000

Karşılaştırma matrisi, faktörlerin birbirlerine göre önem seviyelerini belirli bir mantık içerisinde gösterir. Ancak bu faktörlerin bütün içerisindeki ağırlıklarını, diğer bir deyişle yüzde önem dağılımlarını belirlemek için, karşılaştırma matrisini oluşturan sütun vektörlerinden yararlanılır ve n adet ve n bileşenli B sütun vektörü oluşturulur.

Aşağıda bu vektör gösterilmiştir:

$$B_i = \begin{bmatrix} b_{11} \\ b_{21} \\ \cdot \\ \cdot \\ \cdot \\ b_{n1} \end{bmatrix}$$

Her bir hücre iki kesişen yönetim sınıfının karşılaştırmasını göstermektedir. Bu aşamada matristeki her bir değer sütunun toplamı olan değere bölünerek ikinci bir tablo oluşturulmuştur. Ayrıca elde edilen değerlerin ortalamaları hesaplanmıştır.

Bu hesaplama aşağıdaki denklem kullanılarak yapılır.

$$b_{ij} = \frac{a_{ij}}{\sum_{i=1}^n a_{ij}}$$

Tablo 3.5: Yönetim sistemlerinin normalize edilmiş önem ağırlıklarının hesaplanması.

Ana Bileşenler	Norm. Edilmiş Akış Yönetimi	Norm. Edilmiş Veri Yönetimi	Norm. Edilmiş İşgücü Yönetimi	Norm. Edilmiş Boru H. Büt. Yönetimi	Norm. Edilmiş Afet Yönetimi	Norm. Edilmiş Tesisat Yönetimi	Norm. Edilmiş Toplamlar	Norm. Edilmiş Önem Değerleri (%)
Akış Yönetimi	0,300	0,737	0,551	0,516	0,052	0,050	2,206	36,766
Veri Yönetimi	0,033	0,082	0,306	0,286	0,366	0,150	1,224	20,401
İşgücü Yönetimi	0,033	0,016	0,061	0,115	0,105	0,150	0,480	8,002
Boru Hattı Büt. Yönetimi	0,033	0,016	0,031	0,057	0,419	0,150	0,706	11,770
Afet Yönetimi	0,300	0,012	0,031	0,007	0,052	0,450	0,852	14,197
Tesisat Yönetimi	0,300	0,137	0,020	0,019	0,006	0,050	0,532	8,864
Toplam	1	1	1	1	1	1	6	100

Elde edilen detaylı sonuçlar Tablo 3.5’ de gösterilmiştir. Tabloda görüldüğü gibi, akış yönetimi akıllı doğal gaz şebekelerinde siber güvenlik açısından doğal gaz dağıtım şirketleri için en önemli kriterdir. Ayrıca siber güvenlik açısından milyonlarca işlem ve müşteri verisinin doğru şekilde korunması ve kaydedilmesi gerektiğinden, bilgi yönetimi en önemli ikinci yönetim kategorisidir. Tablo 3.6’ da ana bileşenlere ait önem ağırlıkları gösterilmiştir.

Tablo 3.6: Yönetim sistemlerinin önem ağırlıkları.

Ana Bileşenler	Önem Ağırlıkları
Akış Yönetimi	36,7665
Veri Yönetimi	20,4006
Afet Yönetimi	14,1966
Boru H. Büt. Yönetimi	11,7702
Tesisat Yönetimi	8,8637
İşgücü Yönetimi	8,0025
Toplam	100

Akış yönetimi, 2. aşamada matristeki her bir değer, sütunun toplamı olan değere bölünerek ikinci bir tablo oluşturulmuştur. Elde edilen bu ortalamalar (AHP yöntemindeki kıyaslama değerlendirmelerinin ortalamaları) konunun uzmanlarınca defaten yapılarak homojenlik ve ağırlıklandırma işleminin doğruluğu arttırılmıştır. Üçüncü olarak her bir kategorideki sistemlerin alt değerlendirmesi için yönetim elemanları olan sistemler yine ikili mukayese yöntemiyle karşılaştırılmıştır. Örnek olarak akış yönetiminin alt elemanları olan SCADA, EBT, AVE ve AMR sistemlerinin önem ağırlıklarının dağılımı Tablo 3.7’ deki gibidir.

Tablo 3.7: Akış yönetimi sistemine ait alt kategorilerinin ikili mukayesesi.

Alt Bileşenler	SCADA	EBT	AVE	AMR
SCADA	1	9	9	9
EBT	0,111	1	8	9
AVE	0,111	0,125	1	9
AMR	0,111	0,111	0,111	1
Toplam	1,333	10,236	18,111	28,000

Ayrıca elde edilen değerlerin toplamı 1' e göre normalize edilmiştir ve her bir alt kriterin satır olarak toplamı Akış Yönetiminin önem ağırlığı toplamına göre alt kriterler %' de olarak önem ağırlıkları Tablo 3.8' de hesaplanmıştır.

Tablo 3.8: Akış yönetimi sistemine ait alt kategorilerinin normalize edilmiş önem ağırlıkları.

Alt Bileşenler	Normalize Edilmiş SCADA	Normalize Edilmiş EBT	Normalize Edilmiş AVE	Normalize Edilmiş AMR	Normalize Edilmiş Toplamlar	Normalize Edilmiş Önem Değerleri (%)	Normalize Edilmiş Akış Yönetiminde Önem Ağırlıkları
SCADA	0,750	0,879	0,496	0,321	2,447	61,190	22,497
EBT	0,083	0,097	0,441	0,321	0,944	23,604	8,678
AVE	0,083	0,012	0,055	0,321	0,472	11,804	4,340
AMR	0,083	0,010	0,006	0,035	0,136	3,400	1,250
Toplam	1	1	1	1	4	100	36,766

Ayrıca, AHP değerlendirmesinin bir sonucu olarak, her bir sisteminin önem ağırlıkları Tablo 3.9' da sunulmuştur. Bu sonuçlar 100 puan üzerinden belirlenmiştir. Akıllı doğal gaz şebekelerinde siber güvenlik açıklarının araştırılması ve olgunluk seviyelerinin belirlenmesinde bu ağırlıklar kullanılacaktır.

Tablo 3.9: Akıllı doğal gaz şebekesi alt bileşenlerinin önem ağırlıkları.

	Ana Bileşenler	Alt Bileşenler	%
1	Akış Yönetimi	SCADA	22,497
2		Elektronik Bülten Tablosu (EBT)	8,678
3		Ölçme ve Raporlama Sistemi (AVE-ÖRS)	4,340
4		Otomatik Sayaç Okuma Sistemi (AMI/AMR)	1,250
5	Veri Yönetimi	Kurumsal Kaynak Planlama (ERP)	2,846
6		Müşteri İlişkileri Yönetimi (CRM)	1,361
7		Siber Güvenlik Sistemi (SGS)	16,194
8	İşgücü Yönetimi	İşletme Otomasyon Sistemi (İOS)	5,761
9		Araç Takip Sistemi (ATS)	1,501
10		Enerji Yönetim Sistemi (EYS)	0,740
11	Boru Hattı Büt. Yönetimi	Boru İçi Denetleme Robotu (BİDR)	1,070
12		Boru Hattı Risk Değerlendirme Sistemi (BHRYS)	1,070
13		Katodik Koruma Sistemi (KKS)	9,630
14	Afet Yönetimi	İhbar Yönetim Sistemi (İYS)	10,647
15		Deprem Risk Azaltım Sistemi (DRAS-SI)	3,549
16	Tesisat Yönetimi	Coğrafi Bilgi Sistemi (CBS)	1,543
17		Şebeke Yük Optimizasyon Sistemi (ŞYOS)	0,523
18		Dijital Proje Onay ve Gaz Açma Sistemi (DPOS&DGAS)	6,797
		Toplam	100,000

Akıllı doğal gaz şebeke uygulamalarında bakıldığında SCADA en önemli alt bileşen olduğu görülmektedir. Diğer alt bileşenlerin önem sıralaması ise SGS, İYS ve KKS olarak sıralanır. SCADA, birçok saha ekipmanlarının izlenmesini ve kontrol edilmesini sağlar. Otomasyon sistemleri ve iş akışı üzerindeki büyük etkisi nedeniyle siber güvenlik zaafiyetlerinin tespiti önemlidir.

3.3. AKIŞ YÖNETİMİ

Akış yönetimi, akış kontrolü doğal gazın dağıtımında güvenli arz için önemli bir konudur. Çoğu dağıtım sistemi arasında, malzeme tipleri, kurulum koşulları ve genel performans geçmişi ile ilgili verilerin olmaması ortak bir eksikliktir. Bu durum bilgisayar sistemi hizmetinden dolayı tüm operatörler arasında farklılıklar görünmektedir (CMMI, 2011). Gaz endüstrisinde, birim zaman başına boru kesitinden geçen gaz miktarının doğru ölçümü (hacimsel veya kütle akış oranı) büyük önem taşımaktadır. Ek olarak, doğal gaz dağıtımının ölçümü ve kontrolü temel olarak Denetim Kontrolü ve Veri Toplama (SCADA) sistemine ve güvenli akış yönetimi için

diğer ölçüm sistemlerine ihtiyaç duymaktadır. Diğer bir deyişle, güvenli dağıtım için tüm dağıtım bileşenlerinin izlenmesi ve kontrolü önemlidir. Genel olarak, dağıtım sistemi, basınç azaltma tesisleri, regülasyon ve ölçüm istasyonları (RMS), servis hatları, bölge regülatörü, servis kutusu ve sayaçlardan oluşmaktadır. Dağıtım sistemleri genellikle farklı çaplardaki farklı boru hatlarında ve değişik basınçlarda çalıştırılır. Operasyonel olarak, doğal gazın dağıtımını birçok izleme ve kontrol sistemi gerektirir. Dahası, akıllı sayaç enerji endüstrisindeki en önemli konulardan biri haline gelmiştir. Akıllı doğal gaz şebekesinin, bir yandan sürekli artan enerji talebi ve enerji kaynaklarının kısıtlı olması zorluğunu verimlilik sayesinde aşması gerekiyor. SCADA merkezi, elektronik bülten panosu sistemi, ölçüm ve raporlama sistemi ve akıllı sayaç sistemi sonraki bölümlerde incelenecektir.

3.3.1. Akıllı Doğal Gaz Şebekesinde SCADA

SCADA (Supervisory Control and Data Acquisition) kelimelerinin ilk harfleri ile oluşturulan bir kısaltmadır. Türkçeye “Danışmalı Kontrol ve Veri Toplama Sistemi” veya “Uzaktan Kontrol ve Gözleme Sistemi” olarak çevrilebilir. SCADA sistemi izleme, danışma/kontrol ve veri toplama ve verilerin saklanması işlevlerini yerine getirmektedir.

SCADA, akıllı doğal gaz dağıtım sistemlerinde çeşitli bilgilerin sahadan toplanması, izlenmesi, uzaktan kontrolü ve yorumlanması olarak bilinmektedir. Fakat toplanan bilgilerin doğruluğu, sıklığı ve çeşitliliği akıllı şebeke bileşeni SCADA’ nın olgunluğu ile ilişkilidir. SCADA üzerinden toplanan bilgiler yirmi farklı özelliğe sahip olmalıdır. SCADA istasyonlarından toplanan verilerin özellikleri, şirketler arasında farklılık göstermektedir. Enerji Piyasasını Denetleme Kurumu (EPDK), SCADA üzerindeki bilgiler hakkında gerekli özellikleri belirledi.

SCADA, sistemleri kullanılarak uygulama yazılımı geliştirmek için protokollerin tanımlanması ve veri tabanı yapısının tanımlanması gerekmektedir. İletişim protokolleri, SCADA’ nın işletmedeki bilgi omurgası olma görevini yapması için birbirleri ile iletişim kurması gereken birimlerin haberleşmesini sağlamaktadır. SCADA sisteminin gözlem ve denetim fonksiyonlarını üstlenmesi için sürece ait giriş ve çıkış bilgileri bir veri tabanında tanımlanır. Bu süreç değişkenlerinin bulunması gereken seviyelerle ilgili alarmlar ve bu değişkenlerin işlenmesi gerektiğinde kullanılacak bilgi blokları veri bilgi tabanı tanımlanması aşamasında gerçekleştirilir. SCADA sistemleri; sistem operatörlerine, merkezi bir kontrol noktasından geniş bir coğrafi alana petrol ve gaz alanları, boru sistemleri, su şebekeleri, termik ve hidrolik

enerji üretim sistemleri ile iletim ve dağıtım tesisleri gibi alanlarda vanaları, kesicileri, ayırıcıları, anahtarları uzaktan açıp kapama, ayar noktalarını değiştirme, alarmları görüntüleme, ölçü bilgilerini toplama işlevlerini güvenilir, emniyetli ve ekonomik olarak yerine getirme avantajı sunmaktadır.

Günümüzde, otomasyon teknolojisinin hızla büyümesi ve bilgisayarların yaygın kullanımı SCADA' yı yeniden gözden geçirilmesini gerekli kılmıştır. Son yıllarda, bu alandaki en popüler uygulama; gözlem, veri toplama ve kontrol sistemlerinden oluşan SCADA' dır. Enerji sektöründe kullanılan SCADA uygulamalarının, işletme maliyetlerini ve kazaları azaltarak, verimlilik ve güvenliği artırarak geniş bir coğrafi alanda yayılan saha araçlarının merkezi olarak izlenmesi ve kontrol edilmesi gibi önemli avantajları bulunmaktadır. Ayrıca, SCADA uygulamaları tüm gaz dağıtım cihazlarında önleyici bakım ile gaz dağıtımının yönetim sürecini içerir. Bu önleyici bakım verimliliği tamamen etkiler. Elektrik ve Elektronik Mühendisleri Enstitüsü, modern SCADA istasyonlarının bir dağıtım ağında yazılım ve donanım kullandığını bildirdi. İşletim gücü, monitör merkezinde gerçek zamanlı bağlı bir Local Area Network (LAN) üzerinden birbiriyle iletilen birkaç bilgisayar ve sunucu arasında dağıtılır.

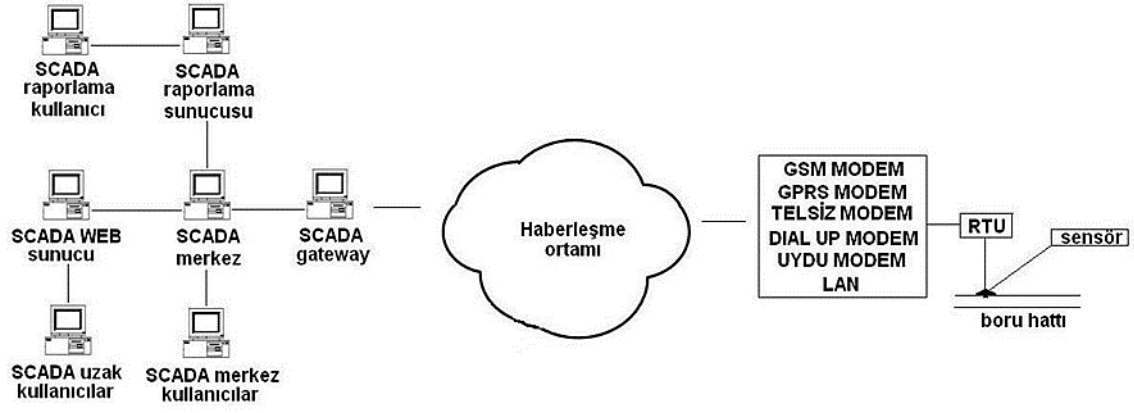
SCADA ve Otomasyon sistemleri belirli temel işlemleri sağlanması olarak görülebilir, örneğin:

- a) Ölçümler,
- b) Durum gösterimi,
- c) Kontrol,
- d) Yardımcı hizmetler,
- e) Zaman senkronizasyonu,
- f) Programlanmış mantık fonksiyonları.

3.3.1.1. SCADA Çalışma Prensipleri

Sahada izlenmek istenen bilgi için işletme ihtiyacına uygun sensör seçilir. Sensör izlenilmek istenen bilgiyi elektrik sinyallerine çeviren elektronik donanımdır. RTU/PLC ise bu sensörlerden veriyi istenilen periyotta okur ve kendi hafızasına kaydeder. Bu bilgi, merkeze gönderilmek üzere hazırlanabildiği gibi, saha tarafında kullanılmak üzere hazırlanabilir.

SCADA



Şekil 3.8: Örnek bir SCADA sistemi.

Modem ise RTU/PLC ile SCADA merkezi haberleştirmek için kullanılır. Saha ile merkez arasında hangi medya var ise modem bilgiyi bu medya üzerinden taşır. Merkeze gelen veri bir gateway'den geçerek veri tabanına kaydedilmektedir. SCADA merkez yazılımı ise bu veriyi alarm/izleme ekranlarına yansıtmakta, görsel/sesli uyarılar vermektedir.

Saha Örnekleri;



Şekil 3.9: SCADA sistemi saha örneği (GAZBİR, 2019).

SCADA ile bir şehrin belki de bir ülkenin 7/24 hizmet gerektiren, bir yada daha fazla sektörü kontrol edilmektedir. Bu özellikleriyle SCADA' lar stratejik öneme sahiptirler. Olası bir siber saldırı/sabotajlara karşı bilişim güvenliği bir kez daha düşünülmelidir.

Genel olarak SCADA sisteminden beklenenler aşağıdaki gibi sıralanabilir:

- Sisteme ait elektriksel ve endüstriyel parametrelerin PC' den izlenebilmesi
- Set edilen değerler için alarm alabilme
- İstenen değerlerin talep edilen periyotlarda kaydedilmesi
- Grafik trend izleme kaydetme imkanı
- Ürün başına indirgenebilen enerji maliyeti
- Enerji sarfiyatının faturalanması
- Tek bir merkezden nokta bazında yük kontrolü
- Öncelik seçimli yük atma ve yük alma
- Arıza takibi
- Sistemdeki her noktaya PC' den kumanda imkanı

3.3.1.2. SCADA Ekipmanları

SCADA genel olarak incelendiğinde RTU, HMI, merkezde bulunan mühendislik bilgisayarları ve RMS-A istasyonlarındaki SCADA yazılımlarının çalıştığı bilgisayarlar ve saha ekipmanlarından (basınç, sıcaklık sensörleri vb.) oluşmaktadır. Ayrıca aynı zamanda verilerin haberleşmesinde LAN, GPRS Modem, fiber optik ve uydu haberleşme sistemleri kullanılmaktadır.

a) RTU/PLC (Remote Terminal Unit):

Sahadaki kontrol noktalarındaki verileri alan, kaydeden ve merkeze ileten, merkezden gelen komutları işleyecek ve ilgili sensörlere yönlendiren ve ölçüm sınırlarının dışını algılayabilen (alarm limiti) akıllı ünitelerdir. En az C ve Leader Lojik pororamlama dillerinde yazılmış yazılımları çalışabilmektedir. Bir noktadan okunacak veri sayısı yada kontrol edilecek çıkış sayısınca sınıflandırılırlar. İşletme ihtiyacına göre tespit edilir. Kontrol/ölçüm yapılacak noktadan kaç tane veri alınacağı belirleyici olacaktır. Mutlaka, gerçek zaman bilgisi üreten saati olmalıdır. Bu üniteyi desteklemek için bağımsız batarya (lityum) desteği olmalı ve bu bilgi yazılımla merkeze taşınabilmelidir. Zaman bilgisindeki hataya karşı merkezi zaman

sunucusuyla senkronize olabilmelidir. Üzerinde ölçüm bilgileri, işletim sistemi ve çalışacak program için yeterli hafıza olmalıdır. Elektrik kesintisinde bunların kaydedilebildiği flash ve işletim sistemi olmalıdır. Cihaz seçiminde montajı yapılacağı yerin çevre şartları mutlaka incelenmelidir. Örn ısı farkından yoğunlaşmanın olacağı bir yere montaj yapılması durumunda, çok kısa bir sürede hasar görecektir.



Şekil 3.10: Örnek bir SCADA RTU (SE, 2020).

b) HMI (Human Machine Interface):

SCADA' nın topladığı verinin kullanıcılara yansıtıldığı ara yüzlerdir. Teknolojik gelişmeler, maliyetlerin düşmesi ve dağıtım şebekelerinin artmasıyla SCADA' lar popüler hale gelmiştir. SCADA sistemiyle sahadaki tesislerden hızlı bir şekilde doğruluğu yüksek veriler merkeze taşınabilir, saha eş zamanlı izlenebilir, gerektiğinde müdahale edebilir, işletmeler kaynak planlaması, hizmet stratejisi belirleyebilir, sahada lojik ihtiyaçlar saha tarafında belirlenip, çalıştırılıp, merkezden izlenebilir.



Şekil 3.11: Örnek bir HMI arayüzü (SE, 2020).

RTU' nun bulunduğu noktadan okunan yada kontrol edilen sistemlerin değerlerini izlemek yada müdahale etmek için kullanılan göstergelerdir. Özellikleri işletme ihtiyacına göre tespit edilir. LCD göstergeye ihtiyaç duyulmuyor ise açık/kapalı gibi ışıklı gösterge kullanılabilir.

c) Basınç Sensörü:

Her türlü fiziki kuvvet ve basınç değişimini algılayan ve bu değişimi elektriksel sinyale çeviren elemanlara basınç sensörü denir. Doğal gazın basınç değerleri ölçülerek merkeze aktarılması sağlanır.



Şekil 3.12: Basınç sensörü.

d) Sıcaklık Sensörü:

Endüstriyel ortamlarda sıcaklık ölçümünün önemi giderek artmaktadır. Farklı ortamlarda birbirinden ayrı özelliklere sahip sıcaklık ölçüm teknikleri ortaya çıkmıştır. Kullanım ortamına, sıcaklık ölçme aralığına ve proses şartlarına göre doğru sıcaklık sensörlerinin secimi önemlidir. Sıcaklık sensörleri, sıcaklık ölçüm aralığına göre çeşitli yarı iletken malzemeler olabileceği gibi, termistörlerde (PTC-NTC vb.) daha düşük sıcaklık uygulamalarında maliyet açısından ön plana çıkmaktadır. Piyasada en yaygın olarak yarı iletken termokupl (Fe-Const, NiCr-Ni, PtRh-Pt) ve termorezistans (PT100-PT1000 vb.) kullanılmaktadır.



Şekil 3.13: Sıcaklık sensörü.

e) Kapı sensörü:

Kapı sensörleri mekanik kapı açılmasını, kapalı/açık elektrik sinyaline dönüştüren sensörlerdir. Kullanılacağı bölgeye göre yaklaşım sensörü kuru kontak, reed röle şeklinde olabilir.



Şekil 3.14: Kapı sensörü.

f) Modem:

Modem, tanım olarak "Modölatör" ve "Demodölatör" kelimelerinin birleşiminden üretilmiştir. Uzak mesafelerde bulunan iki elektronik sistemin birbirleri arasında haberleşmesini sağlayabilmek için dizayn edilmiş aygıtlardır.



Şekil 3.15: GPRS modem (TCAMTECH, 2020).

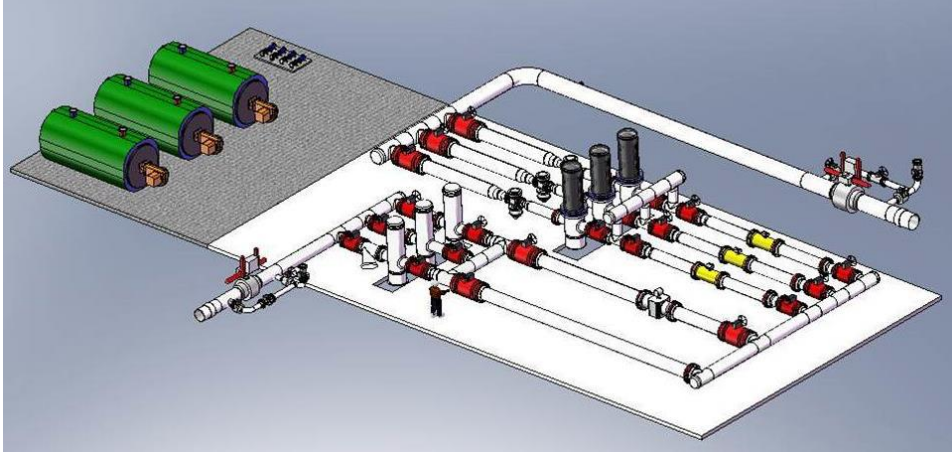
3.3.1.3. SCADA Üzerinden İzlenen Sistemler

a) RMS-A (Reducing And Metering Station):

RMS-A yüksek basınçlı doğal gazın daha düşük basınca düşürüldüğü ve ölçümünün hatta kokulandırılmasının yapıldığı istasyondur. RMS istasyonuna şehir şebekesi doğal gaz giriş istasyonları olarak da adlandırılmaktadır. RMS istasyonlarına 70-75 bar basınç girişi ve 20-23 Bar arasında basınç düşürülerek şehir içi şebekesine gönderilmektedir. RMS istasyonlarında doğal gaz ölçülür, basınç düşürülür, kromotografi ölçümleri yapılır ve kokulandırma yapılarak şehir şebekesine gönderilmektedir. Ayrıca gazın basıncının düşürülmesi ile düşen gazın sıcaklığı yüksek kapasiteli ısıtıcılarla gaz ısıtılır ve çıkış noktasına 15 ° C olarak ayarlanır.

Her bir RMS-A istasyonunda local SCADA' lar mevcuttur. Burada toplanan veriler merkez SCADA' ya iletilir. Verilerin iletimi modem, GPRS, LAN veya uydu sistemleri ile iletilir. RMS istasyonlarında büyük çaplı borular, vanalar, ölçüm sayaçları, basın düşüren regülatörler, analog ve dijital basınç ve sıcaklık sensörleri bulunmaktadır.

Şehir genelinde 15 adet RMS-A istasyonu bulunmaktadır ve her biri kritik öneme sahiptir. Bu istasyonlardan gazın kullanıma göre aktif olma ve kapalı olma durumları vardır. Kış aylarında yüksek debi olduğundan istasyonların bir çoğu açık durumdadır. Bazı istasyonlar doğal gaz direk elektrik üretiminde kullanılmaktadır.



Şekil 3.16: Örnek bir RMS A istasyonu (GAZBİR, 2019).

Bu araçların tüm teknik özellikleri verimlilik üzerinde etkilidir. Ayrıca, bu enstrümanların seçimi analiz edilmelidir. Doğal gaz dağıtımında verimlilik üç noktada incelenir: dağıtımda verimlilik, regülasyon işleminde verimlilik ve RMS’ de verimlilik. Mükemmel gaz yanması bu alandaki diğer önemli konudur. RMS’ de akan gazın optimum ısınması, enerji alanında ele alınması gereken bir diğer konudur.



Şekil 3.17: Örnek bir RMS A istasyonunun iç görünüşü (GAZBİR, 2019).

RMS istasyonlarından izlenebilecek değerler şunlardır;

- Doğal gazın giriş basıncı,
- Doğal gazın çıkış basıncı,
- Doğal gaz giriş sıcaklığı

- Doğal gaz çıkış sıcaklığı
- Filtre kirlilik değeri,
- Çekiş ölçümü,
- Doğal gaz ısıtma sistemi verileri (Basınç düşürülmesi sonrası ısı kaybını gidermek için).

b) Bölge Regülatörü ve Müşteri İstasyonu:

Bölge ve müşteri istasyonları akıllı doğal gaz şehir içi şebekesinin önemli istasyonlardan biridir. Ana giriş olan RMS-A istasyonundan gazın basıncının düşürülmesi ile şehir şebekesine gönderilen gaz bu BR-B ve Mİ-B olarak adlandırılan B tipi istasyonlar 20-23 Bar basınç girişine ve 4 Bar basınç çıkışına ve bazı Mİ-B' de ise müşteriye bağlı olarak çıkış gaz basınçları set edilir.

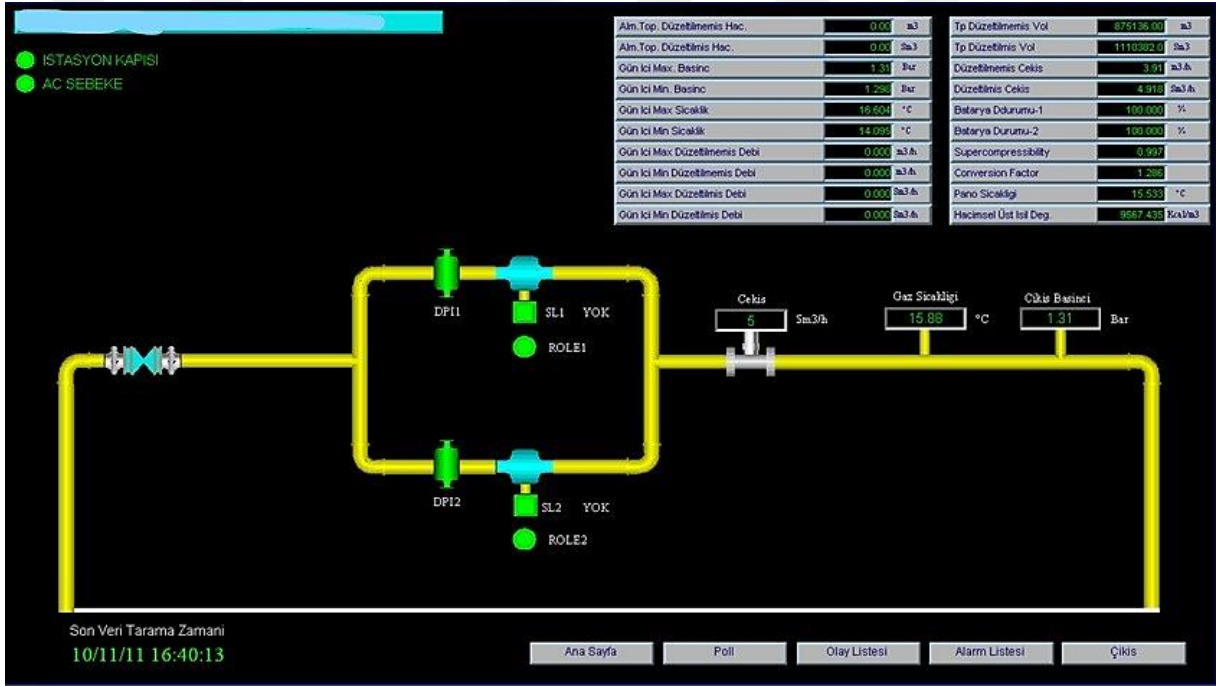


Şekil 3.18: Örnek bir bölge ve müşteri istasyonu (GAZBİR, 2020).

Bölge Regülatörü ve Müşteri istasyonlarından izlenebilecek değerler şunlardır;

- Giriş basıncı,
- Çıkış basıncı,
- Gaz sıcaklığı,
- Çekiş,
- Katodik koruma voltajı,
- Hava sıcaklığı,
- Filtre kirliliği,

- 1.Hat durumu,
- 2.Hat durumu,
- By pass vana kontrolü,
- Nokta kapı açık/kapalı bilgisi,
- RTU kabin kapı bilgisi,
- Elektrik kesintisi,
- Akü voltaj bilgisi,
- Pano sıcaklığı,
- Nokta bakım modu.



Şekil 3.19: Bölge regülatörünün SCADA üzerinden izlenmesi (GAZBİR, 2020).

c) Vana Odaları:

Şebekeyi ayırmak için kullanılan çelik vanaların bulunduğu yer altı odalarıdır. SCADA Sistemi sadece Actuator' lü vanaları kontrol edebilir. SCADA entegrasyonu yapılacak vana odalarında şu hususlara dikkat etmek gerekir;

- Vana odası yeraltı yapısı olduğundan izolasyon problemini yaşamamak için mümkün olduğunca dere yataklarından uzakta olmalıdır. İleride vana odası su ile dolar ise SCADA ekipmanları çalışmayabilir.

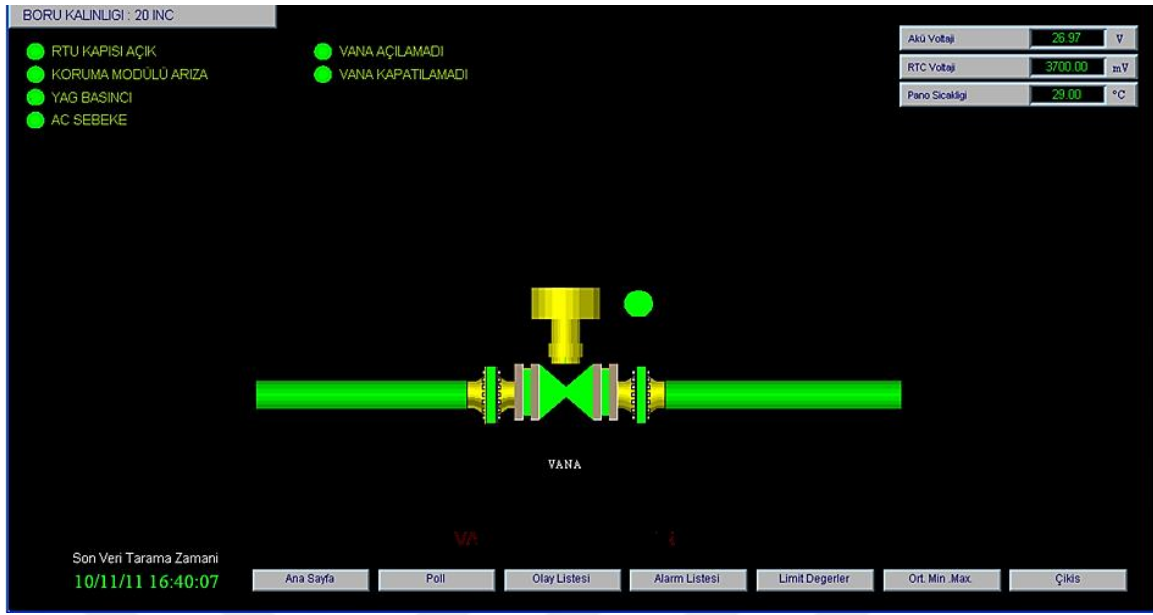
- Trafik, zeminden kaynaklanan zorluklar ve inşaat aşamasındaki zorluklar dikkate alınmalıdır.
- İleride, işletme, bakım-onarım ekiplerinin çalışmaları açısından problem olabilecek ulaşım, araç parkı, belli günlerde çalışmaya engel organizasyon merkezlerinden uzak kurulması gibi hususlara dikkat edilmelidir.
- SCADA entegrasyonu yapılacak vanalar, tahmini kumanda edilen abone büyüklüğüne göre belirlenmelidir. Çünkü yatırım maliyeti yüksek olabilir.



Şekil 3.20: Örnek bir aktuatörlü vana odası (GAZBİR, 2020).

SCADA ile vana odalarında izlenebilecek değerler şunlardır;

- Yağ basıncı,
- Koruma modülü,
- Nokta kapı açık/kapalı bilgisi
- Rtu kabin kapı bilgisi,
- Elektrik kesintisi,
- Akü voltaj bilgisi,
- Pano sıcaklığı,
- Nokta bakım modu.



Şekil 3.21: SCADA sisteminde izlenen örnek bir vana odası (GAZBİR, 2020).

d) Kromatograf:

Gaz kromatografisi son zamanlarda hem laboratuvarlarda, hem de endüstride yaygın biçimde kullanılan çözümleme tekniklerinden biri haline gelmiştir. Gaz kromatografisi, bir karışımın bileşenlerinin etkili biçimde ayrılmasını sağlayan yalın, hızlı ve hassaslığı yüksek bir araçtır. Uygulama alanı aşağı yukarı sınırsızdır. Gaz kromatografisi kavramı ilk kez 1841’ de, A. J. P. Martin ve R.L.M, Synge tarafından ortaya atıldı, ancak 1952 yılında gerçekleşti. 1950’ lerde bu teknik, kendi yaptıkları aygıtları kullanan sayısız araştırmacı tarafından geliştirildi. Gaz kromatografisi hem bir ayırma, hem de bir ölçü tekniği olduğu için, öteki yöntemlerden üstündür. Gaz kromatografisi, kimya endüstrisinin aşağı yukarı bütün dallarında, özellikle de petrol ve eczacılık alanlarında kullanılır. Süreç denetimlerinde, araştırmalarda ve alışılmış çözümleme laboratuvarlarında çok yararlı olur. Plastik, besin, mayalama, biyotıp, tıp ve adli tıp alanlarındaki kullanımları da hızla artmaktadır. Sektörde kullanımı ise doğal gazı oluşturan gazların oranlarını bulmak dolayısı ile gazın kalorifik değerini hesaplama şeklindedir. Kromatografiden elde edilen bu değerler, hacim olarak kullanılan gazın faturalandırılmasında kullanılmaktadır. Her RMS istasyonunda bulunmaktadır.

SCADA ile kromatografiden izlenebilecek değerler şunlardır;

- Doğal gazın bileşim değerleri,
- Üst ısı değeri,

- Nokta kapı açık/kapalı bilgisi,
- Rtu kabin kapı bilgisi,
- Elektrik kesintisi,
- Akü voltaj bilgisi,
- Pano sıcaklığı,
- Nokta bakım modu.



Şekil 3.22: Örnek bir kromatograf cihazın (Dağgaz, 2020).

e) Kokulandırma Ünitesi:

Doğal gaz renksiz ve kokusuz olduğundan dolayı insan duyuları tarafından algılanması, oldukça zordur. Kullanım sırasında olası kaçakların fark edilebilmesi ve önlemlerin zamanında alınabilmesi için içeriğine THT (Tetra Hidro Teofen) maddesi katılarak kokulandırılır. THT maddesi katıldıktan sonra çürük sarımsağa benzer bir koku alan doğalgaz böylelikle insanlar tarafından kolayca fark edilebilir. Bu amaçla THT ve / veya TBM (Tersiyer Bütil Merkaptan) kullanılır. Elektromekanik bir sistemle, boru hattından şehre verilen doğal gaz, sektördeki mevzuata uygun olarak kokulandırılır. Kokulandırma otomasyon sistemiyle çekiş baz alınarak otomatik/manuel yapılabilir. Her RMS istasyonunda bulunmaktadır.

SCADA ile kokulandırma istasyonunda izlenebilecek değerler şunlardır;

- Pompa durumları,
- Hatta verilen koku miktarı,

- Akış bilgisi,
- Sistem hata durumu,
- Koku maddesi depo bilgisi,
- Hatta verilen son koku miktarı,
- Otomatik / manuel bilgisi
- Çekişe göre kokulandırma periyodu,
- Manuel kokulandırma periyodu,
- Nokta kapı açık/kapalı bilgisi,
- RTU kabin kapı bilgisi,
- Elektrik kesintisi,
- Akü voltaj bilgisi,
- Pano sıcaklığı,
- Nokta bakım modu.



Şekil 3.23: Örnek bir kokulandırma ünitesi (Dağgaz, 2020).

f) Online Koku Ölçüm İstasyonları

Şebekenin girişinde hatta verilen koku miktarının bir nevi kontrolü için kullanılır. Şebekeye gerekenden fazla verilen koku ihbar olarak dönecektir. Ayrıca koku maddesinin aşındırıcı özelliğide vardır, maliyeti yüksektir, dünyada birkaç üretici vardır. Şehir genelinde en uç noktalara online koku ölçüm cihazları konumlandırılmıştır. Bu uç ölçüm noktalarından SCADA' ya alınan THT-TBM değerlerine göre RMS istasyonunda kokulandırma ünitlerinin koku değerleri operatörlerce set edilmektedir.

SCADA ile koku ölçüm istasyonlarından izlenebilecek değerler şunlardır;

- Ölçüm sıvı seviyesi,
- Saf su seviyesi,
- Kalibrasyon hatası,
- THT+TBM toplam koku miktarı,
- Nokta kapı açık/kapalı bilgisi,
- Rtu kabin kapı bilgisi,
- Elektrik kesintisi,
- Akü voltaj bilgisi,
- Pano sıcaklığı,
- Nokta bakım modu.



Şekil 3.24: Örnek bir uç nokta koku ölçüm cihazın (Dağgaz, 2020).

SCADA’daki ölçüm bilgileri öenli konuların başında gelmektedir. Ölçüm işlemi sıcaklı, basınç ve debi gibi bazı parametrelere dayalı olarak gerçekleştirilir. Doğal gazın içeriği de önemli bir konudur. Kromatografi, doğal gazın içeriğini belirler ve ilgili verileri sağlar. Doğal gazın filtrelenmesi de önemlidir. Arz güvenliği açısından filtre seçimine dikkat edilmeli ve filtre doluluk oranı SCADA otomasyon sistemi tarafından anlık olarak izlenmelidir.

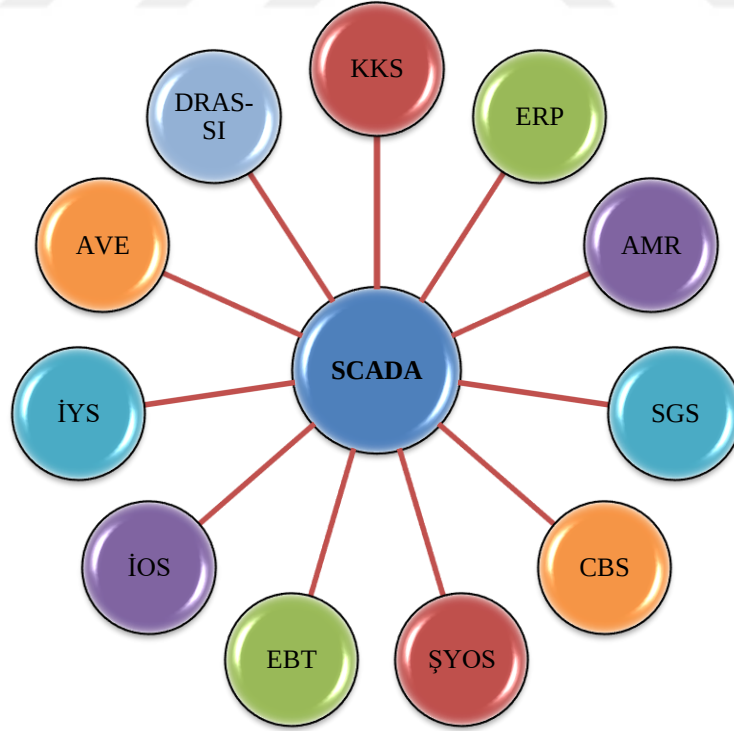
SCADA üzerinden tüm gaz dağıtım enstrümanlarının verileri önleyici bakım açısından değerlendirilmelidir. Bu bakım çalışmaları, verimliliği tamamen etkiler. Buna ek olarak, işletme ve bakım birbiriyle direk bağlantılıdır. Arz güvenliği SCADA için başka bir KPI’ dır. Bunlar dolaylı olarak verimlilik ile ilgilidir. Buna ilave olarak, SCADA’ nın veri aktarım

yöntemi ve alternatifleri de önemli bir konudur. Ayrıca, SCADA için güç kaynağı ve alternatif enerji kaynağı önem taşımaktadır.

Genel olarak bakıldığında KURUM-A' da 15 RMS-A şehir giriş istasyonu, 95 çelik kritik vana odası, 769 adet bölge regülatörü, 726 adet müşteri istasyonları, 761 adet SI deprem sensörü, 20 katodik koruma trafo redresör ünitesi, 7 uç noktada koku ölçüm cihazları ve bütün bu sistemler SCADA üzerinden takip edilmektedir. SCADA' nın akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki anahtar performans göstergeleri örnek olarak Tablo 3.10' da sunulmuştur. Bu KPI' lar, doğal gaz özelliklerine ilişkin olarak SCADA' daki süreçleri ele almaktadır.

3.3.1.4. SCADA Sistemi İle Haberleşen Sistemler

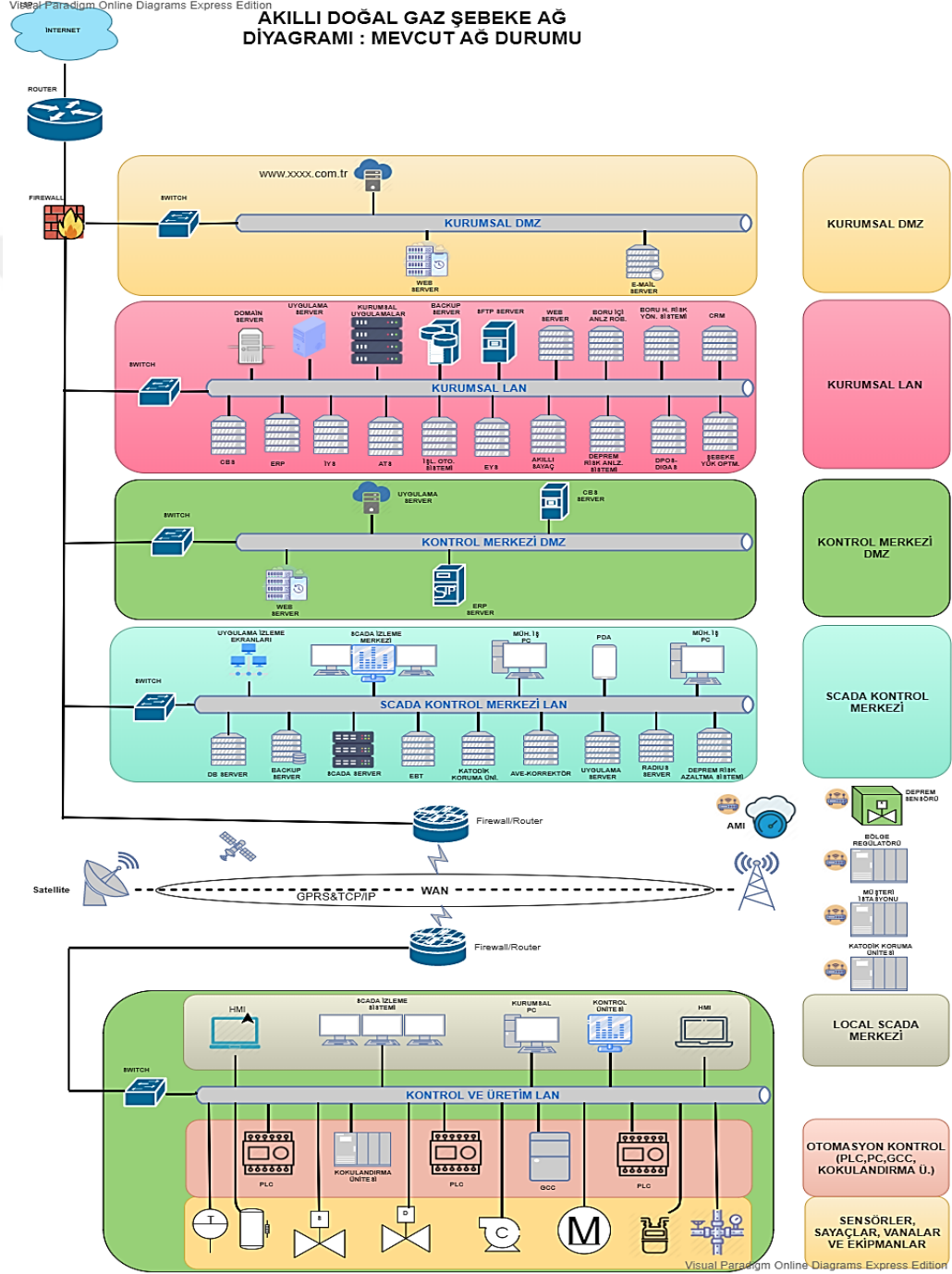
Örnek alınan sistemler incelendiğinde kurumsal olarak akıllı doğal gaz şebekesinin en büyük bileşeni olan SCADA sisteminin olduğu gözlemlenmektedir. SCADA sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü haberleşen sistemler aşağıdaki Şekil 3.25' de gösterilmiştir.



Şekil 3.25: SCADA sistemi ile haberleşen sistemler.

3.3.1.5. SCADA Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan SCADA sistemi incelenerek mevcut ağ mimarisi Şekil 3.26’ da verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.26: SCADA sistemi ağ mimarisi.

3.3.1.6. SCADA Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi SCADA sistemleri incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.10’ da verilmiştir. Bu KPI listesine göre kurumlardaki uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.10: SCADA siber güvenlik olgunluk seviyesi ve KPI örnek listesi.

SCADA Sistemi KPI Listesi		AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
SCADA Özellikleri (NIST SP-800, EPDK, CİS, COBIT, ISO/IEC 27001-27002-27019, KVKK, PCI DSS, ISA/IEC 62443:2009)		3,741	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
1	Erişim ve Kimlik Yönetimi											
(Büyük önem arz eden bir sistemde fiziksel erişim veya bilgilerin erişimi ve kullanılması için özel izlenimler, cevap verilmesi veya reddedilmesi sürecidir. Bir BT sistemindeki kaynaklara erişim, izin verilmesinin ön şartı olarak belirli kimlik bilgileri (örn. parola/şifre, biyometrik) kullanmak suretiyle bir kullanıcının, işletme veya cihazın kimliğinin doğrulanması sürecidir.)												
1.1	Kurumda, SCADA sistemlerinde erişim kontrol yönetim politikası ve prosedürü bulunuyor mu?		8	7	9	8	9	8,200	0,170	4,545	0,139	
1.2	Kurumda, SCADA sistemlerinde kullanıcı hesaplarının yönetimi politikası ve prosedürü bulunuyor mu?		2	1	4	3	4	2,800	0,058	1,552	0,016	
1.3	Kurumda, SCADA kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?		5	4	5	6	5	5,000	0,104	2,772	0,052	
1.4	Kurumda, SCADA uygulamalarına internet üzerinden erişim var mı?		1	2	1	2	1	1,400	0,029	0,776	0,004	
1.5	(Evetse), internete açık olan uygulamalarda hangi veri iletim protokolü kullanılıyor mu?		1	1	1	0	1	0,800	0,017	0,443	0,001	
1.6	(Evetse), WEB sunucularına erişimde veri yitilme yöntemi var mı?		1	3	1	1	1	1,400	0,029	0,776	0,004	
1.7	Kurumda, Rol Bazlı Erişim Kontrolü (RBK) kullanıcı erişim düzeylerini düzenlemek için roller, hiyerarşiler ve kısıtlamalar var mı?		5	4	5	6	5	5,000	0,104	2,772	0,052	
1.8	Kurumda, SCADA kullanıcıları için kimlik doğrulama sistemi var mı?		6	8	6	5	6	6,200	0,129	3,437	0,080	
1.9	Kurumda, SCADA'nın çalışma sistemini bozmayacak şekilde kullanılmayan port ve servislerin engelleniyor mu?		7	3	7	8	7	6,400	0,133	3,548	0,085	
1.10	Kurumda, SCADA ağı ve cihazlarına fiziksel erişimi kısıtlaması yapılıyor mu?		6	7	6	7	6	6,400	0,133	3,548	0,085	
1.11	Kurumda, SCADA sistemine özel güvenlik politikaları oluşturuluyor mu?		8	8	8	7	8	7,800	0,162	4,324	0,126	
1.12	Kurumda, OT ağlarda kritik iletişimin en güvenli katmanda gerçekleşmesini sağlayacak şekilde katmanlı bir ağı topolojisi var mı?		8	7	8	7	8	7,600	0,158	4,213	0,120	
1.13	Kurumda, OT ağılar ve IT ağılar topolojisi/fiziksel/manıksal olarak birbirinden ayrılmış/yalıtılmış mıdır?		9	7	9	8	9	8,400	0,174	4,656	0,146	
1.14	Kurumda, kurum ve SCADA ağıları arasında doğrudan trafiği önlemek için DMZ ağı mimarisini uyguluyor mu?		9	7	6	7	6	7,000	0,145	3,880	0,102	
1.15	(Evetse), DMZ' de uygulamalar bulunduruluyor mu?		10	7	9	8	9	8,600	0,178	4,767	0,153	
1.16	(Evetse), DMZ' de bir erişim yönetim prosedürü var mı?		9	7	9	9	9	8,600	0,178	4,767	0,153	
1.17	Kurumda, SCADA sistemlerine başarısız giriş denemeleri loglanmakta mıdır?		2	3	2	2	2	2,200	0,046	1,220	0,010	
1.18	Kurumda, SCADA sistemlerine uzaktan erişim yapılıyor mu?		5	4	5	6	5	5,000	0,104	2,772	0,052	
1.19	Kurumda, SCADA ve OT ağı erişim sağlayıcı dış kaynakların veya sistemlerin listesi var mıdır?		5	5	5	4	5	4,800	0,100	2,661	0,048	
1.20	Kurumda, SCADA sistemlerinde ve OT ağlarda internete erişim kısıtlanıyor mu?		7	6	7	6	7	6,600	0,137	3,659	0,090	
1.21	Kurumda, IT ağı üzerinden OT ağılarına bağlanma/erişim sağlanıyor mu?		6	7	6	7	6	6,400	0,133	3,548	0,085	
1.22	Kurumda, OT ağı üzerinden IT ağılarına bağlanma/erişim sağlanıyor mu?		8	6	8	9	8	7,800	0,162	4,324	0,126	
1.23	(Evetse), IT ağılar üzerinden OT ağılarına bağlanma/erişimde uygulanan güvenlik kontrolleri var mı?		2	3	2	3	2	2,400	0,050	1,330	0,012	
1.24	Kurumda, SCADA sistemlerinde operatör/mühendis bilgisayarlarının dahil olduğu ağına internete erişimi var mı?		6	4	6	5	6	5,400	0,112	2,993	0,060	
1.25	(Evetse), bu ağı üzerinde kablosuz erişim var mı?		8	9	6	5	6	6,800	0,141	3,769	0,096	
1.26	(Evetse), bu ağıya personelin özel mobil cihazları bağlanmakta mı?		6	7	6	7	6	6,400	0,133	3,548	0,085	
1.27	(Evetse), bu sistemlerin internete açık olmasının zorunlu olduğu durumlarda ise gerekli güvenlik önlemleri (güvenlik duvarı, uçtan uca şifreleme yöntemleri, yetkilendirme ve kimliklendirme mekanizmaları vb.) alınıyor mu?		4	5	4	5	4	4,400	0,091	2,439	0,040	
1.28	Kurumda, SCADA sistemlerinde erişimde web arayüzü kullanılıyor mu?		8	7	8	6	8	7,400	0,153	4,102	0,114	
1.29	Kurumda, SCADA binalarında kablosuz ağlara erişimde hangi güvenlik erişim protokolü kullanılmaktadır?		2	4	2	1	2	2,200	0,046	1,220	0,010	
1.30	Kurumda, SCADA sistemlerinde tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?		9	6	7	6	7	7,000	0,145	3,880	0,102	
1.31	(Evetse), tanımlama bilginin yönetimi grup ve rol bazlı yönetimi yapılıyor mu?		1	2	1	2	1	1,400	0,029	0,776	0,004	
1.32	Kurumda, SCADA sistemlerinde işletme dış kişiler için kimlik tanımlama ve yetkilendirme yapılıyor mu?		1	3	1	2	1	1,600	0,033	0,887	0,005	
1.33	Kurumda, SCADA sistemlerinde parola doğrulaması yapılıyor mu?		5	6	5	6	5	5,400	0,112	2,993	0,060	
1.34	Kurumda, SCADA sistemlerinde Fiziksel Token veya Akıllı Kart ile kimlik doğrulama yapılıyor mu?		2	3	2	1	2	2,000	0,041	1,109	0,008	
1.35	Kurumda, SCADA sistemlerinde parola belirleme ve kullanım kuralları var mı?		3	5	3	4	3	3,600	0,075	1,996	0,027	
			185	178	180	179	180	180,400	3,741	100,000	2,354	63%

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI' lar toplamlar üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 63 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

SCADA sistemi belirlenen KPI' lara ve soru setlerine göre değerlendirildi. Tüm KPI' lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi SCADA sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 60' ır. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Prosedür, Yasalar ve Mevzuatlara Uyum, Siber Güvenlik Test Yönetimi ve Siber Güvenlik Yatırım Bütçesi Planlama olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından SCADA sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 60 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından düşük olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. SCADA sistemlerinde kurumların tüm siber saldırı yöntemlerini dikkate alarak kurumun IT ve OT sistemlerini en yüksek seviyede korumaları önem arz etmektedir. Özellikle enerji altyapılarına ve kurumlara en yaygın saldırılar olan Hizmet Kesintisi (DDoS), Araya Girme Saldırısı (MITM), Zararlı Yazılımlar (Malware (Worm,Trojan, Rootkit, Virus)), Replay Saldırısı, Sahtecilik (Spoofing) (ARP,IP,GPS), MODBUS/TCP Protocol Attack, DNP3 Protocol Attack, Malicious Command and Software Injection, Buffer Overflow, Sosyal Mühendislik, Fiziksel Saldırı (Sensör, Actuator, Kamera), SQL Injection, Zero Day Attack ve Phishing (Oltalama) saldırıları ile akıllı doğal gaz şebekelerine sahip enerji kurumları tarafından bu saldırılara maruz kalmaktadırlar. Bu saldırıların engellenmesi için standartlara uyum, log yönetimi, yama yönetimi, ağ segmentasyon, sıkılaştırma, açık portların kapatılması, verilerin gizliliği, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

Günümüzde hayati derecede önem taşıyan SCADA sistemlerinin güvenliğinin sağlanması için aşağıdaki hususların göz önünde bulundurulması fayda sağlayacaktır:

- Truva atı sayesinde boru hattı basınç değerlerinin değiştirilmesi önlenmesi için RTU, PLC ve modem vb. sistemlerin tüm güvenlik önlemleri fiziksel ve uygulama olarak alınmalıdır. Tüm ssitemlerin güvenlik testleri yapılmalıdır.
- Saldırganlar kablolu ve kablosuz güvenlik kameralarında bulunan zafiyeti sömürerek ağa dahil olabilecekleri bilinmektedir. Dahil olunan kamera ağından kontrol ağına sızan saldırganlar saha elemanlarına ulaşmaları engellenmelidir. Bu nedenle ağların bölümlenmesi önem arz etmektedir.
- Operatör hataları göz önünde bulundurulmalıdır ve risk olarak ele alınmalıdır.
- Yazılımsal hatalar göz önünde bulundurulmalıdır ve risk olarak ele alınmalıdır.
- DDOS saldırıları ile SCADA sistemlerine web uygulamaları üzerinden hizmet kesintisi ve kurumsal ağlara yapılan saldırılar, VPN kimlik bilgilerine erişebilmesi sayesinde şirket içi ağlarda dolaşabilir hale gelmiştir. Bu nedenle DDoS saldırılarını önlemek için

VPN üzerinden bağlantılar ve site to site bağlantıların DDoS önelemek için güvenlik testleri yapılmalı ve güvenlik açısından önlemler alınmalıdır.

- Veritabanına SQL injection saldırısı yapılmaması için yazılımsal ve donanımsal güvenlik testleri geliştirme safhasında ve satın alım aşamasında penetrasyon test sonuçları istenilmelidir.
- Zararlı yazılımlar (APT, Malware, Solucan vb.) ile SCADA sistemlerine saldırıların yapılması ve basınç,sıcaklık ve ölçülebilen değerlere müdahale edilerek sistemlere zarar verilmesini önlemek için ağ bölümlene yapılmalı ve cihazlar internete kapalı olmalıdır.
- SCADA MITM saldırganlar açık metin olarak iletilen trafiği dinleyebilmekte ve paketler üzerinde değişiklik yaparak sahadaki işleyişe müdahale edebilmektedir. Bu neden ile araya girme saldırılarının önlenmesi için iletilen verilerin clear text değil verilerin şifreli olarak kullanılmalıdır.
- Zero Day Atakları: Yerel ağda yayılırken kendini gizlemek için 4 adet sıfırıncı gün açığını kullanmaktadır. PLC cihazına ulaştığında ise koda müdahale ederek kendini gizlemektedir. Bu nedenle tüm cihazlar şifreli olmalı ve güncellemeleri zamanında yapılmalıdır.
- Gerekli yetki ve sorumlulukların belirlenmesi için sadece ilgili kişiler RBEC yöntemi ile belirlenmelidir.
- Ağ mimarisinin kontrol edilmeli ve gereksiz alanların erişime kapatılmalıdır .(Sisteme internetten doğrudan/dolaylı erişim var mı?)
- Yama, güncelleme ve yaşam döngüsü yönetimi süreçlerinin oluşturulmalıdır ve kurumda yama yönetimi yapılmalıdır. Uygulama ve işletim sistemi yamaları zamanında yapılmalıdır.
- Ağ bölmelerinin düzenlenmesi gereklidir (Web sunucularıyla kullanıcıların ortak ağda olması tehlikelidir.)
- Kritik önem taşıyan parçaların fiziksel güvenliğinin sağlanmalıdır.
- Güvenlik personeli sayısının artırılması ve görevlerinin tam olarak belirlenmesi önemlidir.
- Çalışmasına izin verilen uygulamaları belirlenmesi ve uzak bağlantılarda kimlik doğrulaması sistemi mutlaka kullanılmalıdır.
- Sistemlerin takibi için gerekli güvenlik izleme sisteminin kurulmalıdır.

- SIEM uygulaması ile tüm güvenlik logları takip edilemelidir.

3.3.2. Akıllı Doğal Gaz Şebekesinde Elektronik Bülten Tablosu (EBT)

Akıllı doğal gaz şebekesinde doğal gaz dağıtımının akıllı şebeke mantığında yapılması için gerekli bir diğer sistem de Elektronik Bülten Tablosu' dur. Elektronik Bülten Tablosu (EBT); piyasada faaliyet gösteren tarafların piyasa hareketlerini takip edebilmeleri için kurulmuş olan ve iletim şirketince işletilen sistemdir (EMRA, 2002). EBT sisteminin asıl amacı boru hatlarının optimum kullanımını sağlamaktır. Yıl içinde kış aylarında oluşan pik tüketimlerdeki doğal gaz arz güvenliğini sağlamak maksadıyla tüketimler takip edilmekte EBT üzerinden raporlanmakta ve kriz senaryoları oluşturmada veri havuzu oluşturmaktadır. Veriler sayesinde doğru tüketim tahminleri yapmak ve alım-satım kontratları ayarlamak mümkün hale gelmektedir. Doğal gaz alım-satım sözleşmelerinde uygulanmakta olan “take or pay” cezasına düşmeyecek şekilde Türkiye eylem planını optimum noktaya getirmektir. Eğer, al ya da öde taahhüdü miktarının altında gaz teslim alınmışsa, taahhüt miktarı ile teslim alınan miktar arasındaki fark al ya da öde ödemesi olarak satıcıya ödenmesi gerekmektedir (Roberts, 2011).

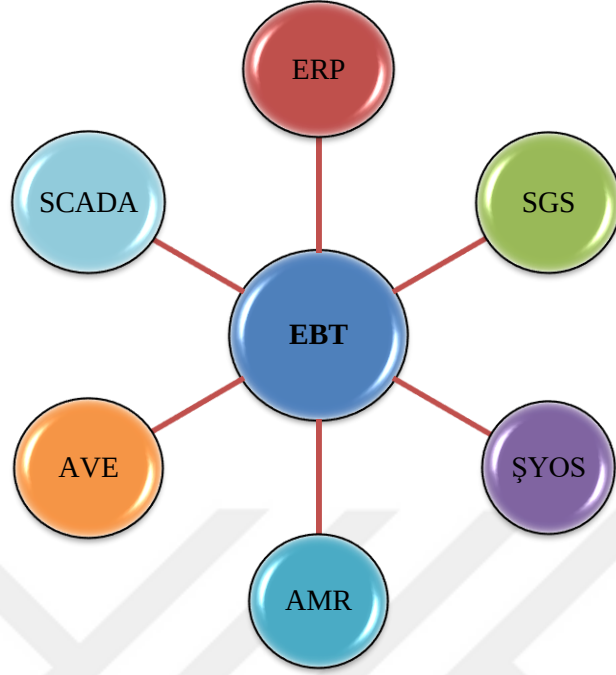
Doğal gaz dağıtım firmalarının sevkiyat kontrol merkezleri bu sistem üzerinden raporlarını EPDK' ya iletmektedir. Bu veriler bir sistem üzerinden iletmektedir. EPDK bu sistemin kurulmasını 31.12.2004 tarihine kadar tüm gaz dağıtıcılarına zorunlu tutmuştur. EPDK yayınlamış olduğu “Doğal Gaz İletim Şebekesi İşleyiş Yönetmeliği” gereğince, doğal gaz dağıtım şirketleri, işleyişin takip edilmesi amacıyla gerekli ölçüm verilerini BOTAŞ' a bu sistem üzerinden sunmaktadır. Ayrıca dengeleme gazı piyasası çalışmaları ile siber güvenlik olgunluğu arttırılmaya çalışılmaktadır. İletim şirketi, BOTAŞ, bu sistem üzerinden; taşıma miktarı, programlanan ve iletilen miktarlar, kesinti veya azaltma talep ve miktarları, sistem dengeleme talimatları ve kapasite tahsisleri gibi iletim şebekesinin işleyişini takip etmektedir.

Şekil 3.27: EBT giriş ekranı (BOTAS, 2020).

Kurumlar tarafından RMS-A istasyonlarına ait tüm ölçüm verileri otomatik olarak BOTAS' ın EBT sistemine online ve otomatik olarak aktarılmaktadır (İGDAŞ, 2014). Arz güvenliğinin sağlanması ve yıllık tüketilecek gaz miktarının hesaplanması için o yılki gaz istatistikleri büyük önem taşımaktadır. Aynı şekilde bu sisteme aktarılan bilgilerin doğruluğu da sistemin ürettiği değerlendirmeleri etkileyecektir. Dolayısıyla EBT' ye aktarılan verilerin doğru, anlık, hatasız, noktasal olarak sağlanması sistemin olgunluğunu göstermektedir. Bu olgunluğu tespit etmek için performans göstergeleri ek olarak belgelenmiştir. EBT' nin akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki anahtar performans göstergeleri örnek olarak Tablo 3.11' de sunulmuştur. Mevzuat ve şartnameye bağlı olarak bu faktörlerin düzeyleri belirlenmiştir.

3.3.2.1. EBT Sistemi İle Haberleşen Sistemler

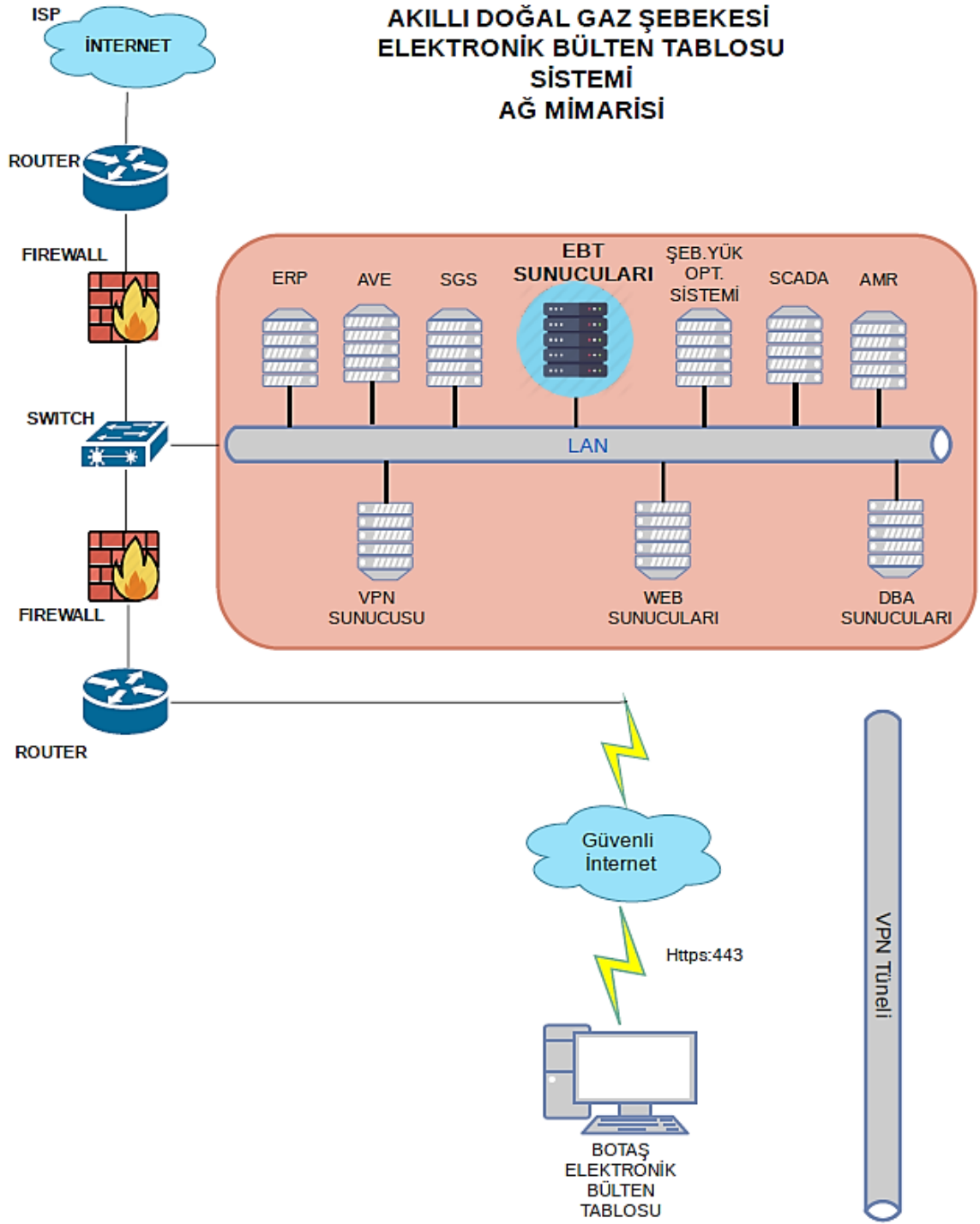
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde EBT sistemi akıllı şebekenin bir parçasıdır. EBT sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.28' de gösterilmiştir.



Şekil 3.28: EBT sistemi ile haberleşen sistemler.

3.3.2.2. EBT Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan EBT sistemi incelenerek mevcut ağ mimarisi Şekil 3.29’da verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.29: EBT sistemi ağ mimarisi.

3.3.2.3. EBT Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi EBT sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.11’ de verilmiştir. Bu KPI listesine göre kurumlardaki

uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.11: EBT siber güvenlik olgunluk seviyesi ve KPI listesi.

Elektronik Bülten Tablosu (EBT) KPI Listesi										AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
EBT Özellikleri (NIST SP-800, EPDK, CIS, COBIT, ISO/IEC 27001-27002-27019, KVKK, PCI DSS, ISA/IEC 62443:2009)										1,832	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
1 Erişim ve Kimlik Yönetimi																				
(Büyük sistemler için en azından aşağıdaki faktörlerin her birinin değerlendirilmesi gerekir. Bu EBT sistemlerdeki kayıtlara erişim için verilmemesi de pati olarak kabul edilebilir. (örneğin, parolalar, biyometrik, kullanıcılar, kullanıcılar, işlemler veya cihazlar kimliği) (gizli bilgilerin korunması için).																				
1.1 EBT Sistemlerinde, erişim kontrol yönetim politikası ve prosedürü bulunuyor mu?										7	8	7	6	7	7	0,093	5,095	0,065		
1.2 EBT Sistemlerinde, kullanıcı hesapları yönetim politikası ve prosedürü bulunuyor mu?										7	8	7	8	7	7,4	0,099	5,386	0,073		
1.3 EBT Sistemlerinde, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?										8	5	8	7	8	7,2	0,096	5,240	0,069		
1.4 EBT Sistemlerinde, sunuculara erişimde güvenli bağlantı protokolleri kullanılıyor mu?										1	2	1	1	3	1,6	0,021	1,164	0,003		
1.5 EBT Sistemlerinde, sunuculara erişim güvenli veri şifreleme yöntemi kullanılıyor mu?										4	4	2	4	5	3,8	0,051	2,766	0,019		
1.6 EBT Sistemlerinde, internete ve sistemlere başarısız giriş denemeleri raporlanıyor mu?										9	9	7	9	9	8,6	0,115	6,759	0,099		
1.7 EBT Sistemlerinde, internete ve sistemlere başarısız giriş denemeleri raporlanıyor mu?										6	6	7	6	6	6,2	0,083	4,512	0,051		
1.8 EBT Sistemlerinde, kullanılan uzaktan erişimde güvenli bağlantı protokolleri kullanılıyor mu?										3	4	3	4	3	3,4	0,045	2,475	0,015		
1.9 EBT Sistemlerinde, kullanılan uzaktan bağlantı erişimleri için erişim kuraları var mı?										4	4	4	5	4	4,2	0,056	3,057	0,024		
1.10 EBT Sistemlerinde, kullanılan uzaktan erişim için güvenli veri şifreleme yöntemi var mı?										1	1	3	2	1	1,6	0,021	1,164	0,003		
1.11 EBT Sistemlerinde, erişim yetkilendirmeleri ve kısıtlamaları belirlenerek bilgi paylaşımı yapılıyor mu?										1	1	2	1	1	1,2	0,016	0,873	0,002		
1.12 EBT Sistemlerinde, Rol Bazlı Erişim Kontrolü (RBEX) kullanıcı erişim düzeylerini düzenlemek için roller, hiyerarşiler ve kısıtlamalar kullanılıyor mu?										7	7	8	7	7	7,2	0,096	5,240	0,069		
1.13 EBT Sistemlerinde, kurumsal ağa erişim sağlayan dış kaynakların veya sistemlerin listesi var mı?										8	8	7	8	8	7,8	0,104	5,677	0,081		
1.14 EBT Sistemlerinde, yetkisiz erişim eylemlerini tespit etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapılıyor mu?										6	6	6	7	6	6,2	0,083	4,512	0,051		
1.15 EBT Sistemlerinde, farklı kaynaklar üzerinden elde edilen kullanıcı erişim iz kayıtları ile verinin toplanması ve ilişkilendirilmesi (korelasyon) yapılıyor mu?										4	4	4	5	4	4,2	0,056	3,057	0,024		
1.16 EBT Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?										5	4	5	5	5	4,8	0,064	3,493	0,031		
1.17 EBT Sistemlerinde, işletme dışı kişiler için kimlik tanımlama ve yetkilendirme yapılıyor mu?										3	4	3	4	3	3,4	0,045	2,475	0,015		
1.18 EBT Sistemlerinde, parola doğrulaması yapılıyor mu?										2	2	4	2	2	2,4	0,032	1,747	0,008		
1.19 EBT Sistemlerinde, parola belirlenme ve kullanım kuralları var mı?										9	9	8	9	9	8,8	0,117	6,405	0,103		
1.20 EBT Sistemlerinde, ayrıcalıklı hesapların yönetimi yapılıyor mu?										10	8	9	10	9	9,2	0,123	6,696	0,113		
1.21 EBT Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları tutuluyor mu?										5	5	6	5	5	5,2	0,069	3,785	0,036		
1.22 EBT Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?										5	5	4	5	5	4,8	0,064	3,493	0,031		
1.23 EBT Sistemlerinde, mobil iletişim sadece online ile haberleşme sağlanıyor mu?										6	8	7	6	6	6,6	0,088	4,803	0,058		
1.24 EBT Sistemlerinde, belirlenen uygulamalarında dışında herhangi bir uygulama çalışıyor mu?										8	8	7	8	8	7,8	0,104	5,677	0,081		
1.25 EBT Sistemlerinde, mobil cihazlara uygulama yüklemeye yetkisi var mı?										2	2	0	2	2	1,6	0,021	1,164	0,003		
1.26 EBT Sistemlerinde, mobil cihazlara erişim yetkisi sınırlı mı?										5	5	6	5	5	5,2	0,069	3,785	0,036		
										136	137	135	141	138	137,4	1,832	100,000	1,164	64%	

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI' lar toplamı üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 64 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

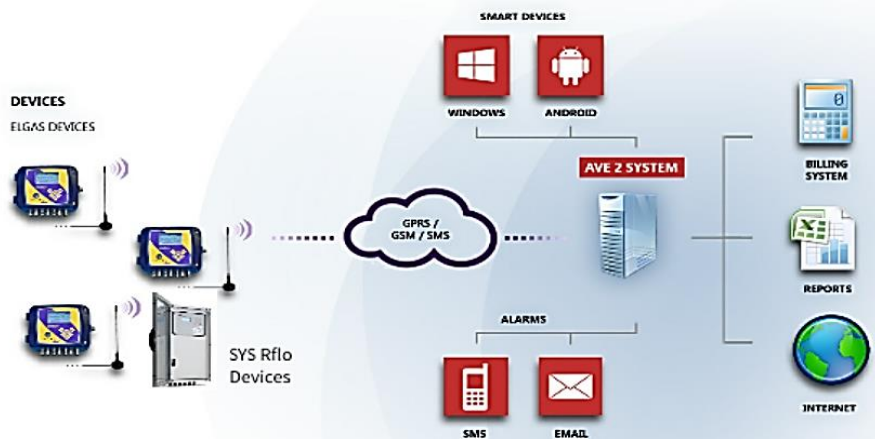
EBT sistemi belirlenen KPI' lara ve soru setlerine göre değerlendirildi. Tüm KPI' lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi EBT sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 74' tür. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi / Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından EBT sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 74 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. EBT sistemlerine siber saldırı yöntemi olarak Hizmet Kesintisi (DDoS), Araya Girme Saldırısı (MITM), Zararlı Yazılımlar (Malware (Worm, Trojan, Rootkit, Virus)), Replay Saldırısı ve Sahtecilik (Spoofing) (ARP, IP, GPS) saldırıları

yapılabileceği görülmektedir. Bu saldırılara karşı güvenlik önlemleri alınmalıdır. Öncelikle uygulamanın veritabanı ve sunucular arasındaki verilerin şifreli olması iletişim güvenlik protokoller üzerinden sağlanması gerekmektedir. Ayrıca yama ve log yönetimi, envanter yönetimi, varlık yönetimi yapılmalıdır. Güvenli protokoller ve sertifikalar kullanılarak VPN erişimleri sağlanmalıdır.

3.3.3. Akıllı Doğal Gaz Şebekesinde Ölçme ve Raporlama Sistemi (ÖRS-AVE)

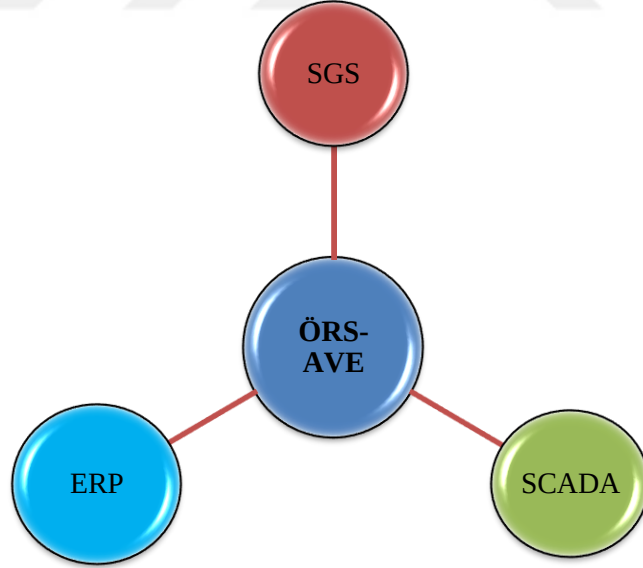
Akıllı doğal gaz dağıtımını akıllı şebeke konseptinde yapılabilmesi için gerekli bir diğer sistem de ölçme raporlama sistemidir. Bu sistemini temel amacı 300 mbar üzerinde basınçla gaz kullanan serbest tüketicilerin ve bölge regülatörlerinin ve gaz tüketim miktarlarının online olarak takip edebilmelerini sağlamaktır. Sistem doğal gaz tesisatına entegre Korrektör yardımıyla sıcaklık ve basınç değerlerine göre tüketilen gaz miktarını düzelterek anlık doğru ölçüm ve kayıt yapmaktadır. Sistem 15 dk aralıkla okuma yapmakta ve düzeltme işlemi yapmaktadır. Ayrıca sistem normal hacim, düzeltilmiş hacim, basınç, sıcaklık ve düzeltme katsayısı değerlerini kaydetmektedir. Başka bir ifadeyle, sistem faturalandırmada esas alınmak üzere anlık hacim düzeltme işlemi ve online raporlama yapmaktadır. Bu sayede firmalar tüketimlerini online takip ederek tüketim profillerini analiz ederek verimlilik için adım atabileceklerdir. Sistem aynı zamanda bölge regülatörlerindeki fiziksel saha ekipmanı SCADAPack-RTU (Remote Terminal Unit) yardımıyla SCADA sistemine erişimi sağlamaktadır. ÖRS sistemini bir parçası olan RTU sahadan gelen sinyal ve bilgileri merkez kontrol sistemine ileten ve merkez kontrol sisteminden gelen komutları sahaya taşıyan elektronik bir cihazdır. ÖRS sistemi, otomasyon sistemlerinin bir bileşeni olarak doğal gaz dağıtım ağına çok önemli bir katkı sağlar. Sistemin çalışma prensibi, yüksek kapasitede gaz kullanan müşterilerin tüketim miktarını doğru bir şekilde ölçmek ve SCADA birimine GPRS (general packet radio service) aracılığıyla ulaştırmaktır. AVE' nin akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.12' de sunulmuştur. Mevzuat ve şartnameye bağlı olarak bu faktörlerin düzeyleri belirlenmiştir.



Şekil 3.30: Örnek ÖRS-AVE sistem mimarisi.

3.3.3.1. ÖRS-AVE Sistemi İle Haberleşen Sistemler

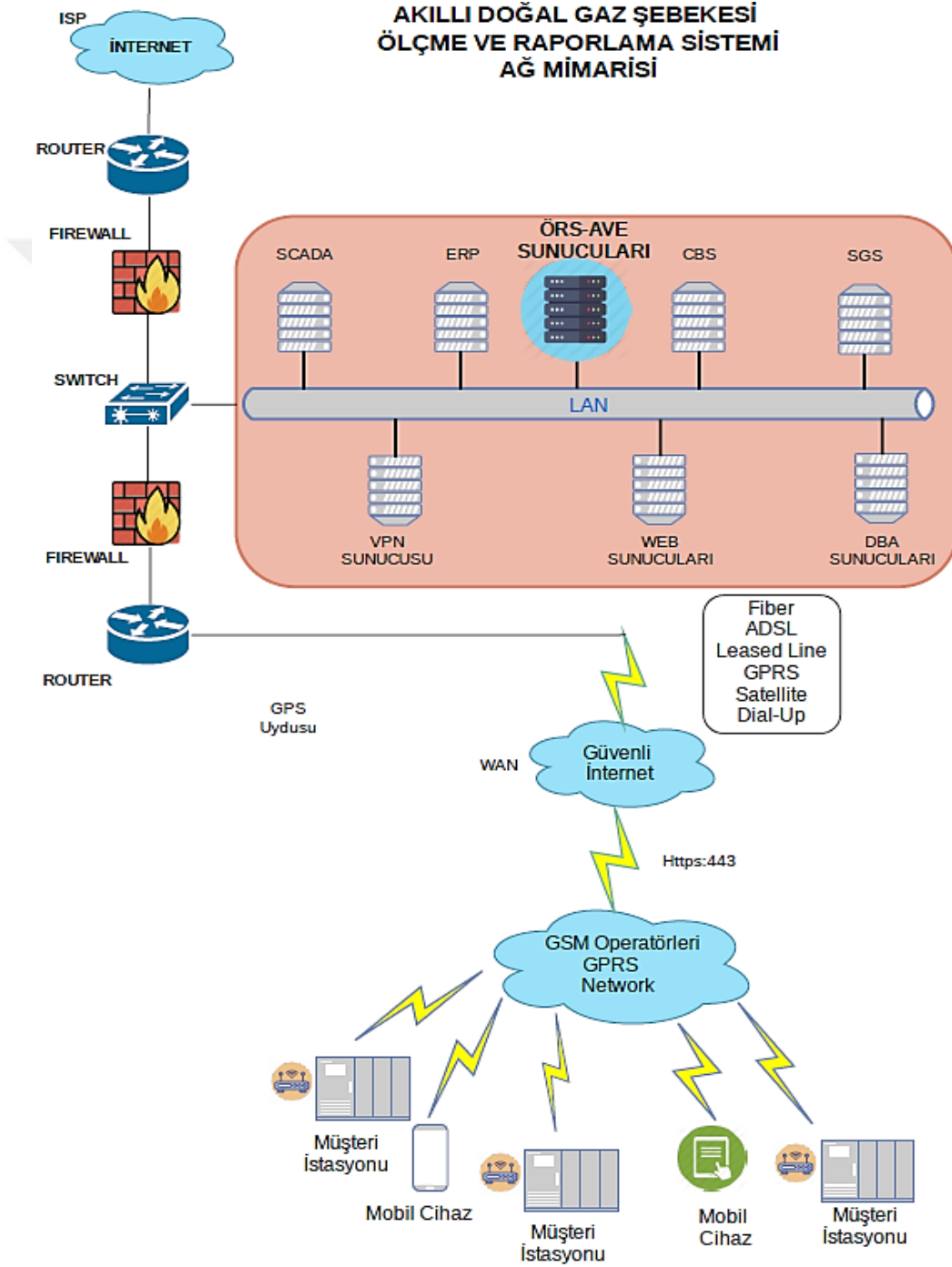
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde ÖRS-AVE sistemi akıllı şebekenin bir parçası olduğu gözlemlenmektedir. ÖRS-AVE sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.31’ de gösterilmiştir.



Şekil 3.31: ÖRS-AVE sistemi ile haberleşen sistemler.

3.3.3.2. ÖRS-AVE Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan ÖRS-AVE sistemi incelenerek mevcut ağ mimarisi Şekil 3.32’ de verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.32: ÖRS-AVE sistemi ağ mimarisi.

3.3.3.3. ÖRS-AVE Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi ÖRS-AVE sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.12’ de verilmiştir. Bu KPI listesine göre kurumlardaki uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.12: ÖRS-AVE siber güvenlik olgunluk seviyesi ve KPI listesi.

Ölçüm Raporlama Sistemi (ÖRS&AVE) KPI Listesi		AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
1	Erjişim ve Kimlik Yönetimi	0,939	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
	(Bilgi sistem ortamında kullanıcı faaliyetlerini yapıp bilgileri edinirken ve bu faaliyetleri için dış sistemlere erişim vermesini sağlayan uygulamaları içerir. Bir BT sisteminde kullanıcıların erişim vermesini denetleyen ve bunu kontrol eden uygulamaları içerir.)											
1.1	ÖRS&AVE Sistemlerinde, erişim kontrol yönetimi politikası ve prosedürü bulunuyor mu?	7	8	9	8	7	7,8	0,039	4,176	0,031		
1.2	ÖRS&AVE Sistemlerinde, kullanıcı hesapları yönetimi politikası ve prosedürü bulunuyor mu?	7	9	7	8	7	7,6	0,038	4,069	0,029		
1.3	ÖRS&AVE Sistemlerinde, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?	8	7	8	9	8	8	0,040	4,283	0,032		
1.4	ÖRS&AVE Sistemlerinde, sunuculara erişimde güvenli bağlantı protokolleri kullanılıyor mu?	7	8	7	9	3	6,8	0,034	3,640	0,023		
1.5	ÖRS&AVE Sistemlerinde, sunuculara erişim güvenli veri şifreleme yöntemleri kullanılıyor mu?	4	6	4	5	5	4,8	0,024	2,570	0,012		
1.6	ÖRS&AVE Sistemlerinde, internete ve sistemlere bağlanış erişim denemeleri kullanılıyor mu?	7	7	9	8	9	8,4	0,042	4,897	0,035		
1.7	ÖRS&AVE Sistemlerinde, internete ve sistemlere bağlanış erişim denemeleri raporlanıyor mu?	9	9	9	9	6	8,4	0,042	4,897	0,035		
1.8	ÖRS&AVE Sistemlerinde, kullanılan uzaktan erişimde güvenli bağlantı protokolleri kullanılıyor mu?	8	9	8	9	8	8,4	0,042	4,897	0,035		
1.9	ÖRS&AVE Sistemlerinde, kullanılan uzaktan bağlantı erişimleri için erişim kuralları var mı?	7	6	7	4	6	6	0,030	3,212	0,018		
1.10	ÖRS&AVE Sistemlerinde, kullanılan uzaktan erişim için güvenli veri şifreleme yöntemi var mı?	5	6	5	6	5	5,4	0,027	2,891	0,015		
1.11	ÖRS&AVE Sistemlerinde, erişim yetkilendirmeleri ve kısıtlamaları belirlemek bilgi paylaşım yapıyor mu?	6	6	8	6	5	6,2	0,031	3,319	0,019		
1.12	ÖRS&AVE Sistemlerinde, Rol Bazlı Erişim Kontrolü (RBK) kullanıcı erişim düzeylerini düzenlemek için roller, hiyerarji ve kısıtlamalar kullanılıyor mu?	7	7	7	8	7	7,2	0,036	3,854	0,026		
1.13	ÖRS&AVE Sistemlerinde, kurumsal ağa erişim sağlayıcılar dış kaynaklılar için düzenli tarama var mı?	8	7	8	8	8	7,8	0,039	4,176	0,031		
1.14	ÖRS&AVE Sistemlerinde, yetkileri erişim eylemlerini tespit etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapıyor mu?	6	6	8	7	6	6,6	0,033	3,533	0,022		
1.15	ÖRS&AVE Sistemlerinde, farklı kaynaklar üzerinden elde edilen kullanıcı erişim iz kayıtları ile verinin toplanması ve ilişkilendirilmesi (korelasyon) yapıyor mu?	4	6	4	6	4	4,8	0,024	2,570	0,012		
1.16	ÖRS&AVE Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?	5	7	5	6	5	5,6	0,028	2,998	0,016		
1.17	ÖRS&AVE Sistemlerinde, işletme dış kişiler için kimlik tanımlama ve yetkilendirmeye yapıyor mu?	6	7	5	7	6	6,2	0,031	3,319	0,019		
1.18	ÖRS&AVE Sistemlerinde, parola doğrulaması yapıyor mu?	6	7	6	7	6	6,8	0,034	3,640	0,023		
1.19	ÖRS&AVE Sistemlerinde, parola belirleme ve kullanım kuralları var mı?	7	9	8	9	9	8,4	0,042	4,897	0,035		
1.20	ÖRS&AVE Sistemlerinde, ayrıcalıklı hesapların yönetimi yapıyor mu?	9	10	9	10	9	9,4	0,047	5,032	0,044		
1.21	ÖRS&AVE Sistemlerinde, uygulamalar üzerinde yapılan işlemlerin logları tutuluyor mu?	9	9	9	9	9	8,2	0,041	4,390	0,034		
1.22	ÖRS&AVE Sistemlerinde, uygulamalar üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?	9	9	9	9	9	8,2	0,041	4,390	0,034		
1.23	ÖRS&AVE Sistemlerinde, mobil iletişim sadece online kanı merkez ile haberleşme sağlanıyor mu?	6	6	6	6	6	6	0,030	3,212	0,018		
1.24	ÖRS&AVE Sistemlerinde, belirlenen uygulamalarının dışında herhangi bir uygulama çalışıyor mu?	8	8	9	8	8	8,2	0,041	4,390	0,034		
1.25	ÖRS&AVE Sistemlerinde, mobil cihazlara uygulama yüklemek yetkisi var mı?	10	10	10	10	7	9,2	0,046	4,925	0,043		
1.26	ÖRS&AVE Sistemlerinde, mobil cihazlara erişim yetkisi sınırlı mı?	5	7	8	7	6	6,4	0,032	3,426	0,021		
		184	194	194	194	196	186,8	0,939	100,000	0,696		74%

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI' lar toplamı üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 74 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

ÖRS-AVE sistemi belirlenen KPI' lara ve soru setlerine göre değerlendirildi. Tüm KPI' lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi ÖRS-AVE sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 71' dir. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından ÖRS-AVE sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 71 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu

oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. ÖRS-AVE sistemlerinde Hizmet Kesintisi (DDoS), Araya Girme Saldırısı (MITM), Zararlı Yazılımlar (Malware (Worm,Trojan, Rootkit, Virus)), Replay Saldırısı, Sahtecilik (Spoofing) (ARP,IP,GPS), MODBUS/TCP Protocol Attack, DNP3 Protocol Attack, Malicious Command and Software Injection, Buffer Overflow saldırıları ve fiziksel saldırıların yaşandığı gözlemlenmektedir. Bu saldırıların engellenmesi için standartlara uyum, fiziksel güvenlik için gerekli önlemlerin alınması, GPRS modem sistemlerinin çalınmasının engellenmesi, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

3.3.4. Akıllı Doğal Gaz Şebekesinde Akıllı Sayaç (AMI/AMR)

Akıllı şebeke konseptinin olmazsa olmaz diğer bir gereği de akıllı sayaçlardır. Gaz dağıtımında akıllı sayaçlar akış yönetiminin de önemli bir parçasıdır. Akıllı sayaçların temel amacı son kullanıcının tüketim verilerini uzaktan okumak ve şebeke üzerinde kayıp-kaçak kullanımların tespit edilmesidir. Akıllı sayaçlar sistem üzerinde anlık okuma özelliği sayesinde bölgesel olarak toplam kayıp-kaçak kullanım miktarının tespit edilebilmesine imkân sağlamaktadır. Bu açıdan akıllı sayaç, akıllı şebeke konseptinin önemli bir parçasıdır.

Akıllı sayaçların iki farklı sistemle çalışan çeşitleri mevcuttur. Bunlar ölçüm ve haberleşmenin birlikte tamamen elektronik gaz ölçüm sayaçları ve klasik sayaçlara modüler olarak ilave edilebilen çeşitlerdir. Hacimsel ölçüm yapan körüklü ve rotary sayaçlar, eklenen modül yardımıyla akıllı sayaçlar sınıfına girmektedir. Türbin ve ultrosonik sayaç çeşitleri tam elektronik gaz sayaçlarındandır. Bu iki çeşit akıllı sayaç pilot uygulamalarla sektörde kullanılmaktadır. Akıllı sayaçlar konut tüketimlerinde çoğunlukla tercih edilmemektedir. Akıllı sayaçların diğer bir özelliği de yapısındaki korrektör cihazı sayesinde sıcaklık ve basınç değerlerini kullanarak elde ettikleri düzeltme kat sayısı ile düzeltilmiş gaz hacmini tespit etmektedir. Sanayi tüketimlerinde 300 mbar üzeri gaz tüketimi yapan müşterilerde kullanılmaktadır.

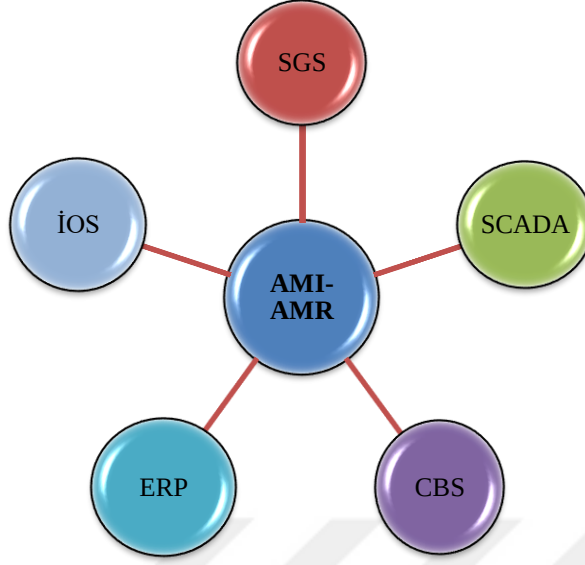
EPDK' nın sayaçlar, dağıtım şirketinin mülkiyeti olup abone bağlantı bedeli dışında hiçbir bedel alınmadan dağıtım şirketince temin edilerek sisteme dâhil edilir, hükmü dolayısıyla akıllı sayaçların maliyetleri dağıtım şirketi üzerindedir. Ayrıca akıllı sayacın kendisinin, pil değişim

ve bakım maliyetlerinin yüksek olması dolayısıyla sektörde kullanım oranı düşüktür. Bu durum ülkemizde akıllı sayaç uygulamalarını yavaşlatmaktadır. Ortalama 4-5 yıl olduğu tespit edilen akıllı sayaç pil ömürlerinin uzatılması bu engeli ortadan kaldıracaktır. EPDK' nın, ihbarname ve/veya faturayı, son ödeme tarihinden en az yedi gün önce abone adresine bırakır hükmünden dolayı dağıtım şirketi tasarruf sağlayamamaktadır.

Akıllı sayaç üreticilerinin ve düzenleyici kurumların sektör ihtiyaçlarına göre yapacakları değişikliklerle akıllı sayaç kullanımının yaygınlaşması beklenmektedir (EMRA, 2002). Akıllı sayaçların ölçüm ve veri aktarımı konusunda birçok standart mevcuttur. Avrupa birliği sayaçların sahip olması gereken özellikleri Ölçüm Aletleri Yönergesinde (MID) belirlemiştir (European Norm, 2013). Bu itibarla MID onayı akıllı sayaçlarda aranan bir kriterdir. Akıllı sayaçların performans kriterlerini belirleyen diğer bir husus olan veri aktarımı GPRS (Operatör) ve RF (Radio Frekans) üzerinden yapılmaktadır. Bu alanda veri aktarımının yapıldığı M-bus (Meter-Bus) Avrupa normu olan haberleşme protokolüdür (BSI, 2020). Akıllı sayaçların uzaktan okunmasını ya da harici bir merkezi kontrol cihazına veri aktarımı yapılarak binanın enerji dengesini daha esnek bir şekilde gözlemlemenizi sağlamaktadır. Bu protokol, IEC (International Electrotechnical Commission) tarafından tanımlanmış olup IP 55 koruma kodu herhangi bir dış müdahaleyi engellemek ve tüketim bilgilerinin aktarılması için gerekmektedir (Hauge, 2003). Bu koruma protokolleri akıllı sayaçların siber güvenliğini sağlamaktadır. Akıllı sayaçların pil ömrü, alt-üst sıcaklık ve nem çalışma aralığı, veri iletim kapasitesi vb. birçok anahtar performans kriteri vardır. Akıllı sayaçların, akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.13' de sunulmuştur.

3.3.4.1. AMI/AMR Sistemi İle Haberleşen Sistemler

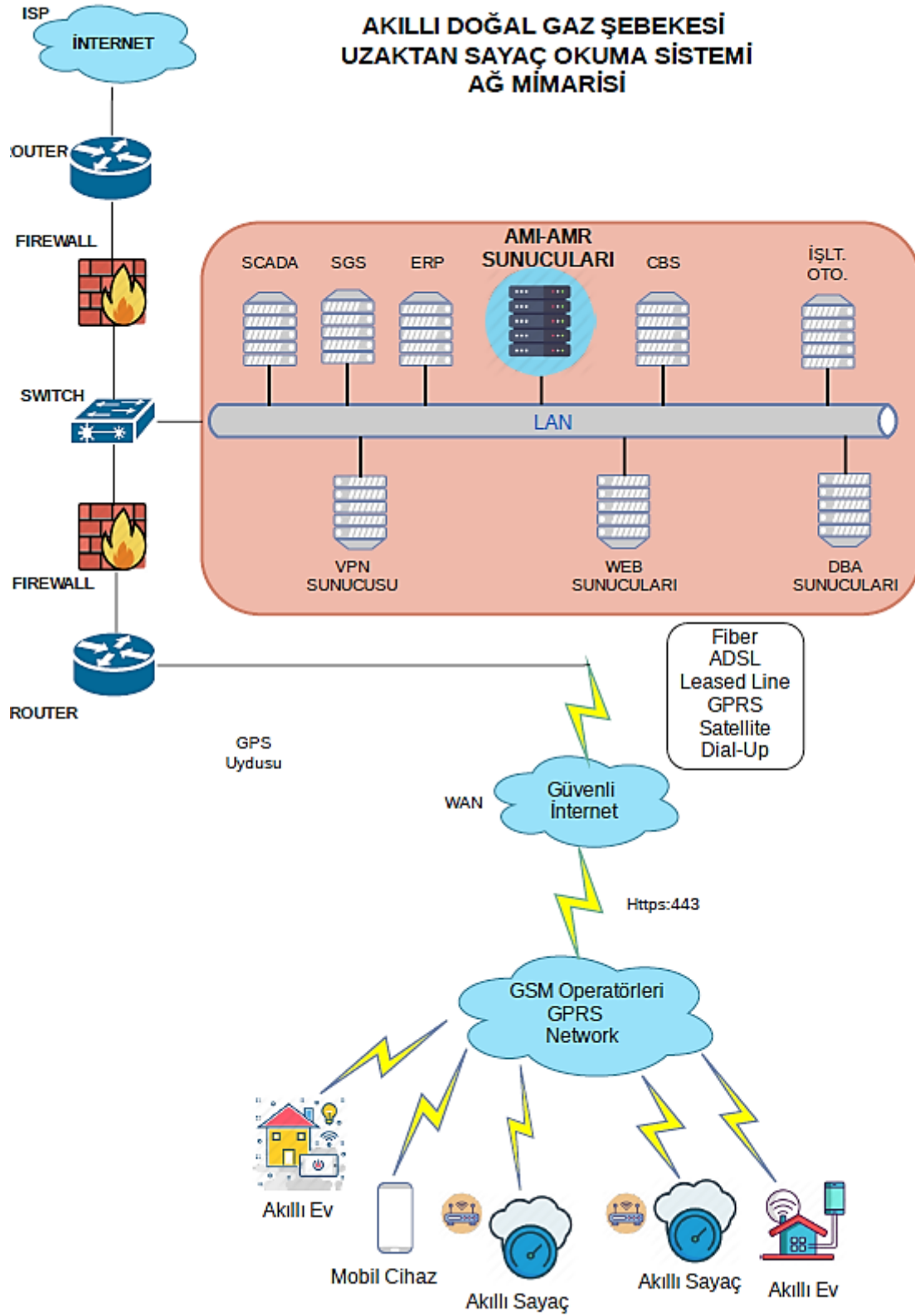
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde AMI/AMR uzaktan otomatik sayaç okuma sistemi akıllı şebekenin bir parçasıdır. AMI/AMR sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.33' de gösterilmiştir.



Şekil 3.33: AMI/AMR sistemi ile haberleşen sistemler.

3.3.4.2. AMI/AMR Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan AMI/AMR uzaktan otomatik sayaç okuma sistemi incelenerek mevcut ağ mimarisi Şekil 3.34’ de verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.34: AMI/AMR sistemi ağ mimarisi.

3.3.4.3. AMI/AMR Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi AMI/AMR uzaktan otomatik sayaç okuma sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.13’ de verilmiştir. Bu KPI listesine göre kurumlardaki uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.13: AMI/AMR siber güvenlik olgunluk seviyesi ve KPI listesi.

Otomatik Sayaç Okuma Sistemi (AMI&AMR) KPI Listesi									AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
	AMI&AMR Özellikleri (NIST SP-800, EPOK, CS, COBIT, ISO/IEC 27001-27002-27019, KVKK, KPI DSS, ISA/IEC 62449:2009)																		
1	Erişim ve Kimlik Yönetimi								0.414	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
	Bilgi sistem ortamında kullanıcı fiziksel erişim veya dijital erişim ve kimliklerinin işlevi için isteklere cevap verilmesi veya reddedilmesi süreçleri. Bir ET sisteminde kaynakları erişim izin verilmemesi ile parti olarak belirlenmiş birleşimler (örneğin, parantez içinde belirtilenler) bu kriterden, işletme veya cihaz yönetimi (dijital erişime yönelik).																		
	1.1.AMI&AMR Sistemlerinde, erişim kontrolü yönetim politikası ve prosedürü bulunuyor mu?								7	8	9	8	7	7.8	0.017	4.131	0.013		
	1.2.AMI&AMR Sistemlerinde, kullanıcı hesapları yönetim politikası ve prosedürü bulunuyor mu?								7	9	7	8	7	7.6	0.017	4.025	0.013		
	1.3.AMI&AMR Sistemlerinde, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?								8	7	8	9	8	8	0.018	4.237	0.014		
	1.4.AMI&AMR Sistemlerinde, sunuculara erişimde güvenli bağlantı protokolleri kullanılıyor mu?								7	8	7	9	3	6.8	0.018	3.602	0.010		
	1.5.AMI&AMR Sistemlerinde, sunuculara erişim güvenliği veri şifreleme yöntemi kullanılıyor mu?								4	4	4	5	5	4.8	0.011	2.542	0.005		
	1.6.AMI&AMR Sistemlerinde, internete ve sistemlere bağlanma giriş denemeleri loglanıyor mu?								9	7	9	8	9	8.4	0.018	4.449	0.015		
	1.7.AMI&AMR Sistemlerinde, internete ve sistemlere bağlanma giriş denemeler raporlanıyor mu?								9	9	9	9	6	8.4	0.018	4.449	0.015		
	1.8.AMI&AMR Sistemlerinde, kullanılan uzaktan erişimde güvenli bağlantı protokolleri kullanılıyor mu?								9	9	8	9	8	8.4	0.018	4.449	0.015		
	1.9.AMI&AMR Sistemlerinde, kullanılan uzaktan bağlantı erişimleri için erişim kuralları var mı?								8	8	7	4	6	6.6	0.014	3.496	0.010		
	1.10.AMI&AMR Sistemlerinde, kullanılan uzaktan erişim için güvenli veri şifreleme yöntem var mı?								5	6	6	5	5	5.4	0.012	2.860	0.006		
	1.11.AMI&AMR Sistemlerinde, erişim yetkilendirmeleri ve kısıtlamaları belirlemek için paylaşımlı yapıyorlar mı?								6	6	6	6	5	6.2	0.014	3.284	0.008		
	1.12.AMI&AMR Sistemlerinde, Rol Bazlı Erişim Kontrolü (RBAC) kullanarak erişim düzeylerini tanımlamak için roller, hiyerarşiler ve kısıtlamalar kullanılıyor mu?								7	7	7	8	7	7.2	0.016	3.814	0.011		
	1.13.AMI&AMR Sistemlerinde, kurumsal ağa erişim sağlayıcılar da kaynakların erişim sistemleri listesi var mı?								8	6	7	8	8	7.8	0.017	4.131	0.013		
	1.14.AMI&AMR Sistemlerinde, yetkiyi erişim engellemi tespit etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapılıyor mu?								6	6	8	8	8	7.2	0.016	3.814	0.011		
	1.15.AMI&AMR Sistemlerinde, farkla kaynaklar üzerinden edilebilir kullanıcı erişimi için kayıtları ile verinin toplamması ve iflykendirilmesi (Korelasyon) yapılıyor mu?								8	6	4	6	8	6.4	0.014	3.390	0.009		
	1.16.AMI&AMR Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?								5	7	5	5	5	5.6	0.012	2.956	0.007		
	1.17.AMI&AMR Sistemlerinde, işletme dışı kişiler için kimlik tanımlama ve yetkilendirme yapıyorlar mı?								7	7	5	3	6	5.4	0.012	2.860	0.006		
	1.18.AMI&AMR Sistemlerinde, parola doğrulaması yapılıyor mu?								8	6	7	6	7	6.8	0.015	3.602	0.010		
	1.19.AMI&AMR Sistemlerinde, parola belirleme ve kullanım kuralları var mı?								7	9	8	9	9	8.4	0.018	4.449	0.015		
	1.20.AMI&AMR Sistemlerinde, ayrıcalıklı hesapları yönetiyorlar mı?								9	10	9	10	9	9.4	0.021	4.979	0.019		
	1.21.AMI&AMR Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları tutuluyor mu?								9	9	9	9	5	8.2	0.018	4.343	0.015		
	1.22.AMI&AMR Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?								9	9	9	9	9	8.2	0.018	4.343	0.015		
	1.23.AMI&AMR Sistemlerinde, mobil iletişim sadece online işlem merkez ile haberleşme sağlanıyor mu?								6	6	6	6	6	6	0.013	3.178	0.008		
	1.24.AMI&AMR Sistemlerinde, belirlenen uygulamalarında dışarıya herhangi bir uygulama kullanılıyor mu?								8	8	9	8	8	8.2	0.018	4.343	0.015		
	1.25.AMI&AMR Sistemlerinde, mobil cihazlara uygulama yükleme yetkisi var mı?								10	9	10	10	7	9.2	0.020	4.873	0.019		
	1.26.AMI&AMR Sistemlerinde, mobil cihazlara erişim yetkisi sınırı mı?								5	7	5	5	7	6.4	0.012	3.390	0.009		
									189	196	191	193	125	185.8	0.414	100.00%	0.309	75%	

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI' lar toplamlar üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 75 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

AMI/AMR sistemi belirlenen KPI' lara ve soru setlerine göre değerlendirildi. Tüm KPI' lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi AMI/AMR sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 72' dir. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından AMI/AMR sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 72 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu

oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. AMI/AMR sistemlerinde uzaktan okuma yapılan sayaçlarda MITM araya girme saldırıları, sinyal kesintisi ve fiziksel saldırıların yaşandığı gözlemlenmektedir. En çok yaşanan saldırı yöntemleri Hizmet Kesintisi (DDoS), Araya Girme Saldırısı (MITM), Zararlı Yazılımlar (Malware (Worm, Trojan, Rootkit, Virus)), Replay Saldırısı ve Sahtecilik (Spoofing) (ARP, IP, GPS) gibi saldırılardır. Bu saldırıların engellenmesi için standartlara uyum, fiziksel güvenlik için gerekli önlemlerin alınması, GPRS modem sistemlerinin çalınmasının engellenmesi, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir. Ayrıca SCADA üzerinde alarm sisteminin bu sayaçlar ve uzaktan okuma sistemleri içinde aktif hale getirilmelidir.

3.4. VERİ YÖNETİMİ

Veri yönetimi sektördeki en önemli alanlardan biridir. Özellikle, bilgi yönetimi altyapı hizmetlerini doğru bir şekilde elde etmek için vazgeçilmez bir unsurdur. Günümüzde, milyonlarca müşteriye ait bilgiler, bakım işlemleri, faturalar, ödemeler, doğalgaz dağıtımı için bilgi yönetimini gerektirmektedir. Akıllı şehir üreten bir unsur varsa, bu bilgidir. Ek olarak, akıllı doğal gaz şebeke teknolojisinin bileşenleri düzenli olarak veri üretir. Dolayısıyla, bir gaz dağıtım şirketinin veriyi yönetmek, geliştirmek, korumak, kontrol etmek, geliştirmek ve sunmak için üç bileşeni vardır. Bunlar; Kurumsal Kaynak Planlama (ERP), Müşteri İlişkileri Yönetimi (CRM) ve Siber Güvenlik Sistemi (SGS)' dir. Bu bileşenler sonraki bölümlerde incelenecektir.

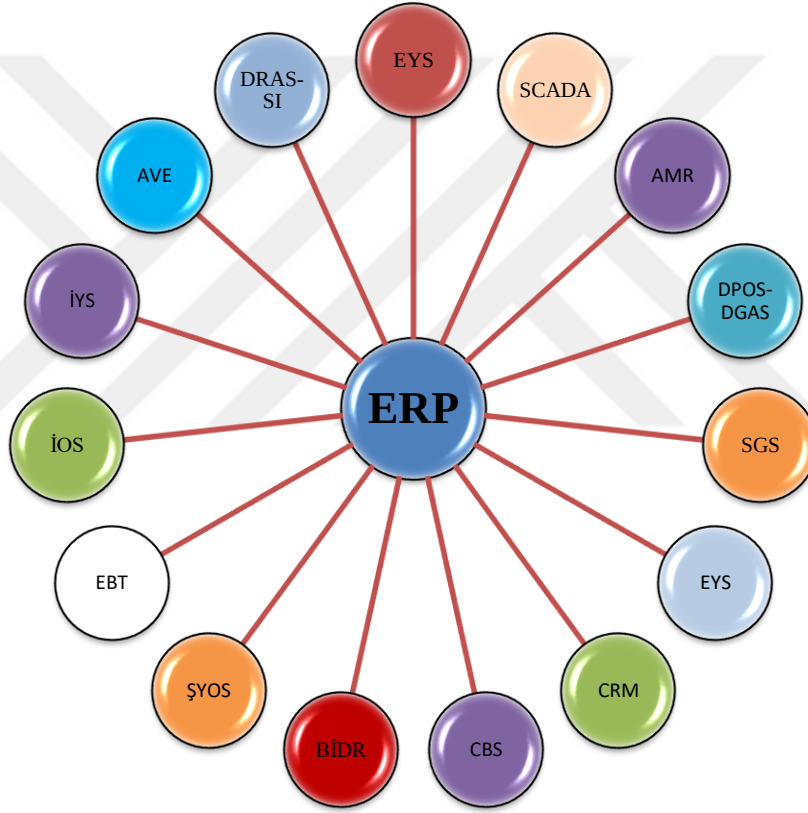
3.4.1. Akıllı Doğal Gaz Şebekesinde Kurumsal Kaynak Planlama (ERP)

SAP ERP, akıllı şebeke konsepti için vazgeçilmez bir araçtır. ERP, doğal gaz dağıtım yönetiminin akışını kolaylaştıran en önemli bileşenlerden biridir. Küreselleşen dünyada, ERP projeleri süreçleri optimize ederek verimliliği artırmaya yönelik mutlak bir gereklilik sağlamıştır. Ayrıca, ERP işlem hızını artırıyor. ERP tüm veri alışverişinin bilgi altyapısını teşkil etmektedir. İş sürekliliği ERP' nin en önemli parçasıdır. ISO 22301 İş sürekliliği yönetiminin gerekliliği ERP ile karşılanmaktadır. ERP projesinin performansı, KPI ile ölçülebilir (İGDAŞ, 2014). İzin verilen maksimum kapalı kalma süresi, kabul edilebilir duruş süresi ve kabul edilebilir veri kaybı gibi birçok ERP anahtar performans kriterleri vardır. ERP' nin akıllı doğal

gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.14’ de sunulmuştur. ERP hakkında mevzuat ve spesifikasyonlara ışığında bu faktörlerin düzeyleri belirlenmiştir.

3.4.1.1. ERP Sistemi İle Haberleşen Sistemler

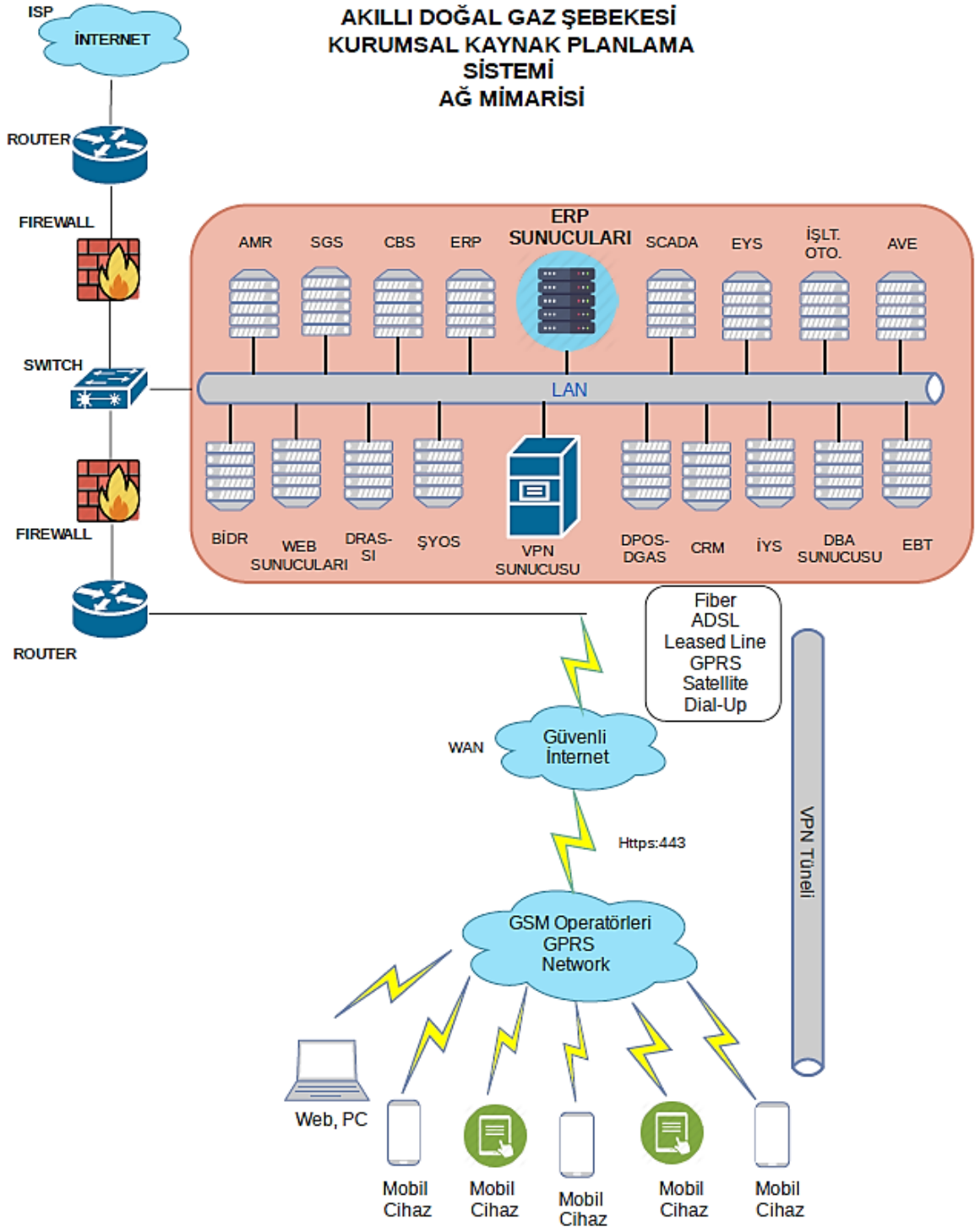
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde ERP sistemi akıllı şebekenin bir parçasıdır. ERP sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.35’ de gösterilmiştir.



Şekil 3.35: ERP sistemi ile haberleşen sistemler.

3.4.1.2. ERP Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan ERP sistemi incelenerek mevcut ağ mimarisi Şekil 3.36’ da verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.36: ERP sistemi ağ mimarisi.

3.4.1.3. ERP Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi ERP sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.14’ de verilmiştir. Bu KPI listesine göre kurumlardaki uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.14: ERP siber güvenlik olgunluk seviyesi ve KPI listesi.

Kurumsal Kaynak Yönetimi (ERP) Sistemi KPI Listesi										AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
ERP Özellikleri (NIST SP-800, EPDK, CIS, COBIT, ISO/IEC 27001-27002-27013, KVKK, PCI DSS, ISA/IEC 62443:2009)										0,724	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
1 Erişim ve Kimlik Yönetimi																				
(Bilgi sistemi ortamında fiziksel erişim veya bilgilerin edit edilmesi ve kullanılması için özel izneleri talep verilmesi veya reddedilmesi sözünüdür. Bir BT sistemdeki kayıtlara erişim izni verilmesinin de parti olarak kabulü kimlik bilgileri (örn. seneler, işletim sistemi kullanma saatıyla bir kullanıcı, işletim veya cihazın kimliği) ile doğrulanması sözünüdür.)																				
1.1	ERP Sistemlerinde, erişim kontrol yönetim politikası ve prosedürü bulunuyor mu?	7	8	9	8	9	8,2	0,030	4.137	0,025										
1.2	ERP Sistemlerinde, kullanıcı hesapları yönetim politikası ve prosedürü bulunuyor mu?	7	9	7	8	7	7,6	0,028	3.835	0,021										
1.3	ERP Sistemlerinde, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?	8	7	8	9	8	8	0,029	4.036	0,022										
1.4	ERP Sistemlerinde, sunuculara erişimde güvenli bağlantı protokolleri kullanılıyor mu?	7	8	7	9	3	6,8	0,025	3.431	0,017										
1.5	ERP Sistemlerinde, sunuculara erişim güvenli veri şifreleme yöntemi kullanılıyor mu?	4	6	4	5	5	4,8	0,018	2.422	0,008										
1.6	ERP Sistemlerinde, internete ve sistemlere başarısız giriş denemeleri loglanıyor mu?	9	7	9	8	9	8,4	0,031	4.238	0,026										
1.7	ERP Sistemlerinde, internete ve sistemlere başarısız giriş denemeleri raporlanıyor mu?	9	9	9	9	6	8,4	0,031	4.238	0,026										
1.8	ERP Sistemlerinde, kullanılan uzaktan erişimde güvenli bağlantı protokolleri kullanılıyor mu?	8	9	8	9	8	8,4	0,031	4.238	0,026										
1.9	ERP Sistemlerinde, kullanılan uzaktan erişimde güvenli bağlantı protokolleri kullanılıyor mu?	9	9	7	9	6	8	0,029	4.036	0,022										
1.10	ERP Sistemlerinde, kullanılan uzaktan erişim için güvenli veri şifreleme yöntemi var mı?	5	6	5	6	5	5,4	0,020	2.725	0,011										
1.11	ERP Sistemlerinde, erişim yetkilendirmeleri ve kısıtlamaları belirlenerek bilgi paylaşımı yapılıyor mu?	6	9	8	9	9	8,2	0,030	4.137	0,025										
1.12	ERP Sistemlerinde, Rol Bazlı Erişim Kontrolü (RBAC) kullanılarak erişim düzeylerini düzenlemek için roller, hiyerarşiler ve kısıtlamalar kullanılıyor mu?	7	9	9	7	7	7,8	0,028	3.935	0,022										
1.13	ERP Sistemlerinde, kurumsal ağa erişim sağlayan dış kaynakların veya sistemlerin listesi var mı?	8	7	8	8	8	7,8	0,028	3.935	0,022										
1.14	ERP Sistemlerinde, yetkisiz erişim eylemlerini tespit etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapılıyor mu?	9	6	8	6	9	7,6	0,028	3.835	0,021										
1.15	ERP Sistemlerinde, farklı kaynaklar üzerinden elde edilen kullanıcı erişim izni kayıtları ile verinin toplanması ve ilişkilendirilmesi (korelasyonu) yapılıyor mu?	9	6	9	6	4	6,8	0,025	3.431	0,017										
1.16	ERP Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?	5	7	5	6	5	5,6	0,020	2.825	0,011										
1.17	ERP Sistemlerinde, işletme dışı kişiler için kimlik tanımlama ve yetkilendirme yapılıyor mu?	6	7	9	9	6	7,4	0,027	3.734	0,020										
1.18	ERP Sistemlerinde, parola doğrulaması yapılıyor mu?	8	6	7	6	7	6,8	0,025	3.431	0,017										
1.19	ERP Sistemlerinde, parola belirleme ve kullanım kuralları var mı?	7	9	8	9	9	8,4	0,031	4.238	0,026										
1.20	ERP Sistemlerinde, ayrıcalıklı hesapların yönetimi yapılıyor mu?	9	10	9	10	9	9,4	0,034	4.743	0,032										
1.21	ERP Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları tutuluyor mu?	9	9	9	9	9	9	0,033	4.541	0,030										
1.22	ERP Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?	9	8	9	8	9	8,6	0,031	4.339	0,027										
1.23	ERP Sistemlerinde, mobil iletişim sadece online ilek merkez ile haberleşme sağlanıyor mu?	6	6	6	6	6	6	0,022	3.027	0,013										
1.24	ERP Sistemlerinde, belirlenen uygulamalarında dışarıda herhangi bir uygulama çalışıyor mu?	8	8	9	8	8	8,2	0,030	4.137	0,025										
1.25	ERP Sistemlerinde, mobil cihazlara uygulama yüklemeye yetkisi var mı?	10	9	10	10	7	9,2	0,034	4.642	0,031										
1.26	ERP Sistemlerinde, mobil cihazlara erişim yetkisi sınırlı mı?	5	7	9	7	9	7,4	0,027	3.734	0,020										
		194	201	205	204	187	198,2	0,724	100,000	0,564										78%

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI’ lar toplamlar üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 78 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

ERP sistemi belirlenen KPI’ lara ve soru setlerine göre değerlendirildi. Tüm KPI’ lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi ERP sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 75’ dir. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından ERP sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 75 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu oranın

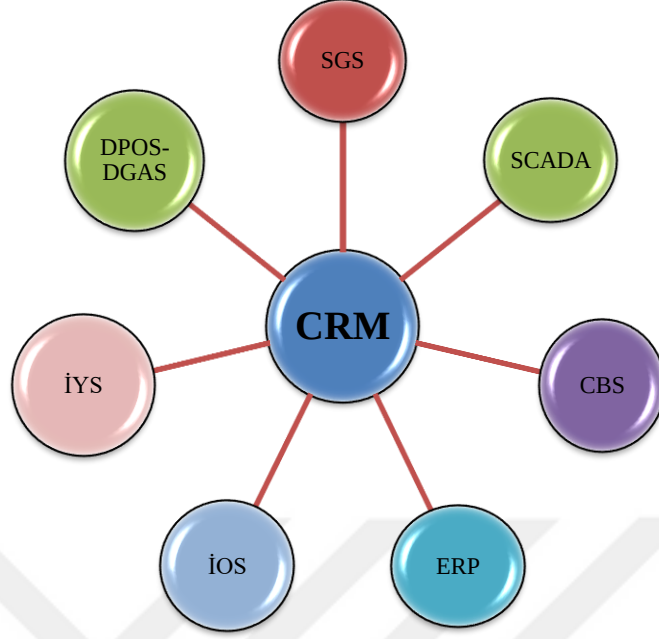
daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. ERP sistemlerinde MITM araya girme saldırıları, sinyal kesintisi, DDoS saldırıları, Zararlı Yazılımlar (Malware (Worm,Trojan, Rootkit, Virus)) saldırıları, Spoofing, SQL Injection ve Sosyal Mühendislik saldırıları yaşandığı gözlemlenmektedir. Bu saldırıların engellenmesi için standartlara uyum, fiziksel güvenlik için gerekli önlemlerin alınması, GPRS modem sistemlerinin çalınmasının engellenmesi, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

3.4.2. Akıllı Doğal Gaz Şebekesinde Çağrı Merkezi (CRM)

Müşteri memnuniyeti ve hizmet kalitesinin artırılması amacıyla CRM verileri analiz edilmektedir. Böylece iddia ve şikâyetlerin altında yatan nedenleri ortaya çıkarmak için girişimlerde bulunmaktadır. CRM verileri kullanılarak, işlem süreçleri müşteri bakış açısıyla analiz edilerek iyileştirme alanları belirlenmeye çalışılmalıdır. Dolayısıyla, müşteri taleplerinin altyapı tasarımı ve işlem prosedüründe önemli etkileri vardır. CRM raporlarının değerlendirilmesinin akıllı doğal gaz şebekesine önemli bir katkı sağlar. CRM' nin akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.15' de sunulmuştur. CRM ile ilgili mevzuat ve standartları ışığında bu faktörlerin düzeyleri belirlenmiştir.

3.4.2.1. CRM Sistemi İle Haberleşen Sistemler

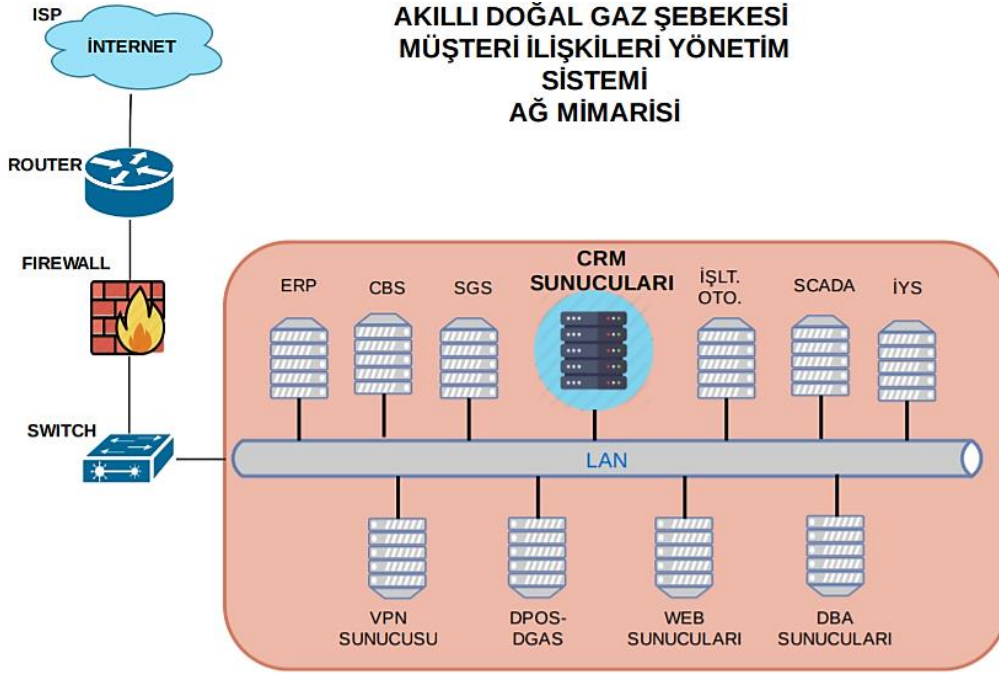
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde CRM sistemi akıllı şebekenin bir parçasıdır. CRM sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.37' de gösterilmiştir.



Şekil 3.37: CRM sistemi ile haberleşen sistemler.

3.4.2.2. CRM Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan CRM sistemi incelenerek mevcut ağ mimarisi Şekil 3.38’ da verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.38: CRM sistemi ağ mimarisi.

3.4.2.3. CRM Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi CRM sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.15’ de verilmiştir. Bu KPI listesine göre kurumlardaki uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.15: CRM siber güvenlik olgunluk seviyesi ve KPI listesi.

Müşteri İlişkileri Yönetimi (CRM) Sistemi KPI Listesi							AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
CRM Özellikleri (NIST SP-800, EPDK, CIS, COBIT, ISO/IEC 27001-27002-27015, KVKK, PCI DSS, ISA/IEC 62443-2009)							0,508	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
1	Erişim ve Kimlik Yönetimi																
[KPI listesi ayrıntıları burada yer almaktadır]																	
1.1	CRM Sistemlerinde, erişim kontrol yönetim politikası ve prosedürü bulunuyor mu?						7	8	9	8	9	8,2	0,021	4,137	0,017		
1.2	CRM Sistemlerinde, kullanıcı hesapları yönetim politikası ve prosedürü bulunuyor mu?						7	9	7	8	7	7,6	0,019	3,835	0,015		
1.3	CRM Sistemlerinde, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?						8	7	8	9	8	8	0,020	4,036	0,016		
1.4	CRM Sistemlerinde, sunuculara erişimde güvenli bağlantı protokolleri kullanılıyor mu?						7	8	7	9	3	6,8	0,017	3,431	0,012		
1.5	CRM Sistemlerinde, sunuculara erişim güvenli veri şifreleme yöntemi kullanılıyor mu?						4	6	4	5	5	4,8	0,012	2,422	0,006		
1.6	CRM Sistemlerinde, internet ve sistemlere başarısız giriş denemeleri raporlanıyor mu?						9	7	9	8	9	8,4	0,022	4,238	0,018		
1.7	CRM Sistemlerinde, internet ve sistemlere başarısız giriş denemeleri raporlanıyor mu?						9	9	9	9	6	8,4	0,022	4,238	0,018		
1.8	CRM Sistemlerinde, kullanılan uzaktan erişimde güvenli bağlantı protokolleri kullanılıyor mu?						8	9	8	9	8	8,4	0,022	4,238	0,018		
1.9	CRM Sistemlerinde, kullanılan uzaktan bağlantı erişimleri için erişim kuralları var mı?						9	9	7	9	6	8	0,020	4,036	0,016		
1.10	CRM Sistemlerinde, kullanılan uzaktan erişim için güvenli veri şifreleme yöntemi var mı?						5	6	5	6	5	5,4	0,014	2,725	0,007		
1.11	CRM Sistemlerinde, erişim yetkilendirmeleri ve kodlamaları belirlenerek bilgi paylaşımı yapılıyor mu?						6	9	8	9	9	8,2	0,021	4,137	0,017		
1.12	CRM Sistemlerinde, Rol Bazı Erişim Kontrolü (RBK) kullanıcı erişim düzeylerini düzenlemek için roller, hiyerarşiler ve kodlamalar kullanılıyor mu?						7	9	9	7	7	7,8	0,020	3,935	0,016		
1.13	CRM Sistemlerinde, kurumsal ağa erişim sağlayan dış kaynakların veya sistemlerin listesi var mı?						8	7	8	8	8	7,8	0,020	3,935	0,016		
1.14	CRM Sistemlerinde, yetkili erişim eylemlerini tespit etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapılıyor mu?						9	6	8	6	9	7,6	0,019	3,835	0,015		
1.15	CRM Sistemlerinde, farklı kaynaklar üzerinden elde edilen kullanıcı erişim iz kayıtları ile verinin toplanması ve ilişkilendirilmesi (korelasyon) yapılıyor mu?						9	6	9	6	4	6,8	0,017	3,431	0,012		
1.16	CRM Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?						5	7	5	6	5	5,6	0,014	2,825	0,008		
1.17	CRM Sistemlerinde, işletme dışı kişiler için kimlik tanımlama ve yetkilendirme yapılıyor mu?						6	7	9	9	6	7,4	0,019	3,734	0,014		
1.18	CRM Sistemlerinde, parola doğrulaması yapılıyor mu?						8	6	7	6	7	6,8	0,017	3,431	0,012		
1.19	CRM Sistemlerinde, parola belirleme ve kullanımı kuralları var mı?						7	9	8	9	9	8,4	0,022	4,238	0,018		
1.20	CRM Sistemlerinde, ayrıcalıklı hesapların yönetimi yapılıyor mu?						9	10	9	10	9	9,4	0,024	4,743	0,023		
1.21	CRM Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları tutuluyor mu?						9	9	9	9	9	9	0,023	4,541	0,021		
1.22	CRM Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?						9	8	9	8	9	8,6	0,022	4,389	0,019		
1.23	CRM Sistemlerinde, mobil işletim sistemi online ileerme merkez ile habersizleşme sağlanıyor mu?						6	6	6	6	6	6	0,015	3,027	0,009		
1.24	CRM Sistemlerinde, belirlenen uygulamalarında dışında herhangi bir uygulama çalışıyor mu?						8	8	9	8	8	8,2	0,021	4,137	0,017		
1.25	CRM Sistemlerinde, mobil cihazlara uygulama yüklemeye yetkisi var mı?						10	9	10	10	7	9,2	0,024	4,642	0,022		
1.26	CRM Sistemlerinde, mobil cihazlara erişim yetkisi sınırlı mı?						5	7	9	7	9	7,4	0,019	3,734	0,014		
							194	201	205	204	187	198,2	0,508	100,000	0,396	78%	

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç

puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI' lar toplamlar üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 78 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

CRM sistemi belirlenen KPI' lara ve soru setlerine göre değerlendirildi. Tüm KPI' lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi CRM sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 75' dir. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından CRM sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 75 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. CRM sistemlerinde MITM araya girme saldırıları, sinyal kesintisi, DDoS saldırıları, Zararlı Yazılımlar (Malware (Worm,Trojan, Rootkit, Virus)) saldırıları, Spoofing, SQL Injection ve Sosyal Mühendislik saldırıları yaşandığı gözlemlenmektedir. Bu saldırıların engellenmesi için standartlara uyum, fiziksel güvenlik için gerekli önlemlerin alınması, GPRS modem sistemlerinin çalınmasının engellenmesi, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

3.4.3. Akıllı Doğal Gaz Şebekesinde Siber Güvenlik Sistemi (SGS)

Gelişen teknolojileri ile birlikte akıllı doğal gaz şebekelerinde siber güvenlik, operasyonel teknolojilerde ve bilgi teknolojilerinde büyük etkisi nedeniyle en popüler konuların başında gelmektedir. İstatistiklere göre, siber saldırılar petrol ve gaz endüstrisinde günde 8,4 milyon dolarlık maddi zarara neden oluyor ve bunların % 50' sinden fazlası SCADA sistemlerine yöneliktir (William, 2016). Bu tehlikelerden dolayı siber güvenlik konusundaki çalışmalar hız kazanmıştır. Kurumsal bir uygulama için siber güvenlik açısından dikkate alınması gereken birçok katman vardır. Bu katmanlar veri merkezi güvenliği, cihaz güvenliği, işletim sistemi güvenliği, katman yazılımı güvenliği, veri ambarı güvenliği, ağ güvenliği, erişim güvenliği ve

şifreleme güvenliği olarak ifade edilmektedir. Bunlar OSI (open system interconnection) katmanı şeklinde isimlendirilmektedir. Bu katmanlardaki gerekli olan çalışma farklı uzmanlık ve duyarlılık gerektirmektedir (ISO, 1994).

Kurumsal uygulamaların üzerinde çalıştığı işletim sistemi ve ara katman yazılımı güvenlik açıkları yetkili personel tarafından takip edilmeli ve bu ürünlerin güvenlik açıklarını kapatan güvenlik yamaları güncel tutulmalıdır.

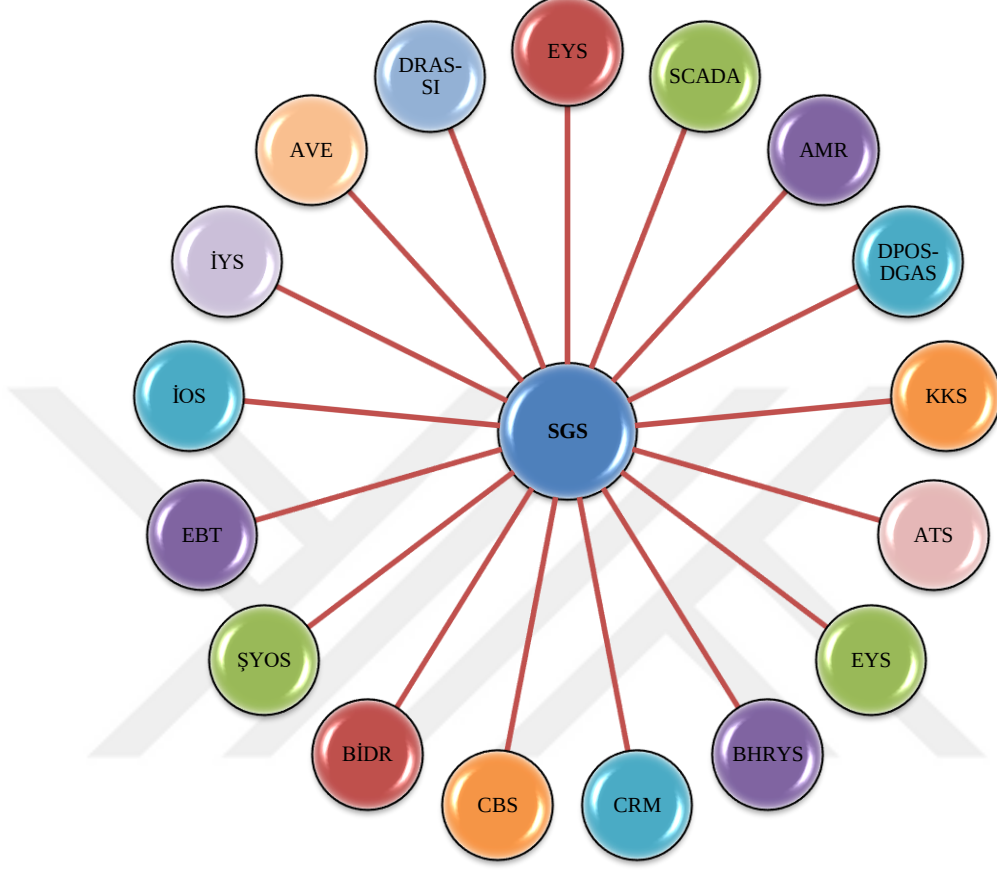
Siber güvenliğin bir başka boyutu da iş sürekliliği yönetim sistemine sahip olma becerisidir. İş sürekliliği, otomasyon sistemlerinin güvenliğinde en önemli parametrelerden biridir. Süreç kesintisi durumunda iş sürekliliğinde maksimum tolere edilebilen bozulma süresi (MTPOD), iyileşme zamanı hedefi (RTO) ve geri kazanım noktası hedefi (RPO) kavramlarına göre sağlanmalıdır (ISO, 2011). Ayrıca, Bilgi sistemleri ve güvenlik sistemleri birbirini denetleyen bağımsız yapılar olarak tasarlanmalı ve yönetilmelidir. SGS raporlarının değerlendirilmesi, akıllı şebeke yapısına değerli bir katkı sağlar. Akıllı doğal gaz şebekelerinde SGS siber güvenlik olgunluk seviyesini ölçmek için Tablo 3.16' daki KPI listesi kullanılmıştır. Doğal gaz dağıtımında SGS için tüm anahatar performans göstergelerini sunulmuştur. SGS ile ilgili mevzuat ve standartlar ışığında bu faktörlerin seviyesini belirlenmiştir.

SGS, kurumun tamamına bakarak bilgi ve siber güvenlik açısından kullanılan IT ve OT sistemlerdeki siber güvenlik açıklarının tespiti ve kurumun bu saldırılara karşı olan dayanıklılığı üzerine çalışma yapılması gerektiğini göstermektedir. Kurumun siber güvenlik olgunluk modelini oluşturabilmek için gerekli alt bileşenlerden biridir. Bu konu üzerindeki KPI göstergelerimiz Tablo 3.16' de verilmiştir. KPI oluştururken siber güvenlik konusunda yapılması gereken en iyi uygulamalar ve tavsiyeler kullanılmıştır ve birçoğu yasalara ve mevzuatlara uygun olması gerektiği için yapılması mecburi olan alanlardır.

3.4.3.1. SGS Sistemi İle Haberleşen Sistemler

Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde SGS sistemi akıllı şebekenin bir parçası olmakla birlikte tüm sistemler ile değerlendirilmesi gereken bir sistemdir. SGS sistemleri kurumun ana birleşeni olup tüm sistemlerin arkasında olan ve izlenen tüm IT sistemlere verilen genel bir addır. SGS sistemleri siber güvenlik açısından değerlendirildiğinde koruma, izleme ve denetleme sistemleri olarak adlandırılabilir. SGS sistemi ile veri iletişim

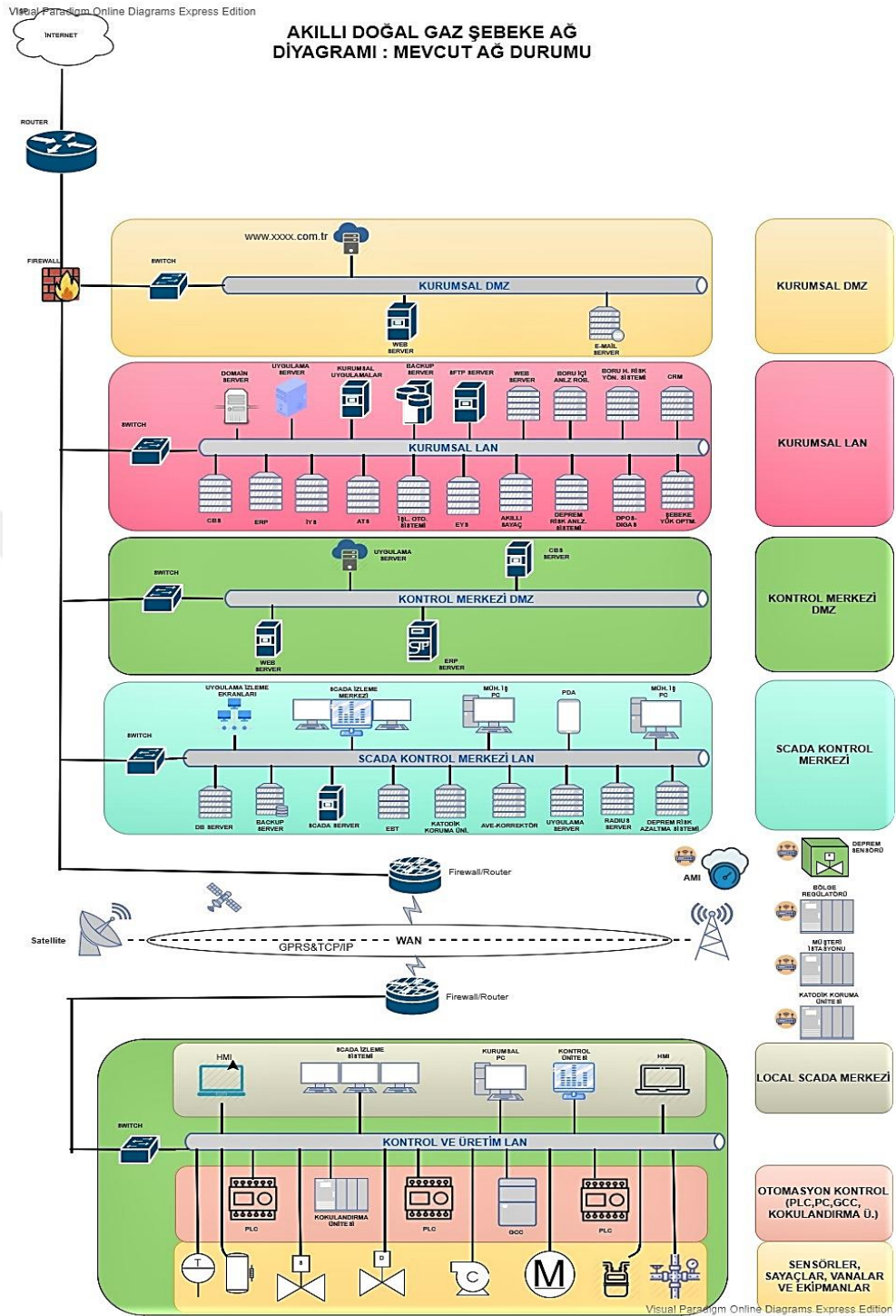
açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.39' da gösterilmiştir.



Şekil 3.39: SGS sistemi ile haberleşen sistemler.

3.4.3.2. SGS Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan SGS sistemi incelenerek mevcut ağ mimarisi Şekil 3.40' da verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.40: SGS sistemi ağ mimarisi.

3.4.3.3. SGS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi SGS sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.16’ da verilmiştir. Bu KPI listesine göre kurumlardaki

uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.16: SGS siber güvenlik olgunluk seviyesi ve KPI listesi.

SGS Sistemi KPI Listesi		AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
SGS Özellikleri (NIST SP-800, EPDK, CIS, COBIT, ISO/IEC 27001-27002-27019, KVKK, PCI DSS, ISA/IEC 62443-2009)		3,053	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
1	Erişim ve Kimlik Yönetimi											
	(Bilgi sistemi ortamındaki cihazlara fiziksel erişim veya bilgilerin edinilmesi ve kullanılmasını için özel iznalarla cevap verilmeli veya reddedilmeli sözünüdür. Bir BT sistemindeki kayıtlara erişim bir verimlilikten de yola çıkarak belirli kurallara bağlıdır (örn. parola, kimlik, yetkilendirme kullanmak suretiyle bir kullanıcı, erişim veya cihazın kontrolünü değiştirilmesi sözünüdür.)											
1.1	Kurumda, erişim kontrolü yönetim politikası ve prosedürü bulunuyor mu?		8	7	9	8	9	8,200	0,078	2,549	0,064	
1.2	Kurumda, kullanıcı hesapları yönetim politikası ve prosedürü bulunuyor mu?		2	1	4	3	4	2,800	0,027	0,870	0,007	
1.3	Kurumda, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?		5	4	5	6	5	5,000	0,047	1,554	0,024	
1.4	Kurumda, WEB sunucularına erişimde güvenli bağlantı protokolu var mı?		8	9	8	8	8	8,200	0,078	2,549	0,064	
1.5	Kurumda, WEB sunucularına erişim veri şifreleme yöntemi var mı?		8	9	9	8	8	8,400	0,080	2,611	0,067	
1.6	Kurumda, internete açık sunucular üzerinde çalışan uygulamalarda DMZ kullanılıyor mu?		8	9	9	1	1	5,600	0,053	1,741	0,030	
1.7	(Evetse), DMZ'de uygulamalar bulunduruluyor mu?		5	9	5	6	5	6,000	0,057	1,865	0,034	
1.8	(Evetse), DMZ'de bir erişim yönetim prosedürü var mı?		6	8	6	5	6	6,200	0,059	1,927	0,036	
1.9	Kurumda, internete ve sistemlere başarsız giriş denemeleri loglanıyor mu?		7	9	7	8	7	7,600	0,072	2,363	0,055	
1.10	Kurumda, internete ve sistemlere başarsız giriş denemeleri raporlanıyor mu?		6	7	6	7	6	6,400	0,061	1,990	0,039	
1.11	Kurumda, kullanıcıları uzaktan erişimde güvenli bağlantı protokolu kullanılıyor mu?		8	8	8	7	8	7,800	0,074	2,425	0,058	
1.12	Kurumda, kullanıcıları uzaktan bağlantı erişimleri için erişim kuralları var mı?		8	7	8	7	8	7,600	0,072	2,363	0,055	
1.13	Kurumda, kullanıcıları uzaktan erişim için güvenli veri şifreleme yöntemi var mı?		9	7	9	8	9	8,400	0,080	2,611	0,067	
1.14	Kurumda, erişim yetkilendirmeleri ve kısıtlamaları belirlemek için paylaşımlı yapıyor mu?		9	7	6	7	6	7,000	0,066	2,176	0,047	
1.15	Kurumda, Rol Bazı Erişim Kontrolü (RBK) kullanıcıları erişim düzeylerini düzenlemek için roller, hiyerarşiler ve kısıtlamalar kullanılıyor mu?		10	7	9	8	9	8,600	0,082	2,674	0,070	
1.16	Kurumda, kurumsal ağa erişim sağlayan dış kaynakların veya sistemlerin listesi var mıdır?		9	7	9	9	9	8,600	0,082	2,674	0,070	
1.17	Kurumda, Endüstriyel Kontrol Sistemlerinin (OT ağlar) internete erişimi kısıtlanıyor mu?		6	8	7	7	8	7,200	0,068	2,238	0,049	
1.18	Kurumda, OT ağlar ve IT ağlar topolojik/fiziksel/manipülasyon olarak birbirinden ayrılmış/yalıtılmış mı?		5	4	5	6	5	5,000	0,047	1,554	0,024	
1.19	Kurumda, IT ağı üzerinden OT ağlarına bağlanma/erişim sağlanıyor mu?		5	5	5	4	5	4,800	0,046	1,492	0,022	
1.20	Kurumda, OT ağı üzerinden IT ağlarına bağlanma/erişim sağlanıyor mu?		7	6	7	6	7	6,600	0,063	2,052	0,041	
1.21	(Evetse), IT ağlar üzerinden OT ağlarına bağlanma/erişimde uygulanan güvenlik kontrolleri var mı?		6	7	6	7	6	6,000	0,061	1,990	0,039	
1.22	Kurumda, OT ağların operatör/mühendis bilgisayarlarının dahil olduğu ağın internete erişimi var mı?		8	6	8	9	8	7,800	0,074	2,425	0,058	
1.23	(Evetse), bu ağı üzerinde kablosuz erişim var mı?		8	9	7	7	7	7,600	0,072	2,363	0,055	
1.24	(Evetse), bu ağa personelin özel mobil cihazları erişim var mı?		6	4	6	5	6	5,400	0,051	1,679	0,028	
1.25	(Evetse), bu sistemlerin internete açık olmasının zorunlu olduğu durumlarda ise gerekli güvenlik önlemleri (güvenlik duvarı, uçtan uca tünelleme yöntemleri, yetkilendirme ve kimliklendirme mekanizmaları vb.) alınıyor mu?		8	9	6	5	6	6,800	0,065	2,114	0,044	
1.26	Kurumda, OT ağların erişimde web arayüzü kullanılıyor mu?		8	9	6	5	6	6,800	0,065	2,114	0,044	
1.27	Kurumda, yetkilendirme erişim yetkilerinin test edilerek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapılıyor mu?		8	9	6	5	6	6,800	0,065	2,114	0,044	
1.28	Kurumda, kurum ağlarında gerçekleştirilen normal karışan olayların belirlenmesi yapılıyor mu?		8	9	6	5	6	6,800	0,065	2,114	0,044	
1.29	Kurumda, farklı kaynaklar üzerinden elde edilen kullanıcı erişim iz kayıtları ile verinin toplanması ve ilişkilendirilmesi (korelasyon) yapılıyor mu?		8	9	6	5	6	6,800	0,065	2,114	0,044	
1.30	Kurumda, kablosuz ağlara erişimde hangi güvenlik erişim protokolu kullanılıyor mu?		8	9	6	5	6	6,800	0,065	2,114	0,044	
1.31	Kurumda, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?		8	9	6	5	6	6,800	0,065	2,114	0,044	
1.32	(Evetse), tanımlama ve kimlik yönetim grup ve rol bazlı yönetimi yapılıyor mu?		8	9	6	5	6	6,800	0,065	2,114	0,044	
1.33	Kurumda, işletme dış kişiler için kimlik tanımlama ve yetkilendirme yapılıyor mu?		8	9	6	5	6	6,800	0,065	2,114	0,044	
1.34	Kurumda, parola doğrulaması yapılıyor mu?		8	9	6	5	6	6,800	0,065	2,114	0,044	
1.35	Kurumda, Fiziksel Token veya Akıllı Kart ile kimlik doğrulama yapılıyor mu?		8	9	6	5	6	6,800	0,065	2,114	0,044	
1.36	Kurumda, parola belirlenme ve kullanım kuralları var mı?		8	9	6	5	6	6,800	0,065	2,114	0,044	
1.37	Kurumda, ayrıcalıklı hesapların yönetimi yapılıyor mu?		6	7	6	7	6	6,400	0,061	1,990	0,039	
1.38	Kurumda, sistemlerde tanımlı E-imza kullanılıyor mu?		4	5	4	5	4	4,400	0,042	1,368	0,018	
1.39	Kurumda, kritik verilerin internete kapalı ve fiziksel güvenliği sağlanmış bir ağı erişim kontrollü sağlanıyor mu?		8	7	8	6	8	7,400	0,070	2,301	0,052	
1.40	Kurumda, kablosuz (Wi-Fi) kullanıcıların erişimi, kullanıcıların bir kullanıcı sertifikasıyla veya Kullanıcı Kimlik Doğrulama Çevirmeli Bir Kullanıcı Hizmeti (RADUS) aracılığıyla kimlik doğrulama güvenli bir kimlik doğrulama protokolu (örneğin, TLS EAP-TLS) kullanılıyor mu?		9	8	9	8	9	8,600	0,082	2,674	0,070	
1.41	Kurumda, kablosuz (Wi-Fi) ağda Genişletilebilir Kimlik Doğrulama Protokolu (EAP) kullanılarak IEEE 802.1x kimlik doğrulaması kullanılıyor mu?		9	6	7	6	7	7,000	0,066	2,176	0,047	
1.42	Kurumda, kablosuz (Wi-Fi) ağda MAC filtreleme doğrulaması kullanılıyor mu?		8	7	8	7	7	7,400	0,070	2,301	0,052	
1.43	Kurumda, kullanıcıların ağı bağlanmaları için posture kontrolü yapılıyor mu?		9	8	9	7	7	8,000	0,076	2,487	0,061	
1.44	Kurumda, kullanıcıların internete erişiminde güvenliğini arttırmak için NAC vb araçlar kullanılıyor mu?		5	6	5	6	5	5,400	0,051	1,679	0,028	
1.45	Kurumda, kullanıcıların yasal içerikte olmayan WEB sayfalarına erişimleri engelleniyor mu?		9	7	6	8	8	7,600	0,072	2,363	0,055	
			330	333	302	277	293	321,667	2,914	95,440	2,050	67%

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI' lar toplamlar üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 67 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

SGS sistemi belirlenen KPI' lara ve soru setlerine göre değerlendirildi. Tüm KPI' lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi SGS sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 66' dır. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından SGS sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 66 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. SGS sistemlerinde kurumların tüm siber saldırı yöntemlerini dikkate alarak kurumun IT ve OT sistemlerini en yüksek seviyede korumaları önemlidir. Özellikle enerji altyapılarına ve kurumlara en yaygın saldırılar olan DDoS, Malware, Spoofing, ransomware, sniffing MITM araya girme saldırıları, sinyal kesintisi, SQL injection fiziksel ve sosyal mühendislik saldırılarının yaşandığı gözlemlenmektedir. Bu saldırıların engellenmesi için standartlara uyum, log yönetimi, yama yönetimi, ağ segmentasyon, sıkılaştırma, açık portların kapatılması, verilerin gizliliği, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

3.5. İŞGÜCÜ YÖNETİMİ

İş ekiplerinin ve varlıklarının etkili bir şekilde yönetilmesi, kullanımı güçlü bir iş yönetim sistemi ile gerçekleştirilebilir. İşgücü yönetim sistemi iş becerilerinde uyumluluğun nasıl gerçekleştirileceğine dair ayrıntılı bir yol sunar. İşgücü yönetim sistemi, özellikle doğal gaz dağıtım alanında verimli güç kullanımı için önemli bir araçtır. Bir doğal gaz dağıtım şirketi için çalışma yönetimi kapasitesi, şebeke otomasyon sistemi, araç takip sistemi ve bina enerji yönetim sistemi sırasıyla bu kısımda değerlendirilmiştir.

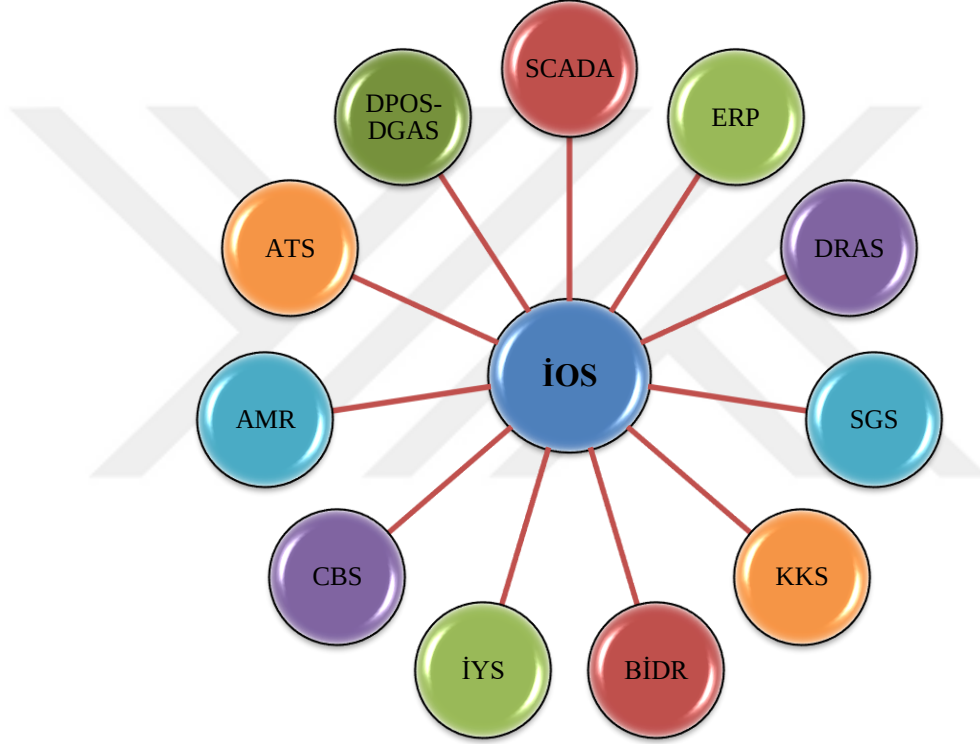
3.5.1. Akıllı Doğal Gaz Şebekesinde İşletme Otomasyon Sistemi (İOS)

İşletme otomasyon sistemi, otomasyon sistemlerinin bir bileşeni olarak akıllı doğal gaz şebekelerine önemli bir katkı sağlar. Şu anda, altyapı sektöründe faaliyet gösteren bir şirket için saha ekiplerinin etkin yönetimi, iş sürekliliği açısından kritik öneme sahiptir. Servis ağı genişledikçe, operasyonları planlamak, yönetmek ve raporlamak için bu sistem zorunlu hale gelmiştir. İşletme otomasyon sisteminin raporlarının değerlendirilmesi, akıllı şebekenin kompozisyonuna değerli bir katkı sağlar. İşletme otomasyon sisteminin, akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.17' de sunulmuştur. Akıllı doğal gaz dağıtımında işletme otomasyon sistemi için tüm anahtar performans göstergeleri

tespit edilmiştir. Bu alandaki mevzuat ve standartlar ışığında bu faktörlerin düzeyleri seviyelendirilmiştir.

3.5.1.1. İOS Sistemi İle Haberleşen Sistemler

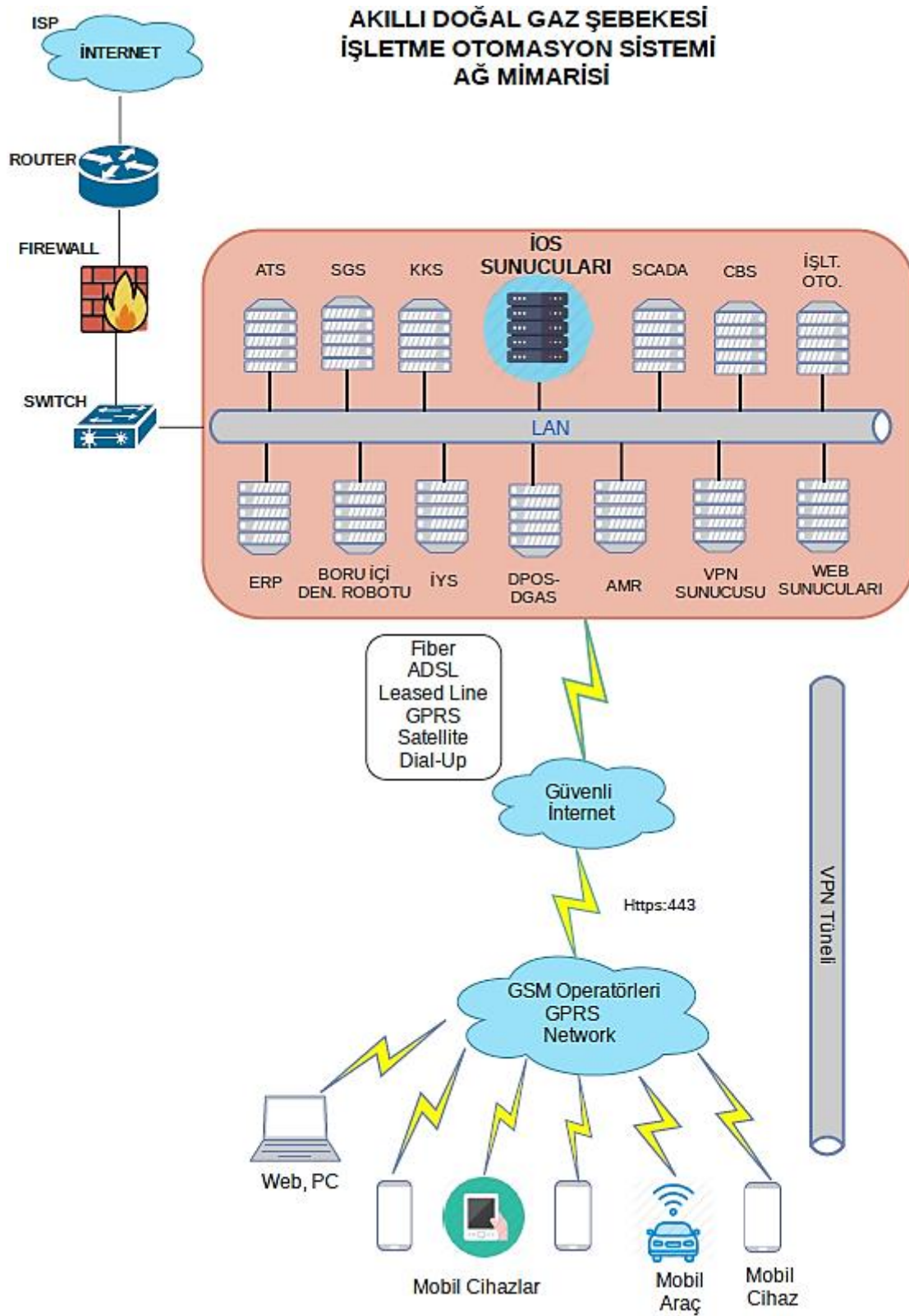
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde İOS sistemi akıllı şebekenin bir parçasıdır. İOS sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.41’ de gösterilmiştir.



Şekil 3.41: İOS sistemi ile haberleşen sistemler.

3.5.1.2. İOS Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan İOS sistemi incelenerek mevcut ağ mimarisi Şekil 3.42’ de verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.42: İOS sistemi ağ mimarisi.

3.5.1.3. İOS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi İOS sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.17’ de verilmiştir. Bu KPI listesine göre kurumlardaki uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.17: İOS siber güvenlik olgunluk seviyesi ve KPI listesi.

İşletme Otomasyon Sistemi (İOS) KPI Listesi										AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
İOS Özellikleri (NIST SP-800, EPOK, CIS, COBIT, ISO/IEC 27001-27002-27019, KVMK, PCI DSS, ISA/IEC 62443:2009)										1,386	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
1 Erişim ve Kimlik Yönetimi																				
(Bilgi sistemi ortamındaki alarmlara fiziksel erişim veya bilgilerin edinilmesi ve kullanılması için özel istisnalar talep edilmesi veya reddedilmesi sürecidir. Bir BT sistemdeki kaynaklara erişim izin verilmemesi de parti olarak belirli kimlik bilgileri (örn. parolalar, şifreler) kullanması suretiyle bir kullanıcı, işletme veya cihazın kimliğini doğrulamaya çalışması.)																				
1.1 İOS Sistemlerinde, erişim kontrol yönetim politikası ve prosedürü bulunuyor mu?										7	8	9	8	9	8,2	0,058	4,197	0,048		
1.2 İOS Sistemlerinde, kullanıcı hesapları yönetim politikası ve prosedürü bulunuyor mu?										7	9	7	8	7	7,6	0,054	3,889	0,041		
1.3 İOS Sistemlerinde, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?										8	7	8	9	8	8	0,057	4,094	0,045		
1.4 İOS Sistemlerinde, sunuculara erişimde güvenli bağlantı protokolleri kullanılıyor mu?										7	8	7	9	3	6,8	0,048	3,480	0,033		
1.5 İOS Sistemlerinde, sunuculara erişim güvenliği veri şifreleme yöntemi kullanılıyor mu?										4	6	4	5	5	4,8	0,034	2,456	0,016		
1.6 İOS Sistemlerinde, internete ve sistemlere bağlanış giriş denemeleri loglanıyor mu?										9	7	8	8	9	8,4	0,060	4,299	0,050		
1.7 İOS Sistemlerinde, internete ve sistemlere bağlanış giriş denemeleri raporlanıyor mu?										9	9	9	9	6	8,4	0,060	4,299	0,050		
1.8 İOS Sistemlerinde, kullanılan uzaktan erişimde güvenli bağlantı protokolleri kullanılıyor mu?										8	7	8	9	8	8	0,057	4,094	0,045		
1.9 İOS Sistemlerinde, kullanılan uzaktan erişimleri için erişim kuraları var mı?										9	9	7	9	6	8	0,057	4,094	0,045		
1.10 İOS Sistemlerinde, kullanılan uzaktan erişim için güvenli veri şifreleme yöntemi var mı?										5	6	5	6	5	5,4	0,038	2,764	0,021		
1.11 İOS Sistemlerinde, erişim yetkilendirmeleri ve kısıtlamaları belirlenerek bilgi paylaşımı yapılıyor mu?										6	9	8	9	9	8,2	0,058	4,197	0,048		
1.12 İOS Sistemlerinde, Rol Bazlı Erişim Kontrolü (RBEC) kullanıcı erişim düzeylerini düzenlemek için roller, hiyerarşiler ve kısıtlamalar kullanılıyor mu?										7	7	9	7	7	7,4	0,053	3,787	0,039		
1.13 İOS Sistemlerinde, kurumsal ağa erişim sağlayan dış kaynakların veya sistemlerin listesi var mı?										8	7	8	8	8	7,8	0,055	3,992	0,043		
1.14 İOS Sistemlerinde, yetkili erişim eylemlerini tespit etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapılıyor mu?										9	6	8	6	9	7,6	0,054	3,889	0,041		
1.15 İOS Sistemlerinde, farklı kaynaklar üzerinden elde edilen kullanıcı erişim iz kayıtları ile verinin toplanması ve ilişkilendirilmesi (korelasyon) yapılıyor mu?										9	6	9	6	4	6,8	0,048	3,480	0,033		
1.16 İOS Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?										5	7	5	6	5	5,6	0,040	2,866	0,022		
1.17 İOS Sistemlerinde, işletme dışı kişiler için kimlik tanımlama ve yetkilendirme yapılıyor mu?										6	7	9	9	6	7,4	0,053	3,787	0,039		
1.18 İOS Sistemlerinde, parola doğrulaması yapılıyor mu?										8	6	7	6	7	6,8	0,048	3,480	0,033		
1.19 İOS Sistemlerinde, parola belirlenme ve kullanım kuralları var mı?										7	9	8	9	9	8,4	0,060	4,299	0,050		
1.20 İOS Sistemlerinde, ayrıcalıklı hesapların yönetimi yapılıyor mu?										7	7	7	7	9	7,4	0,053	3,787	0,039		
1.21 İOS Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları tutuluyor mu?										9	9	9	9	8	9	0,064	4,606	0,057		
1.22 İOS Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?										9	8	9	8	9	8,6	0,061	4,401	0,052		
1.23 İOS Sistemlerinde, mobil iletişim sadece online ile değil merkez ile haberleşme sağlanıyor mu?										6	6	6	6	6	6	0,043	3,071	0,026		
1.24 İOS Sistemlerinde, belirlenen uygulamalarında dışında herhangi bir uygulama çalışıyor mu?										8	8	9	8	8	8,2	0,058	4,197	0,048		
1.25 İOS Sistemlerinde, mobil cihazlara uygulama yüklemeye yetkisi var mı?										10	9	10	10	7	9,2	0,065	4,708	0,060		
1.26 İOS Sistemlerinde, mobil cihazlara erişim yetkisi sınırlı mı?										5	7	9	7	9	7,4	0,053	3,787	0,039		
										192	194	209	201	187	195,4	1,386	100,000	1,063	77%	

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI’ lar toplamlar üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 77 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

İOS sistemi belirlenen KPI’ lara ve soru setlerine göre değerlendirildi. Tüm KPI’ lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi İOS sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 74’ dir. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından İOS sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 74 olarak belirlenmiştir. Belirlenen bu oran olgunluk

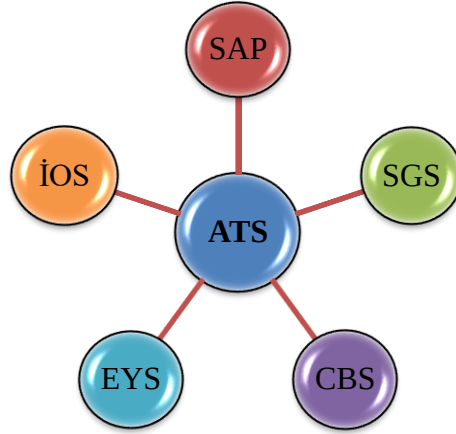
seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. İOS sistemlerinde kurumların tüm siber saldırı yöntemlerini dikkate alarak kurumun IT ve OT sistemlerini en yüksek seviyede korumaları önem arz etmektedir. Özellikle enerji altyapılarına ve kurumlara en yaygın saldırılar olan Hizmet Kesintisi (DDoS), Araya Girme Saldırısı (MITM), Zararlı Yazılımlar (Malware (Worm,Trojan, Rootkit, Virus)), Replay Saldırısı, Sahtecilik (Spoofing) (ARP,IP,GPS), MODBUS/TCP Protocol Attack, DNP3 Protocol Attack, Malicious Command and Software Injection, Buffer Overflow, Sosyal Mühendislik, Fiziksel Saldırı (Sensör, Actuator, Kamera), SQL Injection, Zero Day Attack ve Phishing (Oltalama) saldırıları akıllı doğal gaz şebeklerine sahip enerji kurumları tarafından yaşanabilmektedir. Bu saldırıların engellenmesi için standartlara uyum, log yönetimi, yama yönetimi, ağ segmentasyon, sıkılaştırma, açık portların kapatılması, verilerin gizliliği, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

3.5.2. Akıllı Doğal Gaz Şebekesinde Araç Takip Sistemi (ATS)

Araç Takip Sistemi (ATS), otomasyon sistemlerinin bir bileşeni olarak doğal gaz dağıtım şebekesine önemli bir katkı sağlamaktadır. ATS' nin raporlarının değerlendirilmesi, akıllı doğal gaz şebekesinin yapısal olarak verimliliğini arttıracaktır. ATS' nin akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.18' de sunulmuştur. Doğal gaz dağıtımında ATS için tüm temel performans göstergelerini belirtiyoruz. ATS ile ilgili mevzuat ve standartlar standartlar açısından bu faktörlerin düzeyleri belirlenmiştir.

3.5.2.1. ATS Sistemi İle Haberleşen Sistemler

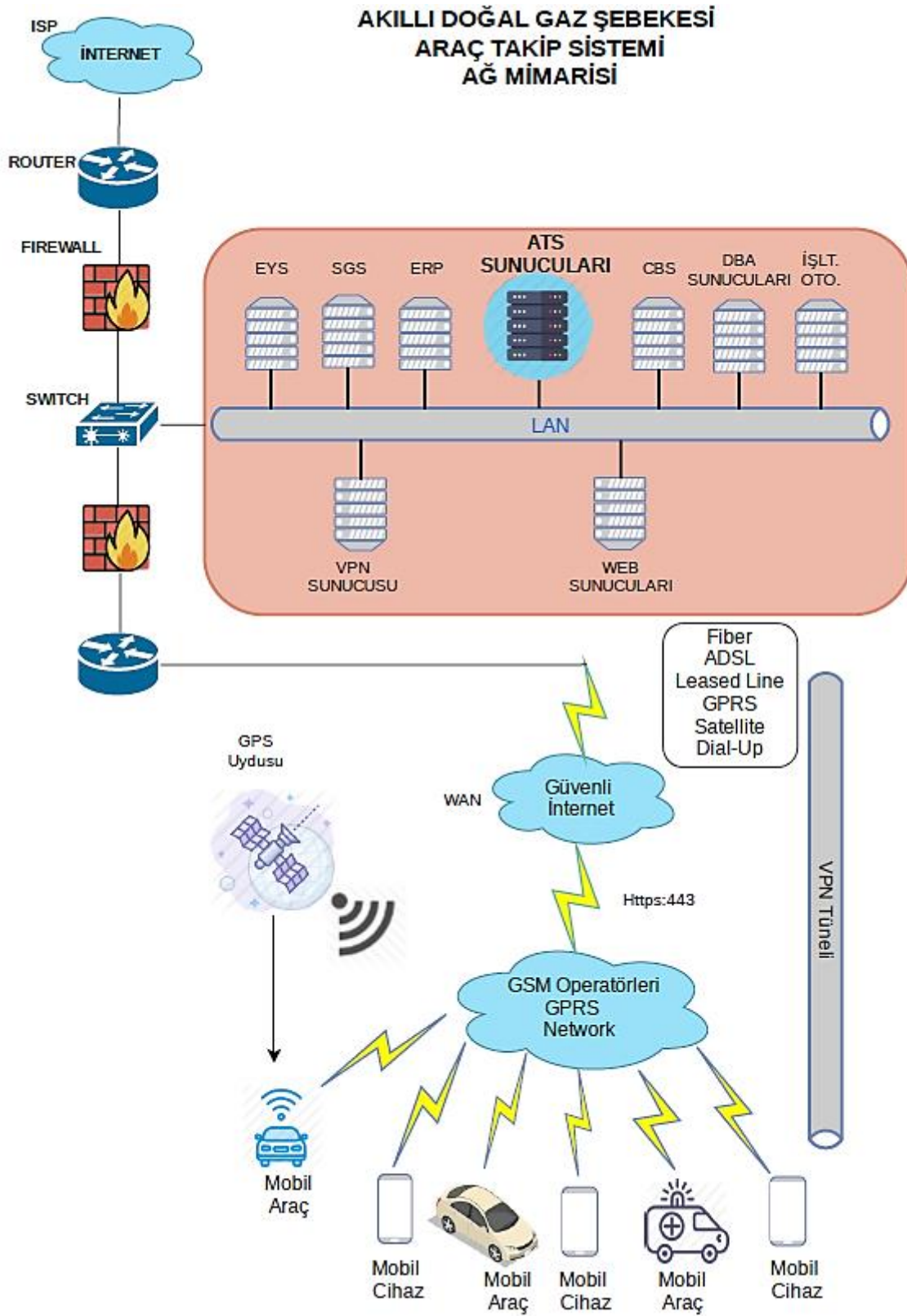
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde ATS sistemi akıllı şebekenin bir parçasıdır. ATS sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.43' de gösterilmiştir.



Şekil 3.43: ATS sistemi ile haberleşen sistemler.

3.5.2.2. ATS Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan ATS sistemi incelenerek mevcut ağ mimarisi Şekil 3.44’ de verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.44: ATS sistemi ağ mimarisi.

3.5.2.3. ATS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi ATS sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.18’ de verilmiştir. Bu KPI listesine göre kurumlardaki uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.18: ATS siber güvenlik olgunluk seviyesi ve KPI listesi.

Araç Takip Sistemi (ATS) KPI Listesi		AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
ATS Özellikleri (NIST SP-800, EPDİ, CIS, COBIT, ISO/IEC 27001-27002-17, KVKK, PCI DSS, ISA/IEC 62443-2009)												
1	Erişim ve Kimlik Yönetimi	0,448	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
(Bülg sistemi ortama aldıkları fiziksel erişim veya bilginin edinimini ve kullandığını çok fazla izdenleme onay verilmeyen veya reddedilmemiş süreçler; Bir BT sistemdeki kaynaklara erişim için verilmeyen bir yetki dağılımı belirli kullanıcılar için ayrılarak; Benzerlik kullandıkları süreçler ve kullandıkları, izlenen veya cihaz kullandıkları dağılımlarına göre)												
1.1	ATS Sistemlerinde, erişim kontrolü yönetim politikası ve prosedürü bulunuyor mu?	7	8	9	8	9	8,2	0,019	4,253	0,016		
1.2	ATS Sistemlerinde, kullanıcı hesapları yönetim politikası ve prosedürü bulunuyor mu?	9	9	7	8	7	7,6	0,018	3,942	0,013		
1.3	ATS Sistemlerinde, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?	7	7	8	9	8	7,8	0,018	4,046	0,014		
1.4	ATS Sistemlerinde, kullanıcılar erişimde güvenli bağlantı protokolleri kullanıyor mu?	7	8	8	9	8	7,8	0,018	3,942	0,013		
1.5	ATS Sistemlerinde, sunuculara erişim güvenli veri şifreleme yöntemi kullanılıyor mu?	4	6	4	5	5	4,8	0,011	2,490	0,005		
1.6	ATS Sistemlerinde, internete ve sistemlere bağışız giriş denemeleri loglanıyor mu?	9	7	9	8	9	8,4	0,020	4,357	0,016		
1.7	ATS Sistemlerinde, internete ve sistemlere bağışız giriş denemeleri raporlanıyor mu?	9	9	9	9	9	8,4	0,020	4,357	0,016		
1.8	ATS Sistemlerinde, kullanıcılar uzaktan erişimde güvenli bağlantı protokolleri kullanıyor mu?	8	7	8	9	7	7,8	0,018	4,046	0,014		
1.9	ATS Sistemlerinde, kullanıcılar uzaktan erişim için güvenli veri şifreleme yöntemi var mı?	6	9	7	6	7	7,6	0,018	3,942	0,013		
1.10	ATS Sistemlerinde, kullanıcılar uzaktan erişim için güvenli veri şifreleme yöntemi var mı?	5	6	5	6	5	5,4	0,013	2,801	0,007		
1.11	ATS Sistemlerinde, erişim yetkilendirmeleri ve kısıtlamaları belirlenerek bilgi paylaşım yapılıyor mu?	6	9	8	8	9	8,2	0,019	4,253	0,016		
1.12	ATS Sistemlerinde, Rol Bazlı Erişim Kontrolü (RBK) kullanıcı erişim düzeylerini düzenlemek için roller, hiyerarşiler ve kısıtlamalar kullanılıyor mu?	7	7	9	7	7	7,4	0,017	3,638	0,013		
1.13	ATS Sistemlerinde, kurumsal ağa erişim sağlanan da kaynakların veya sistemlerin listesi var mı?	8	7	8	8	8	7,8	0,018	4,046	0,014		
1.14	ATS Sistemlerinde, erişim yetkileri tespit etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapılıyor mu?	9	8	8	8	6	7,2	0,017	3,734	0,012		
1.15	ATS Sistemlerinde, farklı kaynaklar üzerinden elde edilen kullanıcı erişim kayıtları ile verinin toplanması ve işlendiği (korelasyon) yapılıyor mu?	9	9	6	9	6	8,4	0,016	3,537	0,011		
1.16	ATS Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?	6	7	5	6	5	5,6	0,013	2,905	0,007		
1.17	ATS Sistemlerinde, işletim dışı kuyruklar için kimlik tanımlama ve yetkilendirme yapılıyor mu?	6	7	7	9	6	7	0,016	3,631	0,011		
1.18	ATS Sistemlerinde, parola doğrulaması yapılıyor mu?	8	6	7	6	7	6,8	0,016	3,527	0,011		
1.19	ATS Sistemlerinde, parola belirleme ve kullanımı kullanılıyor var mı?	7	9	8	9	9	8,4	0,020	4,357	0,016		
1.20	ATS Sistemlerinde, ayrıcalıklı hesapların yönetimi yapılıyor mu?	7	7	7	7	9	7,4	0,017	3,638	0,013		
1.21	ATS Sistemlerinde, uygulamaya üzerinde yapılan işlemlerin logları tutuluyor mu?	7	9	9	9	9	8,6	0,020	4,461	0,017		
1.22	ATS Sistemlerinde, uygulamaya üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?	7	8	9	7	9	8	0,019	4,149	0,015		
1.23	ATS Sistemlerinde, mobil iletişim sadece online için merkez ile habereleşme sağlanıyor mu?	6	6	6	6	6	6	0,014	3,112	0,008		
1.24	ATS Sistemlerinde, belirlenen uygulamalarda dışında herhangi bir uygulama çalışıyor mu?	8	8	9	8	8	8,2	0,019	4,253	0,016		
1.25	ATS Sistemlerinde, mobil cihazlara uygulamaya yüklemeye yetkisi var mı?	10	9	10	10	7	9,2	0,021	4,772	0,020		
1.26	ATS Sistemlerinde, mobil cihazlara erişim yetkisi sunulmuş mu?	5	7	5	7	9	7,4	0,017	3,638	0,013		
		187	194	201	198	184	192,8	0,448	10,000	0,339	76%	

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI' lar toplamı üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 76 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

ATS sistemi belirlenen KPI' lara ve soru setlerine göre değerlendirildi. Tüm KPI' lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi ATS sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 73' tür. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından ATS sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 73 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu oranın

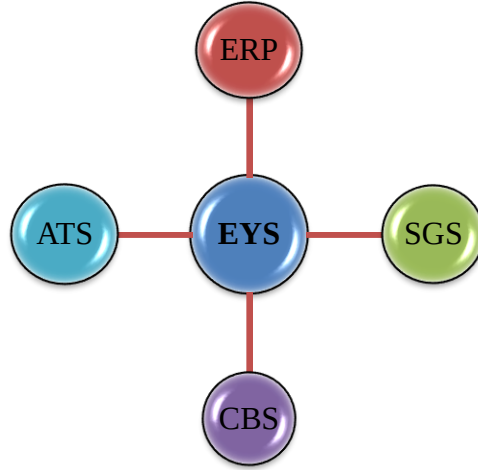
daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. ATS sistemlerinde kurumların tüm siber saldırı yöntemlerini dikkate alarak kurumun IT ve OT sistemlerini en yüksek seviyede korumaları önem arz etmektedir. Özellikle enerji altyapılarına ve kurumlara en yaygın saldırılar olan Hizmet Kesintisi (DDoS), Araya Girme Saldırısı (MITM), Zararlı Yazılımlar (Malware (Worm,Trojan, Rootkit, Virus)), Sosyal Mühendislik, Fiziksel Saldırı (Sensör, Actuator, Kamera), SQL Injection, Zero Day Attack ve Phishing (Oltalama) saldırıları akıllı doğal gaz şebekelerine sahip enerji kurumları tarafından yaşanabilmektedir. Bu saldırıların engellenmesi için standartlara uyum, log yönetimi, yama yönetimi, ağ segmentasyon, sıkılaştırma, açık portların kapatılması, verilerin gizliliği, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

3.5.3. Akıllı Doğal Gaz Şebekesinde Bina Enerji Yönetim Sistemi (EYS)

Enerji Yönetim Sistemi (EYS), kamu ve resmi olmayan piyasa şirketlerine enerji verimliliğini artırmak, harcamaları azaltmak ve enerji performansını yükseltmek için yönetim politikaları ile katkıda bulunur (Steemers, 2003). Ayrıca, akıllı sayaçların binalarda kullanımı ve binaların akıllı binalara dönüştürülmesi, şebeke tasarımında gerekli iyileştirmelere yol açacaktır. Şirketin kendi binalarındaki akıllı uygulamalar, akıllı şebekelere geçişte çok önemli bir adımdır. EYS' in raporlarının değerlendirilmesi, akıllı şebeken yapısına değerli bir katkı sağlar. EYS' in akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.19' da sunulmuştur. Doğal gaz dağıtımında EYS için tüm anahtar performans göstergelerini tespit edilmiştir. Bu faktörlerin seviyeleri EYS ile ilgili mevzuat ve standartlar ışığında belirlenmiştir.

3.5.3.1. EYS Sistemi İle Haberleşen Sistemler

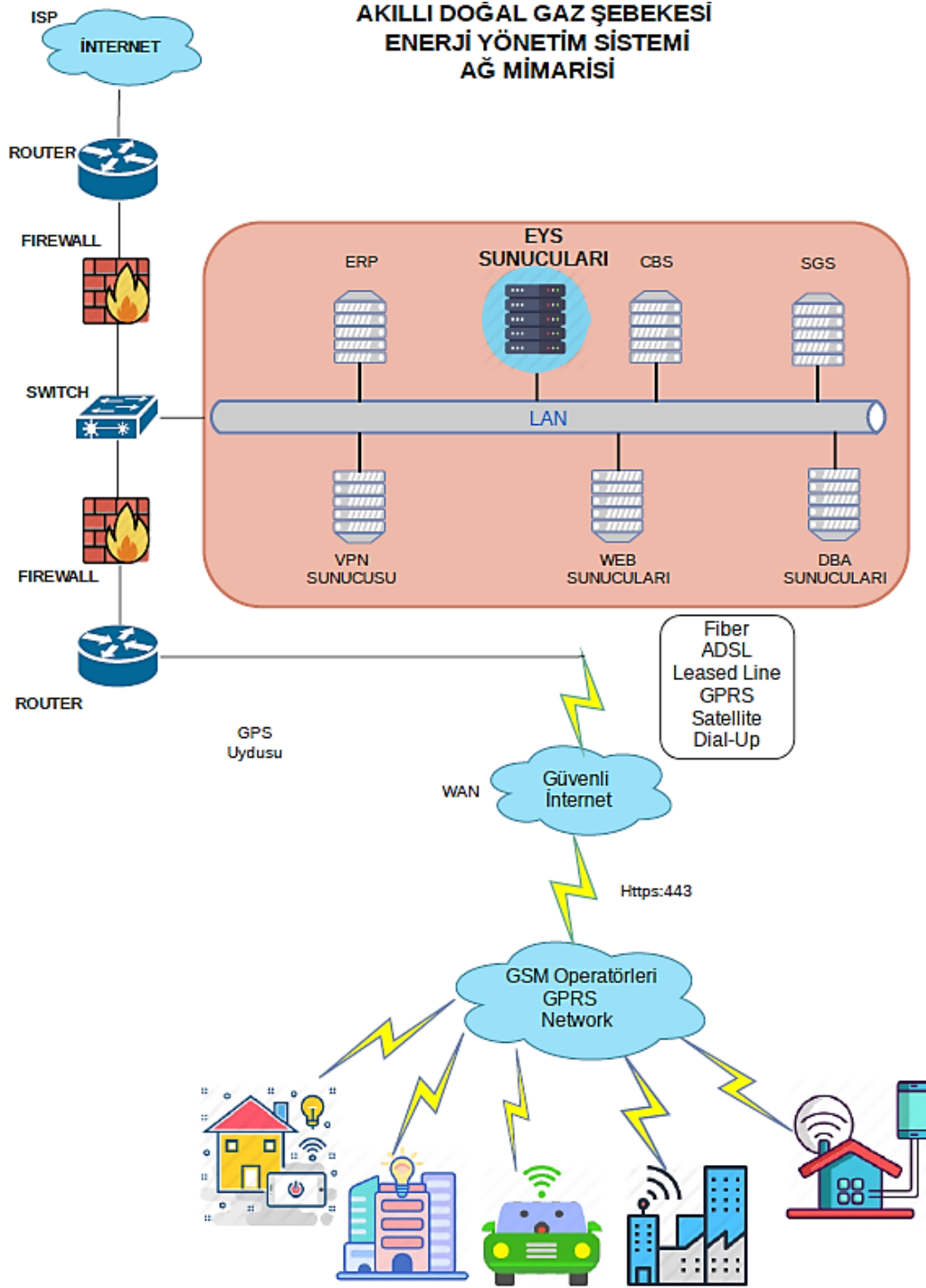
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde EYS sistemi akıllı şebekenin bir parçasıdır. EYS sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.45' de gösterilmiştir.



Şekil 3.45: EYS sistemi ile haberleşen sistemler.

3.5.3.2. EYS Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan EYS sistemi incelenerek mevcut ağ mimarisi Şekil 3.46’da verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.46: EYS sistemi ağ mimarisi.

3.5.3.3. EYS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi EYS sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.19’ da verilmiştir. Bu KPI listesine göre kurumlardaki

uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.19: EYS siber güvenlik olgunluk seviyesi ve KPI listesi.

Enerji Yönetim Sistemi (EYS) KPI Listesi		AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
EYS Özellikleri (NIST SP-800, EPOK, CIS, COBIT, ISO/IEC 27001-27002-27019, KVKK, PCI DSS, ISA/IEC 62443-2009)												
1	Erişim ve Kimlik Yönetimi	0,488	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
1.1	EYS Sistemlerinde, erişim kontrol politikası ve prosedürü bulunuyor mu?	7	8	9	8	9	8,2	0,020	4,184	0,017		
1.2	EYS Sistemlerinde, kullanıcı hesapları yönetim politikası ve prosedürü bulunuyor mu?	7	9	7	8	7	7,6	0,019	3,878	0,014		
1.3	EYS Sistemlerinde, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?	9	7	8	9	8	8,2	0,020	4,184	0,017		
1.4	EYS Sistemlerinde, sunuculara erişimde güvenli bağlantı protokolleri kullanılıyor mu?	7	8	7	9	3	6,8	0,017	3,469	0,012		
1.5	EYS Sistemlerinde, sunuculara erişim güvenli veri şifreleme yöntemi kullanılıyor mu?	4	6	4	5	5	4,8	0,012	2,443	0,006		
1.6	EYS Sistemlerinde, internete ve sistemlere başarsız giriş denemeleri loglanıyor mu?	9	7	9	8	9	8,4	0,021	4,286	0,018		
1.7	EYS Sistemlerinde, internete ve sistemlere başarsız giriş denemeleri raporlanıyor mu?	9	9	9	9	6	8,4	0,021	4,286	0,018		
1.8	EYS Sistemlerinde, kullanılan uzaktan erişimde güvenli bağlantı protokolleri kullanılıyor mu?	8	7	8	9	7	7,8	0,019	3,980	0,015		
1.9	EYS Sistemlerinde, kullanılan uzaktan bağlantı erişimleri için erişim kısıtları var mı?	9	9	7	7	6	7,6	0,019	3,878	0,014		
1.10	EYS Sistemlerinde, kullanılan uzaktan erişim için güvenli veri şifreleme yöntemi var mı?	5	6	5	6	5	5,4	0,013	2,755	0,007		
1.11	EYS Sistemlerinde, erişim yetkilendirmeleri ve kısıtlamaları belirlenerek bilgi paylaşımı yapılıyor mu?	6	9	8	9	9	8,2	0,020	4,184	0,017		
1.12	EYS Sistemlerinde, rol bazlı erişim kontrolü (RBAC) kullanıcı erişim düzeylerini düzenlemek için roller, hiyerarşiler ve kısıtlamalar kullanılıyor mu?	7	7	8	7	7	7,4	0,018	3,776	0,014		
1.13	EYS Sistemlerinde, kurumsal ağa erişim sağlayan dış kaynaklara veya sistemlerin listesi var mı?	8	7	8	8	8	7,8	0,019	3,980	0,015		
1.14	EYS Sistemlerinde, yetkisiz erişim eylemlerini tespit etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapılıyor mu?	9	6	8	6	7	7,2	0,018	3,673	0,013		
1.15	EYS Sistemlerinde, farklı kaynaklar üzerinden elde edilen kullanıcı erişim iz kayıtları ile verinin toplanması ve ilişkilendirilmesi (korelasyon) yapılıyor mu?	9	9	9	6	4	7,4	0,018	3,776	0,014		
1.16	EYS Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?	9	7	5	6	5	6,4	0,016	3,265	0,010		
1.17	EYS Sistemlerinde, işletme dışı kişiler için kimlik tanımlama ve yetkilendirme yapılıyor mu?	6	9	9	9	6	7,8	0,019	3,980	0,015		
1.18	EYS Sistemlerinde, parola doğrulaması yapılıyor mu?	8	6	9	6	7	7,2	0,018	3,673	0,013		
1.19	EYS Sistemlerinde, parola belirleme ve kullanım kısıtları var mı?	7	9	8	9	9	8,4	0,021	4,286	0,018		
1.20	EYS Sistemlerinde, ayrıcalıklı hesapların yönetimi yapılıyor mu?	7	7	7	7	9	7,4	0,018	3,776	0,014		
1.21	EYS Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları tutuluyor mu?	7	9	9	9	9	8,6	0,021	4,388	0,018		
1.22	EYS Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?	7	8	9	7	9	8	0,020	4,082	0,016		
1.23	EYS Sistemlerinde, mobil iletişim sadece online ile merkez ile haberleşme sağlanıyor mu?	6	6	6	6	6	6	0,015	3,061	0,009		
1.24	EYS Sistemlerinde, belirlenen uygulamaların dışında herhangi bir uygulama çalışıyor mu?	8	9	9	8	8	8,4	0,021	4,286	0,018		
1.25	EYS Sistemlerinde, mobil cihazlara uygulama yükleme yetkisi var mı?	10	9	10	10	7	9,2	0,023	4,694	0,021		
1.26	EYS Sistemlerinde, mobil cihazlara erişim yetkisi sınırlı mı?	5	7	9	7	9	7,4	0,018	3,776	0,014		
		193	200	205	198	184	196	0,488	100,000	0,374	77%	

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI' lar toplamlar üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 77 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

EYS sistemi belirlenen KPI' lara ve soru setlerine göre değerlendirildi. Tüm KPI' lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi EYS sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 75' dir. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından EYS sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 75 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. EYS sistemlerinde kurumların tüm siber saldırı yöntemlerini dikkate alarak kurumun IT ve OT sistemlerini en yüksek seviyede korumaları

önem arz etmektedir. Özellikle enerji altyapılarına ve kurumlara en yaygın saldırılar olan Hizmet Kesintisi (DDoS), Zararlı Yazılımlar (Malware (Worm, Trojan, Rootkit, Virus)), Sosyal Mühendislik, Fiziksel Saldırı (Sensör, Actuator, Kamera), SQL Injection, Zero Day Attack ve Phishing (Oltalama) saldırıları akıllı doğal gaz şebeklerine sahip enerji kurumları tarafından yaşanabilmektedir. Bu saldırıların engellenmesi için standartlara uyum, log yönetimi, yama yönetimi, ağ segmentasyon, sıkılaştırma, açık portların kapatılması, verilerin gizliliği, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

3.6. BORU HATTI BÜTÜNSSEL YÖNETİMİ

Boru hattı bütünlüğü yönetimi (PIM) üç fonksiyonel aktivite gerektirir. Bunlar önleme, tespit ve azaltma aktiviteleridir. Tatmin edici bir PIM oluşturmak için tüm malzeme, tasarım ve yapım kayıtları gereklidir (Kariyawasam, 2008). Bunlar diğer sistemlerin temel göstergeleridir. PIM, boru içi muayene robot sistemi ve katodik koruma sistemi ve risk değerlendirme sistemine göre gerçekleştirilebilir. Bu sistemler sonraki bölümlerde sunulmaktadır. Ayrıca, doğal gaz, petrol ve kömür ağırlıklı olarak hidrokarbonlardan oluşmaktadır. Hidrokarbonlar, hidrojen, karbon ve çeşitli katışıklardan oluşur. Doğal gaz çoğunlukla metan (CH₄), etan (C₂H₆), propan (C₃H₈), bütan (C₄H₁₀), içermektedir. Doğal Gaz, karbon dioksit (CO₂), hidrojen sülfür (H₂S), hidrojen, azot, helyum ve argon gibi hidrokarbon olmayan bileşenleri içerebilir. Tipik bir doğal gaz bileşimi Tablo 3.20:’ de sunulmaktadır (Demirbaş, 2010). Ayrıca, hava kirliliği ve boru hattı korozyonuna neden olabileceğinden, satıştan önce CO₂ ve H₂S doğal gaz akışından ayrılmalıdır.

Tablo 3.20: Doğal gazın temel bileşenleri.

Bileşen	Tipik Analiz (mole %)	Aralık (mole %)
Methane CH ₄	95.2	87.0
Ethane C ₂ H ₆	2.5	1.5 - 5.1
Propane C ₃ H ₈	0.2	0.1 - 1.5
iso-Butane C ₄ H ₁₀	0.03	0.01 - 0.3
normal-Butane C ₄ H ₁₀	0.03	0.01 - 0.3
iso-Pentane C ₅ H ₁₂	0.01	trace - 0.14
normal-Pentane C ₅ H ₁₂	0.01	trace - 0.04
Hexane plus C ₆ H ₁₄	0.01	trace - 0.06
Nitrogen N ₂	1.3	0.7 - 5.6
Carbon Dioxide CO ₂	0.7	0.1 - 1.0

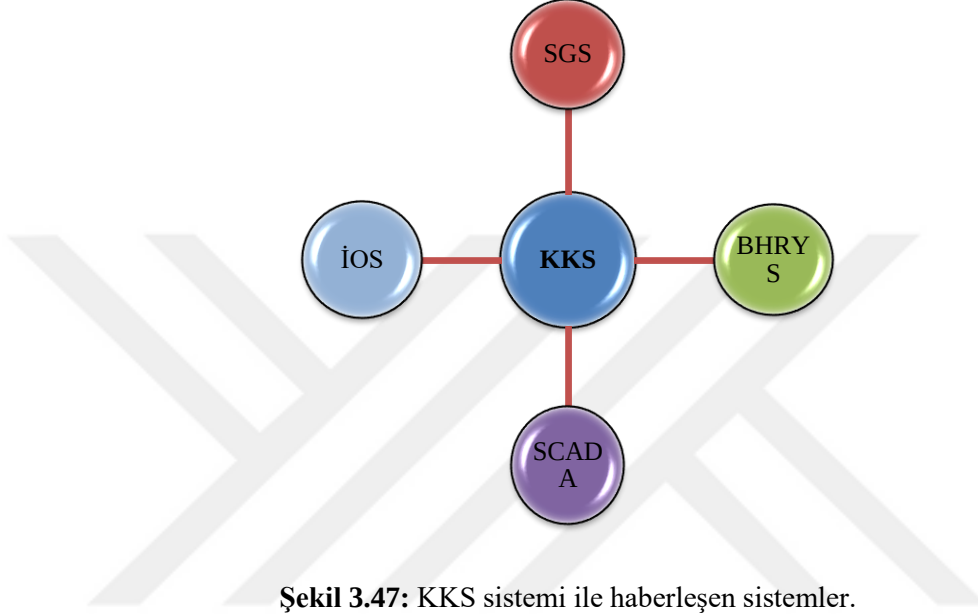
3.6.1. Akıllı Doğal Gaz Şebekesinde Katodik Koruma Sistemi (KKS)

Boru hatlarında kullanılan katodik koruma yöntemi yaklaşık olarak bir asırdır kullanılan bir koruma sistemidir. Boru hattının ve diğer tesislerin canlılığını etkileyen sayısız unsur bulunmaktadır. Bunlar yapı kalitesi, gazın özellikleri, çevresel durumlar, tercih edilen malzemeler ve bakım kalitesi ve katodik koruma (KK) sistemlerini içermektedir. Gaz boru hatlarındaki sorunların en önemli nedeni korozyondur. Ayrıca, gaz dağıtım şebekesi ve hizmetleri için bir tehlikedir. Korozyon, boru kalınlığının düşmesine ve mukavemet kaybına neden olabilir. Ek olarak, korozyon nedeniyle milyarlarca dolar kaybedilmektedir. Korozyonun karmaşık azaltımını sağlayan birçok unsur vardır, bu nedenle, boru hattının çoğunluğunun doğrudan gözlemlenmesi gereklidir. Doğal gaz, su buharı ve karbondioksit gibi az miktarda kirlenici içerebilir. Bu bileşenler iç korozyona neden olabilir. Korozyon, birçok faktöre bağlıdır dolayısıyla; başlıca korozyon-kontrol sistemleri türleri, karmaşık mühendislik çalışmaları ve çalışmanın hesaplanması sırasında gerçek araştırma verileri ve laboratuvar bilgisi gerektirir. Verimli bir korozyon koruma programı, potansiyel tehlikelerin ve sonuçların erken tanımlanmasını teşvik eder ve sorunları mümkün olan en kısa sürede çözer. Başarılı bir korozyon kontrol programı 3 temel aşamadan oluşmaktadır: beklenti, risk ve tehdit değerlendirmeleri, korozyon kontrolü ve korozyon izleme. Boru hattı korozyon kontrol yöntemlerinin tasarımında mühendisler bütünsel bir koruma düşünmelidirler. Aksi halde, korozyon sorunları, arızaların giderilmesi ve tasarımın düzeltilmesi daha fazla maliyete neden olabilir. Yetkin bir korozyon yönetim planı bu ekstra maliyetleri önleyebilir (Castillo, 2016).

Buna ek olarak, su kütleleri, komşu demiryolu sistemleri, farklı gerilim iletim hatları ve çevredeki diğer boru hattı sistemleri, yeraltı su seviyeleri, pH seviyeleri ve arazinin korozivitesine işaret eden redoks potansiyelleri, başarılı bir katodik koruma için ifade edilmesi gereken diğer kriterler arasındadır. Yeraltı çelik boru hatları, EN 12954 katodik koruma kurallarının uygulanması ile korunmalıdır (BSI, 2001). Bu nedenle, KKS' nin pH seviyeleri, diğer altyapı geçişleri ve korozyon vb. gibi birçok performans kriteri bulunmaktadır. KKS' nin akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.21' de sunulmuştur. Doğal gaz dağıtımında KKS için tüm anahtar performans göstergelerini belirtilmiştir. Bu faktörler KKS ile ilgili mevzuat ve standartlar ışığında seviyelendirilmiştir.

3.6.1.1. KKS Sistemi İle Haberleşen Sistemler

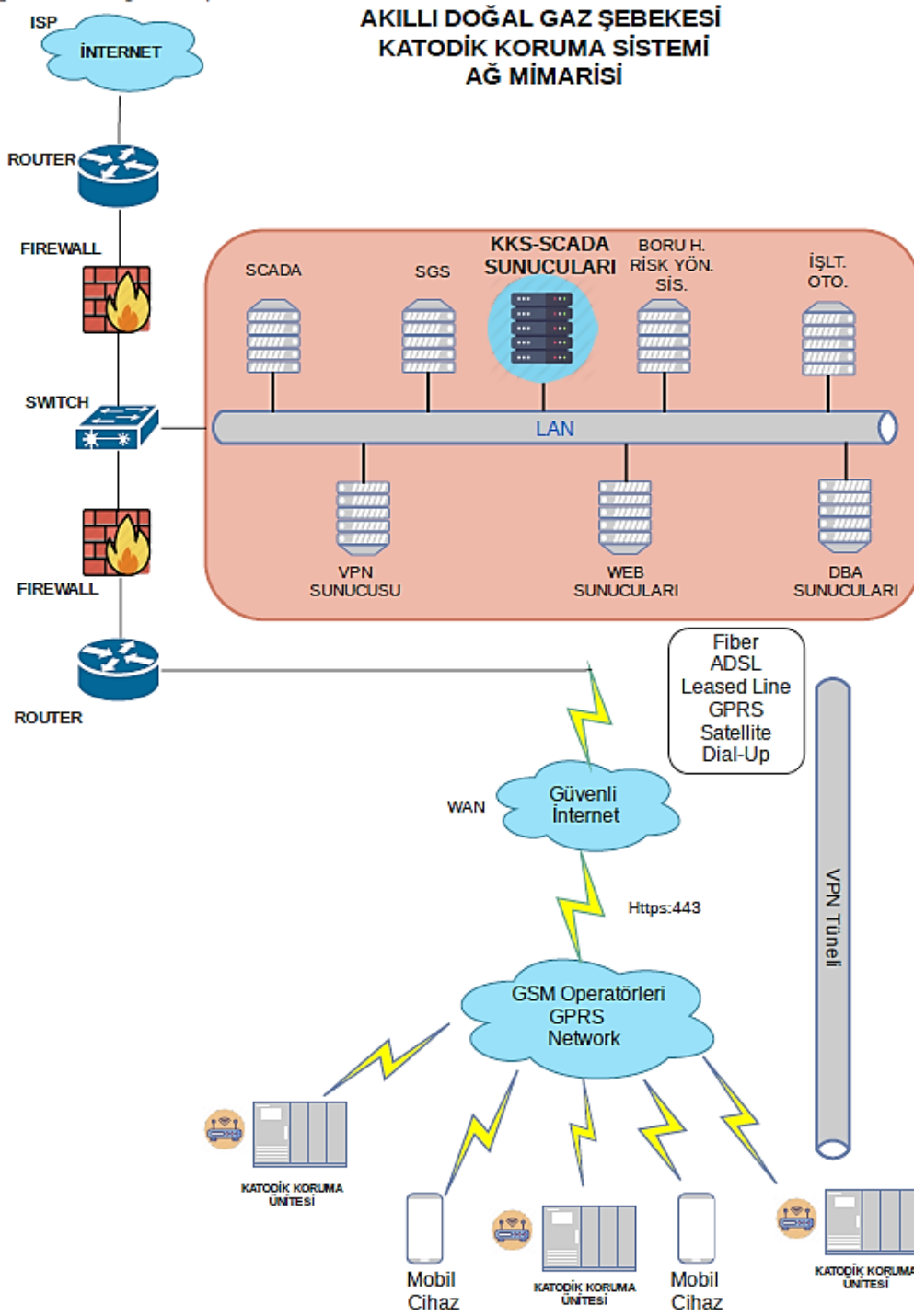
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde KKS sistemi akıllı şebekenin bir parçasıdır. KKS sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.47’ de gösterilmiştir.



Şekil 3.47: KKS sistemi ile haberleşen sistemler.

3.6.1.2. KKS Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan KKS sistemi incelenerek mevcut ağ mimarisi Şekil 3.48’ de verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.48: KKS sistemi ağ mimarisi.

3.6.1.3. KKS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi KKS sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.21’ de verilmiştir. Bu KPI listesine göre kurumlardaki

uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.21: KKS siber güvenlik olgunluk seviyesi ve KPI listesi.

Katodik Koruma Sistemi (KKS) KPI Listesi		AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Önem. Önem. Ağırlık	Olgunluk Seviyesi (%)
KKS Özellikleri (NIST SP-800, EPOK, CIS, COBIT, ISO/IEC 27001-27002-27015, KVKK, PCI DSS, ISA/IEC 62443-2009)		2,035	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
1	Erişim ve Kimlik Yönetimi											
	(Erişim yönetimi ayrıntıdaki alt sistemler için değil, sadece erişim ve kimlik için değerlendirilmelidir. Bu KPI sistemdeki hesaplara erişim için verilmelidir. Bu gereklilik belirlenmelidir.)											
1.1	KKS Sistemlerinde, erişim kontrol yönetim politikası ve prosedürü bulunuyor mu?	7	8	9	8	9	8,2	0,088	4,311	0,072		
1.2	KKS Sistemlerinde, kullanıcı hesapları yönetim politikası ve prosedürü bulunuyor mu?	7	9	7	8	7	7,6	0,081	3,996	0,062		
1.3	KKS Sistemlerinde, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?	9	7	8	9	8	8,2	0,088	4,311	0,072		
1.4	KKS Sistemlerinde, sunuculara erişimde güvenli bağlantı protokolleri kullanılıyor mu?	7	8	7	9	3	6,8	0,073	3,575	0,049		
1.5	KKS Sistemlerinde, sunuculara erişim güvenliği veri şifreleme yöntemi kullanılıyor mu?	4	6	4	5	5	4,8	0,051	2,524	0,025		
1.6	KKS Sistemlerinde, internete ve sistemlere başkasız giriş denemeleri loglanıyor mu?	9	7	6	8	9	7,8	0,083	4,101	0,065		
1.7	KKS Sistemlerinde, internete ve sistemlere başkasız giriş denemeleri raporlanıyor mu?	9	9	9	9	6	8,4	0,090	4,416	0,076		
1.8	KKS Sistemlerinde, kullanımdan uzakta erişimde güvenli bağlantı protokolleri kullanılıyor mu?	8	7	8	9	7	7,8	0,083	4,101	0,065		
1.9	KKS Sistemlerinde, kullanımdan uzakta erişimleri için erişim kuraları var mı?	9	9	7	7	6	7,6	0,081	3,996	0,062		
1.10	KKS Sistemlerinde, kullanımdan uzakta erişim için güvenli veri şifreleme yöntemi var mı?	5	6	5	6	5	5,4	0,058	2,839	0,031		
1.11	KKS Sistemlerinde, erişim yetkilendirmeleri ve kısıtlamaları belirlenerek bilgi paylaşımı yapılıyor mu?	6	9	8	9	9	8,2	0,088	4,311	0,072		
1.12	KKS Sistemlerinde, Rol Bazlı Erişim Kontrolü (RBEC) kullanıcı erişim düzeylerini düzenlemek için roller, hiyerarşiler ve kısıtlamalar kullanılıyor mu?	7	7	9	7	7	7,4	0,079	3,891	0,059		
1.13	KKS Sistemlerinde, kurumsal ağa erişim sağlayan dış kaynakların veya sistemlerin listesi var mı?	8	7	8	6	6	7	0,075	3,680	0,052		
1.14	KKS Sistemlerinde, yetkilisi erişim yetkileri tespit etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapılıyor mu?	9	6	8	6	6	7	0,075	3,680	0,052		
1.15	KKS Sistemlerinde, farklı kaynaklar üzerinden elde edilen kullanıcı erişim iz kayıtları ile verinin toplanması ve ilişkilendirilmesi (korelasyon) yapılıyor mu?	9	9	9	6	4	7,4	0,079	3,891	0,059		
1.16	KKS Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?	9	7	5	6	5	6,4	0,068	3,365	0,044		
1.17	KKS Sistemlerinde, işletme dışı kişiler için kimlik tanımlama ve yetkilendirme yapılıyor mu?	6	6	9	6	6	6,6	0,071	3,470	0,047		
1.18	KKS Sistemlerinde, parola doğrulaması yapılıyor mu?	8	6	9	6	7	7,2	0,077	3,785	0,055		
1.19	KKS Sistemlerinde, parola belirleme ve kullanım kuraları var mı?	7	9	8	9	9	8,4	0,090	4,416	0,076		
1.20	KKS Sistemlerinde, ayrıcalıklı hesapların yönetimi yapılıyor mu?	7	7	7	7	9	7,4	0,079	3,891	0,059		
1.21	KKS Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?	7	9	9	9	9	8,6	0,092	4,522	0,079		
1.22	KKS Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?	7	8	9	7	9	8	0,086	4,206	0,068		
1.23	KKS Sistemlerinde, mobil iletişim sadece online ile haberleşme sağlanıyor mu?	6	6	6	6	6	6	0,064	3,155	0,039		
1.24	KKS Sistemlerinde, belirlenen uygulamalarında dışında herhangi bir uygulama çalışıyor mu?	8	9	6	8	8	7,8	0,083	4,101	0,065		
1.25	KKS Sistemlerinde, mobil cihazlara uygulama yüklemeye yetkisi var mı?	10	9	6	6	6	7,4	0,079	3,891	0,059		
1.26	KKS Sistemlerinde, mobil cihazlara erişim yetkisi sınırlı mı?	5	7	9	7	6	6,8	0,073	3,575	0,049		
		193	197	195	189	177	190,2	2,035	100,000	1,512	74%	

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI' lar toplamlar üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 74 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

KKS sistemi belirlenen KPI' lara ve soru setlerine göre değerlendirildi. Tüm KPI' lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi KKS sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 73' tür. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından KKS sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 73 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. KKS sistemlerinde kurumların tüm siber saldırı yöntemlerini dikkate alarak kurumun IT ve OT sistemlerini en yüksek seviyede korumaları

önem arz etmektedir. Özellikle enerji altyapılarına ve kurumlara en yaygın saldırılar olan Hizmet Kesintisi (DDoS), Araya Girme Saldırısı (MITM), Zararlı Yazılımlar (Malware (Worm,Trojan, Rootkit, Virus)), Replay Saldırısı, Sahtecilik (Spoofing) (ARP, IP, GPS), MODBUS/TCP Protocol Attack, DNP3 Protocol Attack, Malicious Command and Software Injection, Buffer Overflow, Sosyal Mühendislik, Fiziksel Saldırı (Sensör, Actuator, Kamera), SQL Injection ve Zero Day saldırıları akıllı doğal gaz şebeklerine sahip enerji kurumları tarafından yaşanabilmektedir. Bu saldırıların engellenmesi için standartlara uyum, log yönetimi, yama yönetimi, ağ segamntasyon, sıkılaştırma, açık portların kapatılması, verilerin gizliliği, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

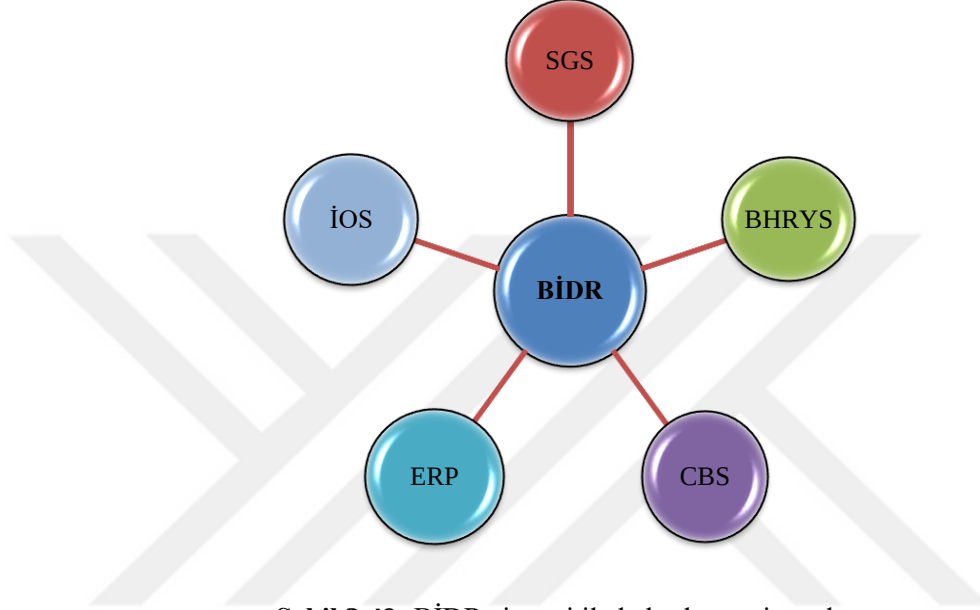
3.6.2. Akıllı Doğal Gaz Şebekesinde Boru İçi Denetleme Robotu (BİDR)

Boru içi denetleme robotu, otomasyon sistemlerinin bir bileşeni olarak akıllı doğal gaz dağıtım şebekesine önemli bir katkı sağlar. Boru içi kontrolü, genellikle “akıllı pigler” ya da boru hattına yayılmış boru içi kontrol ekipmanı olarak teknolojik yenilikçi ekipman kullanımını içerir. Akıllı robotlar aslında bir boru hattı boyunca seyahat ederken yaptıkları gıcırta sesi sayesinde bilgiler alınır. Başlangıçta boru hattı içerisindeki denetimler için akıllı pigler tercih edilirdi. Ancak, günümüzde ise boru hattı içerisinde meydana gelen anormal durumların tespiti ve boru hatlarının iç kontrolleri için yaygın olarak kullanılmaktadırlar (ISO, 2011). Boru hattı denetleme robotu borulara ait yükseklik, korozyon, boru et kalınlığı, malzeme kaybı ve hasar bilgilerinin alınmasında yardımcı olmaktadır. Robot üzerinde mobil batarya, GPS ve veri depolama ünitesi bulunmaktadır. Robot aynı zamanda hem gazlı hemde gazsız ortamda aynı zamanda belirli çaplardaki borularda çalışabilmektedir.

Doğruluk limitleri, veri kalitesi vb. gibi birçok performans kriteri bulunmaktadır. Boru içi denetleme robotunun akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.22’ de sunulmuştur. BİDR ile ilgili mevzuat ve standartlar ışığında bu temel performans göstergelerinin düzeyleri belirlenmiştir.

3.6.2.1. BİDR Sistemi İle Haberleşen Sistemler

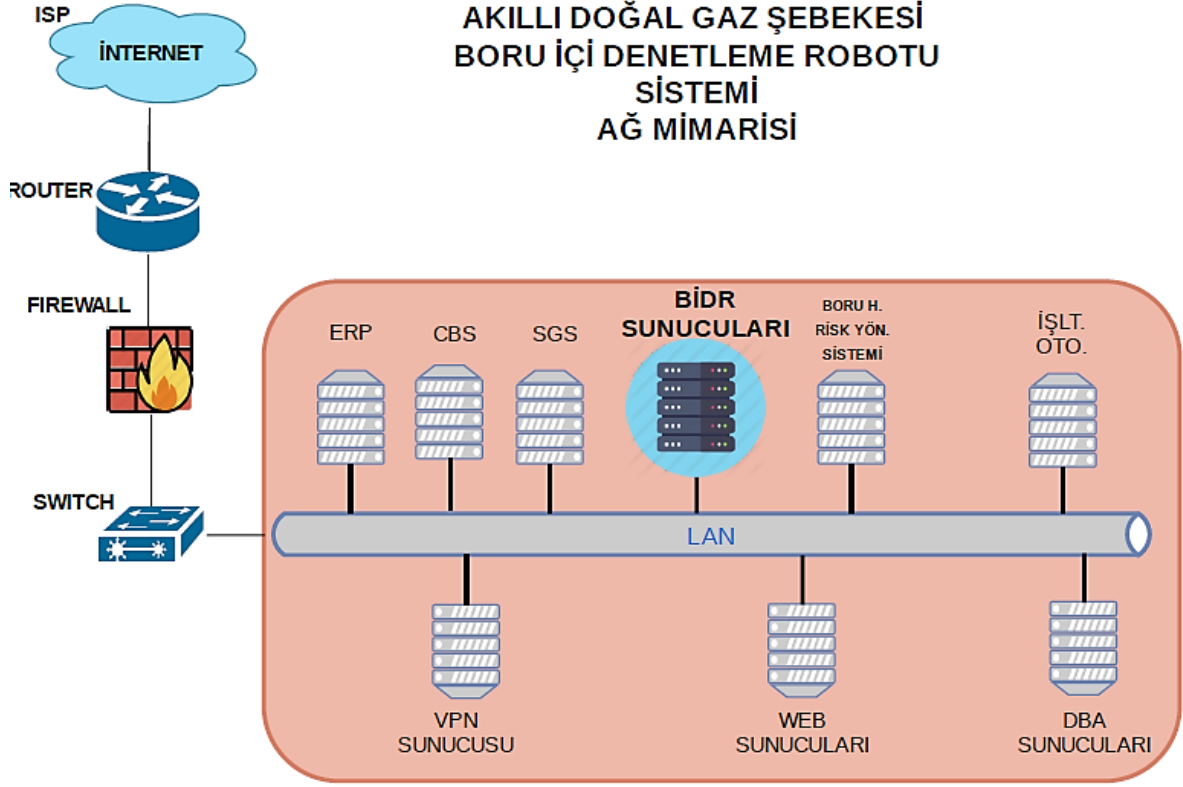
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde BİDR sistemi akıllı şebekenin bir parçasıdır. BİDR sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.49’ da gösterilmiştir.



Şekil 3.49: BİDR sistemi ile haberleşen sistemler.

3.6.2.2. BİDR Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan BİDR sistemi incelenerek mevcut ağ mimarisi Şekil 3.50’ de verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.50: BİDR sistemi ağ mimarisi.

3.6.2.3. BİDR Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi BİDR sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.22’ de verilmiştir. Bu KPI listesine göre kurumlardaki uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.22: BİDR siber güvenlik olgunluk seviyesi ve KPI listesi.

Boru İçi Denetleme Robotu (BİDR) KPI Listesi										AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Göre Önem Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
BİDR Özellikleri (NIST SP-800, EPDK, CIS, COBIT, ISO/IEC 27001-27002-27015, RVKK, PKI DSS, ISA/IEC 62443:2009)										0,394	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
1. Erişim ve Kimlik Yönetimi																				
1.1 BİDR Sistemlerinde, erişim kontrol yönetim politikası ve prosedürü bulunuyor mu?											7	8	9	8	9	8,2	0,017	4,385	0,014	
1.2 BİDR Sistemlerinde, kullanıcı hesapları yönetim politikası ve prosedürü bulunuyor mu?											7	9	7	8	7	7,6	0,016	4,064	0,012	
1.3 BİDR Sistemlerinde, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?											9	7	8	9	8	8,2	0,017	4,385	0,014	
1.4 BİDR Sistemlerinde, sunuculara erişimde güvenli bağlantı protokolleri kullanılıyor mu?											7	8	7	9	3	6,8	0,014	3,636	0,010	
1.5 BİDR Sistemlerinde, sunuculara erişim güvenli veri şifreleme yöntemi kullanılıyor mu?											4	6	4	5	5	4,8	0,010	2,567	0,005	
1.6 BİDR Sistemlerinde, internete ve sistemlere başarıyla giriş denemeleri loglanıyor mu?											9	7	6	8	9	7,8	0,016	4,171	0,013	
1.7 BİDR Sistemlerinde, internete ve sistemlere başarıyla giriş denemeleri raporlanıyor mu?											9	9	9	9	6	8,4	0,018	4,492	0,015	
1.8 BİDR Sistemlerinde, kullanılan uzaktan erişimde güvenli bağlantı protokolleri kullanılıyor mu?											8	7	8	9	7	7,8	0,016	4,171	0,013	
1.9 BİDR Sistemlerinde, kullanılan uzaktan erişim için erişim kuralları var mı?											9	9	7	7	6	7,6	0,016	4,064	0,012	
1.10 BİDR Sistemlerinde, kullanılan uzaktan erişim için güvenli veri şifreleme yöntemi var mı?											5	6	5	6	5	5,4	0,011	2,888	0,006	
1.11 BİDR Sistemlerinde, erişim yetkilendirmeleri ve kullanılan belirlenenek bilgi paylaşımı yapılıyor mu?											6	9	8	9	9	8,2	0,017	4,385	0,014	
1.12 BİDR Sistemlerinde, Rol Bazı Erişim Kontrolü (RBK) kullanıcı erişim düzeylerini düzenlemek için roller, hiyerarşiler ve kısıtlamalar kullanılıyor mu?											7	7	9	7	7	7,4	0,016	3,957	0,012	
1.13 BİDR Sistemlerinde, kurumsal ağa erişim sağlayan dış kaynakların veya sistemlerin listesi var mı?											8	7	8	6	6	7	0,015	3,743	0,010	
1.14 BİDR Sistemlerinde, yetkisiz erişim eylemlerini tespit etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapılıyor mu?											9	6	8	6	6	7	0,015	3,743	0,010	
1.15 BİDR Sistemlerinde, farklı kaynaklar üzerinden elde edilen kullanıcı erişim iz kayıtları ile verinin toplanması ve ilişkilendirilmesi (korelasyon) yapılıyor mu?											9	9	9	6	4	7,4	0,016	3,957	0,012	
1.16 BİDR Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?											7	9	5	6	5	6,4	0,013	3,422	0,009	
1.17 BİDR Sistemlerinde, işletme dış kişiler için kimlik tanımlama ve yetkilendirme yapılıyor mu?											6	6	9	6	6	6,6	0,014	3,529	0,009	
1.18 BİDR Sistemlerinde, parola doğrulaması yapılıyor mu?											8	6	9	6	7	7,2	0,015	3,850	0,011	
1.19 BİDR Sistemlerinde, parola belirlene ve kullanımları var mı?											7	9	8	9	9	8,4	0,018	4,492	0,015	
1.20 BİDR Sistemlerinde, yalncaklı hesapların yönetimi yapılıyor mu?											7	7	7	7	9	7,4	0,016	3,957	0,012	
1.21 BİDR Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları tutuluyor mu?											7	9	5	5	5	6,2	0,013	3,316	0,008	
1.22 BİDR Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?											7	8	5	7	9	7,2	0,015	3,850	0,011	
1.23 BİDR Sistemlerinde, mobil iletişim sadece online iken merkez ile haberleşme sağlanıyor mu?											6	6	6	6	6	6	0,013	3,209	0,008	
1.24 BİDR Sistemlerinde, belirlenen uygulamalarında dışında herhangi bir uygulama çalışıyor mu?											8	9	6	8	8	7,8	0,016	4,171	0,013	
1.25 BİDR Sistemlerinde, mobil cihazlara uygulama yüklemeye yetkisi var mı?											10	9	6	6	6	7,4	0,016	3,957	0,012	
1.26 BİDR Sistemlerinde, mobil cihazlara erişim yetkisi sınırlı mı?											5	7	9	7	6	6,8	0,014	3,636	0,010	
											193	197	187	185	173	187	0,394	100,000	0,287	73%

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI' lar toplamı üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 73 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

BİDR sistemi belirlenen KPI' lara ve soru setlerine göre değerlendirildi. Tüm KPI' lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi BİDR sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 72' dir. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından BİDR sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 72 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. BİDR sistemlerinde kurumların tüm siber saldırı yöntemlerini dikkate alarak kurumun IT ve OT sistemlerini en yüksek seviyede korumaları önem arz etmektedir. Özellikle enerji altyapılarına ve kurumlara en yaygın saldırılar olan Hizmet Kesintisi (DDoS), Sahtecilik (Spoofing) (ARP, IP, GPS), Sosyal Mühendislik, Fiziksel Saldırı (Sensör, Actuator, Kamera), Zero Day, Phishing (Oltalama) saldırıları akıllı doğal gaz şebekelerine sahip enerji kurumları tarafından yaşanabilmektedir. Bu saldırıların engellenmesi için standartlara uyum, log yönetimi, yama yönetimi, ağ segmentasyonu, sıkılaştırma, açık portların kapatılması, verilerin gizliliği, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

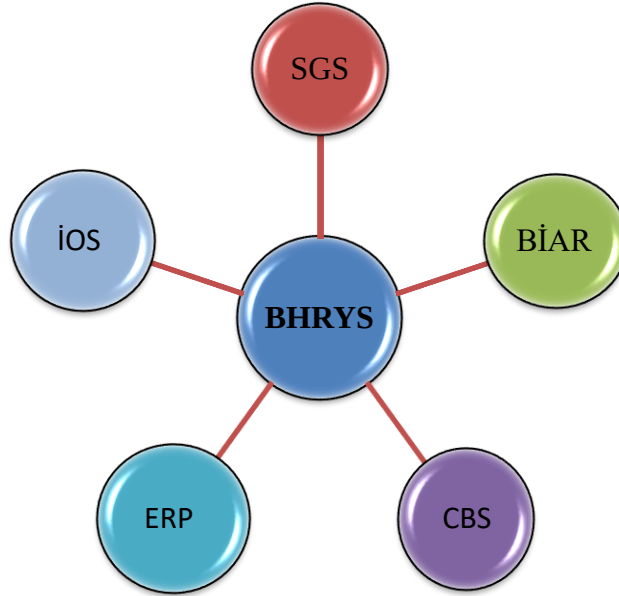
3.6.3. Akıllı Doğal Gaz Şebekesinde Boru Hattı Risk Yönetim Sistemi (BHRYIS)

Boru Hattı Risk Yönetim Sistemi (BHRYIS), akıllı doğal gaz şebekesini bir bileşeni olarak doğal gaz dağıtım şebekesine önemli bir katkı sağlayan yazılım uygulamasıdır. Bu uygulama sayesinde kuruma ait boru hattı bilgisi, hasar, arıza yoğunluğu, ihbar yoğunluğu, metal kaybı,

hatalı işletme vb. birçok performans kriteri vardır. Risk yönetimi ile birlikte varlık yönetimi önemli bir konu haline gelmektedir. Dünya ve Türkiye genelindeki akıllı doğal gaz şebekelerinde siber saldırılar nedeni ile birçok boru hatlarda patmalar meydana geldiği görülmektedir. Öncelikle tüm şebekenin güvenliğinin sağlanması ve sistemlerin siber saldırılara karşı korumak için önlemlerin üst seviyede olması gerekmektedir. Boru hattı üzerinde ve dolaylı olarak ilgili ekipmanların üzerinde oluşabilecek siber saldırıların belirlenmesi ve geleceğe yönelik oluşabilecek siber saldırı risklerinin tahmin edilmesi amaçlanmaktadır. BHRYS' nin akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.23' de sunulmuştur. BHRYS' nin doğal gaz dağıtımında tüm performans göstergelerini belirtilmiştir. BHRYS ile ilgili mevzuat ve standartlar ışığında bu faktörlerin düzeyini belirtilmiştir.

3.6.3.1. BHRYS Sistemi İle Haberleşen Sistemler

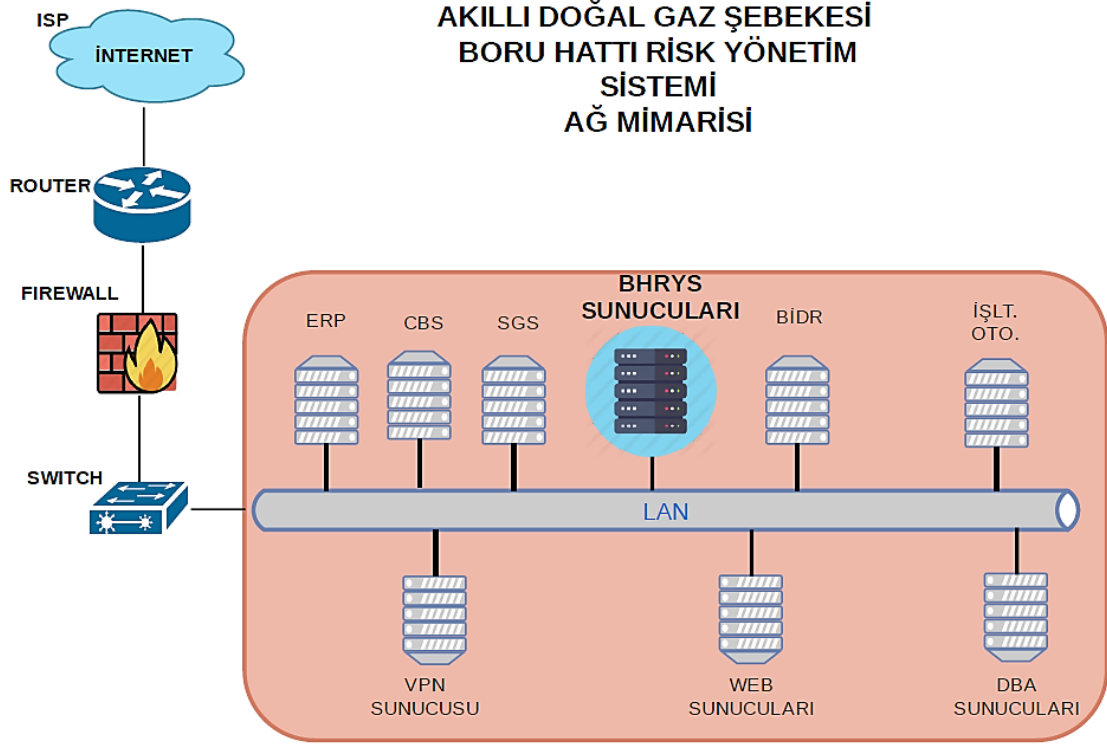
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde BHRYS sistemi akıllı şebekenin bir parçasıdır. BHRYS sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.51' de gösterilmiştir.



Şekil 3.51: BHRYS sistemi ile haberleşen sistemler.

3.6.3.2. BHRYS Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan BHRYS sistemi incelenerek mevcut ağ mimarisi Şekil 3.52’ de verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.52: BHRYS sistemi ağ mimarisi.

3.6.3.3. BHRYS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi BHRYS sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.23’ de verilmiştir. Bu KPI listesine göre kurumlardaki uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.23: BHRYS siber güvenlik olgunluk seviyesi ve KPI listesi.

Boru Hattı Risk Yönetim Sistemi (BHRYS) KPI Listesi		AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
BHRYS Özellikleri (NIST SP-800, EPDK, CIS, COBIT, ISO/IEC 27001-27002-27019, KVKK, PCI DSS, ISA/IEC 62443:2009)		0,355	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
1	Erişim ve Kimlik Yönetimi											
(Erişim izleni atararak zararlı faaliyet erişim veya bilgilerin edinilmesi ile kullanımları için dış sistemlere talep edilmesi veya reddedilmesi sürecidir. Bir BT sisteminde, kaynaklara erişim için verilecekleri bir parçanın belirli bir kısımlarını (örneğin, parollar, kimlikler, yetkiler) kullanmak suretiyle bir kullanıcının, işletme veya cihazın kimliğini doğrulaması sürecidir.)												
1.1	BHRYS Sistemlerinde, erişim kontrol yönetim politikası ve prosedürü bulunuyor mu?		7	8	9	8	9	8,2	0,015	4,266	0,012	
1.2	BHRYS Sistemlerinde, kullanıcı hesapları yönetim politikası ve prosedürü bulunuyor mu?		7	9	7	8	7	7,6	0,014	3,954	0,011	
1.3	BHRYS Sistemlerinde, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?		9	7	8	9	8	8,2	0,015	4,266	0,012	
1.4	BHRYS Sistemlerinde, sunuculara erişimde güvenli bağlantı protokolleri kullanılıyor mu?		7	8	7	9	3	6,8	0,013	3,538	0,009	
1.5	BHRYS Sistemlerinde, sunuculara erişim güvenli veri şifreleme yöntemi kullanılıyor mu?		4	6	4	5	5	4,8	0,009	2,497	0,004	
1.6	BHRYS Sistemlerinde, internete ve sistemlere başarısız giriş denemeleri loglanıyor mu?		9	7	6	8	9	7,8	0,014	4,058	0,011	
1.7	BHRYS Sistemlerinde, internete ve sistemlere başarısız giriş denemeleri raporlanıyor mu?		9	9	9	9	6	8,4	0,016	4,370	0,013	
1.8	BHRYS Sistemlerinde, kullanılan uzaktan erişimde güvenli bağlantı protokolleri kullanılıyor mu?		8	7	8	9	7	7,8	0,014	4,058	0,011	
1.9	BHRYS Sistemlerinde, kullanılan uzaktan erişim için güvenli veri şifreleme yöntemi var mı?		9	9	7	9	6	8	0,015	4,162	0,012	
1.10	BHRYS Sistemlerinde, kullanılan uzaktan erişim için güvenli veri şifreleme yöntemi var mı?		9	6	5	6	5	6,2	0,011	3,226	0,007	
1.11	BHRYS Sistemlerinde, erişim yetkilendirmeleri ve kısıtlamaları belirlenerek bilgi paylaşımı yapılıyor mu?		6	9	8	9	9	8,2	0,015	4,266	0,012	
1.12	BHRYS Sistemlerinde, Rol Bazlı Erişim Kontrolü (RBAC) kullanıcı erişim düzeylerini düzenlemek için roller, hiyerarşiler ve kısıtlamalar kullanılıyor mu?		7	7	9	7	7	7,4	0,014	3,850	0,010	
1.13	BHRYS Sistemlerinde, kurumsal ağa erişim sağlayan dış kaynakların veya sistemlerin listesi var mı?		8	7	8	6	6	7	0,013	3,642	0,009	
1.14	BHRYS Sistemlerinde, yetkili erişim yetkilerini tespit etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapılıyor mu?		9	6	8	6	6	7	0,013	3,642	0,009	
1.15	BHRYS Sistemlerinde, farklı kaynaklar üzerinden elde edilen kullanıcı erişim iz kayıtları ile verinin toplanması ve ilişkilendirilmesi (korelasyon) yapılıyor mu?		9	9	9	6	4	7,4	0,014	3,850	0,010	
1.16	BHRYS Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?		9	7	9	6	5	7,2	0,013	3,746	0,010	
1.17	BHRYS Sistemlerinde, işletme dışı kişiler için kimlik tanımlama ve yetkilendirme yapılıyor mu?		6	6	9	6	6	6,6	0,012	3,434	0,008	
1.18	BHRYS Sistemlerinde, parola doğrulaması yapılıyor mu?		8	6	9	6	7	7,2	0,013	3,746	0,010	
1.19	BHRYS Sistemlerinde, parola belirleme ve kullanım kuralları var mı?		7	9	8	9	9	8,4	0,016	4,370	0,013	
1.20	BHRYS Sistemlerinde, ayrıcalıklı hesapların yönetimi yapılıyor mu?		7	7	7	7	8	7,4	0,014	3,850	0,010	
1.21	BHRYS Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?		7	9	9	9	9	8,6	0,016	4,475	0,014	
1.22	BHRYS Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?		7	8	9	7	9	8	0,015	4,162	0,012	
1.23	BHRYS Sistemlerinde, mobil iletişim sadece online ile merkez ile haberleşme sağlanıyor mu?		6	6	6	6	6	6	0,011	3,122	0,007	
1.24	BHRYS Sistemlerinde, belirlenen uygulamalarda dışında herhangi bir uygulama çalışıyor mu?		8	9	6	8	8	7,8	0,014	4,058	0,011	
1.25	BHRYS Sistemlerinde, mobil cihazlara uygulama yüklemeye yetkisi var mı?		10	9	6	6	6	7,4	0,014	3,850	0,010	
1.26	BHRYS Sistemlerinde, mobil cihazlara erişim yetkisi sınırlı mı?		5	7	9	7	6	6,8	0,013	3,538	0,009	
			197	197	199	191	177	192,2	0,355	100,000	0,266	75%

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI' lar toplamı üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 75 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

BHRYS sistemi belirlenen KPI' lara ve soru setlerine göre değerlendirildi. Tüm KPI' lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi BHRYS sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 75' tir. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından BHRYS sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 79 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. BHRYS sistemlerinde kurumların tüm siber saldırı yöntemlerini dikkate alarak kurumun IT ve OT sistemlerini en yüksek seviyede korumaları önem arz etmektedir. Özellikle enerji altyapılarına ve kurumlara en yaygın saldırılar olan Hizmet Kesintisi (DDoS), Sahtecilik (Spoofing) (ARP, IP, GPS), Sosyal Mühendislik,

Zero Day, Phishing (Oltalama) saldırıları akıllı doğal gaz şebekelerine sahip enerji kurumları tarafından yaşanabilmektedir. Bu saldırıların engellenmesi için standartlara uyum, log yönetimi, yama yönetimi, ağ segamntasyon, sıkılaştırma, açık portların kapatılması, verilerin gizliliği, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

3.7. AFET YÖNETİMİ

Akıllı doğal gaz şebekelerinin ana kriterlerden biri olan afet yönetimi tüm dünyada olduğu gibi Türkiye’ de de akıllı yönetimi önem arz etmektedir. Afet yönetimi için kullanılan sistemlerin güvenliği oluşabilecek zararlar açısından kurumlar son yıllarda yatırımlarını artırmaktadır. Depremler, fırtına, sel, yangın, tehlikeli maddeler, vb. felaketler heran ve her yerde birçok farklı şekilde meydana gelebilir. Bu nedenle daha önce gaz arzı güvenceye alınması için risk değerlendirmesi yapılmalıdır. ISO 22320, talimatlar oluşturma ve organizasyon çerçevelerini ve prosedürlerini yönetme, yargı desteği, izlenebilirlik ve veri yönetimi konularında en iyi çalışmayı tanımlar (ISO, 2011). Akıllı doğal gaz şebekesi üzerinde afet yönetimi iki bileşenle gerçekleştirilebilir. Bunlar Deprem Risk Azaltma Sistemi (DRAS-SI) ve İhbar Yönetim Sistemi (İYS)’ dir.

3.7.1. Akıllı Doğal Gaz Şebekesinde Deprem Risk Azaltım Sistemi (DRAS-SI)

Akıllı doğal gaz şebekesi konseptinde önemli konulardan biri de deprem riskinin azaltmasıdır. KOERI (Kandilli Rasathanesi ve Deprem Araştırma Enstitüsü) ve TÜBİTAK (Türkiye Bilimsel ve Teknolojik Araştırma Merkezi) işbirliğiyle kurumun Doğal Gaz Şebekesi Deprem Riski Azaltma Sistemi (DRAS-SI) projesi aşağıdaki 4 aşamada gerçekleştirilmiştir:

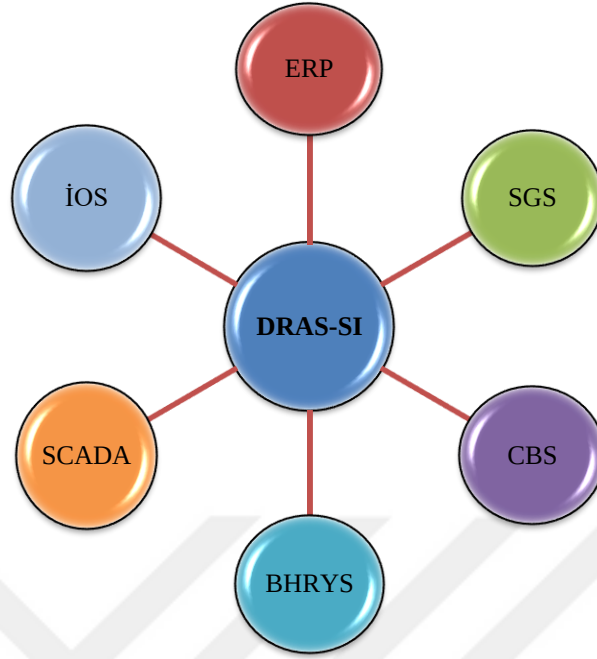
1. **Risk Analizi:** Doğal Gaz Şebekesi için senaryo bazlı tehlike ve hasar tespiti çalışmaları yapılmaktadır.
2. **İzleme - Erken Uyarı - Acil Durum Müdahale Bilgi Servisi:** Kuruma ait akıllı doğal gaz şebekesindeki bölge regülatörleri izlenmekte, Deprem Erken Uyarı uyarısı olan veya olmayan yer hareketi parametrelerinin eşik aşımına göre gerçek zamanlı yer hareketi veri parametreleri hesaplanmakta ve kapama mekanizması devreye alınmaktadır. Acil müdahale bilgisi sistem üzerinden dağıtılmaktadır.

3. **Bilgi Değişimi ve İletişim:** Veriler, ilgili kişilerin gerekli cevabı verebilmeleri için basit ve anlaşılabilir bir hale getirilmiştir. Muhtemel hasar ve alarm uyarıları şirket içi, ulusal ve uluslararası iletişim kanalları aracılığıyla yayılmaktadır.
4. **Acil Durum Müdahale Kapasitesi:** Deprem senaryoları planlanan Deprem Risk Azaltma Sistemi, kurumun Acil Durum Müdahale ekiplerinin karşılaştıkları riskleri anlama ve bu risklere nasıl cevap vermeleri gerektiğini öğrenme noktasında önemli bir rol oynamaktadır.

Bu sistem, güçlü yer hareketi sensörü ile titreşim verilerini toplar ve çelik hatlar ve bölge regülatörleri gibi doğal gaz dağıtım enstrümanlarında tahribat hakkında bilgi verir. Kandilli Rasathanesi ile eş zamanlı olarak çalışarak oluşan yer hareketleri uydu haberleşme sistemi üzerinden alınmaktadır. Sistem üzerinde oluşabilecek siber güvenlik zaafiyetler yanlış SI değeri oluşturularak tüm akıllı doğal gaz şebekesinin gazsız kalmasına neden olabilir ve bu açıdan değerlendirildiğinde ekonomik ve kurumsal prestij olarak kurumlar zarara uğrayabilmektedir. DRAS-SI'ın akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.24' de listelenmiştir. Doğal gaz dağıtımında deprem risk azaltım sisteminin tüm performans göstergelerini sunulmuştur. Sistemin ile ilgili mevzuat ve standartlar ışığında bu göstergelerin düzeyleri belirlenmiştir.

3.7.1.1. DRAS-SI Sistemi İle Haberleşen Sistemler

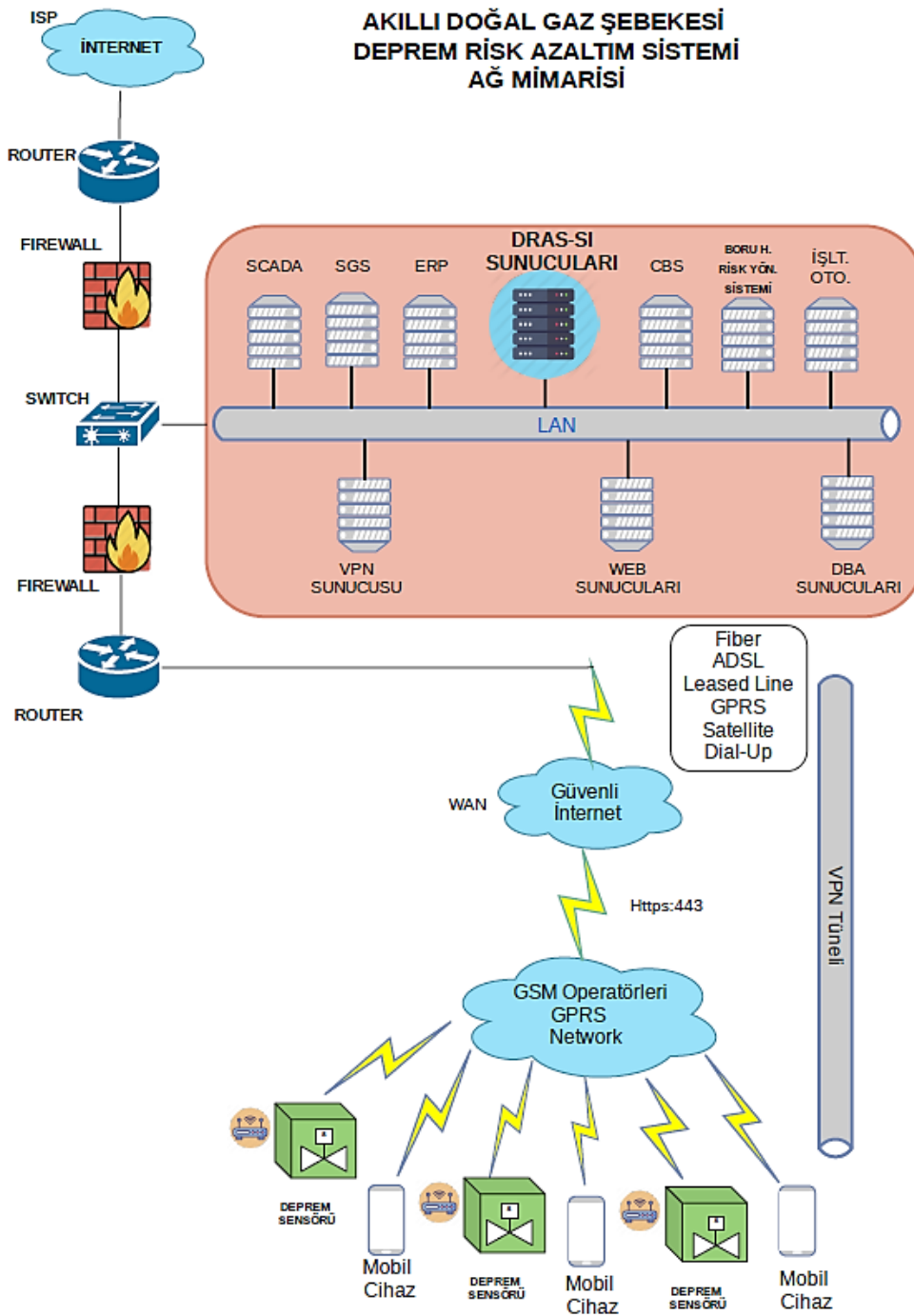
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde DRAS-SI sistemi akıllı şebekenin bir parçasıdır. DRAS-SI sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.53' de gösterilmiştir.



Şekil 3.53: DRAS-SI sistemi ile haberleşen sistemler.

3.7.1.2. DRAS-SI Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan DRAS-SI sistemi incelenerek mevcut ağ mimarisi Şekil 3.54’ de verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.54: DRAS-SI sistemi ağ mimarisi.

3.7.1.3. DRAS-SI Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi DRAS-SI sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.24’ de verilmiştir. Bu KPI listesine göre kurumlardaki uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.24: DRAS-SI siber güvenlik olgunluk seviyesi ve KPI listesi.

Deprem Risk Analiz Sistemi (DRAS&SI) KPI Listesi										AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
DRAS&SI Özellikleri (NIST SP-800, EPDK, CIS, COBIT, ISO/IEC 27001-27002-27019, KVKK, PCI DSS, ISA/IEC 62443-2009)																				
1	Erişim ve Kimlik Yönetimi									0,946	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
(Bilgi sistemi ortamındaki alandaki fiziksel erişim veya dijital erişimi ve kullanımını için dış sistemlere cevap verilmesi veya reddedilmesi sürecidir. Bir BT sistemindeki kaynaklara erişim izni verilmesinden din partı olarak belirli kimlik bilgileri için, parola, kimlik ve kimlik doğrulama süreçleri bir saldırıya, erişim veya çıkışa izin (kimlik doğrulama süreci).																				
1.1	DRAS&SI Sistemlerinde, erişim kontrol yönetim politikası ve prosedürü bulunuyor mu?										7	8	9	8	9	8,2	0,039	4,137	0,032	
1.2	DRAS&SI Sistemlerinde, kullanıcı hesapları yönetim politikası ve prosedürü bulunuyor mu?										9	9	7	8	7	8	0,038	4,036	0,031	
1.3	DRAS&SI Sistemlerinde, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?										9	7	8	9	8	8,2	0,039	4,137	0,032	
1.4	DRAS&SI Sistemlerinde, sunuculara erişimde güvenli bağlantı protokolleri kullanılıyor mu?										7	8	7	9	9	8	0,038	4,036	0,031	
1.5	DRAS&SI Sistemlerinde, sunuculara erişim güvenli veri şifreleme yöntemi kullanılıyor mu?										9	9	9	9	9	9	0,043	4,541	0,039	
1.6	DRAS&SI Sistemlerinde, internete ve sistemlere başarısız giriş denemeleri loglanıyor mu?										9	7	6	8	9	7,8	0,037	3,935	0,029	
1.7	DRAS&SI Sistemlerinde, internete ve sistemlere başarısız giriş denemeleri raporlanıyor mu?										9	9	9	9	6	8,4	0,040	4,238	0,034	
1.8	DRAS&SI Sistemlerinde, kullanılan uzaktan erişimde güvenli bağlantı protokolleri kullanılıyor mu?										8	7	8	9	7	7,8	0,037	3,935	0,029	
1.9	DRAS&SI Sistemlerinde, kullanılan uzaktan bağlantı erişimleri için erişim kuralları var mı?										9	9	7	7	6	7,6	0,036	3,835	0,028	
1.10	DRAS&SI Sistemlerinde, kullanıcıların uzaktan erişim için güvenli veri şifreleme yöntemi var mı?										5	6	5	6	5	5,4	0,026	2,725	0,014	
1.11	DRAS&SI Sistemlerinde, erişim yetkilendirmeleri ve kısıtlamaları belirlenerek bilgi paylaşımı yapılıyor mu?										6	9	8	9	9	8,2	0,039	4,137	0,032	
1.12	DRAS&SI Sistemlerinde, Rol Bazı Erişim Kontrolü (RBAC) kullanıcı erişim düzeylerini düzenlemek için roller, hiyerarşiler ve kısıtlamalar kullanılıyor mu?										7	7	9	7	7	7,4	0,035	3,734	0,026	
1.13	DRAS&SI Sistemlerinde, kurumsal ağa erişim sağlayan dış kaynakların veya sistemlerin listesi var mı?										8	7	8	6	6	7	0,033	3,532	0,023	
1.14	DRAS&SI Sistemlerinde, yetkisiz erişim eylemlerini tespit etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapılıyor mu?										9	6	8	6	6	7	0,033	3,532	0,023	
1.15	DRAS&SI Sistemlerinde, farklı kaynaklar üzerinden elde edilen kullanıcı erişim izni kayıtları ile verinin toplanması ve ilişkilendirilmesi (korelasyon) yapılıyor mu?										9	9	9	9	4	7,4	0,035	3,734	0,026	
1.16	DRAS&SI Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?										9	7	5	6	5	6,4	0,031	3,229	0,020	
1.17	DRAS&SI Sistemlerinde, işletme dışı kişiler için kimlik tanımlama ve yetkilendirme yapılıyor mu?										6	6	9	6	6	6,6	0,032	3,330	0,021	
1.18	DRAS&SI Sistemlerinde, parola doğrulaması yapılıyor mu?										8	6	9	6	7	7,2	0,034	3,633	0,025	
1.19	DRAS&SI Sistemlerinde, parola belirlenme ve kullanım kuralları var mı?										9	9	8	9	9	8,8	0,042	4,440	0,037	
1.20	DRAS&SI Sistemlerinde, ayrıcalıklı hesapların yönetimi yapılıyor mu?										9	7	7	9	9	8,2	0,039	4,137	0,032	
1.21	DRAS&SI Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları tutuluyor mu?										9	9	9	9	9	9	0,043	4,541	0,039	
1.22	DRAS&SI Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?										7	8	9	7	9	8	0,038	4,036	0,031	
1.23	DRAS&SI Sistemlerinde, mobil iletişim sadece online ilen merkez ile haberleşme sağlanıyor mu?										6	6	6	6	6	6	0,029	3,027	0,017	
1.24	DRAS&SI Sistemlerinde, belirlenen uygulamalarda dışında herhangi bir uygulama çalışıyor mu?										8	9	9	8	8	8,4	0,040	4,238	0,034	
1.25	DRAS&SI Sistemlerinde, mobil cihazlara uygulama yüklemeye yetkisi var mı?										10	9	6	6	6	7,4	0,035	3,734	0,026	
1.26	DRAS&SI Sistemlerinde, mobil cihazlara erişim yetkisi sınırlı mı?										5	7	9	7	6	6,8	0,032	3,431	0,022	
										206	200	203	195	187	198,2	0,946	100,000	0,731	77%	

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI' lar toplamı üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 77 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

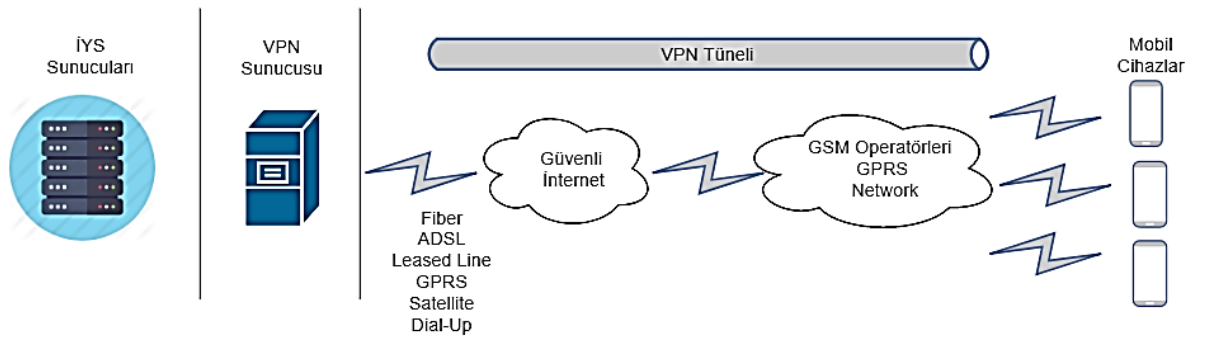
DRAS-SI sistemi belirlenen KPI' lara ve soru setlerine göre değerlendirildi. Tüm KPI' lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi DRAS-SI sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 76' dır. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından DRAS-SI sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 76 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. DRAS-SI sistemlerinde kurumların tüm siber saldırı yöntemlerini dikkate alarak kurumun IT ve OT sistemlerini en yüksek seviyede korumaları önem arz etmektedir. Özellikle enerji altyapılarına ve kurumlara en yaygın saldırılar olan Hizmet Kesintisi (DDoS), Sahtecilik (Spoofing) (ARP, IP, GPS) ve Replay saldırıları akıllı

doğal gaz şebekelerine sahip enerji kurumları tarafından yaşanabilmektedir. Bu saldırıların engellenmesi için standartlara uyum, log yönetimi, yama yönetimi, ağ segmentasyonu, sıkılaştırma, açık portların kapatılması, verilerin gizliliği, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

3.7.2 Akıllı Doğal Gaz Şebekesinde İhbar Yönetim Sistemi (İYS)

İhbar Yönetim Sistemi (İYS), otomasyon sistemlerinin bir bileşeni olarak akıllı doğal gaz dağıtım şebekesine çok önemli bir katkı sağlar. Özellikle acil ihbarların değerlendirilerek arz güvenliğinin sağlanması İYS sisteminin en önemli görevlerinden biridir. Ayrıca ihbar çeşidine göre hedef erişim süreleri mevzuatta belirlenmiştir, ihbarların sınıflandırılması ve ihbar kayıtlarının tutulması İYS üzerinden takip edilmektedir. Patlama, yangın, daire içi koku gibi konulardaki ihbarlar İYS marifetiyle şirket içersindeki ilgili birimlere iletilmekte ve müdahale edilmektedir. İYS sisteminin siber güvenlik açısından güvenli bir sistem olması hedeflenmektedir. Sistem üzerinden oluşabilecek güvenlik zaafiyetleri nedeni ile ilişkili olduğu sistemlere kötü niyetli kişilerin sızmasına neden olabilir. Özellikle İYS sistemi SCADA sistemine alarm göndermektedir oluşabilecek sızmalardan dolayı yanlış alarmlardan dolayı ekonomik ve kurumsal prestij zararları veya diğer sistemlere sızma yapılarak bütün sistemlere zarar verme olasılığı bulunmaktadır. İYS' nin akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.25' de sunulmuştur. Doğal gaz dağıtımında İYS için tüm temel performans göstergeleri tespit edilmiştir. İYS ile ilgili mevzuat ve standartlar ışığında bu temel performans göstergelerinin düzeyleri belirlenmiştir.

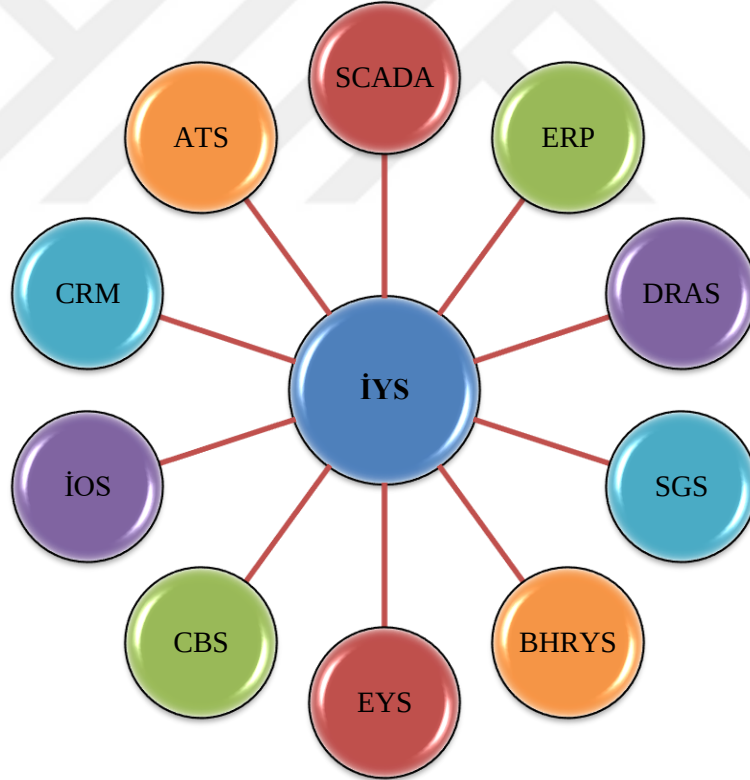


Şekil 3.55: Örnek İYS çalışma mimarisi.

Genel olarak Şekil 3.55’ de sistem saha iletişiminde merkezden yedekli “Leased Line” bağlantılı internet servis sağlayıcısının internet altyapısı ile başka bir kurumsal operatörün operasyon merkezine erişilmekte, buradan da kuruma özel kurulmuş bir APN (Erişim Noktası Adı) GPRS üzerinden sahadaki mobil cihazlarla iletişim sağlanmaktadır, mobil cihazlar bu özel ağa bağlıdır, internet erişimleri yoktur. Bu iletişim modelinin özel bir ağ olması itibariyle ciddi güvenlik avantajı mevcuttur ancak kesintisiz çalışma, yedekleme vb. konularda alternatifsiz olması nedeniyle sorunları mevcuttur.

3.7.2.1. İYS Sistemi İle Haberleşen Sistemler

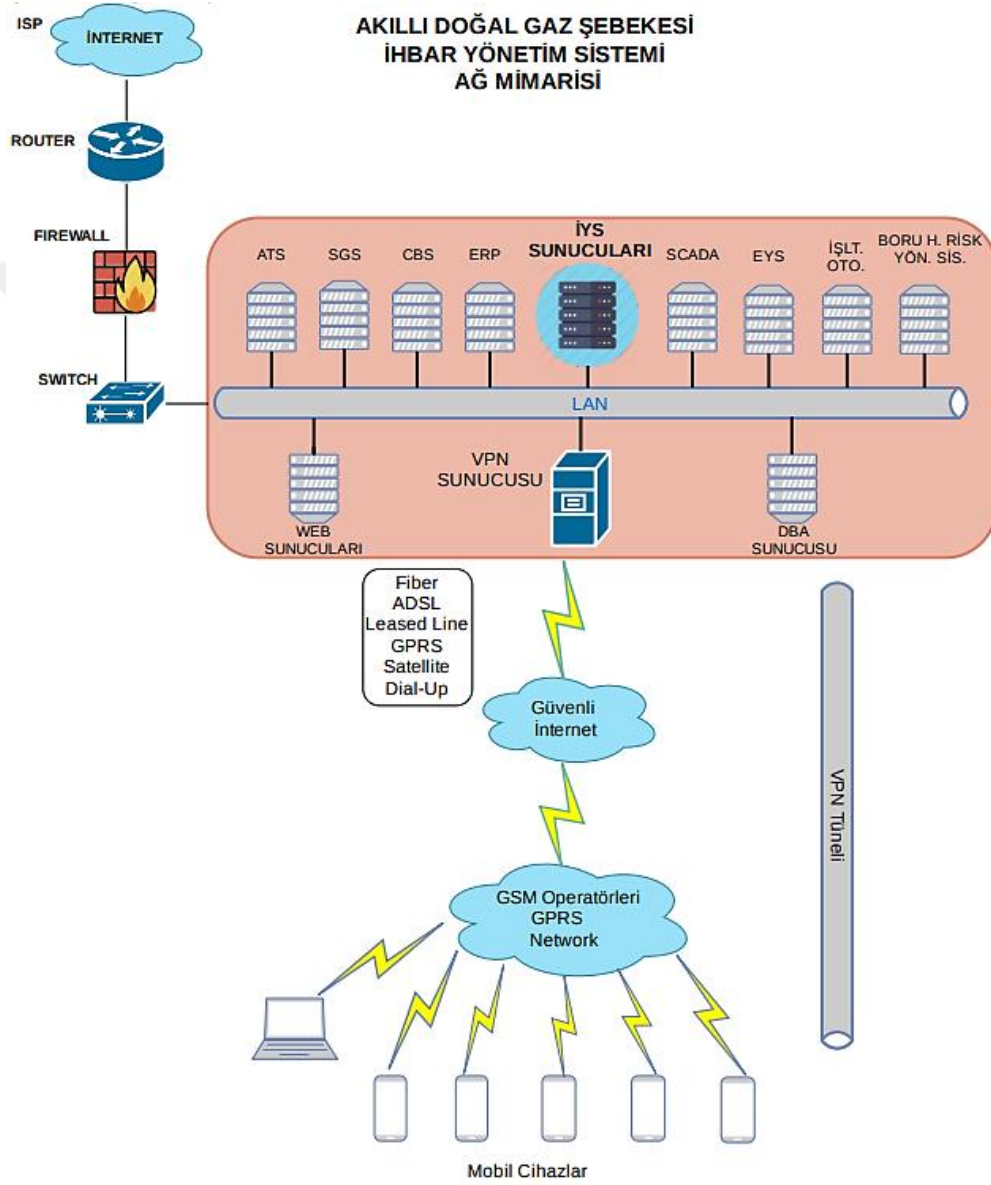
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde İYS sistemi akıllı şebekenin bir parçasıdır. İYS sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.56’ da gösterilmiştir.



Şekil 3.56: İYS sistemi ile haberleşen sistemler.

3.7.2.2. İYS Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan İYS sistemi incelenerek mevcut ağ mimarisi Şekil 3.57’ de verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.57: İYS sistemi ağ mimarisi.

3.7.2.3. İYS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi İYS sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.25’ de verilmiştir. Bu KPI listesine göre kurumlardaki

önem arz etmektedir. Özellikle enerji altyapılarına ve kurumlara en yaygın saldırılar olan Hizmet Kesintisi (DDoS), Araya Girme Saldırısı (MITM), Zararlı Yazılımlar (Malware (Worm,Trojan, Rootkit, Virus)), Replay Saldırısı, Sahtecilik (Spoofing) (ARP,IP,GPS), MODBUS/TCP Protocol Attack, DNP3 Protocol Attack ve Malicious Command and Software Injection saldırıları akıllı doğal gaz şebeklerine sahip enerji kurumları tarafından yaşanabilmektedir. Bu saldırıların engellenmesi için standartlara uyum, log yönetimi, yama yönetimi, ağ segmentasyon, sıkılaştırma, açık portların kapatılması, verilerin gizliliği, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

3.8. TESİSAT YÖNETİMİ

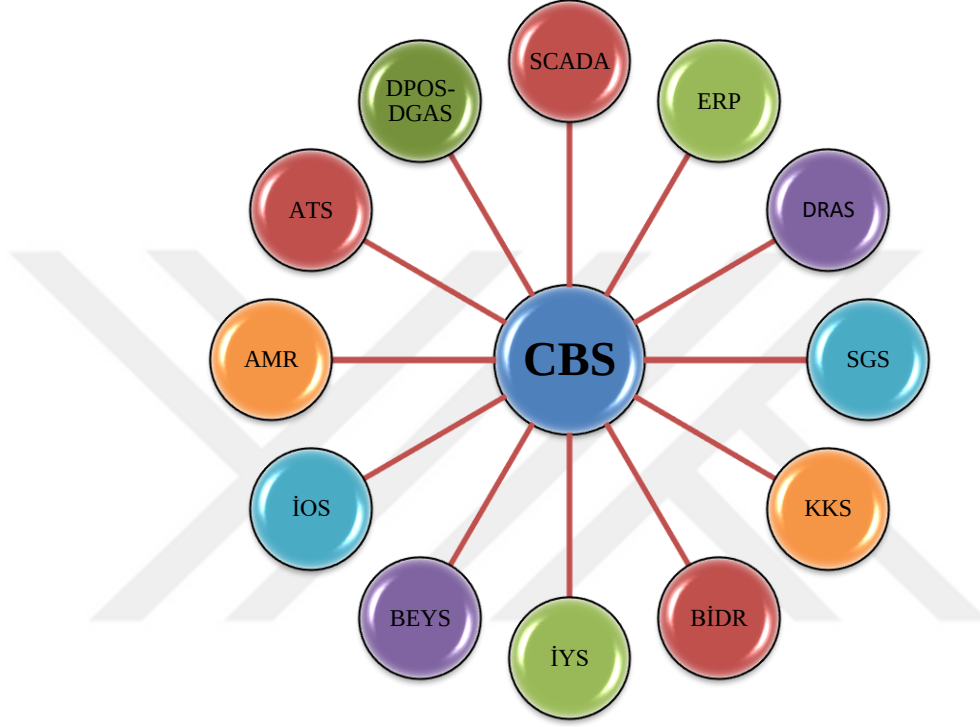
Doğal gaz şebekesi üzerindeki kurulum yönetimi üç bileşenle gerçekleştirilebilir. Bunlar Coğrafi Bilgi Sistemi (CBS), Dijital Proje Onay Sistemi (DPOS) & Dijital Gaz Açma Sistemi (DIGAS) ve Şebeke Yük Optimizasyon sistemidir.

3.8.1. Akıllı Doğal Gaz Şebekesinde Coğrafi Bilgi Sistemi (CBS)

CBS (Coğrafi Bilgi Sistemi), çelik ve polietilen hatların tam konumunu, regülatör, servis kutusu gibi tüm estrümanlar hakkında ayrıca bölgesel kadastro bilgileri ve saha görüntü bilgisi sağlayan bir uygulamadır. CBS, doğal gaz dağıtım alanında, akıllı doğal gaz şebeke sistemlerinin entegrasyonunda önemli bir yer tutmaktadır. Hatların tam konumunun sahada görüntülenebilmesi akıllı şebeke konseptinde gerekliliğidir. Ayrıca diğer alt yapı şirketleri ile ortak CBS kurulması akıllı şehir konsepti ve birlikte hareket edilebilme açısından önem arz etmektedir. Ayrıca, bu çalışmaya göre akıllı şebekelerin birbirine bütünlüğü, akıllı şebeke politikası ve diğer alt yapı şirketlerinin işbirliğinde CBS çok önemli bir yer tutmaktadır. Standart ve mevzuat ışığında CBS performans kriterleri belirlenmiş ve seviyelere ayrılmıştır. CBS' nin akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.26' da gösterilmiştir.

3.8.1.1. CBS Sistemi İle Haberleşen Sistemler

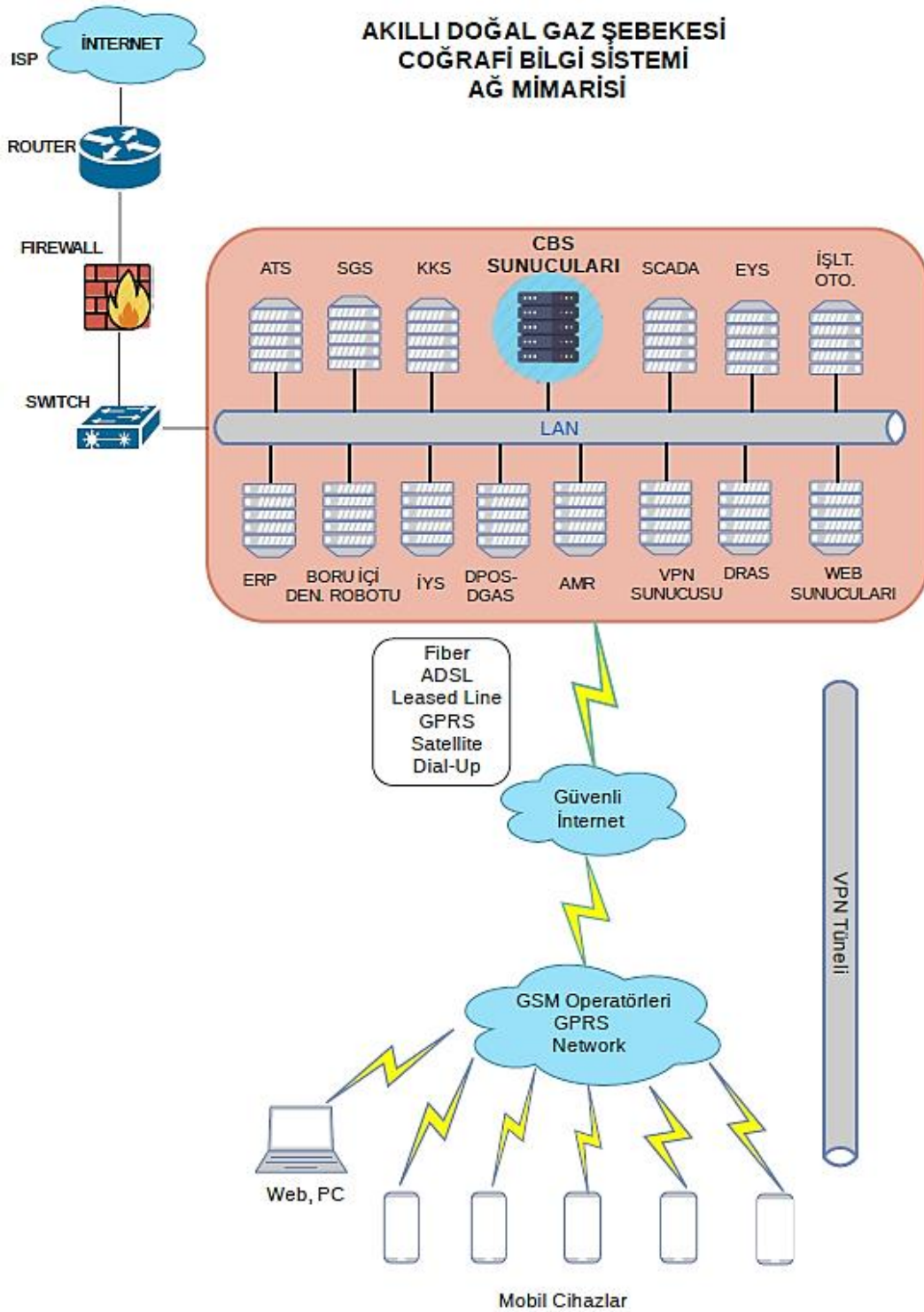
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde CBS sistemi akıllı şebekenin bir parçasıdır. CBS sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.58’ de gösterilmiştir.



Şekil 3.58: CBS sistemi ile haberleşen sistemler.

3.8.1.2. CBS Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan CBS sistemi incelenerek mevcut ağ mimarisi Şekil 3.59’ da verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.59: CBS sistemi ağ mimarisi.

3.8.1.3. CBS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi CBS sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.26’ da verilmiştir. Bu KPI listesine göre kurumlardaki

uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.26: CBS siber güvenlik olgunluk seviyesi ve KPI listesi.

Coğrafi Bilgi Sistemi (CBS) KPI Listesi							AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
CBS Özellikleri (NIST SP-800, EPOK, CIS, COBIT, ISO/IEC 27001-27002-27019, KVKK, PCI DSS, ISA/IEC 62443-2009)							0,497	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
1 Erişim ve Kimlik Yönetimi																	
(Erişim yönetimi, erişim kontrol politikası, erişim kontrol prosedürü, erişim kontrol politikası ve prosedürü bulunuyor mu?)																	
1.1	CBS Sistemlerinde, erişim kontrol politikası ve prosedürü bulunuyor mu?						7	8	9	8	9	8,2	0,021	4,205	0,017		
1.2	CBS Sistemlerinde, kullanıcı hesapları yönetim politikası ve prosedürü bulunuyor mu?						7	9	7	8	7	7,6	0,019	3,897	0,015		
1.3	CBS Sistemlerinde, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?						9	7	8	9	8	8,2	0,021	4,205	0,017		
1.4	CBS Sistemlerinde, sunuculara erişimde güvenli bağlantı protokolleri kullanılıyor mu?						7	8	7	9	3	6,8	0,017	3,487	0,012		
1.5	CBS Sistemlerinde, sunuculara erişim güvenli veri şifreleme yöntemi kullanılıyor mu?						4	6	4	5	5	4,8	0,012	2,462	0,006		
1.6	CBS Sistemlerinde, internete ve sistemlere başkasız giriş denemeleri loglanıyor mu?						9	7	6	8	9	7,8	0,020	4,000	0,015		
1.7	CBS Sistemlerinde, internete ve sistemlere başkasız giriş denemeleri raporlanıyor mu?						9	9	9	9	6	8,4	0,021	4,308	0,018		
1.8	CBS Sistemlerinde, kullanılan uzaktan erişimde güvenli bağlantı protokolleri kullanılıyor mu?						8	7	8	9	7	7,8	0,020	4,000	0,015		
1.9	CBS Sistemlerinde, kullanılan uzaktan bağlantı erişimleri için erişim kısıtları var mı?						9	9	7	7	6	7,6	0,019	3,897	0,015		
1.10	CBS Sistemlerinde, kullanılan uzaktan erişim için güvenli veri şifreleme yöntemi var mı?						5	6	5	6	5	5,4	0,014	2,769	0,007		
1.11	CBS Sistemlerinde, erişim yetkilendirmeleri ve kısıtlamaları belirlenerek bilgi paylaşımı yapılıyor mu?						6	9	8	9	9	8,2	0,021	4,205	0,017		
1.12	CBS Sistemlerinde, Rol Bazlı Erişim Kontrolü (RBAC) kullanımı erişim düzeylerini düzenlemek için roller, hiyerarşiler ve kısıtlamalar kullanılıyor mu?						7	7	9	7	7	7,4	0,019	3,795	0,014		
1.13	CBS Sistemlerinde, kurumsal ağa erişim sağlayan dış kaynakların veya sistemlerin listesi var mı?						8	9	8	9	9	8,6	0,022	4,410	0,019		
1.14	CBS Sistemlerinde, yetkilisi erişim yetkilerini talep etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapılıyor mu?						9	6	8	6	9	7,6	0,019	3,897	0,015		
1.15	CBS Sistemlerinde, farklı kaynaklar üzerinden elde edilen kullanıcı erişim iz kayıtları ile verinin toplanması ve ilişkilendirilmesi (korelasyon) yapılıyor mu?						9	9	9	6	9	8,4	0,021	4,308	0,018		
1.16	CBS Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?						9	7	5	6	9	7,2	0,018	3,692	0,013		
1.17	CBS Sistemlerinde, işletme dışı kişiler için kimlik tanımlama ve yetkilendirme yapılıyor mu?						6	6	9	6	6	6,6	0,017	3,385	0,011		
1.18	CBS Sistemlerinde, parola doğrulaması yapılıyor mu?						8	6	9	6	7	7,2	0,018	3,692	0,013		
1.19	CBS Sistemlerinde, parola belirleme ve kullanım kısıtları var mı?						9	9	8	9	9	8,8	0,022	4,513	0,020		
1.20	CBS Sistemlerinde, ayrıcalıklı hesapların yönetimi yapılıyor mu?						7	9	7	7	9	7,8	0,020	4,000	0,015		
1.21	CBS Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları tutuluyor mu?						7	9	9	9	9	8,6	0,022	4,410	0,019		
1.22	CBS Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?						7	8	9	7	9	8	0,020	4,103	0,016		
1.23	CBS Sistemlerinde, mobil iletişim sadece online iken merkez ile haberleşme sağlanıyor mu?						6	6	6	6	6	6	0,015	3,077	0,009		
1.24	CBS Sistemlerinde, belirlenen uygulamalarında dışında herhangi bir uygulama çalışıyor mu?						8	9	6	8	8	7,8	0,020	4,000	0,015		
1.25	CBS Sistemlerinde, mobil cihazlara uygulama yüklemeye yetkisi var mı?						10	9	6	6	6	7,4	0,019	3,795	0,014		
1.26	CBS Sistemlerinde, mobil cihazlara erişim yetkisi sınırlı mı?						5	7	9	7	6	6,8	0,017	3,487	0,012		
							195	201	195	192	192	195	0,497	100,000	0,378	76%	

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI' lar toplamı üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 76 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

CBS sistemi belirlenen KPI' lara ve soru setlerine göre değerlendirildi. Tüm KPI' lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi CBS sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 75' tir. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından CBS sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 75 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. CBS sistemlerinde kurumların tüm siber saldırı yöntemlerini dikkate alarak kurumun IT ve OT sistemlerini en yüksek seviyede korumaları

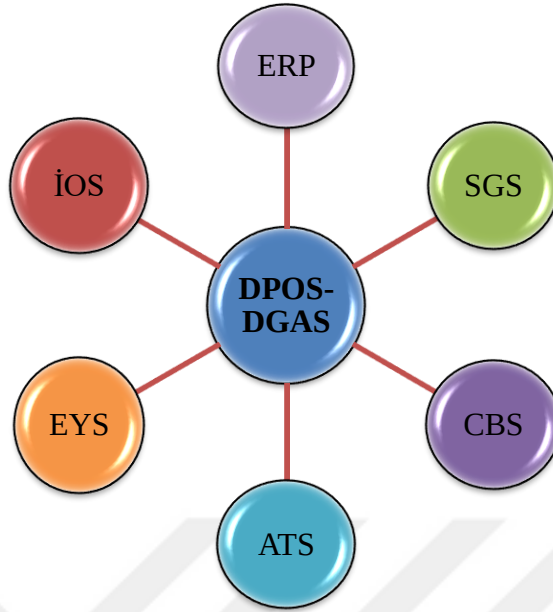
önem arz etmektedir. Özellikle enerji altyapılarına ve kurumlara en yaygın saldırılar olan Hizmet Kesintisi (DDoS), Zararlı Yazılımlar (Malware (Worm,Trojan, Rootkit, Virus)) ve Sahtecilik (Spoofing) (ARP,IP,GPS) ile ilgili saldırılar akıllı doğal gaz şebeklerine sahip enerji kurumları tarafından yaşanabilmektedir. Bu saldırıların engellenmesi için standartlara uyum, log yönetimi, yama yönetimi, ağ segamntasyon, sıkılaştırma, açık portların kapatılması, verilerin gizliliği, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

3.8.2. Akıllı Doğal Gaz Şebekesinde DPOS & DGAS

Dijital Proje Onaylama Sistemi (DPOS) ve Dijital Gaz Açma Sistemi (DGAS), otomasyon sistemlerinin bir bileşeni olarak doğal gaz dağıtım ağına önemli katkılar sağlamaktadır. DPOS-DGAS, doğal gaz yurt içi montaj projelerinin ve uygulamalarının kontrol ve onayını sağlar. Kurumun teknik şartnamesi, Doğal Gaz Standardı - projelerin prensipleri ve binalardaki tesislerin uygulamaları, mülk sahipliği ve Yangın Yönetmeliğine göre sertifikalı firmalar tarafından gönderilen projelerin ve uygulamaların kontrolü ve kabulü sağlanmaktadır. Doğal gaz dağıtımında DPOS & DGAS'ın tüm anahtar performans göstergeleri belirlenmiştir. DPOS & DGAS'ın akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.27' de sunulmuştur. DPOS & DGAS için mevzuat ve standartlar ışığında bu kriterler belirlenmiş ve seviyelerine göre sıralanmıştır.

3.8.2.1. DPOS & DGAS Sistemi İle Haberleşen Sistemler

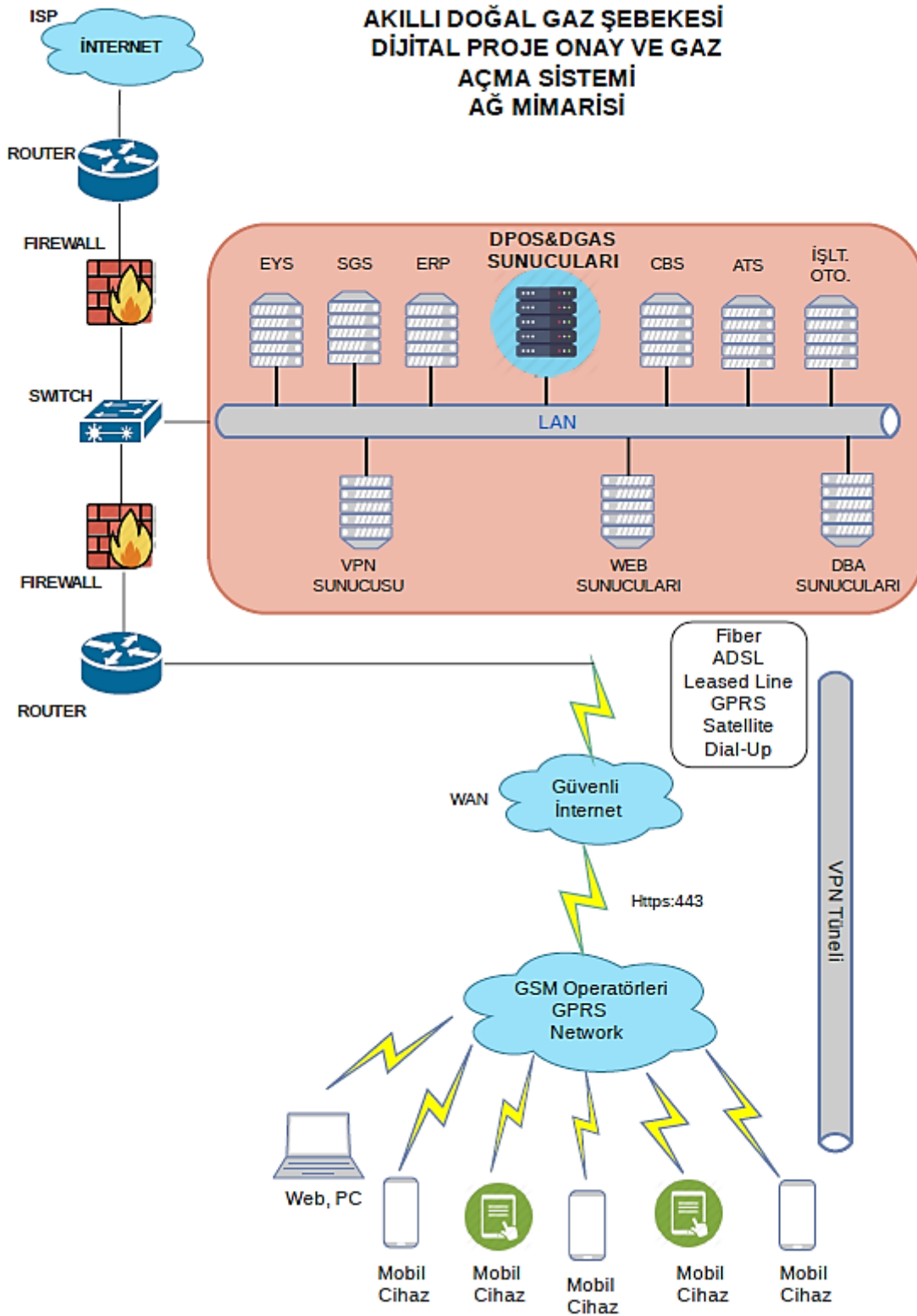
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde DPOS & DGAS sistemi akıllı şebekenin bir parçasıdır. DPOS & DGAS sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.60' da gösterilmiştir.



Şekil 3.60: DPOS & DGAS sistemi ile haberleşen sistemler.

3.8.2.2. DPOS & DGAS Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan DPOS & DGAS sistemi incelenerek mevcut ağ mimarisi Şekil 3.61’ de verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.61: DPOS & DGAS sistemi ağ mimarisi.

3.8.2.3. DPOS & DGAS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi DPOS & DGAS sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.27’ de verilmiştir. Bu KPI listesine göre kurumlardaki uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.27: DPOS & DGAS siber güvenlik olgunluk seviyesi ve KPI listesi.

Dijital Proje Onay ve Gaz Açma Sistemi (DPOS&DGAS) KPI Listesi										AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
DPOS&DGAS Özellikleri (MST SP-800, EPDK, CIS, COBIT, ISO 27001-27002-27015, KVKK, PCI DSS, ISA/IEC 62443-2009)										1,544	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
1	Erişim ve Kimlik Yönetimi																			
(Büyük işletmelerin devamlı fiziksel erişimi ve kullanıcıların işleri için devamlı erişim verimliliği ve reddedilmesi arasında; Bir BT sistemindeki kayıplara ilişkin verimliliğin de parti çalışması belirli bir ölçüde, işletmeler için geçerlidir. İşaretleri kullanılarak kontrolde bir kullanıcıya, işletme veya cihaz kontrolünü (uyumlanabilir) yapar.)																				
1.1	DPOS&DGAS Sistemlerinde, erişim kontrol yönetim politikası ve prosedürü bulunuyor mu?									9	8	9	8	9	8,6	0,067	4,313	0,057		
1.2	DPOS&DGAS Sistemlerinde, kullanıcı hesapları erişim politikası ve prosedürü bulunuyor mu?									7	9	7	8	7	7,6	0,059	3,811	0,045		
1.3	DPOS&DGAS Sistemlerinde, kullanıcı hesap yetkileri en azı yetiresimle göre yönetiliyor mu?									9	8	8	9	8	8,4	0,065	4,213	0,055		
1.4	DPOS&DGAS Sistemlerinde, sunuculara erişimden güvenli bağlantı protokolleri kullanılıyor mu?									7	8	7	9	8	7,8	0,060	4,012	0,050		
1.5	DPOS&DGAS Sistemlerinde, sunuculara erişimden güvenli veri alış verişinde güvenli kullunılıyor mu?									8	8	9	9	9	8,9	0,070	4,514	0,063		
1.6	DPOS&DGAS Sistemlerinde, internete ve sistemlere bağlanış giriş denemeleri loglanıyor mu?									9	7	6	8	9	7,8	0,060	3,912	0,047		
1.7	DPOS&DGAS Sistemlerinde, internete ve sistemlere bağlanış giriş denemeleri raporlanıyor mu?									9	9	9	9	6	8,4	0,065	4,213	0,055		
1.8	DPOS&DGAS Sistemlerinde, kullanılan uzaktan erişimde güvenli bağlantı protokolleri kullanılıyor mu?									8	7	8	9	7	7,8	0,060	3,912	0,047		
1.9	DPOS&DGAS Sistemlerinde, kullanıcılar uzaktan bağlantı erişimleri için erişim kuralları var mı?									9	9	7	7	6	7,6	0,059	3,811	0,045		
1.10	DPOS&DGAS Sistemlerinde, kullanıcılar uzaktan erişim için güvenli veri alış verişinde kullanılıyor mu?									9	9	9	9	9	9,0	0,070	4,514	0,063		
1.11	DPOS&DGAS Sistemlerinde, erişim yetkilendirmeleri ve kısıtlamaları birbirinebne bağlı yapılaşım yapıyorlar mu?									6	9	8	9	7	7,8	0,060	3,912	0,047		
1.12	DPOS&DGAS Sistemlerinde, Rol Bazlı Erişim Kontrolü (RBK) kullanıcılar erişim düzeylerini denetlemek için roller, hiyerarşiler ve kısıtlamalar kullanılıyor mu?									7	7	9	7	7	7,4	0,057	3,711	0,042		
1.13	DPOS&DGAS Sistemlerinde, kurumsall ağla erişim sağlayılan dış kaynaklara veya sistemlerin listesi var mı?									8	9	7	9	9	8,4	0,065	4,213	0,055		
1.14	DPOS&DGAS Sistemlerinde, yetkili erişim yetkilendirme tespit etmek ve raporlamak için spesifik sorumluluklara atanması ve tanımlanması yapıyorlar mu?									7	6	8	6	9	7,2	0,056	3,611	0,040		
1.15	DPOS&DGAS Sistemlerinde, farklı kaynaklar üzerinden elde edilen kullanıcılar için kayıtları ile verinin toplanması ve işiklendirilmesi (korelasyon) yapıyorlar mu?									9	7	7	7	9	7,6	0,059	3,811	0,045		
1.16	DPOS&DGAS Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?									7	7	5	6	9	6,8	0,053	3,410	0,036		
1.17	DPOS&DGAS Sistemlerinde, işletme dışı kişiler için kimlik tanımlama ve yetkilendirme yapıyorlar mu?									6	6	9	6	6	6,6	0,051	3,310	0,034		
1.18	DPOS&DGAS Sistemlerinde, parola doğrulama ve yetkilendirme yapıyorlar mu?									8	6	9	6	7	7,2	0,056	3,611	0,040		
1.19	DPOS&DGAS Sistemlerinde, parola belirleme ve kullanıcı kuralları var mı?									9	7	8	9	9	8,4	0,065	4,213	0,055		
1.20	DPOS&DGAS Sistemlerinde, ayrıcalıklı hesapların yönetimi yapıyorlar mu?									9	7	7	9	9	7,4	0,057	3,711	0,042		
1.21	DPOS&DGAS Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları bulunuyor mu?									7	7	7	7	7	7,0	0,054	3,511	0,038		
1.22	DPOS&DGAS Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları bulunuyor mu?									7	8	9	7	9	8	0,062	4,012	0,050		
1.23	DPOS&DGAS Sistemlerinde, mobil iletişim sadece online ileen merkez ile haberleşme sağlanıyor mu?									6	9	9	9	6	7,8	0,060	3,912	0,047		
1.24	DPOS&DGAS Sistemlerinde, belirlenen uygulamalarında dışında herhangi bir uygulama kullanılıyor mu?									8	9	6	8	8	7,8	0,060	3,912	0,047		
1.25	DPOS&DGAS Sistemlerinde, mobil cihazlara uygulama yükleme yetkisi var mı?									10	6	6	6	6	7,4	0,057	3,711	0,042		
1.26	DPOS&DGAS Sistemlerinde, mobil cihazlara erişim yetkisi sınırlı mı?									5	5	6	7	6	5,8	0,052	3,410	0,036		
										202	200	198	197	200	199,4	1,544	100,000	1,192	77%	

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI' lar toplamlar üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 77 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

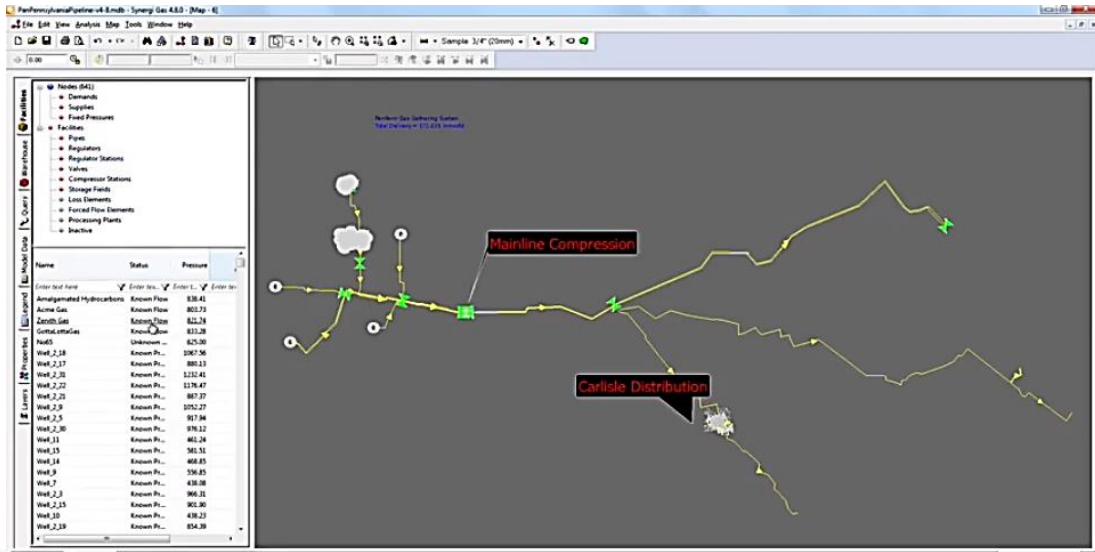
DPOS & DGAS sistemi belirlenen KPI' lara ve soru setlerine göre değerlendirildi. Tüm KPI' lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi DPOS & DGAS sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 79' dur. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından DPOS & DGAS sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 79 olarak belirlenmiştir. Belirlenen bu

oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. DPOS & DGAS sistemlerinde kurumların tüm siber saldırı yöntemlerini dikkate alarak kurumun IT ve OT sistemlerini en yüksek seviyede korumaları önem arz etmektedir. Özellikle enerji altyapılarına ve kurumlara en yaygın saldırılar olan Hizmet Kesintisi (DDoS), Zararlı Yazılımlar (Malware (Worm, Trojan, Rootkit, Virus)) ve Sahtecilik (Spoofing) (ARP, IP, GPS) ile ilgili saldırılar akıllı doğal gaz şebekelerine sahip enerji kurumları tarafından yaşanabilmektedir. Bu saldırıların engellenmesi için standartlara uyum, log yönetimi, yama yönetimi, ağ segmentasyonu, sıkılaştırma, açık portların kapatılması, verilerin gizliliği, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

3.8.3. Akıllı Doğal Gaz Şebekesinde Şebeke Yük Optimizasyon Sistemi (ŞYOS)

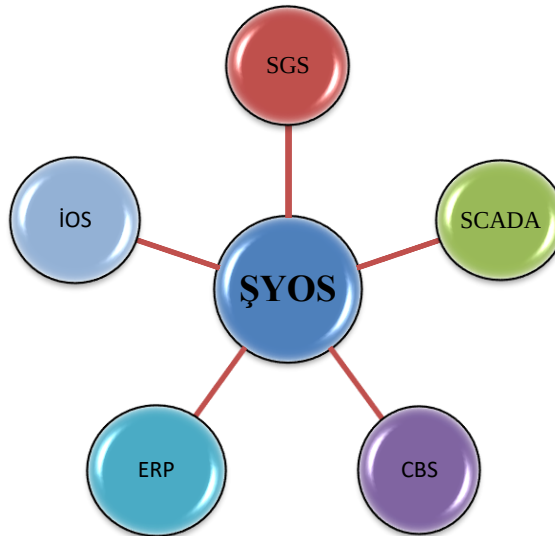
Modern şehirlerde hassas kritik altyapı tasarımı hayati bir öneme sahiptir. Bu açıdan, enerji iletim ve dağıtım şebekeleri, enerji arzının en önemli bileşenlerinin başında gelmektedir. Gaz dağıtım şirketlerinin en yaygın ortak değerlerinden ve hedeflerinden biri de kesintisiz gaz arzı sağlayacak uygun şebeke tasarımıdır. Şebeke simülasyonu, hesaplama programları ve yazılımları bu amaca hizmet etmektedir. Şebeke Yük Optimizasyon Sistemi, Şekil 3.62’ de gösterildiği gibi akıllı doğal gaz şebekelerinin bir bileşeni olarak akıllı doğal gaz dağıtım şebekesine önemli katkılar sağlamaktadır. Bu sistemin optimum şebeke tasarımı gibi birçok performans kriteri vardır. Akıllı doğal gaz şebekesinde Şebeke Yük Optimizasyon Sistemi için tüm ana performans göstergelerini tespit edilmiştir. Bu sisteme ilişkin mevzuat ve standartlar ışığında bu faktörlerin seviyeleri belirlenmiştir. Şebeke Yük Optimizasyon Sistemi’ nin akıllı doğal gaz şebekesi siber güvenlik açıklarının tespiti ve olgunluk modelinin geliştirilmesi açısından doğal gaz dağıtımındaki tüm anahtar performans göstergeleri Tablo 3.28’ de sunulmuştur.



Şekil 3.62: Örnek ŞYOS sistemi.

3.8.3.1. ŞYOS İle Haberleşen Sistemler

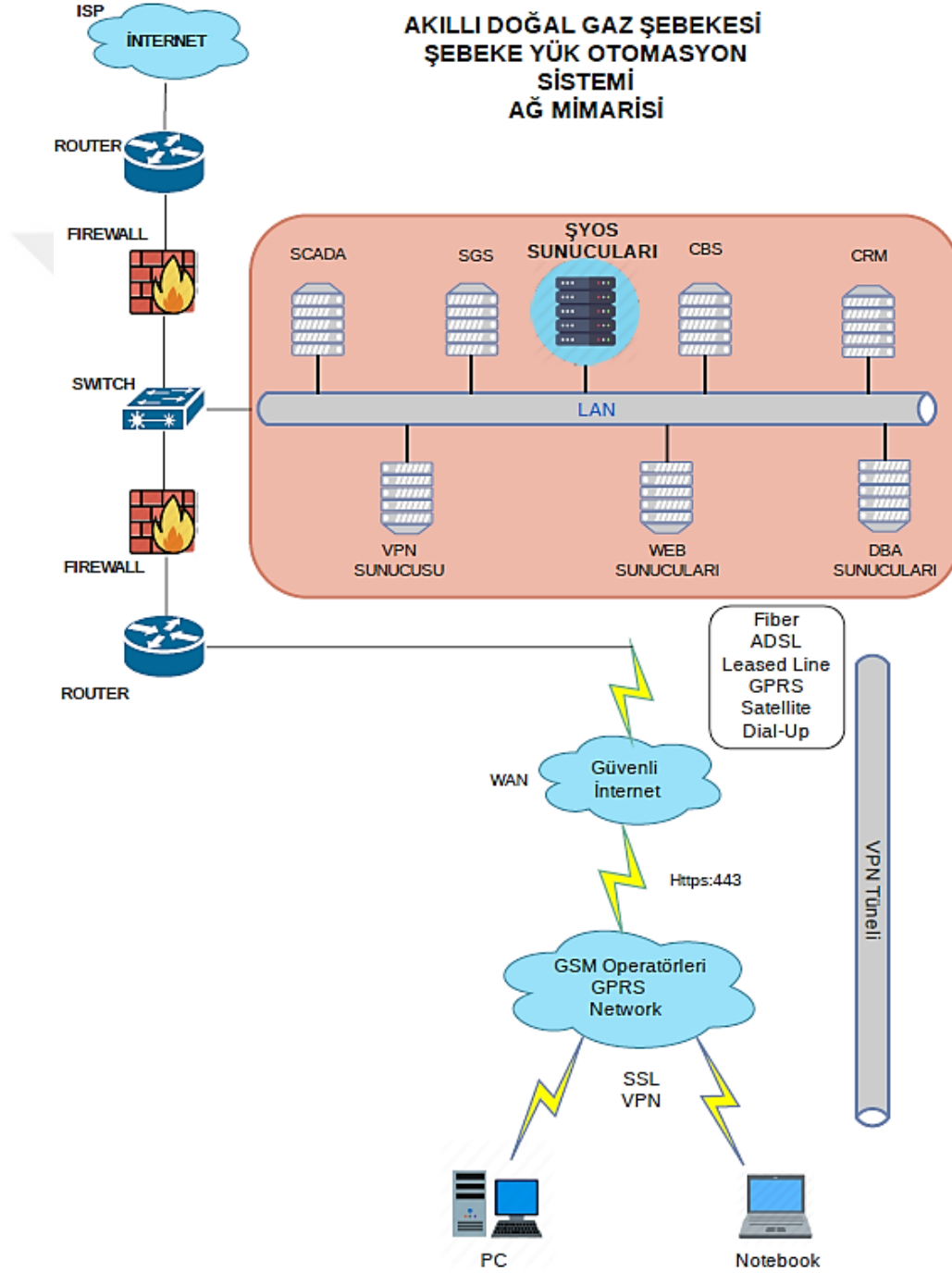
Akıllı doğal gaz şebekesi bileşen sistemleri incelendiğinde ŞYOS sistemi akıllı şebekenin bir parçasıdır. ŞYOS sistemi ile veri iletişim açısından haberleşme sağlayan tek yönlü veya çift yönlü olarak haberleşen sistemler aşağıdaki Şekil 3.63' de gösterilmiştir.



Şekil 3.63: ŞYOS sistemi ile haberleşen sistemler.

3.8.3.2. ŞYOS Sistemi Ağ Mimarisi

Akıllı doğal gaz şebekesi bileşeni olan ŞYOS sistemi incelenerek mevcut ağ mimarisi Şekil 3.64’ de verilmiştir. Aynı zamanda önerilen ağ mimarisi sistemi tüm kurumsal ağ ve operasyonel ağ için tezin sonunda verilecektir.



Şekil 3.64: ŞYOS sistemi ağ mimarisi.

3.8.3.3. ŞYOS Siber Güvenlik Olgunluk Seviyesi ve KPI Listesi

Akıllı doğal gaz şebekesi ŞYOS sistemi incelenerek oluşturulan siber güvenlik performans göstergelerinin KPI listesi Tablo 3.28’ de verilmiştir. Bu KPI listesine göre kurumlardaki uzman kişilerden AHP modelindeki puanlamaya göre karşılaştırmalar yapılarak siber güvenlik olgunluk seviyesi belirlenmektedir.

Tablo 3.28: ŞYOS siber güvenlik olgunluk seviyesi ve KPI listesi.

Şebeke Yük Otomasyon Sistemi (ŞYOS) KPI Listesi		AHP Önem Ağırlık Puanı	1.Uzman Puan (1-10)	2.Uzman Puan (1-10)	3.Uzman Puan (1-10)	4.Uzman Puan (1-10)	5.Uzman Puan (1-10)	Uzman Puan Ort.	Normalize Edilmiş Önem Ağırlık	Önem Ağırlık Yüzdesi (%)	Puana Göre Norm. Önem Ağırlık	Olgunluk Seviyesi (%)
ŞYOS Özellikleri (NIST SP-800, EPDM, CIS, COBIT, ISO/IEC 27001-27002-27019, KVKK, PCI DSS, ISA/IEC 62443:2009)		0,339	U.1	U.2	U.3	U.4	U.5	U.Ort.		%		%
1	Erişim ve Kimlik Yönetimi											
(Bilgi sistemi ortamındaki alanlara fiziksel erişim veya bilgilerin edinilmesi ve kullanılması için özel izinlere cevap verilmesi veya reddedilmesi sürecidir. Bir BT sistemindeki kaynaklara erişim izni verilmemesi de part olarak belirlenir. Kimlik bilgileri (örn. parolalar, şifreler) kullanmak amacıyla bir kullanıcıya, kimliği veya cihazı tanımlama (sancısıdır).)												
1.1	ŞYOS Sistemlerinde, erişim kontrol yönetim politikası ve prosedürü bulunuyor mu?	9	8	9	8	9	8,6	0,014	4,203	0,012		
1.2	ŞYOS Sistemlerinde, kullanıcı hesapları yönetim politikası ve prosedürü bulunuyor mu?	7	9	7	8	7	7,6	0,013	3,715	0,010		
1.3	ŞYOS Sistemlerinde, kullanıcı hesap yetkileri en az yetki prensibine göre yönetiliyor mu?	9	7	8	9	8	8,2	0,014	4,008	0,011		
1.4	ŞYOS Sistemlerinde, sunuculara erişimde güvenli bağlantı protokolleri kullanılıyor mu?	7	8	7	9	9	8	0,013	3,910	0,011		
1.5	ŞYOS Sistemlerinde, sunuculara erişim güvenli veri şifreleme yöntemi kullanılıyor mu?	9	9	9	9	9	9	0,015	4,399	0,013		
1.6	ŞYOS Sistemlerinde, internete ve sistemlere başarısız giriş denemeleri loglanıyor mu?	9	7	6	8	9	7,8	0,013	3,812	0,010		
1.7	ŞYOS Sistemlerinde, internete ve sistemlere başarısız giriş denemeleri raporlanıyor mu?	9	9	9	9	6	8,4	0,014	4,106	0,012		
1.8	ŞYOS Sistemlerinde, kullanılan uzaktan erişimde güvenli bağlantı protokolleri kullanılıyor mu?	8	7	8	9	7	7,8	0,013	3,812	0,010		
1.9	ŞYOS Sistemlerinde, kullanılan uzaktan bağlantı erişimleri için erişim kısıtları var mı?	9	9	7	7	6	7,6	0,013	3,715	0,010		
1.10	ŞYOS Sistemlerinde, kullanılan uzaktan erişim için güvenli veri şifreleme yöntemi var mı?	9	6	5	6	9	7	0,012	3,421	0,008		
1.11	ŞYOS Sistemlerinde, erişim yetkilendirmeleri ve kısıtlamaları belirtenler için bilgi paylaşımı yapılıyor mu?	6	9	8	9	9	8,2	0,014	4,008	0,011		
1.12	ŞYOS Sistemlerinde, Rol Bazlı Erişim Kontrolü (RBK) kullanıcı erişim düzeylerini düzenlemek için roller, hiyerarşiler ve kısıtlamalar kullanılıyor mu?	7	7	9	7	7	7,4	0,012	3,617	0,009		
1.13	ŞYOS Sistemlerinde, kurumsal ağa erişim sağlayan dış kaynakların veya sistemlerin listesi var mı?	8	9	8	9	9	8,6	0,014	4,203	0,012		
1.14	ŞYOS Sistemlerinde, yetkisiz erişim eylemlerini tespit etmek ve raporlamak için spesifik sorumlulukların atanması ve tanımlanması yapılıyor mu?	9	6	8	6	9	7,6	0,013	3,715	0,010		
1.15	ŞYOS Sistemlerinde, farklı kaynaklar üzerinden elde edilen kullanıcı erişim izni kayıtları ile verinin toplanması ve ilişkilendirilmesi (korelasyonu) yapılıyor mu?	9	9	9	6	9	8,4	0,014	4,106	0,012		
1.16	ŞYOS Sistemlerinde, tanımlama ve kimlik doğrulama sistemi kullanılıyor mu?	9	7	5	6	9	7,2	0,012	3,519	0,009		
1.17	ŞYOS Sistemlerinde, işletme dışı kişiler için kimlik tanımlama ve yetkilendirme yapılıyor mu?	6	6	9	6	6	6,6	0,011	3,226	0,007		
1.18	ŞYOS Sistemlerinde, parola doğrulaması yapılıyor mu?	8	6	9	6	7	7,2	0,012	3,519	0,009		
1.19	ŞYOS Sistemlerinde, parola belirleme ve kullanım kuralları var mı?	9	9	8	9	9	8,8	0,015	4,301	0,013		
1.20	ŞYOS Sistemlerinde, ayrıcalıklı hesapların yönetimi yapılıyor mu?	7	9	9	7	9	8,2	0,014	4,008	0,011		
1.21	ŞYOS Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları tutuluyor mu?	7	9	9	9	9	8,6	0,014	4,203	0,012		
1.22	ŞYOS Sistemlerinde, uygulama üzerinde yapılan işlemlerin logları belirlenen sürelerde saklanıyor mu?	7	8	9	7	9	8	0,013	3,910	0,011		
1.23	ŞYOS Sistemlerinde, mobil iletişim sadece online ilemi merkez ile haberleşme sağlanıyor mu?	6	9	9	9	6	7,8	0,013	3,812	0,010		
1.24	ŞYOS Sistemlerinde, belirlenen uygulamalarda dışarda herhangi bir uygulama çalışıyor mu?	8	9	6	8	8	7,8	0,013	3,812	0,010		
1.25	ŞYOS Sistemlerinde, mobil cihazlara uygulama yüklemeye yetkisi var mı?	10	9	6	6	6	7,4	0,012	3,617	0,009		
1.26	ŞYOS Sistemlerinde, mobil cihazlara erişim yetkisi sınırlı mı?	5	7	9	7	6	6,8	0,011	3,324	0,008		
		206	207	205	199	206	204,6	0,339	100,000	0,268	79%	

Örnek tabloda görüldüğü gibi belirlenen bir KPI üzerinde oluşturulmuş soru setlerinden 1 ile 10 arasında bir puanlama yapılarak her bir maddenin AHP yöntemi ile alınan değere karşı kaç puan aldığı belirlenmiştir. Bu sonuç ile belirlenen KPI’ lar toplamı üzerinden siber güvenlik açısından olgunluk seviyesi yüzde olarak hesaplanmıştır. Örnekte olduğu gibi Erişim ve Kimlik Yönetimi KPI bileşeni % 79 olarak hesaplanmıştır. Görüş alınan uzman sayısı 5 adettir ve dolayısı ile uzman sayısı arttıkça verilen doğruluğu o oranda artmaktadır.

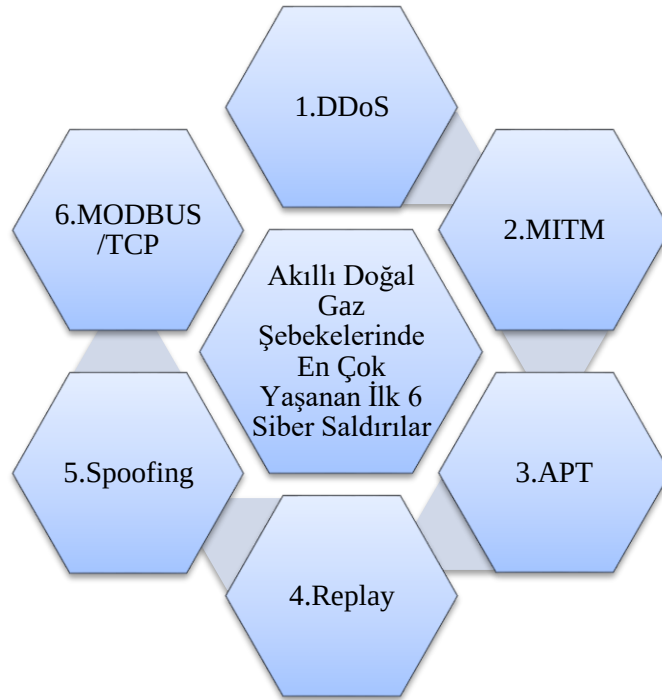
ŞYOS sistemi belirlenen KPI’ lara ve soru setlerine göre değerlendirildi. Tüm KPI’ lar uzman görüşü alınarak AHP yöntemi ile hesaplandı. Akıllı doğal gaz şebekesi ŞYOS sisteminin olgunluk seviyesi KURUM-A için % 100 puan üzerinden % 79’ dur. Bazı iyileştirilebilir alanlar mevcuttur. Bunlar KPI listesinin Farkındalık ve Eğitim, Güvenlik Değerlendirilmesi/Yetkilendirme ve Erişim/Kimlik Yönetimi olmak üzere bu alanlarda iyileştirmeler yapılmalıdır.

Akıllı doğal gaz şebekeleri açısından ŞYOS sistemleri siber güvenlik olgunluk seviyesi açısından incelendiğinde olgunluk seviyesi % 79 olarak belirlenmiştir. Belirlenen bu oran olgunluk seviyesi açısından yüksek olduğu görülmektedir. Eksik yönlerine odaklanıldığında bu

oranın daha yüksek seviyelerde olması sağlanabilir. Bu modelle ile kurumlar siber güvenlik açısından eksik yönlerini tespit etmeleri kolaylaşır. ŞYOS sistemlerinde kurumların tüm siber saldırı yöntemlerini dikkate alarak kurumun IT ve OT sistemlerini en yüksek seviyede korumaları önem arz etmektedir. Özellikle enerji altyapılarına ve kurumlara en yaygın saldırılar olan Hizmet Kesintisi (DDoS), Zararlı Yazılımlar (Malware (Worm, Trojan, Rootkit, Virus)) ve Sahtecilik (Spoofing) (ARP, IP, GPS) ile ilgili saldırılar akıllı doğal gaz şebekelerine sahip enerji kurumları tarafından yaşanabilmektedir. Bu saldırıların engellenmesi için standartlara uyum, log yönetimi, yama yönetimi, ağ segmentasyonu, sıkılaştırma, açık portların kapatılması, verilerin gizliliği, hizmet kesintilerin önlenmesi için güvenli haberleşme sistemlerinin kullanılması, güvenli veri iletişim protokolü kullanmak ve donanım/yazılımların güvenlik testlerinin yapılması önemlidir.

3.9. AKILLI DOĞAL GAZ ŞEBEKELERİNDE EN SIK YAŞANAN SİBER SALDIRI YÖNTEMLERİ

Akıllı doğal gaz şebekelerinde yaşanan siber saldırı yöntemleri incelendiğinde aşağıdaki Şekil 3.65’ de gösterildiği gibi ilk 6 siber saldırı yöntemleri görülmektedir.



Şekil 3.65: Akıllı doğal gaz şebekelerinde en sık yaşanan ilk 6 siber saldırı yöntemleri.

Aşağıdaki Tablo 3.29’ da akademik çalışmalar incelenerek akıllı doğal gaz şebekelerinde yaşanan ve yaşanabilecek tüm siber saldırılar liste olarak verilmiştir. Bu saldırılar aynı zamanda diğer enerji ve kritik altyapı sistemlerine saldırı olarak yapıldığı görülmektedir.

Tablo 3.29: Akıllı doğal gaz şebekelerinde en sık yaşanan siber saldırı yöntemleri.

	Akıllı Doğal Gaz Şebekelerinde En sık Yaşanan Siber Saldırı Yöntemleri
1	Hizmet Kesintisi (DDoS)
2	Araya Girme Saldırısı (MITM)
3	Zararlı Yazılım (APT-Malware (Worm,Trojan, Rootkit, Virus))
4	Replay Saldırısı
5	Sahtecilik (Spoofing) (ARP,IP,GPS)
6	MODBUS/TCP Protocol Attack
7	DNP3 Protocol Attack
8	Malicious Software Injections
9	Malicious Command Injection
10	Buffer Overflow
11	Sosyal Mühendislik
12	Fiziksel Saldırı (Sensör, Actuator, Kamera)
13	SQL Injection
14	Zero Day Attack
15	Phishing (Oltalama)
16	Unauthorized Access Activities
17	Insider-Outsider Attacks
18	Ağ Trafiği Anomalisi
19	Arka Kapılar (Back Doors)
20	Keşif Saldırıları (Reconnaissance Attacks)
21	Ağ Dinleme (Sniffing)
22	Kriptografik (Cryptographic) Saldırısı
23	Process Network Malware Injection
24	Sömürmek (Exploit)
25	Gereksiz Port ve Servisleri Tarama
26	PROFIBUS Protocol Attack
27	Firmware Modification Attack
28	Cross-Site Scripting (XSS)
29	False Data Injection
30	Zehirlleme (Poisoning) (ARP, DNS)
31	Mantık Bombası (Logic Bombs)
32	Casus Yazılım (Spyware)
33	Eavesdropping
34	Response and Measurement Injection
35	Fidye Saldırısı (Ransomware)
36	Çerçeve (Fragmentation) Saldırısı
37	IEC 61850 Protocol Attack

38	Yanlış Alarm Üretilmesi
39	Kaydediciler (Keyloggers)
40	Fraud Attack
41	Reverse-Engineering Attack
42	Kimlik İhlali
43	Default Konfigürasyon
44	RFC Pivoting Attack
45	Köle Bilgisayarlar (Botnets)



4. BULGULAR

4.1. AKILLI DOĞAL GAZ ŞEBEKESİ SİBER GÜVENLİK OLGUNLUK MODELİ ÖNEM AĞIRLIK SONUÇLARI

4.1.1.KURUM-A Ana Bileşenlerin Önem Ağırlık Sonuçları

KURUM-A özelinde yapılan akıllı doğal gaz şebekesi siber güvenlik açıklarının araştırılmasında sistemin ana bileşenlerinin sonuçları aşağıdaki gibidir. Akıllı doğal gaz şebekelerinin 6 ana bileşende incelenmiştir. Bu belirtilen ana bileşenler akıllı şebekelerin temelini oluşturmaktadır. Uzman görüşleri 5 farklı uzmandan alınarak AHP yöntemi ile ikili karşılaştırmalar yapılarak hesaplamalar yapıldı. Uzmanlar seçilirken çalışma tecrübesi olarak 5-15 yıllık olanlardan seçilmiştir.

Tablo 4.1: KURUM-A Ana bileşenlerin önem ağırlıkları.

	Ana Bileşenler	Uzman 1	Uzman 2	Uzman 3	Uzman 4	Uzman 5	Önem Ağırlık Ort. (%)
1	Akış Yönetimi	36,766	34,613	29,237	31,466	30,623	32,541
2	Veri Yönetimi	20,401	19,722	25,479	23,222	24,239	22,613
3	İşgücü Yönetimi	8,002	10,613	9,453	9,653	10,157	9,576
4	Boru Hattı Büt. Yönetimi	11,770	12,424	9,456	9,456	8,865	10,394
5	Afet Yönetimi	14,197	13,112	15,999	16,653	16,101	15,212
6	Tesisat Yönetimi	8,864	9,517	10,376	9,550	10,015	9,664
	Toplam	100,000	100,000	100,000	100,000	100,000	100,000

AHP metoduna göre yapılan bu hesaplamalar uzman görüşleri alınarak ikili karşılaştırmalar yapılmıştır. Akıllı doğal gaz şebekelerinde akış yönetim % 32, 541 olarak en yüksek hesaplanan ana bileşendir. Bu ana bileşen altında bulunan tüm sistemler siber güvenlik açısından daha önemlidir. Bu sisitemlerin siber saldırılara karşı korunması gerekmektedir.

4.1.2. KURUM-A Alt Bileşenlerin Önem Ağırlık Sonuçları

Akıllı doğal gaz şebekesi 18 adet ana alt bileşenden oluşmaktadır. Bu sistemler kurum bazlı olarak değişmektedir. 5 farklı uzmandan alınan sonuçlar aşağıdaki gibidir. Buradaki sonuçlar AHP yöntemi ile siber güvenlik açısından sistemlerin önem ağırlıkları hesaplanmıştır. Sonuçlar incelendiğinde SCADA sistemi % 20,250 puanla önem ağırlığı en yüksek alt bileşendir. SGS siber güvenlik sistemi ise % 17,209 puanla ikinci en önemli sistem olarak tespit edilmiştir.

Tablo 4.2: KURUM-A alt bileşenlerin önem ağırlıkları.

	Alt Bileşenler	Uzman 1	Uzman 2	Uzman 3	Uzman 4	Uzman 5	Önem Ağırlık Ort. (%)
1	SCADA	22,497	18,877	20,763	19,766	19,345	20,250
2	Elektronik Bülten Tablosu (EBT)	8,678	9,001	4,457	5,666	6,011	6,763
3	Ölçme ve Raporlama Sistemi (AVE-ÖRS)	4,340	4,005	3,000	2,989	3,233	3,513
4	Otomatik Sayaç Okuma Sistemi (AMI/AMR)	1,250	2,731	1,016	3,045	2,034	2,015
5	Kurumsal Kaynak Planlama (ERP)	2,846	2,006	3,898	3,888	3,001	3,128
6	Müşteri İlişkileri Yönetimi (CRM)	1,361	1,866	2,909	2,678	2,566	2,276
7	Siber Güvenlik Sistemi (SGS)	16,194	15,851	18,672	16,656	18,672	17,209
8	İşletme Otomasyon Sistemi (İOS)	5,761	4,988	6,005	5,998	6,158	5,782
9	Araç Takip Sistemi (ATS)	1,501	1,909	2,003	1,878	1,999	1,858
10	Enerji Yönetim Sistemi (EYS)	0,740	3,716	1,445	1,777	2,000	1,936
11	Boru İçi Denetleme Robotu (BİDR)	1,070	2,045	1,642	1,642	1,642	1,608
12	Boru Hattı Risk Değerlendirme Sistemi (BHRYs)	1,070	1,325	1,899	1,899	1,545	1,548
13	Katodik Koruma Sistemi (KKS)	9,630	9,054	5,915	5,915	5,678	7,238
14	İhbar Yönetim Sistemi (İYS)	10,647	9,346	11,876	11,876	10,978	10,944
15	Deprem Risk Azaltım Sistemi (DRAS-SI)	3,549	3,766	4,123	4,777	5,123	4,268
16	Coğrafi Bilgi Sistemi (CBS)	1,543	1,890	2,567	2,023	1,990	2,003
17	Şebeke Yük Optimiz. Sistemi (ŞYOS)	0,523	2,004	1,568	1,678	2,455	1,646
18	Dijital Proje ve Gaz Açma Sistemi (DPOS&DGAS)	6,797	5,622	6,242	5,849	5,570	6,016
	Toplam	100,000	100,000	100,000	100,000	100,000	100,000

4.1.3. KURUM-A KPI Parametrelerinin Önem Ağırlık Sonuçları

Akıllı doğal gaz şebekelerinde geliştirilen siber güvenlik olgunluk modelinde dağıtım şebekelerine ve kullanılan sistemlere göre KPI parametre sayıları değişiklik gösterir. İnceleme yapılan kurumda 19 adet KPI parametresi tespit edilmiştir. Bu parametreler artma ve azalma yönünde farklılık gösterebilir. KPI parametreleri olgunluk modelimiz için belirlemiş olduğumuz parametrelerdir. Model içerisinde bu parametreler kullandı ve bu parametrelere ait yaklaşık 3500 adet soru seti bulunmaktadır. KURUM-A açısından AHP yöntemi ile hesaplama sonucunda KPI01 % 18,060 puanla en yüksek öneme sahiptir.

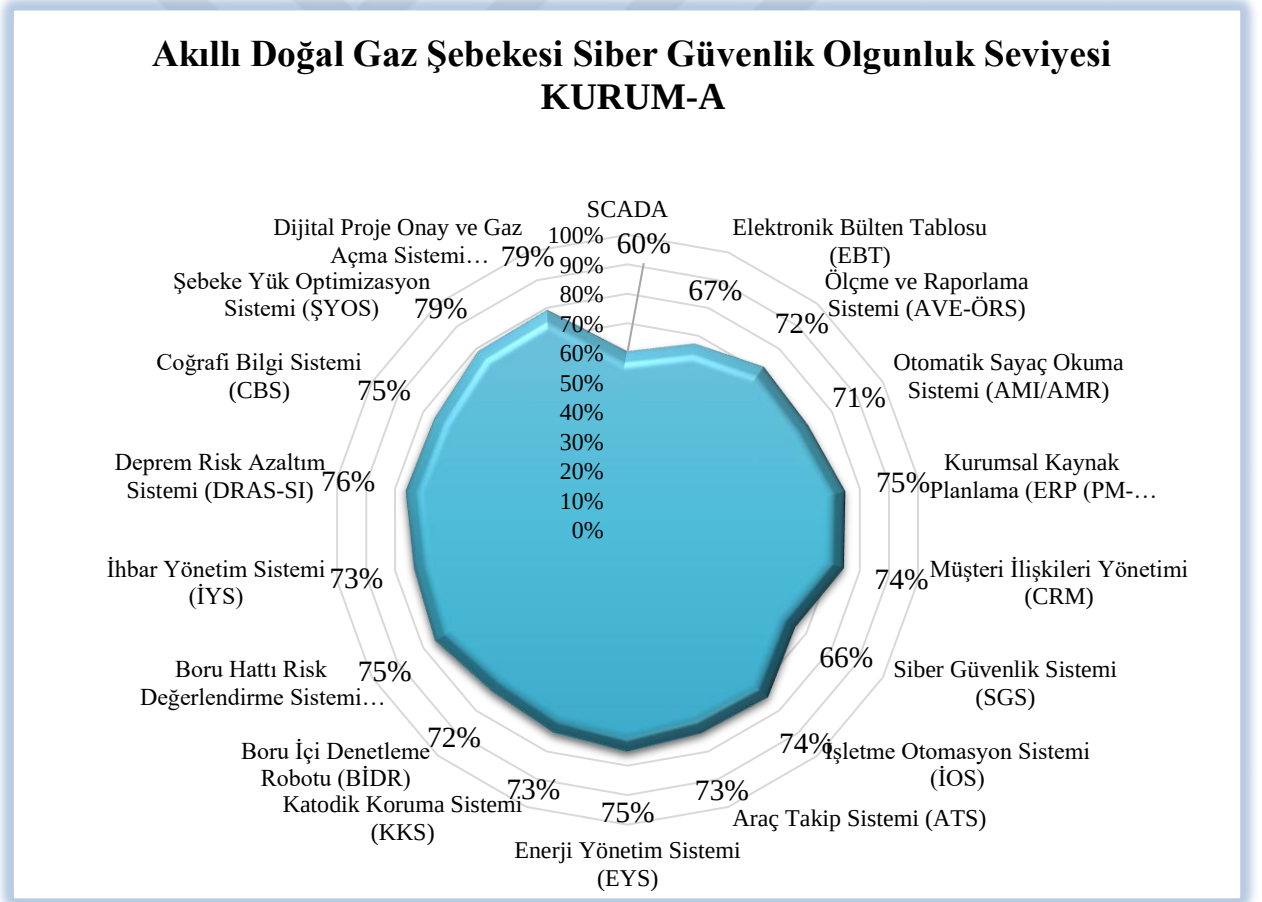
Tablo 4.3: KURUM-A KPI parametrelerinin önem ağırlıkları.

No	KPI	Ortalama	AHP Normalize Edilmiş Toplamlar	AHP Normalize Edilmiş Önem Değerleri (%)
1	KP01	22,279	3,431	18,060
2	KP02	15,836	2,439	12,837
3	KP03	9,846	1,516	7,982
4	KP04	6,964	1,073	5,645
5	KP05	8,318	1,281	6,743
6	KP06	8,007	1,233	6,491
7	KP07	2,558	1,292	6,799
8	KP08	4,058	0,625	3,290
9	KP09	1,466	0,740	3,897
10	KP10	2,355	1,189	6,260
11	KP11	1,428	0,721	3,796
12	KP12	1,122	0,567	2,983
13	KP13	3,629	0,559	2,941
14	KP14	1,953	0,301	1,583
15	KP15	2,621	0,404	2,125
16	KP16	4,957	0,764	4,019
17	KP17	1,280	0,197	1,038
18	KP18	0,457	0,231	1,214
19	KP19	0,864	0,436	2,297
	Toplam	100	19,000	100

4.2. İNCELENEN KURUMLARIN AKILLI DOĞAL GAZ ŞEBEKELERİ SİBER GÜVENLİK OLGUNLUK SEVİYELERİ

4.2.1.KURUM-A Siber Güvenlik Olgunluk Seviyesi

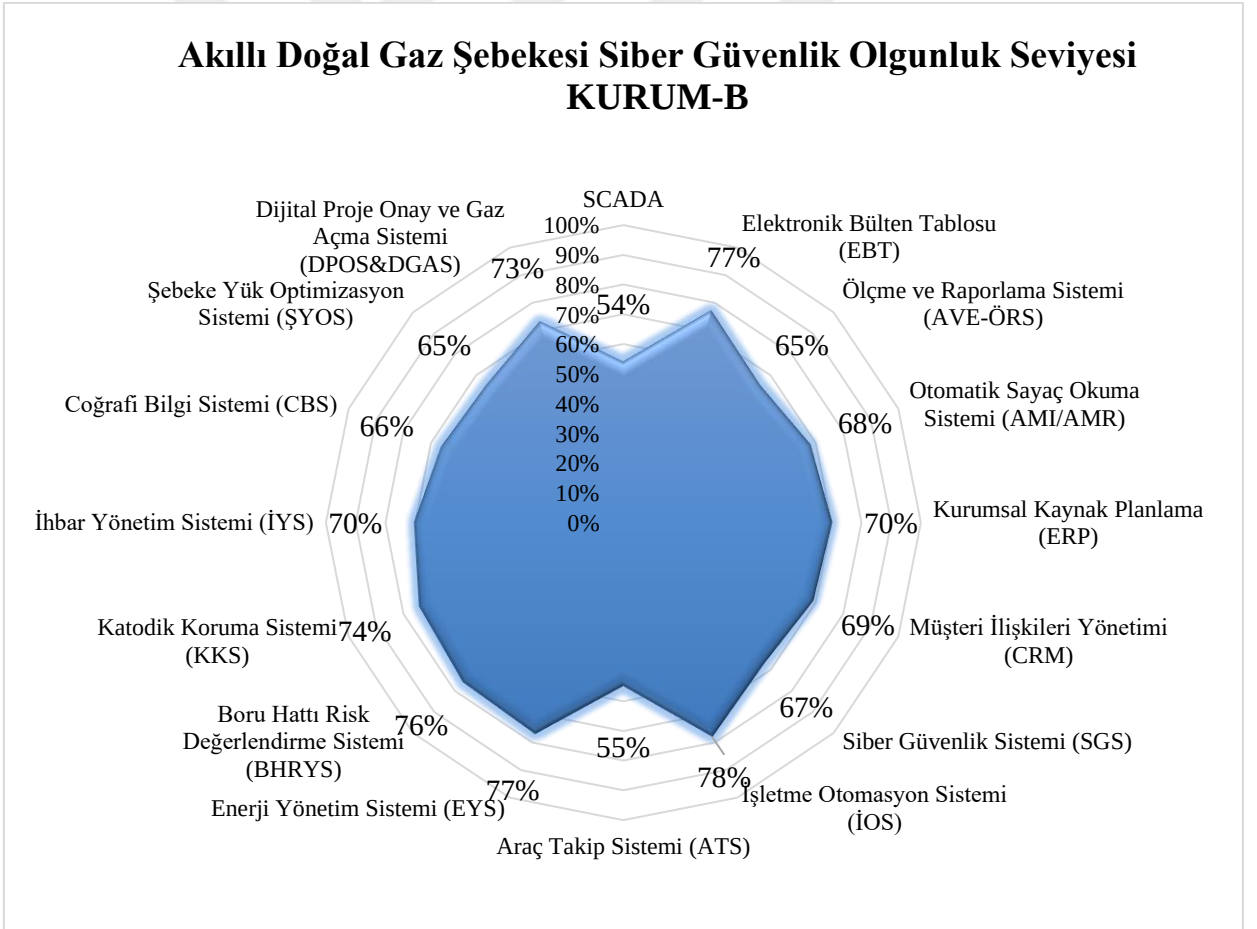
KURUM-A incelendiğinde akıllı doğal gaz şebekelerinin siber güvenlik açısından olgunluk modeli aşağıdaki gibidir. KURUM-A için yapılan ölçüm çalışmasında siber güvenlik olgunluk seviyesi % 72 olarak hesaplanmıştır. Olgunluk seviyeleri ölçüm sonuçları incelendiğinde en düşük olgunluk seviyesi % 60 ile SCADA sisteminin olgunluk seviyesidir. SCADA açısından siber güvenlik soru setleri üzerinden oluşturulan KPI değerleri yeniden incelenerek zayıf alanlarda kurum tarafından iyileştirmeler yapılmalıdır. Ayrıca ölçüm sonucunda alt bileşenler arasında yapılan ölçümlerde SGS sistemi % 66 ve EBT sistemi ise % 67 olarak hesaplanmıştır.



Şekil 4.1: KURUM-A Akıllı doğal gaz şebekesi siber güvenlik olgunluk seviyesi.

4.2.2. KURUM-B Siber Güvenlik Olgunluk Seviyesi

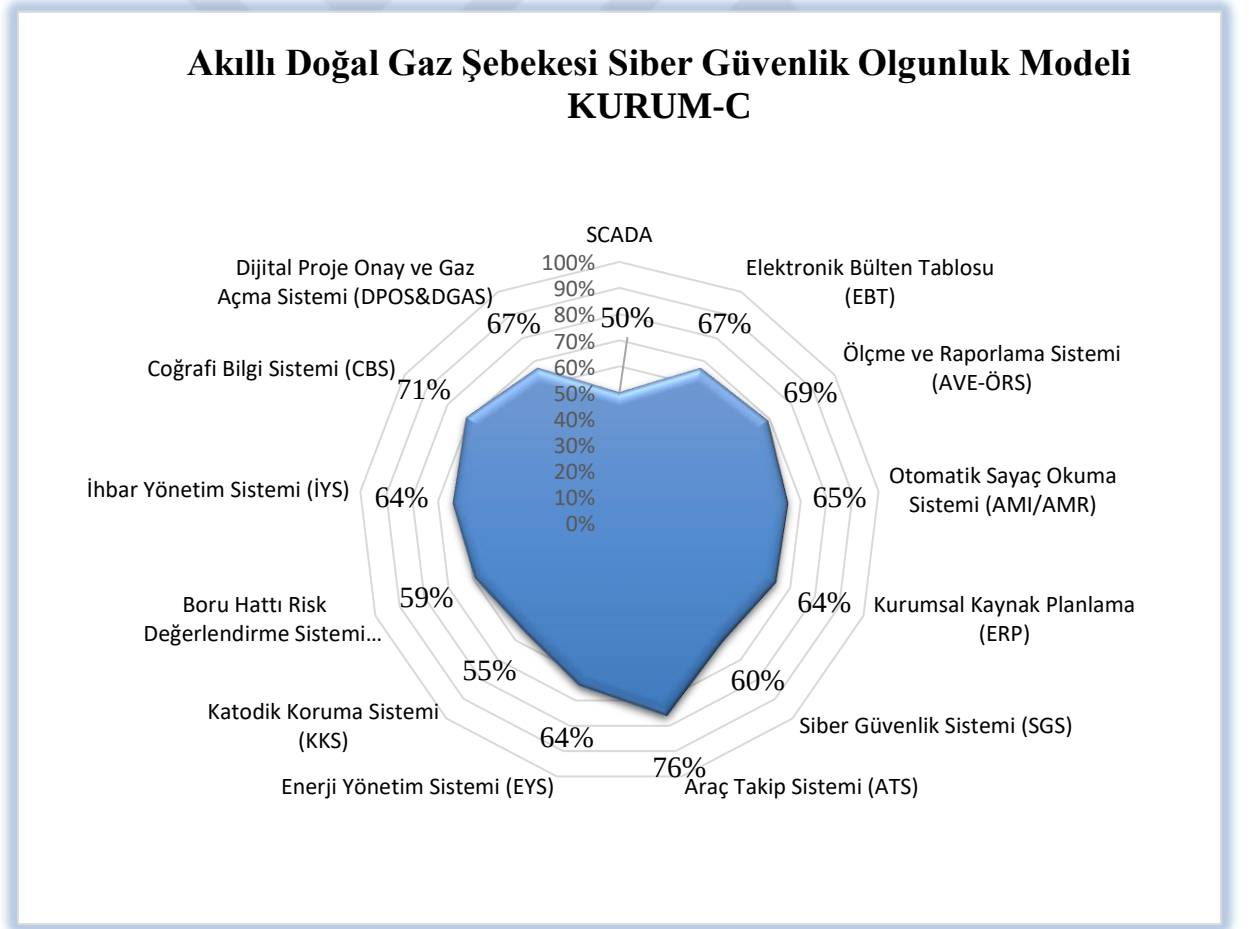
KURUM-B özelinde yapılan olgunluk seviyesi ölçüm çalışmasında akıllı doğal gaz şebekesi alt bileşenlerinden BİDR ve DRAS-SI sistemlerinin bulunmadığı gözlemlenmiştir. Bu sistemlerin olmaması riski ortadan kaldırdığından olgunluk modeli açısından kurumların siber güvenlik olgunluk seviyelerinin ölçülmesini etkilememektedir. KURUM-B için yapılan ölçüm çalışmasında siber güvenlik olgunluk seviyesi % 69 olarak hesaplanmıştır. Olgunluk seviyeleri ölçüm sonuçları incelendiğinde en düşük olgunluk seviyesi % 54 ile SCADA sisteminin olgunluk seviyesidir. SCADA açısından siber güvenlik soru setleri üzerinden oluşturulan KPI değerleri yeniden incelenerek zayıf alanlarda kurum tarafından iyileştirmeler yapılmalıdır. Ayrıca ölçüm sonucunda alt bileşenler arasında yapılan ölçümde ATS sistemi % 55 ve AVE sistemi ise % 65 olarak hesaplanmıştır.



Şekil 4.2: KURUM-B Akıllı doğal gaz şebekesi siber güvenlik olgunluk seviyesi.

4.2.3. KURUM-C Siber Güvenlik Olgunluk Seviyesi

KURUM-C özelinde yapılan olgun seviyesi ölçüm çalışmasında akıllı doğal gaz şebekesi alt bileşenlerinden CRM, İOS, BİDR, DRAS-SI ve ŞYOS sistemlerinin bulunmadığı gözlemlenmiştir. Bu sistemlerin olmaması riski ortadan kaldırdığından olgunluk modeli açısından kurumların siber güvenlik olgunluk seviyelerinin ölçülmesini etkilememektedir. KURUM-C için yapılan ölçüm çalışmasında siber güvenlik olgunluk seviyesi % 64 olarak hesaplanmıştır. Olgunluk seviyeleri ölçüm sonuçları incelendiğinde en düşük olgunluk seviyesi % 50 ile SCADA sisteminin olgunluk seviyesidir. SCADA açısından siber güvenlik soru setleri üzerinden oluşturulan KPI değerleri yeniden incelenerek zayıf alanlarda kurum tarafından iyileştirmeler yapılmalıdır. Ayrıca ölçüm sonucunda alt bileşenler arasında yapılan ölçümlerde KKS sistemi % 55 ve BHRYIS sistemi ise % 59 olarak hesaplanmıştır.



Şekil 4.3: KURUM-C Akıllı doğal gaz şebekesi siber güvenlik olgunluk seviyesi.

4.3. İNCELENEN KURUMLARIN SİBER GÜVENLİK AÇISINDAN OLGUNLUK SEVİYELERİNİN KARŞILAŞTIRILMASI

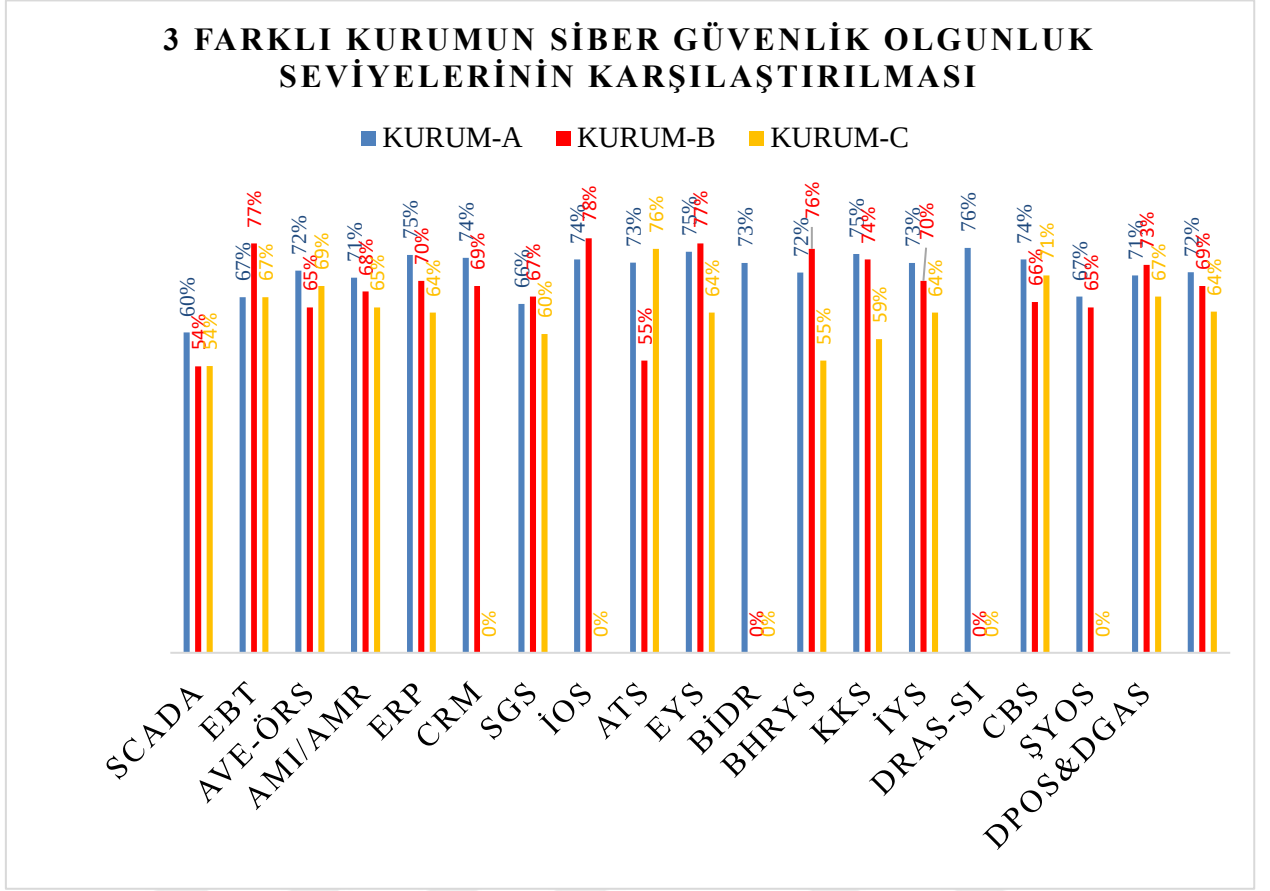
Aşağıdaki Tablo 5.4’ de bakıldığında KURUM-A tüm akıllı doğal gaz bileşenlerine sahip iken KURUM-B’ de BİDR ve DRAS-SI alt bileşenlerine, KURUM-C’ de ise CRM, İOS, BİDR, DRAS-SI ve ŞYOS alt bileşenlerine sahip değildir. Tüm bileşenler incelendiğinde olgunluk seviyesi SCADA sistemine ait olgunluk seviyesi en düşük olduğu tespit edilmiştir.

Tablo 4.4: 3 farklı kurumun akıllı doğal gaz alt bileşenlerinin olgunluk seviyelerinin karşılaştırılması.

	Ana Bileşenler		Alt Bileşenler	KURUM A	KURUM B	KURUM C
1	Akış Yönetimi	1	SCADA	60%	54%	50%
		2	EBT	67%	77%	67%
		3	AVE-ÖRS	72%	65%	69%
		4	AMI/AMR	71%	68%	65%
2	Veri Yönetimi	1	ERP	75%	70%	64%
		2	CRM	74%	69%	X
		3	SGS	66%	67%	60%
3	İşgücü Yönetimi	1	İOS	74%	78%	X
		2	ATS	73%	55%	76%
		3	EYS	75%	77%	64%
4	Boru Hattı Büt. Yönetimi	1	BİDR	73%	X	X
		2	BHRYS	72%	76%	55%
		3	KKS	75%	74%	59%
5	Afet Yönetimi	1	İYS	73%	70%	64%
		2	DRAS-SI	76%	X	X
6	Tesisat Yönetimi	1	CBS	74%	66%	71%
		2	ŞYOS	67%	65%	X
		3	DPOS&DGAS	71%	73%	67%
SİBER GÜVENLİK OLGUNLUK SEVİYESİ				72%	69%	64%

Ayrıca akıllı doğal gaz şebekesi siber güvenlik olgun modeli ile kurumların olgunluk seviyeleri ölçüldü ve bu ölçüm sonuçlarına göre en düşük olgunluk seviyesine KURUM-C sahiptir. En iyi olgunluk seviyesi ise KURUM-A olarak ölçülmüştür. Aşağıdaki Şekil 4.4’ de 3 farklı kurumun siber güvenlik açısından olgunluk seviyeleri grafik olarak verilmiştir.

Alt bileşenlere bakıldığında üç kurumdada SCADA sistemlerinin olgunluk yüzdesi KURUM-A % 60, KURUM-B’ de % 54 ve KURUM-C’ de ise % 50 olarak ölçülmüştür.



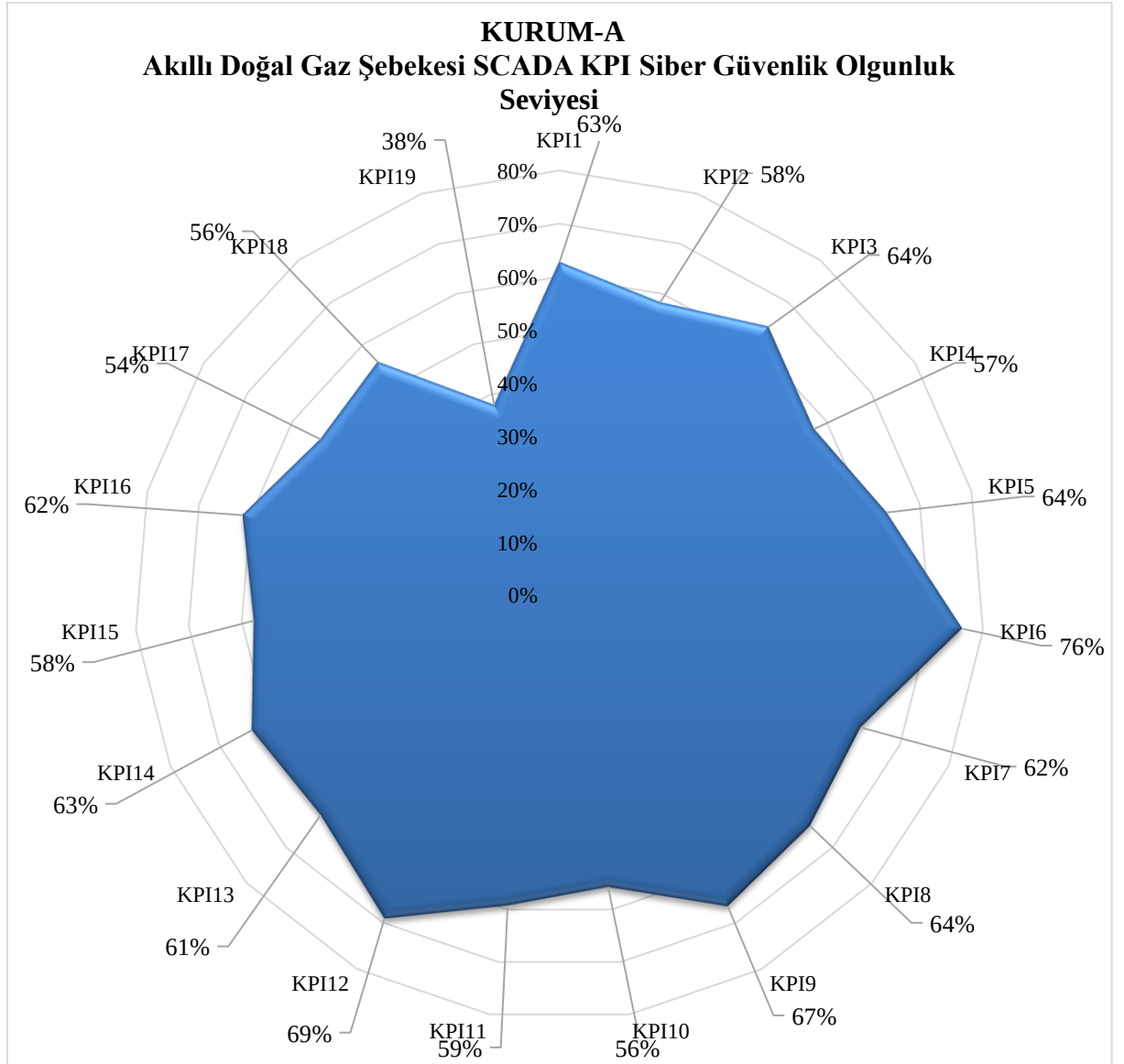
Şekil 4.4: Üç farklı kurumun akıllı doğal gaz alt bileşenlerinin siber güvenlik olgunluk seviyelerinin karşılaştırılması.

Ölçüm sonuçları hesaplanırken oluşturulan olgunluk modeline göre tüm KPI parametrelerine ait soru setleri 1-10 arasında puanlama yapılmıştır. Bu soru setleri 5 farklı uzmana sorularak siber güvenlik olgunluk seviyeleri ölçülmüştür.

Örnek olarak SGS siber güvenlik sistemine bakıldığında KURUM-A' da % 66, KURUM-B' de % 67 ve KURUM-C için ise % 60 olarak olgunluk seviyeleri hesaplanmıştır. Tüm bileşenler kıyaslama açısından grafik olarak verilmiştir.

4.4. KURUM-A AKILLI DOĞAL GAZ ŞEBEKESİ SCADA KPI SİBER GÜVENLİK OLGUNLUK SEVİYESİ

Akıllı doğal gaz şebekelerini siber güvenlik açısından incelediğimizde 19 adet KPI seti bulunmaktadır. KURUM-A için bir adet alt bileşen örnek alınarak olgunluk seviyesine neden olan sebepler incelenmiştir. Örnek sistem olarak SCADA sistemi incelendi. KPI19 özelinde olgunluk seviyesinin düşük olduğu ve iyileştirmeye açık alanların olduğu tespit edilmiştir.



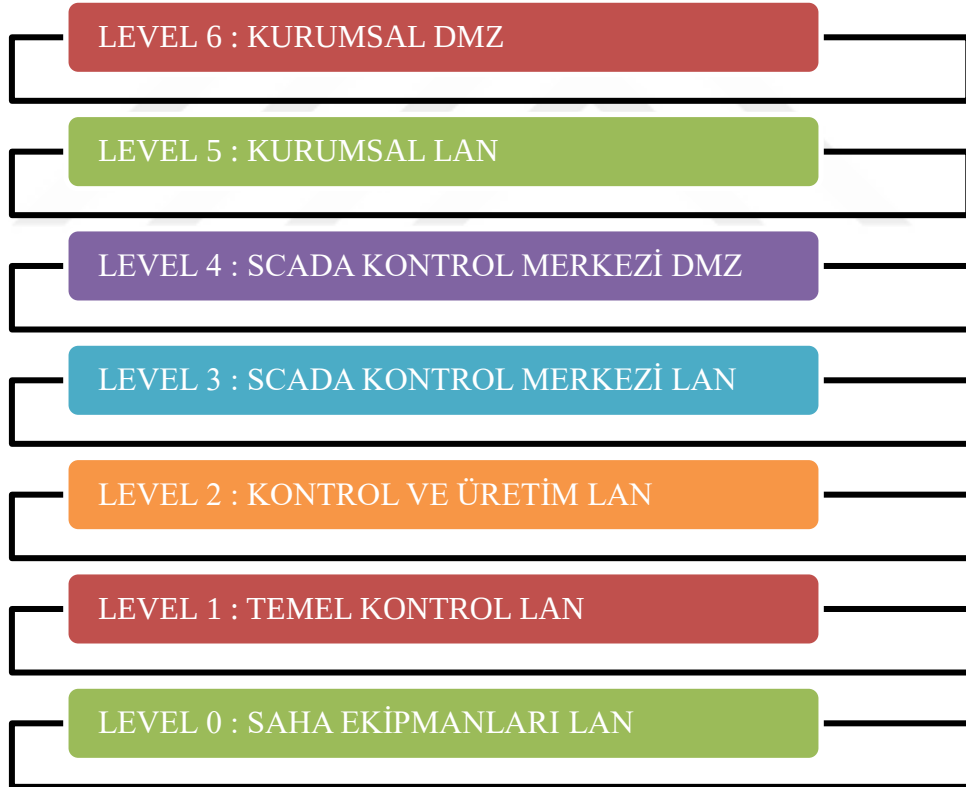
Şekil 4.5: KURUM-A Akıllı doğal gaz şebekesi SCADA KPI siber güvenlik olgunluk seviyesi.

4.5. ÖNERİLEN AĞ KATMANI VE MİMARİSİ

Yapılan çalışma sonucunda inceleme yapılan kurumlarda ağ modellerinin katmanlara ayrılmadığı ve bu katmanlar arasında güvenlik açısından korumaların eksik olduğu görülmektedir. Buradaki çalışmamızda ağların katmanlara ayrılması gerektiği ve siber saldırılara kurumlar maruz kaldığında katmanlar arası ilave edilecek güvenlik korumaları sayesinde diğer katmanlardaki dağıtık yapıdaki sistemlerin korunması sağlanmış olacaktır.

4.5.1. Önerilen Akıllı Doğal Gaz Şebekesi Yeni Ağ Mimarisi Katmanı

Araştırma ve inceleme yapılan kurumlarda katmanlı ağ mimarilerinin uluslararası standartlara göre kapsamlı katmanlara ayrılarak güvenliğin artırılması gerektiği görülmektedir. Bu çalışmalar sonucunda olması gereken ağ mimarisi katmanları için aşağıdaki yapı önerilmiştir.



Şekil 4.6: Önerilen akıllı doğal gaz şebekesi yeni ağ mimarisi katmanları.

4.5.2. Önerilen Akıllı Doğal Gaz Şebekesi Yeni Katmanlı Ağ Mimarisi

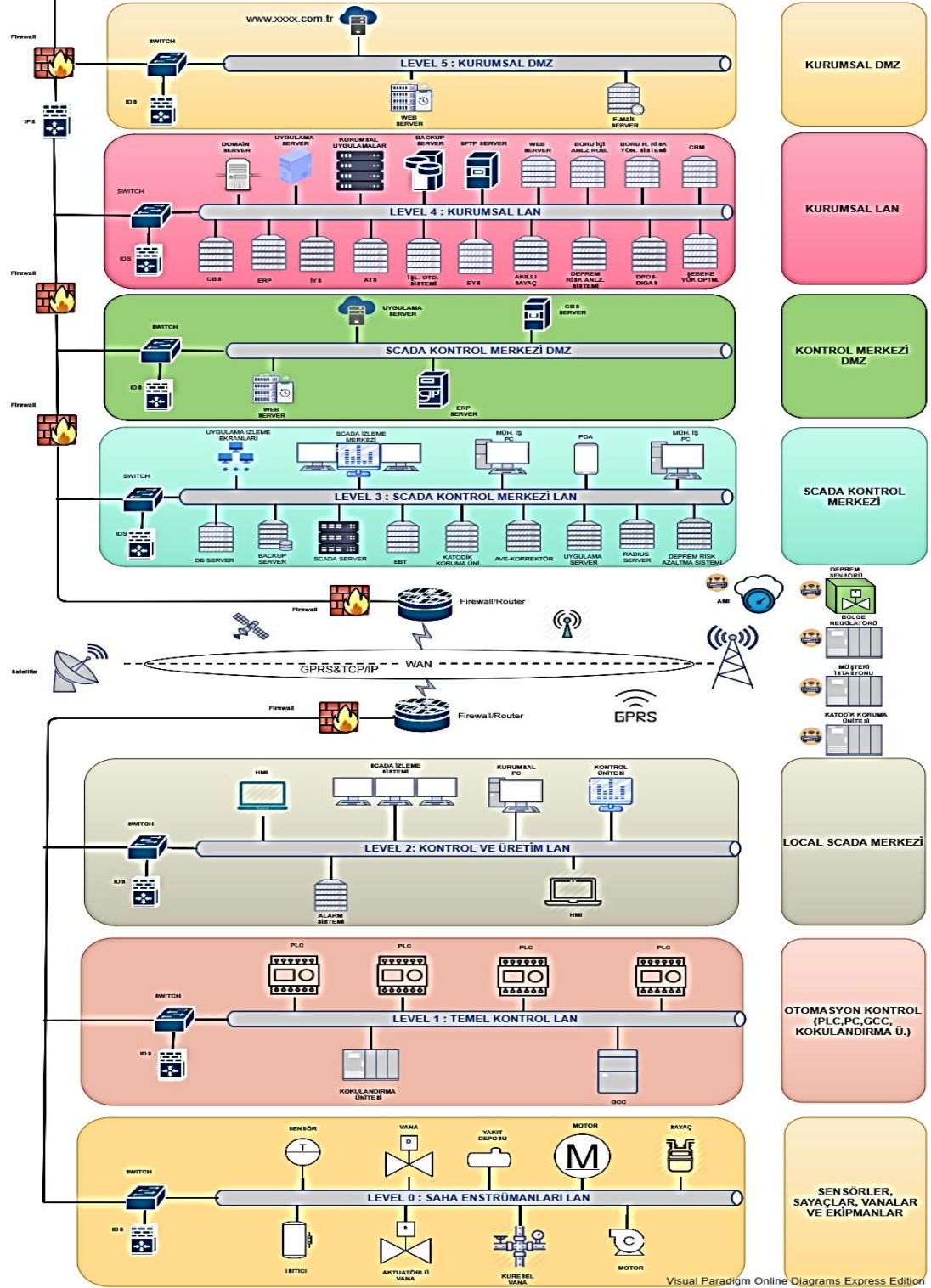
Önerilen ağ mimarisi çalışma yapılan kurumların ağ mimarileri incelenerek öneri olarak sunulmuştur. Kurumlarda yapılan incelemeler sonrasında kurulan ağ mimarileri geleneksel ağ mimarileri olduğu tespit edilmiştir. Her bir sistemin ağ mimarisini iyileştirmek kurumlar açısından ekstra maliyet getirmesi ve hizmet kesintisine sebebiyet vermesi demektir. Ağ mimarilerine genel olarak bakıldığında saha ekipmanlarının hepsinin tek bir ağda toplandığı tespit edilmiştir.

Ağ mimarilerinin katmanlara ayrılacak her bir uç noktanın ve sistemin farklı katmanlarda yer alması güvenlik açısından önemlidir. Akıllı doğal gaz şebekelerine karşı bir siber saldırı olması durumunda saldırganların aynı ağda olan tüm sistemlere erişim sağlaması kaçınılmazdır. Çalışma yapılan kurumlarda ağ mimarilerindeki eksiklikler tespit edilerek olması gereken durum öneri olarak sunulmuştur. Güvenli ağ modelleri kurumlara ait kritik sistemleri korumanın yanı sıra aynı zamanda kurumlara siber saldırılara maruz kalınması açısından ekonomik katkı sunmaktadır.

Güvenli ağ modelleri siber saldırılara karşı katmanlı koruma sağlar. Katmanlı koruma akıllı doğal gaz şebekelerine ait uç nokta olarak bahsedilen PLC, sensör, motor ve ölçüm cihazları lokal SCADA sistemlerinden farklı ağ yapısında birbirileri ile haberleşmesini sağlar. Katmanlara ayrılmış olan ağ mimarileri güvenlik olarak katma değer sunmuş olsa da bu sistemleri kurmak ilk kurulum açısından maliyetleri oldukça yüksektir.

Visual Paradigm Online Diagrams Express Edition

AKILLI DOĞAL GAZ ŞEBEKE AĞ DİYAGRAMI : ÖNERİLEN AĞ MODELİ



Visual Paradigm Online Diagrams Express Edition

Şekil 4.7: Önerilen akıllı doğal gaz şebekesi yeni katmanlı ağ mimarisi.

5. TARTIŞMA VE SONUÇ

Akıllı şebekeler son yıllarda teknoloji ekosistemine ve günlük yaşantımıza hızla girmiştir. Akıllı şebekeler dünyada hızlıca gelişirken ülkemizde de bir çok kurum ve kuruluşların da bu alanda çalışma yaptıkları görülmektedir. Sistemlerin akıllı hale getirilmesi ile güvenlik riskleri de beraberinde gelmektedir. Son yıllarda teknolojilerin gelişmesi ile birlikte siber saldırıların enerji altyapılarına, kritik altyapılarına ve EKS sistemlerine yoğunlaştığı tespit edilmiştir. Ekim 2020 tarihinde 164 adet siber suç, 84 adet siber casusluk, 5 adet siber savaş ve 1 adet haktivizm olayları gerçekleşmiştir (Hackmaggeddon, 2020). Yapılan akademik çalışmaların incelenmesi ve yaşanmış siber saldırılar analiz edildiğinde bu sistemlerde en çok yaşanan siber saldırı yöntemlerinin DDoS hizmet kesintisi, MITM ve Malware zararlı yazılımların olduğu tespit edilmiştir.

Bu tez çalışmasında, siber güvenlik, akıllı şebekeler ve akıllı doğal gaz şebekeleri hakkında genel bilgiler verilerek bu alana dikkat çekilmesi hedeflenmiştir. Ulusal ve uluslararası standartlar incelendiğinde akıllı şebekeler, kritik altyapılar ve endüstriyel kontrol sistemleri özelinde belirli olgunluk modellerinin olmasına rağmen yetersiz olduğu görülmüştür. Akıllı doğal gaz şebekelerinde de siber güvenlik açısından bir olgunluk modeline ihtiyaç olduğu tespit edilmiştir. Bu alanda yapılan akademik çalışmaların, standartların ve yönetmeliklerin tam olarak ihtiyacı karşılamadığı tespit edilmiştir. Bu kapsamda hazırlanan modellerin, standartların ve mevzuatların güvenlik açısından çok yüzeysel olduğu, kontrol ve denetim açısından sadece belirli sayıda başlıklar altında kurum ve kuruluşlara güvenlik çerçevesinde tavsiyeler verildiği görülmüştür.

Bu tez çalışmasında, akıllı doğal gaz şebekesi sistemlerinde siber güvenlik açıklarının araştırılması için bir olgunluk modeli oluşturuldu. Bu model ile kurumların kullandığı sistemlerin daha güvenli olması ve siber saldırılara karşı daha dayanıklı olması sağlanmıştır. Akıllı doğal gaz şebekeleri siber güvenlik olgunluk modeli 6 ana bileşen ve 18 alt bileşenden oluşmaktadır. Ayrıca her bir alt bileşenlerin altında 19 adet KPI parametresi bulunmaktadır. Bu parametreler standartlar, mevzuatlar, yaşanmış siber olaylar, yaşanabilecek siber saldırılar, kıyaslama yöntemi ile tespit edilen riskler ve konusunda 5 ile 15 yıl arasında tecrübeye sahip uzmanların görüşü alınarak tespit edilmiştir. Her bir KPI altında belirli sayıda her sisteme özel soru setleri bulunmaktadır. Tüm KPI parametrelerinin altında 3500 adet soru seti bulunmaktadır.

AHP metodu kullanılarak her bir sistemin önem ağırlıkları hesaplanmıştır. Her bir sistem 100 puan üzerinden değerlendirilmiş olup KPI parametrelerine ait soru setleri ise 1 ile 10 puan arasında puanlama yapılarak sistemlerin güvenilirliği hesaplanmıştır.

Ayrıca olgunluk modeli oluşturulurken inceleme yapılan kurumlara ait ağ mimarileri ve ağ katmanlarında mevcut durum analizi yapılmıştır. Bu mevcut durum analizinde tespit edilen iyileştirmeye açık alanlar ve zaafiyetler uluslararası standartlar dikkate alınarak olması gereken ağ mimarisi için bir öneri sunulmuştur. Yapılan çalışma sonucunda inceleme yapılan kurumlarda ağ modellerin katmanlara ayrılmadığı ve bu katmanlar arasında güvenlik açısından korumaların eksik olduğu görülmüştür. Yeni önerilen katmanlı ağ mimarisi ile ağların katmanlarına daha fazla ayrılması, katmanlar arasına ilave edilecek güvenlik ekipmanların ve uygulamaların sayesinde katmanlardaki dağıtık yapıdaki uç sistemlerin siber saldırılara karşı siber dayanıklılığı daha da artacaktır. Ayrıca bu tez çalışmasında örnek olarak ağ mimarileri verilmiştir. Bu çalışmalar güvenlik açısından risk teşkil ettiğinden dolayı çok fazla detay verilememiştir.

Geliştirilen siber güvenlik olgunluk modeli 3 farklı kurumda test edilmiştir. Seçilen 3 farklı kurum Türkiye özelinde bakıldığında kendi sektörlerinde büyük olan kurumlardır. Her bir ana ve alt bileşenler için uzmanlarla görüşmeler yapıp model çalıştırılmış ve hesaplamalar yapılmıştır. Akıllı doğal gaz şebekesi siber güvenlik olgunluk modeli ile örnek alınan 3 farklı kurumun tüm sistemleri akıllı şebeke konseptinde güvenlik bakış açısı ile olgunluk seviyesi hesaplamaları yapılmıştır. Bu ölçüm yapılan 3 kurumda tüm sonuçları bulgular bölümünde kıyaslama tablosu olarak verilmiştir.

Çalışma yapılan KURUM-A' da 6 ana bileşen ve 18 adet alt bileşen ile inceleme gerçekleştirilmiştir. KURUM-A' nın siber güvenlik açısından olgunluk seviyesi % 72 olarak hesaplanmıştır. Olgunluk seviyeleri ölçüm sonuçları incelendiğinde en düşük olgunluk seviyesi % 60 ile SCADA sisteminin olgunluk seviyesidir. SCADA açısından KPI değerleri yeniden incelenerek zayıf alanlarda kurum tarafından iyileştirmeler yapmalıdır. Ayrıca ölçüm sonucunda alt bileşenler arasında yapılan ölçümlerde SGS sistemi % 66 ve EBT sistemi ise % 67 olarak hesaplanmıştır.

KURUM-B' de ise 6 ana bileşen ve 16 adet alt bileşen ile inceleme gerçekleştirilmiştir. KURUM-B' nin siber güvenlik açısından olgunluk seviyesi % 69 olarak hesaplanmıştır.

Olgunluk seviyeleri ölçüm sonuçları incelendiğinde en düşük olgunluk seviyesi % 54 ile SCADA sisteminin olgunluk seviyesidir. SCADA açısından KPI değerleri yeniden incelenerek zayıf alanlarda kurum tarafından iyileştirmeler yapılmalıdır. Ayrıca ölçüm sonucunda alt bileşenler arasında yapılan ölçümde ATS sistemi % 55 ve AVE sistemi ise % 65 olarak hesaplanmıştır.

KURUM-C' de ise 6 ana bileşen ve 13 adet alt bileşende inceleme yapılmıştır. KURUM-C' nin siber güvenlik açısından olgunluk seviyesi % 64 olarak hesaplanmıştır. Olgunluk seviyeleri ölçüm sonuçları incelendiğinde en düşük olgunluk seviyesi % 54 ile SCADA sisteminin olgunluk seviyesidir. SCADA açısından KPI değerleri yeniden incelenerek zayıf alanlarda kurum tarafından iyileştirmeler yapılmalıdır. Ayrıca ölçüm sonucunda alt bileşenler arasında yapılan ölçümlerde KKS sistemi % 55 ve BHRYS sistemi ise % 59 olarak hesaplanmıştır.

Bu tez çalışmasında geliştirilen olgunluk modeli tamamlanmıştır. Modelin kurulması ile birlikte özellikle akıllı doğal gaz şebekelerinin yanısıra kritik altyapılarda, endüstriyel kontrol sistemlerinde ve farklı sektörlerde de bu alanda çalışmalara örnek model olacaktır. Bu olgunluk modeli ile sektörlerin ve kurumların siber güvenlik açısından olgunluk seviyeleri ve siber saldırılara karşı siber dayanıklılıkları artmış olacaktır. Bu sonuçlar özellikle kurumların siber saldırılara karşı korunmasının yanı sıra siber saldırılarında neden olabileceği ekonomik zararlar önlenecektir.

Sonuç olarak, akıllı doğal gaz şebekelerine ait kapsamlı bir çalışma yapılmıştır. Bu şebekelerin güvenlik açısından belirlenen KPI parametrelerine ve soru setlerine bağlı olarak siber güvenlik olgunluk seviyelerinin ölçülebilmesi sağlanmıştır. Bu çalışmanın ileriki aşamalarında, geliştirilmiş olan model için farklı yöntem ve metodlar kullanılarak hibrit bir model gerçekleştirilmesi planlanmaktadır.

KAYNAKLAR

[Afyonluoglu, 2019, <http://afyonluoglu.org/siberguvenlik/kritik-altyapilar6/> , (21.10.2019).

Ahmad, S. and Tahar, R.M, 2014, Selection of renewable energy sources for sustainable development of electricity generation system using analytic hierarchy process: A case of Malaysia, Renewable energy, 63:458-466.

Akın, M., Sağiroğlu Ş., 2016, Gelişmiş Sürekli Tehditler, 9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiri Kitabı, www.iscturkey.org, s.84.

Aslay, F., 2018, Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi, International Journal of Multidisciplinary Studies and Innovative Technologies, s.24-28.

Baigent, D., Adamiak, M. and Mackiewicz, R., 2004, IEC 61850 communication networks and systems in substations: an overview for users.

Baltaş, R., 2014, Hackerlar Almanya'da Çelik Fabrikasını Hackledi", Technopat, <https://www.technopat.net/2014/12/23/hackerlar-almanyada-celik-fabrikasini-hackledi/>, [Ziyaret tarihi: 27.04.2018].

Başaran1, A., 2014, <http://securitist.blogspot.com.tr/2014/07/siber-savas-tarihinden-baz-olaylar.html>, [Ziyaret tarihi: 21.11.2018].

Başaran2, A., 2014, <http://alperbasaran.com/siber-savas-tarihinden-bazi-olaylar/>, [Ziyaret tarihi: 21.11.2018].

Baykara M., Daş R., Karadoğan İ., 2013, 1st International Symposium on Digital Forensics and Security (ISDFS'13), 20-21 May 2013, Elazığ, Turkey.

Belton V. and Stewart T. J., 1999, Dea and mcda: Competing or complementary approaches?In Advances in decision analysis, Springer, pages 87-104.

BGD, 2019, BGD Siber Güvenlik ve Savunma Kitap Serisi 1, <https://www.cybermagonline.com/img/sayfa/siber-guvenlik-kitap-basila-04-01-2019.pdf>,p.23, [Ziyaret tarihi: 29.01.2019].

Bgasecurity, 2019, <https://www.bgasecurity.com/2014/02/xxe-xml-external-entity-guvenlik/> , [Ziyaret tarihi: 15.10.2019].

Bıçakçı, S., 2012, Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu, Uluslar arası İlişkiler Dergisi, Cilt 9, Sayı 34, s.205-226.

BİLGEM, 2017, Temel Siber Güvenlik Gereksinimleri, TÜBİTAK, Gebze, Kocaeli.

Bilgi Güvenliği Derneği, 2019, http://www.bilgiguvenligi.org.tr/wp-content/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf, [Ziyaret tarihi: 24.01.2019].

- Biznet, 2019, <https://www.biznet.com.tr/wannacry-ne-ilk-ne-de-son-notpetya-ile-tanisin/> , [Ziyaret tarihi: 24.01.2019].
- Bleepingcomputer, 2019, <https://www.bleepingcomputer.com/news/security/over-140-international-airlines-affected-by-major-security-breach/> , [Ziyaret tarihi: 22.10.2019].
- BOTAŞ, 2020, <https://ebt.botas.gov.tr/Login.aspx?ReturnUrl=%2f>, [Ziyaret tarihi: 05.04.2020].
- Bookmark, 2019, <http://www.bookmark.com.tr/dunden-bugune-siber-savaslar-2/>, [Ziyaret tarihi: 22.10.2019].
- Borlase, S., 2016, Smart grids: infrastructure, technology, and solutions, CRC Press.
- British-Standard-Institution, 2014, Pas 181 smart city framework, BSI Corporate, pages 1-15.
- BSI-British-Standard-Institution, 2020, Communication systems for and remote reading of meters dedicated application layer, General principles and application for communications, system, pages 1-156, [Ziyaret tarihi: 26.01.2020].
- BSI-British-Standard-Institution, 2001, Part 4: principle and criteria of cathodic protection. Cathodic protection of buried or immersed metallic structures. General principles and application for pipelines, pages 5-22.
- Caragliu, A., Del Bo, C., and Nijkamp, P., 2009, Smart cities in Europe (2009), In 3rd Central European Conference in Regional Science.
- Castillo, M., 2016, Corrosion Management of Pipelines More Important than Ever, Pipeline & Gas Journal.
- Channelpostmea, 2017, <http://www.channelpostmea.com/2017/03/02/dubai-wants-to-become-a-global-benchmark-for-smart-cities>, [Ziyaret tarihi: 02.03.2017].
- Chatzimouratidis, A. and Pilavachi P., 2009, Technological, economic and sustainability evaluation of power plants using the analytic hierarchy process, energy policy, pages 778-787.
- Cisco Energy Optimization Service, 2019, http://www.cisco.com/web/strategy/docs/energy/energy_optimization_service_aag.pdf, retrieved from CISCO, [Ziyaret tarihi: 21.01.2019].
- CMMI Product, 2011, Capability Maturity Model Integration, CMMI for Services, Version 1.3, Lulu.com.
- Computerworld, 2016, <https://www.computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html>, [Ziyaret tarihi: 01.02.2019].
- Collantes, M. H. and Padilla, A. L., 2017, Protocols and Network Security in ICS Infrastructures, Spanish National Cybersecurity Institute, CERTSI_GUIA_SCI_001_ProtocolosRed_2017_v2.

- CSIS,2018,https://csisprod.s3.amazonaws.com/s3fspublic/180425_Significant_Cyber_Events_List.pdf?pqtWcwV7mvAo33_lAZFlQVQz7.E0qh, Center for Strategic and International Studies (CSIS), Washington, D.C., [Ziyaret tarihi: 01.05.2018].
- Çiftçi, H., 2013, Her Yönüyle Siber Savaş, Tubitak Popüler Bilim Kitapları, Ankara.
- Dağgaz, 2020, <http://daggaz.com/Files/ProductImages/>, [Ziyaret tarihi: 26.01.2020].
- Demirbaş, A., 2010, Methane Gas Hydrate, Springer.
- Do, V. L. and et al., 2017, Security of SCADA Systems Against Cyber-Physical Attacks, IEEE A&E System Magazine.
- Dönmez, M., 2013, Akıllı şebekeler ve entegrasyon (smart grids and integration), BTC Business Technology.
- Drucker P., 2012, Managing in the next society. Routledge.
- East, S. et al., 2009, A Taxonomy of Attacks on the DNP3 Protocol, Critical Infrastructure Protection III, IFIP AICT 311, pp. 67–81.
- EMRA, 2002, Doğal Gaz Piyasası Dağıtım Ve Müşteri Hizmetleri Yönetmeliği, Madde 48.
- Energy, 2019, <https://www.energy.gov/sites/prod/files/2017/04/f34/2017-03-21-C2M2%20Facilitator%20Guide%20v1.1a.pdf> , [Ziyaret tarihi: 21.10.2019].
- EPDK, 2020, <https://www.epdk.org.tr/Detay/Icerik/3-0-94/dogal-gazyillik-sektor-raporu>, [Ziyaret tarihi: 26.01.2020].
- European Norm, 2020, Communication systems for meters and remote reading of meters. Wireless meter readout (Radiometer reading for operation in SRD bands), EN 13757-3, [Ziyaret tarihi: 26.01.2020].
- Erol, S., E., Sağiroğlu, Ş., (2015), Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme, 8th International Conference on Information Security and Cryptology (ISCTurkey).
- Espie, P., Ault, G.W., Burt, G.M, and McDonald, J.R., 2003, Multiple criteria decision-making techniques applied to electricity distribution system planning. IEE Proceedings-Generation, Transmission and Distribution, 150(5):527-535.
- Feroze, F, and Javaid, N., 2017, Towards Enhancing Demand Side Management using Evolutionary Techniques in Smart Grid, 10.13140/RG.2.2.34456.49920.
- Garanti,2020,https://www.garantibbva.com.tr/tr/garanti_hakkinda/garantiden_haberler/2019/ekim/dijital-kanallarimizdaki-hizmetlere-erisim.page, [Ziyaret tarihi: 26.01.2020].
- GAZBİR,2017,<http://www.gazbir.org.tr/uploads/page/Ak%C4%B1ll%C4%B1%20%C5%9Eebekeler.pdf>, [Ziyaret tarihi: 11.04.2019].
- GAZBİR, 2020, <https://www.gazbir.org.tr/yillik-raporlar/150>, [Ziyaret tarihi: 11.04.2020].

- Goel, S. and Jindal A., 2017, Evolving Cyber Security Challenges to the Smart Grid Landscape, International Journal of Advance Research, Ideas and Innovations in Technology.
- Hackmageddon, 2018, <https://www.hackmageddon.com/2018/04/17/16-31-march-2018-cyber-attacks-timeline/>, [Ziyaret tarihi: 21.11.2020].
- Hackmageddon, 2019, <https://www.hackmageddon.com/2019/01/15/2018-a-year-of-cyber-attacks/>, [Ziyaret tarihi: 04.02.2019].
- Hackmageddon, 2019, <https://www.hackmageddon.com/2018-master-table/>, [Ziyaret tarihi: 08.02.2019].
- Hauge S., B., & Mercier, B. A., 2003, Reliability centered Maintenance Maturity Level Roadmap. Paper presented at the Annual Reliability and Maintainability Symposium, 2003Annual, pages 226-231. IEEE.
- IBM, 2020, <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&>, [Ziyaret tarihi: 21.05.2020].
- Imperva, 2018, <https://www.imperva.com/blog/the-state-of-web-application-vulnerabilities-in-2018/>, [Ziyaret tarihi: 21.11.2018].
- ISA-95, 2020, <https://isa-95.com/>, [Ziyaret tarihi: 21.07.2020].
- ISO-IEC. Smart cities, preliminary report, 2015, http://www.iso.org/iso/smart_cities_report-jtc1.pdf, [Ziyaret tarihi: 21.11.2018].
- ISO-International-Standardization-Organization, 1994, Information Technology–Open Systems Interconnection – basic reference model: The basic model. Standard, International Organization for Standardization, Geneva, CH.
- ISO, 2011, Energy management systems - requirements with guidance for use. Standard, International Organization for Standardization, Geneva, CH.
- ISO, 2011, Societal security – Emergency management – Requirements for incident response, International Organization for Standardization, Geneva, CH.
- Iyer, S., 2011, Cyber Security for Smart Grid, Cryptography, and Privacy, International Journal of Digital Multimedia Broadcasting, USA.
- İGDAS, 2014, cdn.igdas.com.tr/Web/Content/IGDAS_Faaliyetyeni2014.pdf, Retrieved from İGDAS, [Ziyaret tarihi: 21.11.2018].
- Kara, M., 2013, Siber Saldırıları-Siber Savaşlar ve Etkileri, Y.Lisans Tezi, İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.
- Kaya, A., 2012, Siber Güvenliğin Milli Güvenlik açısından Önemi, Y.Lisans Tezi, Kara Harp Okulu, Savunma Bilimi Enstitüsü, Ankara.

- Kaya Kurt G. D., 2017, Bilgi Güvenliği ve Siber Güvenlik Kapsamında Bakanlık Uygulamaları İçin Güvenli Yazılım Geliştirme Metodolojisi Önerisi, Uzmanlık Tezi, T.C. Çevre ve Şehircilik Bakanlığı, Ankara.
- Karakuş, C., 2011, Sayısal Haberleşme Sistemleri, www.ckk.com.tr/ders/communication.pdf, [Ziyaret tarihi: 21.11.2018].
- Kariyawasam, S., and P. Warren, P., 2008, Revised corrosion management with reliability based excavation criteria, In 2008 7th International Pipeline Conference, pages 489-500, American Society of Mechanical Engineers.
- Kenandabirkuyu, 2019, <http://www.kenandabirkuyu.org/siber-mucadelenin-sicak-savaslara-etkisi-uzerine-bir-arastirma> , [Ziyaret tarihi: 21.10.2019].
- Knapp, E., 2011, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Elsevier Inc.
- Korkmaz, E. et al., 2016, Industrial Control Systems Security Testbed.
- Meral, M., 2015, Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi, Yüksek Lisan Tezi, Harp Akademileri Stratejik Araştırmalar Enstitüsü, İstanbul.
- Minnaar, J. R., Basson, W., and Vlok, P. J., 2013, Quantitative methods required for implementing pas 55 or the ISO 55000 series for asset management. South African Journal of Industrial Engineering, 24(3):98-111.
- Mishra, P. K., 2013, Analysis of MITM Attack in Secure Simple Pairing, Journal of Global Research in Computer Science, Volume 4, No. 2.
- Mo, Y., and Sinopoli, B., 2010, False data injection attacks in control systems. Preprints of the 1st Workshop on Secure Control Systems.
- Morris, T. H. and Wei Gao, 2013, Industrial Control System Cyber Attacks, 1st International Symposium for ICS & SCADA Cyber Security Research 2013.
- Nam, T., & Pardo, T. A., 2011, Conceptualizing smart city with dimensions of technology, people, and institutions. In Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times (pp. 282–291). ACM.
- NIST, 2019, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>, [Ziyaret tarihi: 05.02.2019].
- Radiflow, 2019, https://radiflow.com/wp-content/uploads/2019/06/Survey_ICS-2019_Radiflow.pdf, [Ziyaret tarihi: 21.10.2019].
- Roberts, P., 2011, Gas sales and gas transportation agreements: principles and practice, Sweet & Maxwell, London.

- Rodofile, N. R. et al., 2017, Framework for SCADA cyber-attack dataset creation, ACSW '17: Proceedings of the Australasian Computer Science Week Multiconference.
- Sang, Z., Luo, Z., and Mulquin, M., 2015, Standardization roadmap for smart sustainable cities. Technical report, International Telecommunication Union (ITU).
- SANS, 2020, <https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327>, [Ziyaret tarihi: 21.10.2020].
- SE, 2020, <https://www.se.com/ww/en/product-range-presentation/61247-scadapack-300%2C-32/>, [Ziyaret tarihi: 21.10.2020].
- Securitynewsdesk, 2018, <http://www.securitynewsdesk.com/examining-threat-posed-cyber-attacks-critical-infrastructure/>, [Ziyaret tarihi: 21.11.2018].
- Siber Güvenlik Danışmanlığı, 2019, <http://siberguvenlikdanismanligi.com/xss-nedir/>, [Ziyaret tarihi: 15.10.2019].
- Siemens Aktiengesellschaft, 2014, Smart grids and the new age of energy, <http://www.energy.siemens.com/hq/de/stromuebertragung/transformatoren/assets/pdf/siemens-transformers-power-engineering-guide-7-1.pdf>.
- STM, 2019, <https://www.stm.com.tr/tr/urunler/siber-fuzyon-merkezi>, [Ziyaret tarihi: 25.01.2019].
- Steeners, K., 2003, Energy and the city: density, buildings and transport, Energy and Buildings, Elsevier Science, 35(1):3-14.
- Symantec, 2014, Regin: Top-tier Espionage Tool Enables Stealthy Surveillance, <http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance>, [Ziyaret tarihi: 27.04.2018].
- Şenol, M., 2016, Siber Güçle Caydırıcılık Ama Nasıl?, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:2, No:2, Ankara, s.10-17.
- T.C. UDHB, 2016, 2016-2019 Ulusal Siber Güvenlik Stratejisi, <http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf>, [Ziyaret tarihi: 02.07.2019].
- Tcamtech, 2020, https://tcamtech.diytrade.com/sdp/352327/4/pd-1639994/1570416-0/TMAS_3G_Modem_Terminal.html, [Ziyaret tarihi: 21.11.2020].
- Threatpost, 2018, <https://threatpost.com/utilities-energy-sector-attacked-mainly-via-it-not-ics/138733/>, [Ziyaret tarihi: 21.11.2018].
- Volker, L., Lei, V., and Ligtvoet, A., 2011, Developing a maturity model for infrastructural asset systems. In 10th Conference on Applied Infrastructure Research (Infraday 2011), Berlin: TU Berlin.

- Washburn, D., Sindhu, U., Dines, R. A., Balaouras, S., Hayes, N. M., & Nelson, L. E. (2010). Helping CIOs Understand “Smart City” Initiatives: Defining the Smart City, Its Drivers, and the Role of the CIO.
- Whatis, 2019, <https://whatis.techtarget.com/definition/crimeware-kit-attack-kit>, [Ziyaret tarihi: 05.02.2019].
- WILSON, C., 2012, Industrial and SCADA Systems May Be Increasingly Targeted for Cyber Attack, http://www.pesolutions-it.com/wp-content/uploads/2014/10/SCADA_Vulnerabilities.pdf, University of Maryland University College, [Ziyaret tarihi: 27.04.2018].
- William, E., 2016, Pipeline cybersecurity issues from marcellus and beyond. Pipeline-Gas Journal, 243(9):28_30.
- Xia, H. and Brustoloni J. C., 2005, Hardening Web Browsers Against Man-in-the-Middle and Eavesdropping Attacks, WWW 2005, May 10–14, Chiba, Japan.
- Yan, Y. and et al., 2012, A Survey on Cyber Security for Smart Grid Communications, IEEE Communications Surveys & Tutorials, Vol. 14, No. 4.
- Yıldız, M., 2014, Siber Suçlar ve Kurum Güvenliği, Denizcilik Uzmanlık Tezi, T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

EKLER

KPI PARAMETRELERİNE AİT ÖRNEK SORU SETLERİ

	Örnek KPI Soru Setleri
1	Önceden belirlenmiş siber olay alarmlarının ve bunlara karşılık gelen eşik değerlerinin belirlendi mi?
2	Kurum ağlarının yaşanması muhtemel siber olaylara karşı sürekli olarak gözlemlenmesi yapılıyor mu?
3	Kurum ağlarında çalışan muhtemel zararlı kodları tespit etmek için yazılım (Anti-Virüs vb.) kullanılıyor mu?
4	Kurumun ağlarında bulunan yetkisiz kullanıcıların, cihazların, bağlantıların ve yazılımların izlenmesi yapılıyor mu?
5	Veri kaybı engelleme yazılımlarının kullanılıyor mu?
6	Kurum ağlarına yönelik sızma testlerinin ve zafiyet arama çalışmaları yapılıyor mu?
7	Siber olay tespit süreçlerinin doğruluğunun gözden geçiriliyor mu?
8	Kurumun siber güvenlik politikaları ve ölçütlerin geliştirilebilmesi için, siber olayların analiz ediliyor mu?
9	Kurum bilgisayarlarında ve/veya ağlarında, son bir yıl içinde tespit edilen zararlı yazılım(lar) oldu mu? Cevabınız evet ise, zararlı yazılım(lar)ın hangi hizmetleri etkilediğini, ne kadar süre kurum ağlarında çalıştığını, kurum ağlarına nasıl bulaştığını ve özelliklerini belirtiniz?
10	Kurumunuz tarafından şifreleme kullanılmakta mıdır? Cevabınız evet ise, hangi kategorilerde ve şartlarda veri, iletişim ve cihazlar şifrelenmektedir?
11	Kurumunuz tarafından, düzenli olarak bilgi güvenliği politikalarının uygunluğu denetlenmekte midir? Cevabınız evet ise, en son denetleme ne zaman ve kimin tarafından gerçekleştirilmiştir?
12	Kurumunuza ait web sitesi veya ağlarına son bir yıl içinde DDoS (Distributed Denial of Service) atağına maruz kalmış mıdır? Cevabınız evet ise, saldırının süresi ve kurumunuza etkisi nedir?
13	Aşağıda belirtilen her bir maddede, kurumunuz tarafından bilgi sistemlerinin ve ağlarının korunması için uygulanan politikaları ve prosedürleri yazılı olarak belirtiniz?
14	Kurumunuz tarafından çalışanlarına, bilgi güvenliği riskleri ve sorumlulukları hakkında yazılı kılavuz ve/veya periyodik eğitim verilmekte midir? Cevabınız evet ise, anılan bu eğitimler ve/veya dokümanlar nelerdir ve en son hangi tarihte, hangi konularda düzenlenmiş ve kimlere verilmiştir?
15	Kurumunuz tarafından, kuruma ait ağlarda meydana gelen veya meydana gelebilecek herhangi bir yetkisiz erişim teşebbüsü veya normal olmayan bir hareket tespiti adına kontrol araçları mevcut mudur? Cevabınız evet ise, anılan bu kontrolleri belirtiniz.
16	Kurumunuz tarafından; işlerin sürekliliği ve ağlara zarar gelmemesi adına, kullanıcıların bu ağları kullanması kısıtlanmış mıdır? Cevabınız evet ise, hangi tür kontroller sebebi ile hangi kısıtlamalar yapılmıştır?
17	Kurumunuz tarafından, kendi çalışma ortamından bağımsız bir biçimde işletilen ve kurumda kullanılan yazılımları ve uygulamaları test etmekte kullanılan başka bir ortam mevcut mudur? Cevabınız evet ise, detaylandırınız.

18	Kurumunuz tarafından, benimsenen ve sürdürülen temel donanım ve yazılım yapılandırma ayarları bulunmakta mıdır? Cevabınız evet ise, kullanıcıların bu temel yapılandırma ayarlarını, yetkililerin izni ve onayı olmadan değiştirmeleri engellenmiş midir?
19	Kurumunuzda, Bilgi Teknolojileri (Information Technologies – IT) varlıklarının sökülmesi, transfer edilmesi ve yerleştirilmesi adına oluşturulmuş bir süreç yönetimi planı mevcut mudur? Cevabınız evet ise, detaylandırınız.
20	Kurumunuzda, güvenlik açıklarına karşılık gelen yazılım yamalarının periyodik olarak yüklenmesini de içeren, düzenli bir sistem bakım süreci mevcut mudur? Cevabınız evet ise, detaylandırınız.
21	Kurumunuzun bilgi güvenliği politikalarında ve eğitimlerinde, taşınabilir ve mobil medya kullanımı hakkında bilgi var mıdır? Cevabınız evet ise, detaylandırınız.
22	Kurumunuzun internete açılan IP adreslerine yönelik gerçekleştirilecek DDoS atağına karşı alınmış önlem var mıdır? Cevabınız evet ise, alınan koruma önlemlerinin neler olduğunu ve bu koruma önlemlerinden kimin sorumlu olduğunu belirtiniz?
23	Kurumunuza ait yazılı bir veri imha politikası var mıdır? Cevabınız evet ise, detaylandırınız.
24	Kurumunuza ait yazılı siber olaylara müdahale politikası mevcut mudur? Cevabınız evet ise, en son hangi tarihte güncellendiğini belirtiniz.
25	Kurumunuza ait siber olaylara müdahale politikası düzenli olarak tatbikatlar ve testler ile değerlendirilmekte midir? Cevabınız evet ise, bu değerlendirmeler en son hangi tarihte ve kimin tarafından yapılmıştır?
26	Kurumunuz tarafından, yedekleme sisteminin düzgün çalışıp çalışmadığı periyodik olarak test edilmekte midir? Cevabınız evet ise, en son hangi tarihte test edilmiştir?
27	Kurumunuz tarafından, bilgi güvenliği mimarisi ve süreçlerini modellemek için Türk Standartları Enstitüsü (TSE) veya Uluslararası Standartlar Örgütü (ISO) gibi kurumların yayımlamış olduğu Siber Güvenlik Risk Yönetim Süreci ile ilgili standartları konu alan dokümanlar kullanılmakta mıdır?
28	Kurumunuz tarafından bilgi güvenliği varlıklarının yönetimi yapılıyor mu?
29	En son yapıldığı tarih nedir?
30	Gerçekleştirilme sıklığı nedir?
31	Gerçekleştirilmesinden sorumlu olan grup veya kişi?
32	Kurum içerisinde yer alan fiziksel cihazlar ve sistemler hakkında envanter tutulması.
33	Kurum içerisinde yer alan yazılım platformları ve uygulamalar hakkında envanter tutulması.
34	Ağ kaynakları, bağlantılar ve veri akışına ait haritalama ve ayrıntılı planlamanın oluşturulması veya güncellenmesi.
35	Kurumun ağına bağlantılı dış kaynakların listelenmesi.
36	Kaynakların (donanım, veri ve yazılım) önemine ve değerine göre korumak için önceliklendirilmesi.
37	İz kaydı kapasitesinin ve uygulamalarının; yeterlilik, uygun saklama ve süreklilik kıstaslarını göz önünde bulundurarak belirlenmesi ve değerlendirilmesi.
38	Kurumunuza ait yazılı bilgi güvenliği politikasını belirtiniz.
39	Kurumunuz tarafından; siber güvenlik tehditlerini, açıklıklarını ve potansiyel sonuçlarını tespit etme adına periyodik olarak risk değerlendirilmesi yapılmakta mıdır? Eğer yapılıyorsa,
40	Kim tarafından yapılıyor ve hangi tarihte en güncel değerlendirme yapılmıştır?

41	En güncel risk değerlendirmenizden çıkan sonuçlar (hiçbir şey bulunamadı/ortalama/yüksek risk) nelerdir?
42	Kurumunuz tarafından; siber güvenlik sorununa sebep olacak fiziksel siber güvenlik tehditlerini ve açıklıklarını tespit etme adına periyodik olarak risk değerlendirilmesi yapılmakta mıdır? Eğer yapılıyorsa,
43	Kim tarafından yapılıyor ve hangi tarihte en güncel değerlendirme yapıldı?
44	En güncel risk değerlendirmenizden çıkan sonuçlar (hiçbir şey bulunamadı/ortalama/yüksek risk) nelerdir?
45	Kurumunuzda çalışanlar ve yöneticiler için siber güvenlik görevleri ve sorumlulukları açık ve detaylı olarak belirtilmiş ve atanmış ise, bunları detaylı olarak yazınız.
46	Herhangi bir siber güvenlik vakasının etkilerini azaltma ve/veya siber güvenlik vakasının ardından normal çalışma sürecine tekrar dönme adına kurumunuza ait yazılı iş sürekliliği sağlama dokümanını belirtiniz.
47	Kurumunuzda siber güvenlikten sorumlu ve yetkili bir yönetici (Chief Information Security Officer) veya eş değer bir pozisyon var mıdır? Eğer varsa, kişinin özellikleri ve sorumluluğu nedir? Eğer yok ise, kurumda muhtemel olabilecek bir siber güvenlik vakasında sorumlu/yetkili kim olacaktır?
48	Kurumunuza ait iş süreçlerine özgü en uygun siber güvenlik tedbirlerinin belirlenmesi nasıl yapılmaktadır?
49	Kurumunuzda, gerçekleşebilecek siber güvenlik vakasının ardından zararları ve harcamaları kapsayacak bir sigortalama mevcut mudur? Eğer mevcut ise, anılan bu sigortanın kapsamını ve içeriğini belirtiniz.