ANALİZ

ENERJİ GÜVENLİĞİ VE DİJİTAL-YEŞİL DÖNÜŞÜM: AKILLI VE KARBONSUZ ŞEBEKELERE GEÇİŞ

EYLÜL 2025

Milli İstihbarat Akademisi

ENERJİ GÜVENLİĞİ VE DİJİTAL-YEŞİL DÖNÜŞÜM: AKILLI VE KARBONSUZ ŞEBEKELERE GEÇİŞ

ANALİZ / EYLÜL 2025

Milli İstihbarat Akademisi

Milli İstihbarat Akademisi

Telif

Yayın Tarihi: Eylül 2025

Millî İstihbarat Akademisi
E-Posta: bilgi@mia.edu.tr

"Bandrol Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 5'inci maddesinin 2'nci fıkrası çerçevesinde bandrol taşıması zorunlu değildir."

ANALİZ / Eylül 2025

ENERJİ GÜVENLİĞİ VE DİJİTAL-YEŞİL DÖNÜŞÜM: AKILLI VE KARBONSUZ ŞEBEKELERE GEÇİŞ

İÇİNDEKİLER

HARİTA

GRAFİK

ŞEKİL

TABLO

YÖNETİCİ ÖZETİ

- Enerjide dijital ve yeşil dönüşüm; elektrik üretiminde fosil yakıt bağımlılığını azaltarak yenilenebilir enerji kaynaklarının payını, enerji güvenliğini ve ekonomik rekabet gücünü artırmak için stratejik bir araç olarak görülmektedir.
- Avrupa Birliği'nin (AB) Avrupa Yeşil Mutabakatı; 2050 yılına kadar net sıfır emisyon, 2030 yılına kadar %55 emisyon azaltımı hedeflemektedir. Türkiye ise 2053 net sıfır emisyon hedefiyle yenilenebilir enerji kurulu gücünü, 2030 yılına kadar %70'e çıkarmayı planlamaktadır.
- Yeşil dönüşüm, yenilenebilir enerji entegrasyonunu artırmak için dijital teknolojilere ihtiyaç duymaktadır. Mevcut güç sistemleri; geleneksel üretim merkezleri ve tahmin edilebilir tüketim davranışları için tasarlanmıştır. Değişken üretim profilli yenilenebilir enerji kaynaklarının ve tüketim davranışlarının sistem kararlılığını olumsuz etkilememesi için şebekenin "gelişmiş kontrol ve izleme sistemleri, akıllı şebekeler, nesnelerin interneti, yapay zekâ ve veri analitiği gibi dijital dönüşüm teknolojileriyle" donatılması zorunlu olmuştur.
- Dijital dönüşüm, sürdürülebilirlik hedeflerini desteklemek için yeşil enerjiye dayanmak durumundadır.
- Dijital ve yeşil dönüşüm süreçlerinin eş güdümlü yürütülememesi; elektrik şebekelerinde arz güvenliğini, kararlılığı, sürdürülebilirliği ve esnekliği olumsuz yönde etkilemektedir. Özellikle Avrupa'da son yıllarda yaşanan büyük ölçekli elektrik kesintileri, arz talep dengesinin sağlanmasında yaşanan zorluklardan doğan frekans ve gerilim kararsızlıklarından kaynaklanmaktadır.
- Şimdiye kadar elektrik şebekelerinde tecrübe edilen arızalara karşı sistem operatörleri tarafından geliştirilen çökmeleri önleme eylemlerinin; dijital ve yeşil dönüşüm sürecinde gelişen tehditlere karşı yetersiz kalması, bu eylemlerin gözden geçirilme gerekliliğini ortaya çıkarmıştır.
- İklim değişikliğine bağlı yaşanan fırtına, kasırga, sel, kuraklık gibi aşırı hava koşulları; dijital dönüşümle desteklenmiş olsa bile yenilenebilir enerji kaynaklarının, entegrasyonun yüksek

olduğu şebekelerde, sistem operatörlerinin rezerv kapasitesini artırmasını gerektirmekte ve karbonsuzlaşma hedefinde endişeler oluşturmaktadır. Bu ve benzeri problemlerin önüne geçmek isteyen ülkeler, devre dışına almayı planladığı nükleer santrallerden bazılarını, acil durum rezervi olarak belirleyerek enerji arz güvenliğini ön plana koymaktadır.

- Enerjide dijital ve yeşil dönüşümün, elektrik şebekelerindeki olumsuz etkilerini azaltmakta çare olarak görülen "yapay zekâ destekli üretim ve talep tahmin algoritmaları, anomali tespit stratejileri, enerji depolama sistemleri ve grid-forming (şebekeyi şekillendirme) kabiliyeti olan güç elektroniği ekipmanları" enerji bağımsızlığına giden yolda, yeni teknolojik bağımlılıklar getirmektedir.

GİRİŞ

Elektrik şebekelerinin güvenilirliğini ve kararlılığını sürdürmek, modern toplumların karşılaştığı en önemli zorluklardan biridir. Elektrik sisteminin tamamen veya kısmen istem dışı enerjisiz kalması, kısaca "sistem oturması" olarak tanımlanmaktadır. Bu olaylar, ekonomik faaliyetleri durdurmakla birlikte günlük yaşamı kesintiye uğratmaktadır. Söz konusu olaylar, bazı durumlarda ise kamu güvenliğini riske atacak noktaya ulaşabilmektedir. 28 Nisan 2025 tarihinde İspanya'da başlayan, Portekiz ve Fransa'yı da etkileyen ve yaklaşık 10 saat süren elektrik kesintisi bunun en güncel örneklerindendir. Binlerce insan metrolarda, tren istasyonlarında, havalimanlarında ve limanlarda mahsur kalmış, bankacılık ve ödeme sistemleri çökmüş, hastaneler acil durumlar dışında hizmet veremez hâle gelmiş ve kamu güvenliğinin sağlanması için olağanüstü hâl kararı alınmıştır. **Son yıllarda dünya genelinde artan elektrik kesintileri ve sistem çökmeleri; bu olayların nedenlerini, mekanizmalarını ve önleme stratejilerini daha iyi anlamanın gerekliliğini ortaya koymuştur. Bu çalışma, akıllı ve karbonsuz şebekeleri hedefleyen dijital-yeşil dönüşüm sürecinde oluşabilecek riskleri enerji arz güvenliği ekseninde incelemeyi hedeflemektedir.**

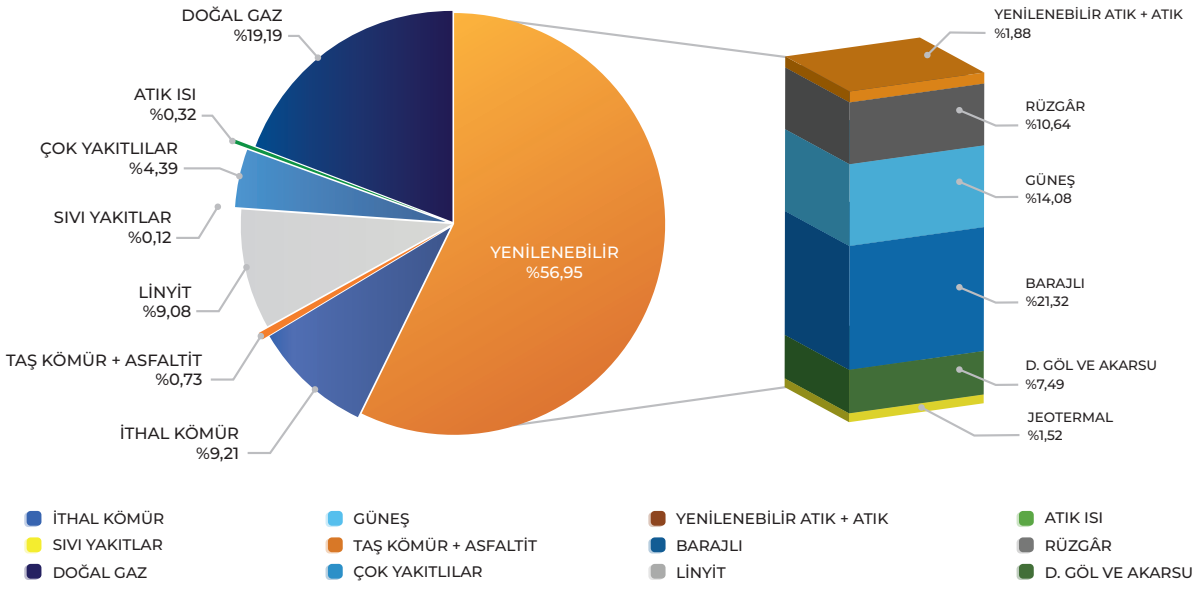
Harita 1: Türkiye'nin Enterkonneksiyon Haritası[1]

Elektrik güç sistemleri; onlarca yıl küçük bir alana hizmet eden düşük güçlü bir jeneratörden "enerji esnekliğini, güvenilirliğini ve ekonomikliğini artırmak, değişen taleplere ve yenilenebilir enerji entegrasyonuna daha kolay uyum sağlamak" amacıyla çok sayıda ülkeyi/kıtayı birbirine bağlayan enterkonnekte bir hâle dönüşmüştür. Türkiye; adı geçen enterkonnekte yapı sayesinde Bulgaristan, Gürcistan, Yunanistan, Suriye, İran ve Irak ile bölgesel enerji paylaşımı yapabilmektedir (bk. Harita 1).

Hayatın birçok alanını etkileyen modern elektrik güç sistemleri; jeneratörler, yükler, iletim hatları, transformatörler, baralar, devre kesiciler, koruma ekipmanları ve diğer çok sayıda bileşenden oluşan insanlığın geliştirdiği en karmaşık sistemlerdendir. Mevcut güç sistemleri; geleneksel enerji kaynaklarının yoğun olduğu bölgelere kurulan, büyük ve sabit güçlü merkezî üretimli yapılar olarak tasarlanmıştır. Bu tasarımda; santrallerde üretilen enerjinin, gerilim düşümleri ve kayıplar dikkate alınarak yüksek gerilim seviyelerinde, kısa veya uzun iletim hatları üzerinden tüketim bölgelerine taşınması planlanmıştır. Bu tasarım ve planlamalar neticesinde enterkonnekte şebekeler, dünya genelinde milyarlarca insana %99,9'un üzerinde güvenilirlikle elektrik enerjisi sağlamaktadır.[2]

Güç elektroniği arayüzüyle yenilenebilir enerji kaynaklarının; güç sistemlerine giderek artan dahli, küçük ve değişken güçlü dağıtık üretimli yapısı, tahmini zor bir üretim profilinin oluşmasına sebep olmaktadır.[3] 2023 sonu itibarıyla küresel yenilenebilir enerji kurulu gücü; 3,87 TW ile toplam kurulu gücün %43,2 seviyelerine ulaşarak bir önceki yıla göre yaklaşık %14,7 artmıştır. Bu kurulu güç, yıllık 8932 TWh enerji üretimiyle toplam üretimin %30,1 seviyelerine ulaşmış ve bir önceki yıla göre %1,3 artış göstermiştir.[4] Türkiye'de ise yenilenebilir enerji kurulu gücü 63,17 GW ile toplam kurulu gücün %57 seviyelerine ulaşarak bir önceki yıla göre %12,8 artmıştır. Türkiye'nin 2023 yılı kurulu gücünün, enerji kaynaklarına göre dağılımı Grafik 1'de gösterilmiştir. Söz konusu kurulu güç; 140,16 TWh enerji üretimiyle toplam üretimin yaklaşık %42,33 seviyelerine ulaşmış ve bir önceki yıla göre %1,68 artış göstermiştir.[5]

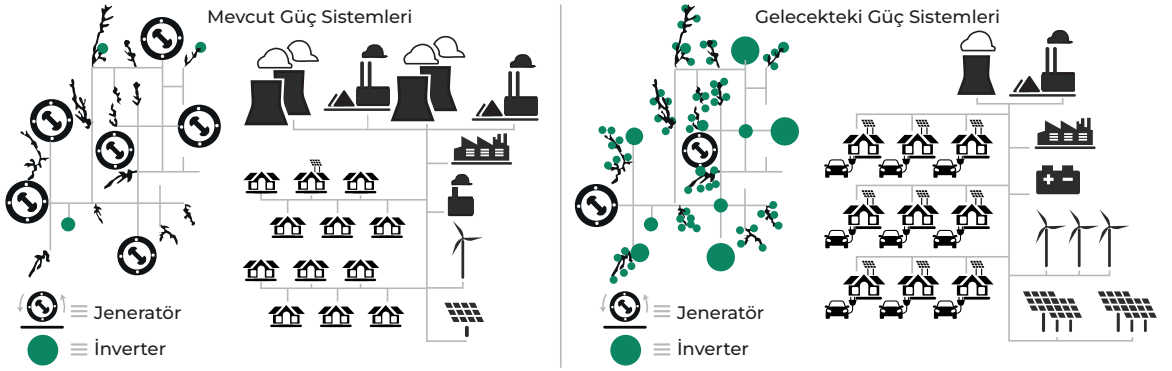
Grafik 1: 2023 Kurulu Gücünün Birincil Enerji Kaynaklarına Göre Dağılımı[6]



Dünyadaki nüfus artışı ve teknolojik gelişmelerle birlikte enerjiye olan ihtiyaçta sürekli bir artış gözlemlenmektedir. Artan enerji talebinin yanı sıra elektronik cihazlar, elektrikli araçlar ve veri merkezlerinin tüketim davranışı gibi ani değişkenlik gösteren enerji tüketim profili; güç sistemlerinin hâlihazırda karmaşık olan yapısına yeni zorluklar getirmektedir. Elektrikli araçlar, 2024 sonu itibarıyla dünyada 17 milyonu, Türkiye'de ise 180.000'i geçmiştir.[7] Uluslararası Enerji Ajansı (UEA; International Energy Agency, IEA) raporuna göre 2030 yılının sonuna kadar dünyada satılan araçların %60'ından fazlasının elektrikli olacağı öngörülmektedir. Buna göre dünyadaki elektrikli otomobil stoku 350 milyon civarına ulaşacaktır.[8] Son 10 yılda, elektrik enerjisi tüketimi üç kat artan ve yapay zekâ temelli yazılımların kullanımını daha da artırdığı veri merkezlerinin; 2030'un sonuna kadar mevcut tüketiminin iki kattan fazla artacağı öngörülmektedir.[9] Bu öngörü, Amerika Birleşik Devletleri (ABD) Enerji Bakanlığı (U.S. Department of Energy) raporlarındaki veri merkezlerinin; 2023'te toplam üretilen elektriğin yaklaşık %4,4'ünü tükettiği ve 2028'e kadar yaklaşık %6,7 ila %12'sini tüketmesinin beklendiği bilgisiyle örtüşmektedir.[10]

Yenilenebilir enerji kaynaklarıyla beslenen sürdürülebilir ve dijitalleşme odaklı enerji dönüşümü, elektrik şebekelerinde köklü değişikliklere yol açmaktadır (bk. Şekil 1). Söz konusu dönüşüm; potansiyel siber saldırı yüzeyi oluşturabilecek akıllı sayaçlar, sensörler ve otomatik kontrol sistemlerine dayanmakta, mevcut şebeke dinamiklerini radikal biçimde değiştirmekte, yeni türden kararsızlıklar ortaya çıkarmakta ve şebeke işletimi, denetimi ile piyasa yapılarının yeniden düşünülmesini gerektirmektedir. Bu bağlamda şebekelerde, daha önce deneyimlenmemiş yeni tehditler ve kırılganlıklar ortaya çıkabilir. Bu nedenle geçmişte yaşanan sistem çökmelerinden çıkarılan dersler, enerji dönüşüm sürecinde yeterli olmayacaktır. Dairesel ataleti yüksek jeneratörlerin domine ettiği, güç elektroniği tabanlı dönüştürücülerin, gelecekte hâkimiyet kazanacağı güç sistemleri Şekil 1'de gösterilmiştir.

Şekil 1: Dairesel Ataleti Yüksek Mevcut Güç Sistemleri ve Düşük Ataletli Gelecekteki Güç Sistemleri[11]

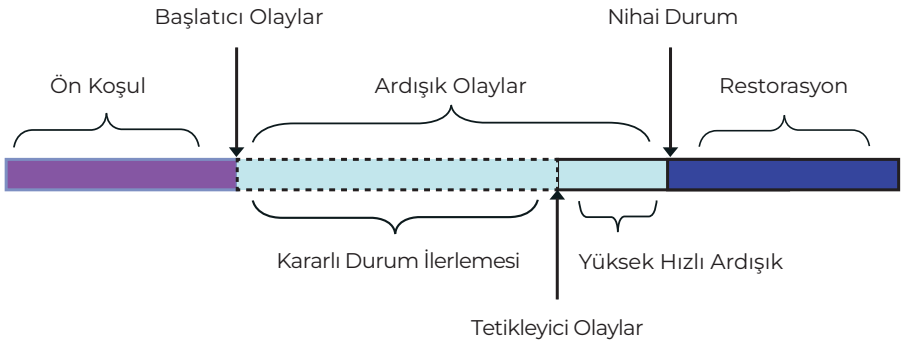


Özetle büyük ölçekli elektrik kesintilerinin etkileri ve önleme yöntemleri; enerjide, yeşil ve dijital dönüşüm ekseninde yenilenebilir enerji kaynaklarını şebekeye bağlayan güç elektroniği ekipmanlarının kontrol yöntemleri; değişken üretim yapısı, değişen tüketici davranış profilleri ve artan siber saldırı riski göz önünde bulundurularak yeniden ele alınmalıdır.

SİSTEM ÇÖKMELERİNİN FAZLARI

Elektrik enerjisine olan talep, artan nüfus ve teknolojik gelişmelerle hızla yükselirken şebeke altyapısına yönelik yatırım yetersizlikleri, sistem güvenilirliğini tehdit etmektedir. Elektrik şebekeleri, yüksek yenilenebilir enerji entegrasyonuna ve modern yüklerin dinamik taleplerine uygun şekilde inşa edilmemiş olup bu durum, çökme risklerini artırmaktadır. Elektrik güç sistemlerinde çökmenin teknik fazları olan "ön koşul, başlatıcı olaylar, ardışık olaylar ve nihai durum ile restorasyon süreçleri" Şekil 2'de gösterilmiştir. Ön koşul fazı, sistemin normal operasyon sınırları içinde çalışmasına rağmen gizli zayıflıklar barındırdığı durumu ifade eder. Yetersiz rezerv kapasitesi, eskiyen altyapı, aşırı yüklenmiş iletim hatları, siber saldırı veya zayıf koordinasyon gibi faktörler; sistemin dış bir tetikleyiciye karşı kırılganlığını artırır. Başlatıcı olaylar, sistemin dengesini bozan ilk arızayı temsil eder. Bir iletim hattının kısa devreye uğraması, jeneratör arızası veya ani talep artışı gibi olaylar; kararlı durum veya geçici durum kararsızlıklarına yol açabilir.

Şekil 2: Elektrik Güç Sistemlerinde Çökmelerin Fazları[12]



Ardışık olaylar, arızanın sistem genelinde yayılmasını ifade eder ve kararlı durum ilerlemesi ile yüksek hızlı ardışık olarak iki alt bölüme ayrılır. Kararlı durum ilerlemesinde, ilk arızadan sonra sistem, yavaş bir şekilde diğer bileşenlere yük kaydırır ve bu süreç dakikalar ölçeğinde ilerleyebilir. Yüksek hızlı ardışık ise koruma sistemlerinin yanlış çalışması veya senkronizasyon kaybı gibi nedenlerle milisaniyeler içinde geniş bir alanı etkiler. Nihai durum, sistemin tam veya kısmi çöküşünü temsil eder. Şebeke, yük talebini karşılayamaz hâle gelir; frekans ve gerilim, kritik sınırların altına düşer; jeneratörler, devre dışı kalır. Restorasyon, sistemin yeniden devreye alınmasını kapsar. Jeneratörler, sırayla senkronize edilir; gerilim ve frekans, kontrollü bir şekilde yükseltilir ve yükler, aşamalı olarak devreye alınır.

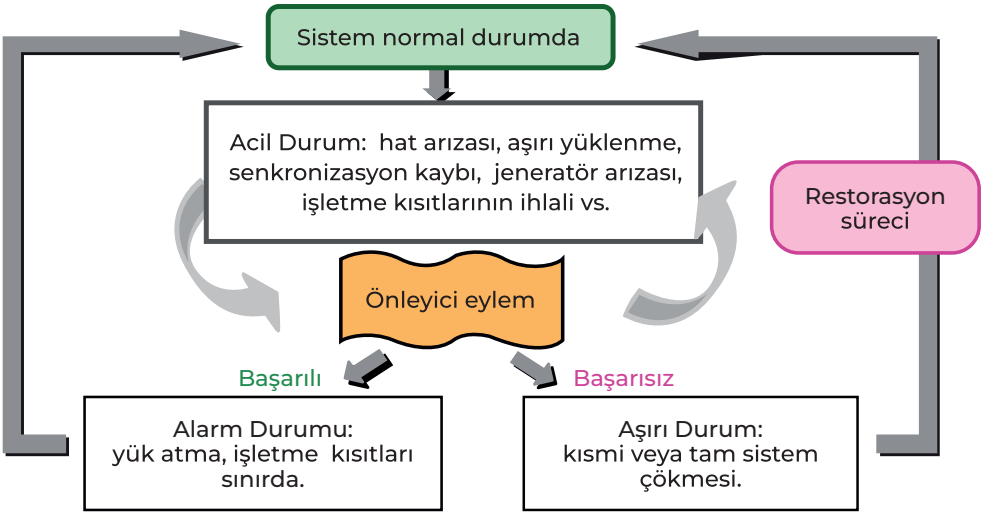
Özetle büyük ölçekli elektrik kesintileri, her zaman bir veya daha fazla başlangıç olayı ile bu olayları kötüleştiren faktörlerin birleşiminden doğar. Söz konusu başlangıç olayları ve kötüleştirici faktörler:

- fırtına, deprem, yıldırım, iletim hattı ile ağaç arasındaki temas vb. doğa olayları,
- kısa devre, ekipman arızası, aşırı yük, kritik ekipmanların bakımı, eskimeye bağlı arızaların teknik sebepleri, anahtarlama hataları ve

- operatörler arasındaki hatalı veya yetersiz iletişim, sabotaj ve acil durumlar için yetersiz eğitim vb. insan etkileri altında kategorize edilir.

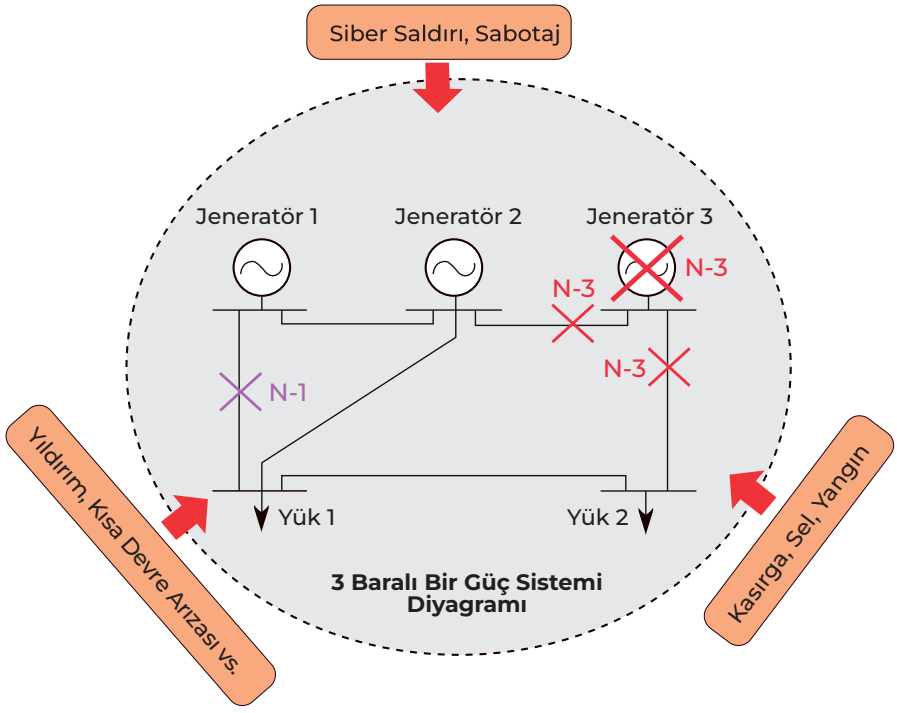
Elektrik güç sistemlerinde yaşanan bozucu etkilere karşı sistem operatörleri; çökmeleri engellemek için Şekil 3'te gösterilen farklı işletme durumlarını yönetmeye ve gerekli önlemleri almaya çalışır.

Şekil 3: Güç Sistemlerinin Operasyon Durumları[13]



Sistem operatörleri; tüm müşterilere elektrik sağlama, frekans, gerilim ve hat akımları gibi tüm sistem değişkenlerinin izin verilen aralıkta kalması kısıtlarını karşıladığında, sistem normal durumda kabul edilir. Bazı değişkenler, limitlerin dışına çıkmasına neden olan bozucu bir etki tarafından tetiklendiğinde ve işletme kısıtları ihlal edildiğinde, sistem acil durumda olur. Operatörün önleyici eylemleri, değişkenleri limitlerin içine geri getirebilirse sistem korunur ve alarm durumuna geçer. Tüm müşterilere elektrik sağlama zorunluluğu tam olarak karşılanmadığında da sistem alarm durumunda kabul edilir. İki kısıtlama aynı anda ihlal edildiğinde, sistem aşırı durumda kabul edilir. Elektrik güç sistemleri, genellikle olasılığı yüksek olarak kabul edilen bozucu etkilere karşı dayanabilecek şekilde tasarlanır. Ancak bu tasarım, aynı zamanda makul maliyetlerle sağlanmak zorundadır. Şebekenin tüm olası senaryolara karşı %100 güvenli çalışması, teknik olarak mümkün olsa bile maliyet açısından son derece yüksek ve pratikte uygulanamazdır. **Şebekeler, işletme maliyetleri ile istenilen güvenlik düzeyi arasında bir denge gözetilerek çalıştırılmaktadır. Bu denge, genellikle "N-1 güvenlik kriteri" ile belirlenir.** Bu kritere göre N adet bileşenden oluşan bir şebeke; herhangi bir anda, bu bileşenlerden herhangi birinin (örneğin bir iletim hattı ya da bir jeneratör) arızalanmasına karşı sistemin çalışmaya devam edebilmesini garanti etmelidir. Elektrik güç sistemlerinde, Şekil 4'te gösterildiği üzere bir ana ekipman kaybı durumunda; N-1 kriteriyle normal şartlarda tekil bir olayın, felaket boyutuna dönüşmesi engellenir.[14]

Şekil 4: N-1 ve N-3 Arıza Örnekleri[15]



Kuzey Amerika Elektrik Güvenilirliği Kurumu (North American Electric Reliability Corporation, NERC) verilerine göre 1984-2006 yılları arasında, en az 50.000 müşteriyi etkileyen elektrik kesintilerinin başlangıç olayları ve kötüleştirici faktörleri incelendiğinde, doğa sebepleri %64 ile ilk sırada gelmektedir. Bunu %22 ile ekipman arızaları ve %8 ile operatör hataları takip etmektedir.[16] Son 25 yılda farklı ülkelerde meydana gelen bazı büyük ölçekli elektrik kesintileri, şebekelerin arızalara karşı kırılganlığı ve bu olayların etkileri Tablo 1'de özetlenmiştir.

Tablo 1: Son 25 Yılda Yaşanan Bazı Sistem Çökmeleri[17]

Yıl	Yer	Ana Sebep	Süre (Saat)	Etkilenen İnsan Sayısı (Milyon)
2003	ABD Kanada	Yazılım hatası, koruma ekipmanlarında hatalı fonksiyon	48	50
2003	Danimarka İsveç	İletim hatlarının aşırı yüklenmesi	6	4
2003	İtalya	Frekans ve gerilim kararsızlıkları	12	55

Yıl	Yer	Ana Sebep	Süre (Saat)	Etkilenen İnsan Sayısı (Milyon)
2006	Almanya Avusturya Bosna Hersek Belçika Bulgaristan İsviçre Çekya İspanya Slovenya Hırvatistan Karadağ Romanya	N-1 kriterinin ihlali, koordinasyon eksikliği	3	15
2009	Brezilya Paraguay	Aşırı hava koşulları	7	60
2012	Hindistan	Aşırı yüklenme, koruma ekipmanlarında hatalı fonksiyon	15	620
2015	Ukrayna	Siber saldırı	6	0,26
2015	Türkiye	Sistem arızası, koordinasyon eksikliği	8	70
2016	Avustralya	Aşırı hava koşulları	6	1,7
2017	ABD	Hava koşulları, koruma ekipmanlarında hatalı fonksiyon	11	21
2019	İngiltere	Yıldırım, sistem arızası	2	1
2019	Endonezya	Enerji üretim santralinde arıza	9	21
2021	Pakistan	Elektrik şebekesindeki arıza	9	200
2021	ABD	Kış fırtınası	6	4
2022	Bangladeş	İletim hattının hatalı koruma durumuna geçmesi	10	140
2025	İspanya Portekiz Fransa	Frekans ve gerilim kararsızlıkları, koordinasyon eksikliği[18, 19]	10	60

Tablo 1'deki verilere ek olarak

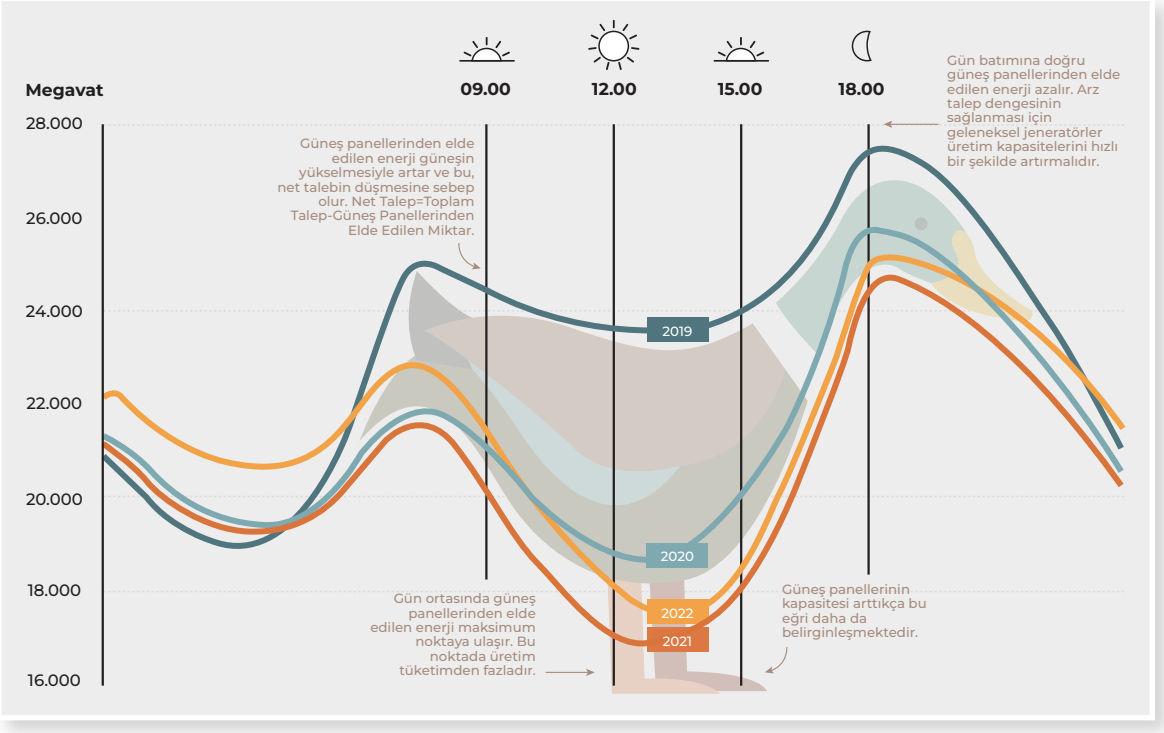
- artan yenilenebilir enerji entegrasyonunun, sistem üzerindeki olumsuz etkilerine pratik çözümler geliştirilemediği,[20]
- son 4 yılda enerji altyapılarını hedef alan siber saldırıların üç kat arttığı ve
- yapay zekâdan destek alınarak hazırlanan bu saldırıların giderek karmaşıklaştığı[21]

hususları göz önüne alındığında, yeni tehditlere karşı yeni önlemler oluşturulması gerekliliği ortaya çıkmaktadır.

YENİLENEBİLİR ENERJİ KAYNAKLARI

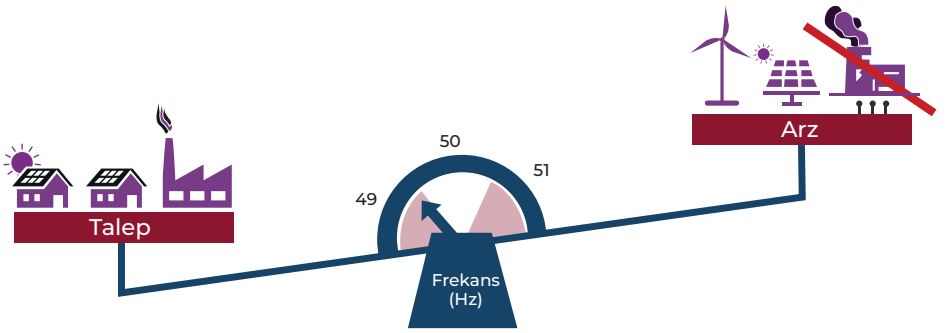
Yenilenebilir enerji kaynaklarının elektrik şebekelerine entegrasyonu; modern enerji sistemlerinin, karbonsuzlaşma hedeflerine ulaşmasında kritik bir rol oynamaktadır. Birçok ülke, teşviklerle yenilenebilir enerji kaynaklarının kullanımdaki payını artıracak hedefler belirlemiştir. Bu geçişin erken aşamalarında yenilenebilir enerji kaynakları, şebeke kararlılığı üzerinde çok az etkiye sahip olmuştur. Düşük katılım seviyeleri nedeniyle gerektiğinde, şebekeye bağlanabilir veya ada modda kullanılmıştır. Ancak yenilenebilir kaynaklar; üretimde ve tüketilen enerjide kullanım payının artmasıyla ve güç akışı planlarındaki değişkenlik, reaktif güç ve sistem ataleti üzerindeki etkisi nedeniyle güç sistemi kararlılığı ve şebeke operatörleri için yeni teknik zorluklar ortaya çıkarmış ve bu durumun büyük ölçekli elektrik kesintisi risklerini artırabileceği görülmüştür.[22] Örneğin yüksek düzeyde güneş enerji santrallerinin entegrasyonunda, elektrik şebekesinde arz talep dengesinin sağlanması açısından (bk. Grafik 2) -özellikle öğle saatlerinde güneş enerjisinin en yüksek düzeye ulaştığı zamanlarda- net talepte meydana gelen belirgin düşüş ve akşam saatlerine doğru üretimin azalmasıyla birlikte net talepte yaşanan ani artış; elektrik şebekesinde ciddi bir baskı oluşturabilir ve konvansiyonel enerji santrallerinin üretim kapasitelerini çok kısa sürede artırmalarını gerektirebilir. Bir diğer önemli sorun, güneş enerji santrallerinin gün ortasında şebekeye anlık tüketimden fazla elektrik enerjisi sunabilme olasılığıdır. Bu aşırı üretim koşullarında, sistemin istikrarını sağlamak amacıyla sistem operatörleri, üretimi kısıtlama yoluna gitmektedir.

Grafik 2: Güneş Enerji Santrallerinin Yüksek Entegrasyonunda Ördek Eğrisine Benzetilen Net Talep Profili[23]



Yenilenebilir enerji kaynaklarından özellikle rüzgâr ve güneş enerjisi, geleneksel senkron jeneratörlere kıyasla farklı dinamik özelliklere sahiptir. Geleneksel termik veya hidroelektrik santraller, şebekeye sabit bir frekans ve gerilim sağlamak için dairesel atalet ve reaktif güç kapasitesi sunarken rüzgâr türbinleri ve güneş panelleri, güç elektroniği ekipmanları ile sisteme bağlanır ve genel olarak düşük veya sıfır atalet oluşturur. Bu durum, sistemin frekans kararlılığını sürdürme kabiliyetini azaltır. Avrupa'da son yıllarda yaşanan büyük ölçekli elektrik kesintileri, arz talep dengesinin sağlanmasında yaşanan zorluklar sebebiyle frekans ve gerilim kararsızlıklarından kaynaklanmıştır (bk. Şekil 5).

Şekil 5: Elektrik Güç Sistemlerinde Frekans Kararlılığında Arz Talep Dengesi[24]



Güneş ve rüzgâr gibi aralıklı yenilenebilir kaynakların payı; geleneksel jeneratörler, kontrol ve koruma ekipmanları baz alınarak tasarlanmış elektrik güç sistemlerinde arttıkça, bu sorunlar belirginleşir.[25] **28 Eylül 2016 tarihinde Avustralya'da meydana gelen elektrik kesintisi, yenilenebilir enerji kaynaklarının yüksek oranda kullanımıyla ilişkilendirilen ilk önemli olay olarak kaydedilmiştir.**[26] Benzer olaylar, Tablo 1'de belirtilen kırılganlıkların üzerine rezerv kapasitesinin eksikliği ve esneklik önlemlerinin yetersizliği nedeniyle 2019 yılında İngiltere'de; 2020 ve 2021 yıllarında sırasıyla ABD'nin Kaliforniya ve Teksas eyaletlerinde yaşanmıştır. İngiltere'de meydana gelen olay; rüzgâr santrallerinin ani üretim kaybı ve düşük sistem ataleti nedeniyle frekansın 48,8 Hz'ye düşmesiyle başlamış, otomatik yük atma mekanizmaları vasıtasıyla daha geniş alana yayılması engellenmiştir.[27]

Benzer şekilde 2020 yılında Avustralya'da, rüzgâr santrallerinin reaktif güç desteğinin yetersiz kalması ve iletim hattı arızasının birleşmesiyle tetiklenmiştir.[28] 2021 yılında ABD'nin Teksas eyaletinde yaşanan olayda, yenilenebilir enerji entegrasyonunun dolaylı etkileri ortaya konulmuştur. Rüzgâr türbinlerinin aşırı soğuklar sebebiyle donması, doğal gaz tedarikindeki aksamalarla birleşerek milyonlarca müşterinin aralıklı olarak günlerce elektriksiz kalmasına yol açmıştır.[29]

Son olarak İspanya'da başlayan, Portekiz ve Fransa'yı da etkileyen sistem çökmesi ele alındığında, tüm detayları yayımlanmamış olmasına rağmen eldeki bilgiler ışığında, yenilenebilir enerjinin şebekedeki payının %70'i geçmemesi önerildiği hâlde olay günü bu oranın %78 civarlarında olması ve bu orana uygun rezerv kapasite sunulamaması dikkat çekmektedir.[30] Burada bazı Avrupa ülkelerinin, 2050 karbon-nötr hedeflerine ulaşmak ve yeşil enerji entegrasyonuna destek vermek adına nükleer

ve kömür yakıtlı termik santralleri devreden çıkarma planlarını uygulamaya koyması;[31] bununla birlikte doğal gaz kombine çevrim santrallerinde üretimin, gaz tedarikinde yaşanan sorunlar[32] nedeniyle sekteye uğraması sonucu, sistem kararlılığının sürdürülmesi konusunda zorluklar yaşanmasında etkili olduğu ifade edilmelidir. Bahsedilen zorlukları aşmak için Almanya ve Belçika; devre dışına almayı planladığı nükleer santrallerden bazılarını, acil durum rezervi olarak belirlemiştir. İngiltere, Fransa, Hollanda ve Polonya ise yeni nükleer santrallerin yapımı için yatırım kararı almıştır.[33]

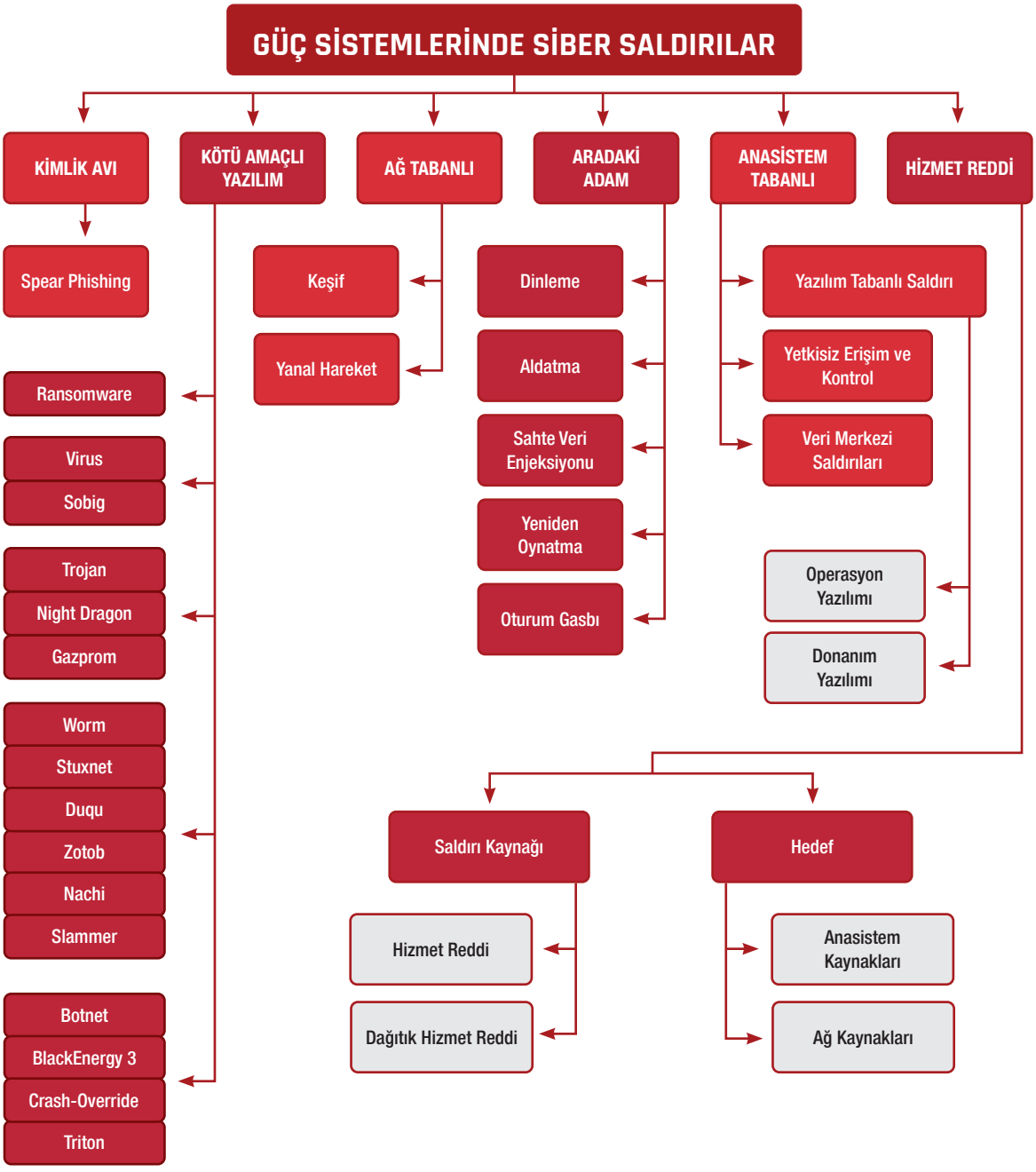
SİBER SALDIRILAR

Enerjide yeşil dönüşüm, yenilenebilir enerji kaynaklarının artan entegrasyonuyla elektrik şebekelerinde değişkenlik ve belirsizlik yaratırken bu durum, dijital dönüşümle desteklenen akıllı şebekelere olan ihtiyacı artırmaktadır. Ancak dijital dönüşümün getirdiği otomasyon ve bağlanabilirlik, siber güvenlik risklerini de artırmaktadır. Enerjide dijital dönüşüm süreci; elektrik güç sistemlerinde, bilgi teknolojisi ve operasyonel teknoloji sistemlerinin birlikte çalışmasını gerekli kılmaktadır. Bu durum, daha iyi izleme ve kontrol imkânı sunarken artan saldırı yüzeyleri sebebiyle siber güvenlik endişelerini de beraberinde getirmektedir. 2015 ve 2016 yıllarında, Ukrayna'nın elektrik güç sistemlerine yönelik siber saldırılarda olduğu gibi birden fazla konumdan gerçekleştirilen karmaşık ve koordineli bir siber saldırı, enterkonnekte sistemin tamamen çökmesine sebep olabilir. UEA; Kasım 2023 tarihli raporunda, dünya genelinde kritik altyapılara yönelik siber saldırıların ortalama sayısının 2020-2022 yılları arasında iki kattan fazla arttığını bildirmiştir.[34]

Elektrik güç sistemlerinin operasyonel dayanıklılığı, yüksek etkili ve düşük olasılıklı olaylar sonrasında enerji arz güvenliğini ve sistemin kararlı çalışmasını sürdürmeyi hedefler. Siber dayanıklılık ise elektrik güç sistemlerinin siber tehditleri öngörme, saldırıların etkisini absorbe etme, bu etkilere uyum sağlama ve hızla toparlanma kapasitesi olarak tanımlanır. "Siber öldürme zinciri" (cyber kill chain) erken aşama keşif faaliyetlerinden saldırı yürütülmesine kadar uzanır ve elektrik kesintilerine, sistem kararsızlığına ve sistem çökmelerine yol açabilir. Elektrik güç sistemi operatörlerine yönelik siber saldırıların öldürme zinciri, genellikle sistemdeki güvenlik açıklarının oltalama e-postaları gibi yöntemlerle yıpratılmasıyla başlar. Kötü amaçlı yazılım; ağ geçitleri açmak ve sistem keşfini, silahlandırmayı ve operasyonel teknoloji sistemlerini hedef almak amacıyla uzaktan erişimi mümkün kılmak için yüklenir. Saldırganlar; bilgi teknolojileri sisteminden operasyonel teknolojiler sistemine erişim yetkilerini ele geçirme, sistemler ve ana bilgisayar arasındaki ağı keşfetme gibi yöntemlerin kullanıldığı "yanal hareketler" gerçekleştirerek elektrik güç sistemleri operasyonlarına erişim sağlayabilir. Böylece saldırganlar; Denetleyici Kontrol ve Veri Toplama (Supervisory Control and Data Acquisition, SCADA) sistemine müdahale edebilir, üretim santralleri ve tüm trafo merkezlerini devre dışı bırakabilir ve kontrol sistemleri aracılığıyla fiziksel hasarlara neden olabilir.[35]

Elektrik güç sistemlerini hedef almak için kullanılabilecek çok sayıda saldırı tekniği bulunmakla birlikte bu tür saldırılar "kimlik avı, kötü amaçlı yazılım, ağ tabanlı, aradaki adam, anasistem tabanlı ve hizmet reddi saldırıları" olmak üzere altı kategoride sınıflandırılabilir. Elektrik güç sistemlerine yönelik, siber saldırıların sınıflandırılması Şekil 6'da özetlenmiştir.

Şekil 6: Elektrik Güç Sistemlerinde Siber Saldırı Türleri[36]



- Kimlik avı; sahte e-postalar veya linkler aracılığıyla hassas bilgilerin çalınması veya kötü amaçlı yazılımların yüklenmesini içerir. "Spear phishing" ise belirli hedeflere yönelik kişiselleştirilmiş sızma girişimlerini kapsamaktadır.

- Gelişmiş kötü amaçlı yazılımların özellikle solucanlar ve botnetlerin, kontrol edilebilirlik özellikleri sayesinde modern siber saldırı vektörleri olarak kullanımları giderek artmaktadır. Ayrıca bağımsız olarak yayılma yetenekleri sayesinde, endüstriyel kontrol sistemlerini hedef alan saldırganlar tarafından tercih edilen siber silahlar hâline gelmiştir.
- Güç şebekelerine yönelik bir siber saldırı bağlamında ağ keşfi süreci, hedef sistemlerin ve kullanılan haberleşme protokollerinin belirlenmesinde temel öneme sahiptir. Yanal hareket ise hedef alınan iletişim altyapısı içinde saldırganın sistemler arası geçiş yaparak ağ üzerinde ilerlemesini ve nihai hedefe ulaşmasını sağlayan aşamalı bir siber saldırı tekniğidir.
- Aradaki adam saldırıları, saldırganın iki iletişim noktası arasına gizlice girerek veri trafiğini izlemesi veya değiştirmesiyle gerçekleştirilen bir siber saldırı türüdür. Aradaki adam saldırıları "dinleme, aldatma, sahte veri enjeksiyonu, yeniden oynatma ve oturum gasbı" olmak üzere farklı saldırı türlerini içermektedir.
- Anasistem tabanlı saldırılar; SCADA sunucuları ve insan-makine arayüzleri, veri tabanları, uygulama sunucuları, uzak uç birimleri, koruma röleleri gibi bileşenleri "yazılım tabanlı saldırılar, veri tabanı saldırıları, yetkisiz erişim ve kontrol saldırılarıyla" ele geçirmeyi hedefler.
- Hizmet reddi saldırıları; ağ bağlantıları, iş kapasitesi, uygulama hizmetleri gibi sistem kaynaklarına meşru kullanıcıların erişimini engellemeyi hedefler. Dağıtık hizmet reddi saldırılarında ise saldırı, birçok farklı kaynaktan eş zamanlı yürütülerek saldırının etkisi artırılır ve tespiti zorlaştırılır.

Elektrik güç sistemlerine yönelik siber saldırıların; 2003 yılında ABD'nin Ohio eyaletinde bulunan Davis-Besse Nükleer Güç Santralinin kontrol ağlarına erişmek amacıyla Microsoft SQL sunucusuna kötü amaçlı yazılımın enjekte edildiği olayla başladığı kabul edilir. **Enjekte edilen kötü amaçlı yazılım, kurumsal ve kontrol ağları arasındaki iletişim ağlarını kesintiye uğratmak için büyük miktarda veri trafiği üretmiş ve denetleme sistemini 5 saatten fazla işlevsiz hâle getirerek çekirdek sıcaklık sensörlerinin takip edilmesini engellemiştir. 2010 yılındaki Stuxnet saldırısı, İran'ın Natanz Nükleer Zenginleştirme Tesislerindeki programlanabilir mantık denetleyicilerini manipüle ederek santrifüjlerin anormal çalışmasına yol açmış ve bu süreçte, sistemin durum tahminini bozarak 984 santrifüjün fiziksel olarak hasar görmesine neden olmuştur.** 2014 yılında Güney Kore'nin nükleer enerji santrallerini işleten firma ise bilgisayar sistemlerine yönelik bir siber saldırı gerçekleştiğini bildirmiştir.[37]

2015 yılında Ukrayna'da, elektrik güç sistemleri operatörünün bilgi teknolojileri sistemlerine yönelik bir siber saldırı düzenlenmiştir. Saldırı; oltalama e-postaları, kötü amaçlı yazılım operasyonları ve kimlik avı gibi yöntemler kullanılarak gerçekleştirilmiştir. Saldırının başlangıç noktası, sistem operatörlüğü çalışanlarının hedef alındığı oltalama e-postaları olmuştur. Saldırganlar, içine makrolar yerleştirdikleri Microsoft Office dosyalarının olduğu e-postalar ve BlackEnergy 3 adlı kötü amaçlı yazılım vasıtasıyla elektrik güç sistemlerine sızmayı başarmıştır. Bu sızma, SCADA sistemine erişmek ve kontrol etmek için uzaktan masaüstü oturumu başlatılana kadar tespit edilememiştir. Daha sonra SCADA kullanıcı arayüzü üzerinden çok sayıda devre kesici anahtar açılmıştır. Ukrayna sistem operatörlüğü çalışanlarının çaresizce izlemek zorunda kaldığı bu saldırı, 7 adet 110 kV ve 23 adet 35 kV trafo merkezini devre dışı bırakmış ve yaklaşık 225.000 kişiyi etkileyen bir elektrik kesintisine yol açmıştır. Bu olay, elektrik güç sistemleri

operasyonlarını doğrudan etkileyen ilk siber saldırı örneği olmuştur. 2016 yılında yine Ukrayna'yı hedef alan haberleşme protokollerindeki güvenlik açıklarını kullanan, daha gelişmiş ve karmaşık bir siber saldırı düzenlenmiştir. Özellikle IEC 101, IEC 104 ve IEC 61850 gibi haberleşme protokollerinin hedef alındığı bu saldırıda "Crash-Override/Industroyer" kötü amaçlı yazılımı kullanılarak endüstriyel kontrol sistemleri yazılımının manipüle edilmesi sağlanmıştır. Bu protokoller ve mesajlar üzerinde yapılan değişiklikler, saldırganların devre kesicilerin durumu gibi fiziksel parametreleri etkilemesine olanak tanımıştır. 2015 yılında yapılan saldırıya kıyasla etkisi sınırlı kalan bu saldırı, kullanılan yöntem itibarıyla ileri düzey bir siber saldırının güç sistemleri üzerinde yıkıcı etkiler yaratabileceği ihtimalini göstermiştir.[38]

2019 yılında Hindistan'ın Kudankulam Nükleer Güç Santralinde gerçekleşen saldırı, internet ağına bağlı bir kişisel bilgisayarda veri hırsızlığı ve sistem izleme yetenekleriyle bilinen "Dtrack" kötü amaçlı yazılımının tespit edilmesiyle ortaya çıkmıştır. 9 Mart 2020 tarihinde Avrupa Elektrik İletim Sistemi İşletmecileri (European Network of Transmission System Operators for Electricity, ENTSO-E) ağının bir siber saldırıyla ihlal edildiği bildirilmiştir.[39] 12 Mayıs 2020 tarihinde, İngiltere'de tevzi merkezi olarak faaliyet gösteren kurumun bilgi teknolojileri sistemi, siber saldırıya uğramıştır. 12 Ekim 2020 tarihinde Hindistan'ın Mumbai şehrinde, elektrik güç sistemlerinde kötü amaçlı yazılım kullanılarak şehir 12 saatten fazla elektriksiz bırakılmıştır.[40] Mart 2022'de, Hindistan'ın Ladakh bölgesine yakın elektrik dağıtım merkezlerini hedef alan iki siber saldırı girişimi rapor edilmiştir. Nisan 2022'de Almanya'da gerçekleştirilen kötü amaçlı bir yazılım, haberleşme sistemlerini hedef almış; yaklaşık 2.000 rüzgâr türbininin denetleme ve kontrol kabiliyeti sekteye uğratılmıştır.

SONUÇ VE ÖNERİLER

SONUÇ VE ÖNERİLER

Enerjide dijital dönüşüm; elektrik şebekelerindeki verimliliği, esnekliği, güvenilirliği ve yenilenebilir enerji payını "akıllı şebekeler, nesnelerin interneti, yapay zekâ, blokzincir, veri analitiği, bulut bilişim" gibi teknolojileri kullanarak artırmayı hedeflemektedir. Bu sürecin elektrik güç sistemlerinde başarılı bir şekilde yürütülmesi; enerji arz güvenliğinin güvence altına alınması, karbon emisyonlarının ve maliyetlerin azaltılması açısından kritik bir öneme sahiptir. **Dünya genelinde yaşanan doğal afetlerin sebep olduğu büyük ölçekli elektrik kesintilerindeki artış; eskiyen altyapı, artan enerji talebi ve yük profilindeki değişiklikler düşünüldüğünde, enerjide dijital ve yeşil dönüşüm sürecinin getirdiği tehditler haricinde "elektrik güç sistemlerinin daha dayanıklı hâle getirilmesi için yeni yatırımlara ihtiyaç olduğu" bir gerçektir.** Bu duruma göre

- eski kontrol ve koruma ekipmanlarının modern ekipman ve tasarımlarla değiştirilmesi,
- enerji santrali ve trafo merkezi ekipmanlarının düzenli bakımının yapılması ve tasarım parametreleri dâhilinde çalışması için gerekli ayarlamaların yapılması,
- düşük gerilim ve frekansta otomatik yük atma gibi koordineli acil durum kontrol mekanizmalarının geliştirilmesi,
- aşırı yüklenmeleri yönetmek, dinamik güç akışı kontrol kabiliyetini ve şebeke kararlılığını artırmak için esnek alternatif akım iletim sistemlerinin (Flexible AC Transmission Systems, FACTS) ilgili yerlerde kullanımının sağlanması,
- gerçek zamanlı anlık durum kestirim, denetleme ve kontrol sistemlerinin yaygınlaştırılması,
- şebeke bütünlüğünü koruma planlarıyla (System Integrity Protection Schemes, SIPS) donatılmış geniş alan gözlemleme, koruma ve kontrol sistemlerinin (Wide-Area Monitoring, Protection and Control, WAMPAC) entegre edilmesi teşvik edilmelidir.

Akıllı ve karbonsuz şebekelere geçişte, dijital-yeşil enerji dönüşümünün getirdiği tehditleri en aza indirmek için aşağıda belirtilen hususlara dikkat edilmelidir:

- **Rüzgâr ve güneş gibi meteorolojik olaylara bağlı yenilenebilir enerji entegrasyonunun yüksek olduğu bölgelerde üretim öngörülebilirliğini artıracak yüksek doğruluklu tahmin modellerinin oluşturulması; anlık üretim dalgalanmalarına bağlı oluşabilecek arz talep dengesizliklerini sönümleyecek enerji depolama sistemlerinin yaygınlaştırılması gerekmektedir.** Burada pompaj depolamalı hidroelektrik santrallerinin birçok açıdan kimyasal enerji depolama sistemlerine göre daha avantajlı olduğu, özellikle yenilenebilir enerji kaynaklı arz fazlası oluştuğu durumlarda ve ördek eğrisi örneğinde gösterildiği üzere net talepteki ani artış anlarında çözüm sunabileceği bilinmelidir.
- Sistem operatörlerinin planlama kabiliyetlerini güçlendirmek, şebeke operasyonlarını yönetmek ve sürdürülebilirliği sağlamak için elektromanyetik transient şebeke modelleri ve optimizasyon algoritmaları geliştirilmelidir.

- Gerilim-frekans kararsızlıklarını ortadan kaldıracak, düşük ve yüksek gerilim arızalarında (low voltage ride through ve high voltage ride through) operasyon sürekliliğini sağlayacak, senkron jeneratör atalet regülasyon davranışlarını taklit ederek (virtual synchronous generator) şebekeye sentetik atalet sağlayacak ve şebeke dinamiklerini şekillendirebilen (grid forming) kontrol stratejilerinin entegre edildiği güç elektroniği araçlarının kullanımı; üretim profili meteorolojik olaylara bağlı olarak değişen yenilenebilir enerji kaynaklarının entegrasyonunda artırılmalıdır. Üretim profili daha öngörülebilir olan yenilenebilir kaynakların şebekeye entegrasyonunda, maliyeti daha uygun olan şebeke dinamiklerini takip eden (grid following) güç elektroniği araçları tercih edilmelidir.
- Tüketim noktalarına uzak mesafede tesis edilen yenilenebilir enerji kaynaklarından üretilen enerji, sisteme yüksek gerilim doğru akım (High Voltage Direct Current, HVDC) iletim hatları üzerinden entegre edilmelidir. Değişen yük profilleri ve kullanıcı davranışlarının yönetimi, akıllı sayaçlar ve dinamik fiyatlandırma kullanılarak talep tarafı yönetim sistemleri geliştirilmeli ve talep esnekliği desteklenmelidir.
- Elektrik güç sistemlerinin siber güvenli olması için öncelikle mevcut Modbus, IEC 61850 ve DNP3 gibi haberleşme protokollerinin şifrelenmesi; **çok faktörlü kimlik doğrulama ve erişim kontrolü aşamalarının IEC 62351 ve IEC 62443 standartlarıyla uyumlu hâle getirilmesi gerekmektedir.**
- En ciddi siber saldırı yöntemi olan "yanlış veri enjeksiyonunu" engellemek için yapay zekâ destekli gerçek zamanlı anomali tespit algoritmaları geliştirilmeli ve uygulanmalıdır.
- Sistem koruma ekipmanları, siber-fiziksel saldırılara karşı yedekli kontrol mekanizmaları ve yedekleme kabiliyetleriyle donatılmalıdır.
- Aralıklı olarak güç sistemlerinde siber-fiziksel stres testi simülasyonları yapılmalı ve gerekli kırılganlıklar tespit edilerek şebeke güçlendirilmelidir.
- Sistem operatörlerinin, siber güvenlik tehditlerini tanır ve hızlı müdahale protokollerini uygular hâle gelebilmesi için eğitim ve farkındalık programları düzenlenmelidir.
- Şebeke operatörleri arasında bölgesel ve uluslararası iş birliği, siber tehdit istihbarat paylaşımına ve koordineli yanıt mekanizmalarının geliştirilmesine olanak sağlayacak şekilde geliştirilmelidir.
- Dijital ve yeşil dönüşümün getirdiği yeni tehditlere karşı geliştirilen önleme yöntemleri, yerli imkânlarla geliştirilmelidir. Enerji bağımsızlığı için gerçekleştirilen bu sürecin, beraberinde teknolojik bağımlılığı getirmemesi için özel bir çaba gösterilmelidir.

KAYNAKÇA

KAYNAKÇA

1 Enterkonneksiyonlar Uluslararası İletim Hatları, TEİAŞ, Erişim Adresi: https://www.teias.gov.tr/enterkonneksiyonlar [Erişim Tarihi: 22.05.2025].

2 Paul Hines, Karthikeyan Balasubramaniam and Eduardo Cotilla Sanchez, Cascading Failures in Power Grids, IEEE Potentials, 28/5, (2009): 24-30, 10.1109/MPOT.2009.933498

3 Florin Capitanescu, Are we Prepared Against Blackouts During the Energy Transition?, IEEE Power and Energy Magazine, 21/3, (2023): 77-86, 10.1109/MPE.2023.3247053

4 Renewables 2023 Analysis and Forecast to 2028, International Energy Agency, Erişim Adresi: https://www.iea.org/reports/renewables-2023/executive-summary [Erişim Tarihi: 24.05.2025].

5 Enerji Bilgi Merkezi - Elektrik, T.C. Enerji ve Tabii Kaynaklar Bakanlığı, Erişim Adresi: https://enerji.gov.tr/bilgi-merkezi-enerji-elektrik [Erişim Tarihi: 22.05.2025].

6 Elektrik İstatistikleri, TEİAŞ, Erişim Adresi: https://www.teias.gov.tr/turkiye-elektrik-uretim-iletim-istatistikleri [Erişim Tarihi: 25.08.2025].

7 EVs to reach 25% of global car sales this year, potential China emissions peak and other nature and climate news, World Economic Forum, Erişim Adresi: https://www.weforum.org/stories/2025/05/evs-reach-quarter-global-car-sales-2025-nature-climate-news/ [Erişim Tarihi: 25.08.2025]; Türkiye's registered electric vehicles soar nearly 130% in 2024, Anadolu Ajansı, Erişim Adresi: https://www.aa.com.tr/en/energy/electricity/turkiye-s-registered-electric-vehicles-soar-nearly-130-in-2024/47077 [Erişim Tarihi: 25.08.2025].

8 Türkiye'nin Şebeke Altyapısı 11 Yıl Sonra 11 Milyon Elektrikli Araca Hazır Olmalı, SHURA Enerji Dönüşümü Merkezi, Erişim Adresi: https://shura.org.tr/wp-content/uploads/2024/07/SHURA-Basin-Bulteni-Ulastirma-Sektoru-Donusumu-10-Temmuz-2024.pdf [Erişim Tarihi: 24.05.2025].

9 Energy and AI, International Energy Agency, Erişim Adresi: https://www.iea.org/reports/energy-and-ai [Erişim Tarihi: 25.05.2025].

10 Evaluating Increase in Electricity Demand from Data Centers, U.S. Department of Energy, Erişim Adresi: https://www.energy.gov/articles/doe-releases-new-report-evaluating-increase-electricity-demand-data-centers [Erişim Tarihi: 25.05.2025].

11 Technical Roadmap Guides Research Direction for Grid-Forming Inverters, The National Renewable Energy Laboratory, Erişim Adresi: https://www.nrel.gov/news/detail/program/2020/technical-roadmap-guides-research-direction-grid-forming-inverters [Erişim Tarihi: 25.05.2025].

12 Kai Strunz ve Feng Gao, Computer Simulation of Scale-Bridging Transients in Power Systems, Handbook of Electrical Power System Dynamics, ed. Mircea Eremia and Mohammad Shahidehpour, (IEEE Press, 2013), 900-927.

13 Alberto Borghetti, Carlo Alberto Nucci ve Mario Paolone, Restoration Process after Blackouts, Handbook of Electrical Power System Dynamics, ed. Mircea Eremia and Mohammad Shahidehpour, (IEEE Press, 2013), 864-899.

14 Yvon Besanger, Mircea Eremia, ve Nikolai Voropai, Major Grid Blackouts: Analysis, Classification, and Prevention, Handbook of Electrical Power System Dynamics, ed. Mircea Eremia and Mohammad Shahidehpour, (IEEE Press, 2013), 789-863.

[15] Florin Capitanescu, Are we prepared against blackouts during the energy transition?.

[16] A. Gholami, F. Aminifar ve M. Shahidehpour, Front Lines Against the Darkness: Enhancing the Resilience of the Electricity Grid Through Microgrid Facilities, IEEE Electrification Magazine, 4/1, (2016): 18-24, 10.1109/MELE.2015.2509879

[17] V. S. Rajkumar, A. Ștefanov, A. Presekal, P. Palensky ve J. L. R. Torres, Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures, IEEE Access, 11, (2023): 103154-103176, 10.1109/ACCESS.2023.3317695

[18] Iberian Peninsula Blackout, ENTSOE, Erişim Adresi: https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/ [Erişim Tarihi: 22.06.2025].

[19] Miscalculation by Spanish Power Grid Operator REE Contributed to Massive Blackout, Report Finds, Reuters, Erişim Adresi: https://www.reuters.com/business/energy/investigation-into-spains-april-28-blackout-shows-no-evidence-cyberattack-2025-06-17/ [Erişim Tarihi: 23.06.2025].

[20] The Impact of Renewable Energy on the Electric Power Grid, Yes Energy, Erişim Adresi: https://blog.yesenergy.com/yeblog/the-impact-of-renewable-energy-on-the-electric-power-grid [Erişim Tarihi: 27.05.2025].

[21] L. Gurina, T. Zoryna ve N. Tomin, Risk Assessment for Digitalization of Facilities of Cyber-Physical Energy System, 2022 International Ural Conference on Electrical Power Engineering (UralCon), (2022): 86-90, 10.1109/UralCon54942.2022.9906686

[22] J. Zhao, F. Li, Q. Zhang, Impacts of Renewable Energy Resources on the Weather Vulnerability of Power Systems, Nature Energy, 9, (2024), 1407-1414, 10.1038/s41560-024-01652-1

[23] Confronting the Duck Curve: How to Address Over-Generation of Solar Energy, U.S. Department of Energy, Erişim Adresi: https://www.energy.gov/eere/articles/confronting-duck-curve-how-address-over-generation-solar-energy [Erişim Tarihi: 25.05.2025].

[24] S. Impram, S. V. Nese ve B. Oral, Challenges of Renewable Energy Penetration on Power System Flexibility: A Survey, Energy Strategy Reviews, 31, (2020): 1-12, 10.1016/j.esr.2020.100539s

[25] Renewable Energy Boom Risks More Blackouts Without Adequate Investment in Grid Reliability, FORBES, Erişim Adresi: https://www.forbes.com/sites/michaelshellenberger/2021/04/20/why-renewables-cause-blackouts-and-increase-vulnerability-to-extreme-weather/ [Erişim Tarihi: 30.06.2025].

[26] R. Yan, N.A. Masood, T. Kumar Saha, F. Bai ve H. Gu, The Anatomy of the 2016 South Australia Blackout: A Catastrophic Event in a High Renewable Network, IEEE Trans. Power Syst., 33/5, (2018): 5374–5388, 10.1109/TPWRS.2018.2820150

[27] Technical Report on the Events of 9 August 2019, National Grid Electricity System Operator, Erişim Adresi: https://www.neso.energy/document/152346/download [Erişim Tarihi: 30.06.2025].

[28] South Australia Renewable Integration Incident Report, Australian Energy Market Operator, Erişim Adresi: https://aemo.com.au/media/files/electricity/nem/security_and_reliability/reports/renewable_energy_integration_in_south_australia_aemo_electranet_report_oct_2014.pdf [Erişim Tarihi: 30.06.2025].

[29] Review of February 2021 Extreme Cold Weather Event, Electric Reliability Council of Texas Report, Erişim Adresi: https://www.ercot.com/files/docs/2021/02/24/2.2_REVISED_ERCOT_Presentation.pdf [Erişim Tarihi: 30.06.2025].

---

[30] Iberian Blackout may have been Caused by Nuclear Phase-out, Cyberattack: Expert, Anadolu Ajansı, Erişim Adresi: https://www.aa.com.tr/en/europe/iberian-blackout-may-have-been-caused-by-nuclear-phase-out-cyberattack-expert/3553376 [Erişim Tarihi: 23.06.2025].

[31] These 10 Countries Are Phasing Out Coal the Fastest, World Resources Institute, Erişim Adresi: https://www.wri.org/insights/countries-phasing-out-coal-power-fastest [Erişim Tarihi: 25.06.2025].

[32] Avrupa Birliği Enerji Güvenliğinde Yeni Tehditler Dönemi, Türk Asya Stratejik Araştırmalar Merkezi, Erişim Adresi: https://tasam.org/tr-TR/Icerik/72507/avrupa_birligi_enerji_guvenliginde_yeni_tehditler_donemi [Erişim Tarihi: 27.06.2025].

[33] Plans For New Reactors Worldwide, World Nuclear Association, Erişim Adresi: https://world-nuclear.org/information-library/current-and-future-generation/plans-for-new-reactors-worldwide [Erişim Tarihi: 27.06.2025].

[34] Cybersecurity is the Power System Lagging Behind?, International Energy Agency, Erişim Adresi: https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind [Erişim Tarihi: 25.06.2025].

[35] Voropai, N. I., Kolosok, I. N., Korkina, E. S., & Osak, A. B. Issues of Cybersecurity in Electric Power Systems, Energy Systems Research, 3/2 (2020): 19-28, 10.38028/esr.2020.02.0003

[36] Presekal, A., Rajkumar, V. S., Ștefanov, A., Pan, K., & Palensky, P., Cyberattacks on Power Systems, Smart Cyber-Physical Power Systems: Fundamental Concepts, Challenges, and Solutions, 1, (2025): 365-403, Erişim Adresi: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781394191529.ch15 [Erişim Tarihi: 30.06.2025].

[37] Tatipatri, N., & Arun, S. L., A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection and Cyber Security, IEEE Access, 12, (2024): 18147-18167, Erişim Adresi: https://ieeexplore.ieee.org/document/10418207 [Erişim Tarihi: 30.06.2025].

[38] H. Zhang, B. Liu and H. Wu, Smart Grid Cyber-Physical Attack and Defense: A Review, IEEE Access, 9, (2021): 29641-29659, Erişim Adresi: https://ieeexplore.ieee.org/document/9352761 [Erişim Tarihi: 30.06.2025].

[39] ENTSO-E Has Recently Found Evidence of a Successful Cyber Intrusion into its Office Network, ENTSOE, Erişim Adresi: https://www.entsoe.eu/news/2020/03/09/entso-e-has-recently-found-evidence-of-a-successful-cyber-intrusion-into-its-office-network/ [Erişim Tarihi: 30.06.2025].

[40] Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group, Recorded Future, Erişim Adresi: https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf [Erişim Tarihi: 25.06.2025].

ENERJİ GÜVENLİĞİ VE DİJİTAL-YEŞİL DÖNÜŞÜM: AKILLI VE KARBONSUZ ŞEBEKELERE GEÇİŞ

EYLÜL 2025