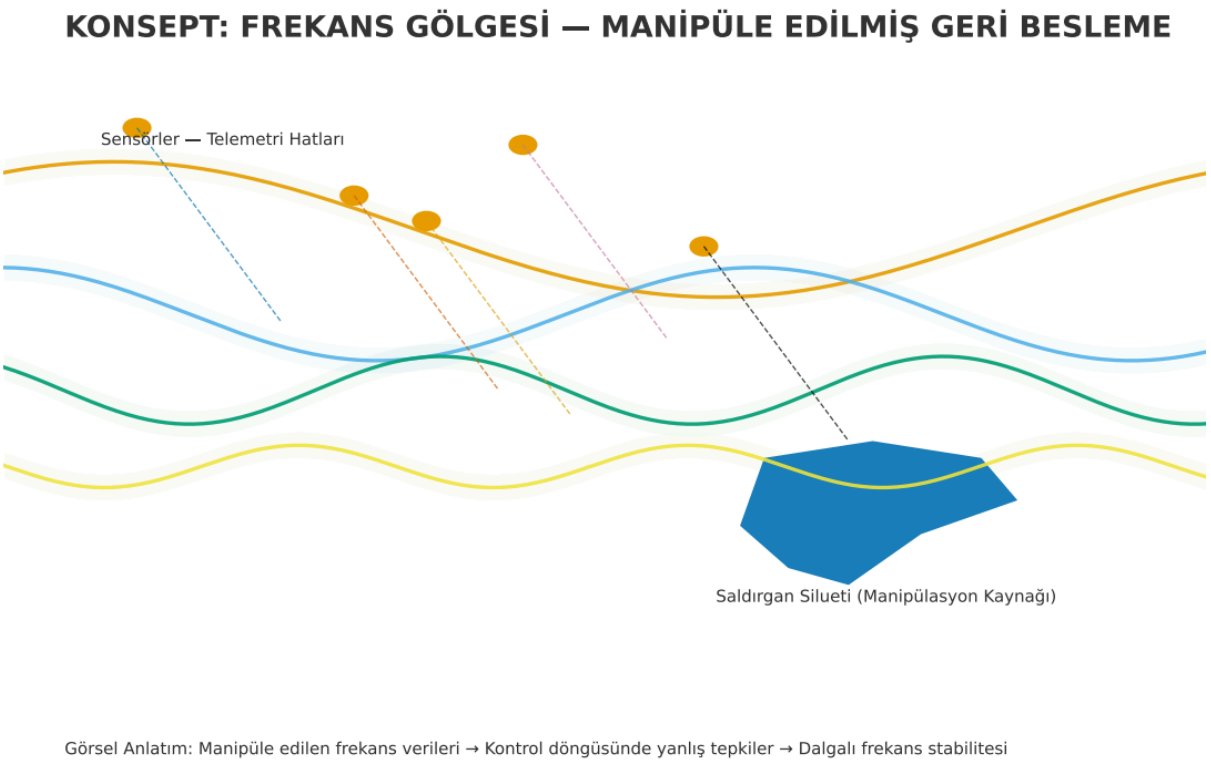
Tarih: 08.11.2025
Versiyon: 2.0
Hazırlayan: Adile Nur Yiğit



Görsel Anlatım: Manipüle edilen frekans verileri → Kontrol döngüsünde yanlış tepkiler → Dalgalı frekans stabilitesi

ANOMALİ SENARYOSU:FREKANS GERİ BESLEME MANİPÜLASYONU (v2.0)

(Detaylı Senaryo, STRIDE Analizi, Adım-adım Akış, Tespit ve Azaltma Önerileri)

1. **Senaryonun Amacı ve Kapsamı**
   Amaç:
   Bu senaryonun temel amacı, modern güç sistemlerinde frekans kontrolü yapan sensörlerden gelen ölçüm verilerinin kötü niyetli biçimde manipüle edilmesi (spoofing/tampering)
   sonucunda kontrol döngülerinin nasıl yanlış kararlar verdiğini ve bunun elektrik şebekesi ile inverter kontrollü kaynaklar (IBR) üzerindeki etkilerini ayrıntılı olarak modellemektir.
   Senaryo, sadece sensör verilerinin değiştirilmesini değil; değişen kontrol tepkilerinin fiziksel sonuçlarını, merkezi dengeleme (CRED gibi)
   algoritmalarının devreye girdiğinde oluşabilecek etkileşimleri ve olası siber-fiziksel zincirleme etkileri de kapsar.

Kapsam:

- Frekans ölçümü yapan saha sensörleri, PMU'lar (Phasor Measurement Unit) ve RTU'lar.

- İletişim katmanı: SCADA, IEC 61850, MQTT, hatta zayıf konfigüre edilmiş HTTP/REST bağlantıları.

- IBR (Inverter Based Resources): Güneş, rüzgâr, batarya depolama ve mikro-yönetim birimleri (microgrid controller) dahil.

- Merkezi regülasyon mekanizmaları: CRED (Control and REstoration Dynamics), AGC (Automatic Generation Control) ve dağıtık droop kontrolü.

- Fiziksel katman: sensörlerin fiziksel donanımı, zaman senkronizasyonu (GPS/GNSS) ve saha sayaçları.

- Siber güvenlik bileşenleri: kimlik doğrulama, şifreleme, zaman damgası doğrulama ve telemetri bütünlüğü kontrolleri.

2. **Özet (Kısa ve Net Tanım)**
   "Frekans Gölgesi" adını verdiğimiz bu saldırı, frekans geri beslemesi sağlayan sensörlerin çıktılarının manipüle edilmesiyle şebeke kontrol döngülerinin yanlış kararlar üretmesini sağlayan ileri düzey bir siber-fiziksel saldırıdır.
   Saldırganın amacı, frekansın gerçekte olması gereken yönden ters bir kontrol tepkisi tetiklemektir (örneğin, üretim artırılması gereken yerde üretimin kısılmasına sebep olmak).
   Bu manipülasyon, sensör verilerinin sahte veya gecikmeli raporlanması, zaman damgası bozulması veya rastgele/pattern tabanlı sapmalar ile sağlanabilir.
   Sonuç olarak frekans sapmaları dalgalı hale gelir, IBR'lerin droop denklemleri sık sık ve düzensiz biçimde yeniden ayarlanır ve sistem stabilizasyonu zorlaşır. Merkezi dengeleme (CRED/AGC) mekanizmaları müdahale etmeye çalışırken gecikmeler ve hatalı düzeltmeler yaşanır.

3. **STRIDE Tehdit Sınıflandırması (Senaryoya Özgü Örneklerle)**
   - Spoofing (Taklit Etme):

- Saldırgan, sahadaki frekans sensörünün kimliğini taklit ederek kontrol sistemine yanlış frekans değeri gönderir.

- Örnek: PMU kimlik bilgileri ele geçirilir veya MitM ile veri akışı taklit edilir; bu sayede 49.70 Hz değeri yerine 50.30 Hz raporlanır.
   - Tampering (Kurcalama/Manipülasyon):

- Sahadan gelen frekans ölçüm paketleri, iletişim hattında değiştirilir veya sensör üzerindeki firmware'e müdahale edilerek ölçüm sonuçları sistematik olarak önyüklenir.

- Örnek: Ölçülen frekans değerine periyodik pozitif/negatif bias uygulanması.
   - Repudiation (İnkar):

- Saldırgan, izleri silme veya log'ları değiştirme yeteneğine sahipse gerçekleştirdiği eylemleri inkar edebilir; olay sonrası adli kanıtların güvenilirliği zarar görür.
   - Information Disclosure (Bilgi Açığa Çıkması):

- Saldırgan, ağ trafiğini dinleyerek kontrol stratejileri, droop ayarları ve merkezi parametreler hakkında bilgi toplayabilir; ileriki adımlar için avantaj sağlar.
   - Denial of Service (Hizmet Engelleme):

- Frekans verilerinin sistemlere iletilmesini geciktirecek veya tamamen engelleyecek bir DoS saldırısı, kontrol döngülerinin tepki vermesini önler veya aşırı tepkiye neden olur.
   - Elevation of Privilege (Aşırı Yetki Kazanma):

- Bir zafiyet üzerinden kontrolcü yazılımına erişim sağlanırsa saldırgan daha kalıcı değişiklikler (ör. droop parametreleri set etmek) yapabilir.

4. **Gerekli Koşullar ve İstismar Edilen Zafiyetler**
   Başarılı bir saldırı için muhtemel ön koşullar ve zafiyetler şunlardır:
   ● Zayıf veya Yok Sayılmış Kimlik Doğrulama:

- Sensör/PMU/RTU ile merkezi sistem arasındaki bağlantıda karşılıklı kimlik doğrulama eksikliği (mutual TLS kullanılmaması).
  ● Şifreleme veya Bütünlük Kontrolünün Zayıf/Olmaması:

- Veri paketlerinin dijital imza veya MAC (Message Authentication Code) ile korunmaması, paketlerin değiştirilebilmesine neden olur.
  ● Zaman Senkronizasyonuna Bağımlılık ve GNSS Zafiyetleri:

- PMU ve ölçüm cihazları GPS/GNSS tabanlı zaman damgasına bağımlıysa, zaman saldırıları (GPS spoofing/jamming) doğru frekans korelasyonu bozar.
  ● Saha Cihazı Firmware'inin Güvenlik Zayıflıkları:

- Bellenim (firmware) güncellemelerinin imzasız veya doğrulamasız olması; bilinen CVE'lerin yamalanmamış olması.
  ● Ağ Segmentasyonu Eksikliği ve Aynı Ağa Erişim:

- Saldırganın saha ekipmanı veya yerel cihazlara fiziksel veya ağ yoluyla erişim sağlayabilmesi (ör. zayıf Wi-Fi, switch'lerde VLAN izolasyonu yok).
  ● Anomali Tespit Sistemlerinin Yetersizliği:

- Çoklu sensör verilerinin çapraz doğrulamasını yapan merkezi algoritmaların olmaması veya yanlış yapılandırılmış olması.

5. **Saldırı Yöntemleri ve Adım Adım Akış**
   Saldırgan Profili:
   Teknik olgunluk seviyesi: Orta-yüksek. Hem siber hem de temel güç sistemi bilgisine sahip; ağ paketlerini manipüle edebilen, firmware analiz ve modifikasyonu yapabilen bir grup veya kişi.

Adım 1 — Keşif (Reconnaissance):

- Hedef bölgedeki PMU/RTU/yeni nesil IBR'lerin üretici ve sürüm bilgileri taranır.

- Açık portlar, zayıf konfigürasyonlu protokoller (ör. telnet, eski SSH, HTTP) ve açık CVE'ler araştırılır.

- Sahadaki ağ topolojisi ve zaman senkronizasyon yöntemleri (GPS/NTP) tespit edilir.

Adım 2 — Erişim Sağlama (Initial Access):

- Fiziksel erişim: Sahaya yakın bir Wi-Fi veya Ethernet noktası üzerinden lokal ağa erişim sağlanır.

- Ağ erişimi: Zayıf kimlik doğraması bulunan cihazların credentials'ları ele geçirilir veya MitM için ARP spoofing gibi teknikler kullanılır.

- Firmware exploit: Bilinen bir CVE kullanılarak bir RTU veya PMU'nun shell/komut satırı erişimi elde edilir.

Adım 3 — Veri Manipülasyonu (Spoofing / Tampering):

- Gerçek zamanlı paket yakalama (packet sniffer) ile frekans ölçümleri izlenir.
- Paketler üzerinde maniplasyon: Frekans değeri +0.2 Hz bias ile sürekli gönderilir (ör. gerçek 49.80 Hz -> raporlanan 50.00 Hz).
- Alternatif: Rastgele periyotlarla pozitif/negatif sapmalar enjekte edilerek "dalgalı" bir frekans görünümü yaratılır.
- Zaman gecikmesi enjeksiyonu: Ölçümler sistemi karıştırmak için belli bir gecikme ile gönderilir.

Adım 4 — Kontrol Döngüsünün Yanıtı ve Kademeli Etki (Pivot):

- IBR kontrolcüler droop eğrisi ve set-point'leri sensör verilerine göre uyarlamaya başlar.
- Bazı IBR'ler üretimi kısar, bazıları artırır; koordinasyonsuz tepki nedeniyle güç akışı döngüsel hale gelir.
- CRED veya AGC, durumu merkezden düzeltmeye çalışırken yanlış ve gecikmeli verilerle beslendiği için daha agresif veya hatalı parametre ayarlamaları yapar.

Adım 5 — İyileştirme ve İzleri Silme (Clean-up / Persistence):

- Saldırgan, bulaştığı cihazlarda arka kapı (backdoor) bırakarak veya düzgün log kaydı bırakmayacak biçimde logları temizleyerek tespit ihtimalini azaltır.
- Kritik zamanlarda (ör. gece-peak dışında) saldırıyı yoğunlaştırarak tespit olasılığını düşürür.

Senkretik Senaryo Notu:
Saldırının bir varyantında saldırgan, koordinedi biçimde birden fazla bölgedeki sensörleri hedef alır. Bu, merkezi regülasyonun da yanlış korelasyonlar yapmasına ve bölgesel frekans dalgalanmalarının geniş alana yayılmasına neden olabilir.

6. **Tespit Yöntemleri ve Anomali Göstergeleri**
   Tespit için çok katmanlı, hem zaman serisi analitiği hem de protokoller arası korelasyon gereklidir. Örnek tespit yöntemleri ve gözlenecek anomaliler şöyledir:

A. Protokoller Arası Korelasyon (Sensor Fusion):

- İlgili anomali: PMU/RTU tarafından raporlanan frekans ile SCADA seviyesindeki telemetri veya lokal analiz cihazlarının doğru sayaç verileri arasındaki tutarsızlık.
- Uygulama: Periyodik olarak ham sayaç verileri paralel toplanır ve OCPP'e benzer yaklaşımla (signed meter readings) merkezi sistemde karşılaştırılır.
- Alarm Kuralı Örneği: "Eğer PMU_frekans - Lokal_frekans > 0.15 Hz ve süre > 2 dk ise alarm oluştur."

B. Zaman Serisi Anomali Tespiti (Statistiksel ve ML Tabanlı):

- İlgili anomali: Frekans zaman serisinde tekrarlayan pattern'ler, ani bias değişimleri veya periyodik sapmalar.

- Uygulama: Seasonal decomposition, ARIMA/Prophet ve basit ML modelleriyle sürekli eğitimli anomaly detector'lar kullanmak.

C. Zaman Damgası ve Senkronizasyon Tutarsızlıkları:

- İlgili anomali: Ölçümlerin zaman damgası jitter'ı, GPS/NTP tutarsızlıkları veya saat sapmaları.
- Uygulama: GNSS alıcılarının integrity check'leri, birden fazla zaman kaynağı kullanımı (GNSS + PTP + NTP fallback) ve zaman damgası imzalama.

D. Sağlık Kontrolleri ve Bütünlük İzleme:

- İlgili anomali: Firmware hash'lerinin beklenen değerlerden sapması; beklenmedik yeniden başlatmalar.
- Uygulama: Secure Boot ve uzaktan periodik firmware hash doğrulama.

E. Operasyonel Gözlemler ve İnsan Faktörü:

- İlgili anomali: Operatör raporları, sahada ekiplerin gözlemleri; kontrol panosunda beklenmedik sıçramalar.
- Uygulama: Olay yanıt playbook'larının varlığı ve operatör eğitimleri; anormal durumlar için hızlı raporlama kanalları.

7. **Olası Etkiler (Finansal, Operasyonel, Güvenliksel ve Toplumsal)**
   - Finansal Etkiler:

- Artan dengeleme maliyetleri (CRED/AGC'nin yanlış düzeltmeleri sonucu).
- IBR üretim planlarının bozulması, gereksiz yakıt tüketimi veya batarya döngü kaybı.
- Tedarikçiler ile yapılan SLA'larda ihlaller ve para cezaları.

- Operasyonel Etkiler:

- Bölgesel kesintilere yol açabilecek yanlış koruma tetiklemeleri.
- Manuel müdahale ihtiyacı, çalışanların fazla mesai ve operasyonel yük artışı.
- Uzun vadede planlama verilerinin bozulması (tahminlerin güvenilirliği azalır).

- Güvenliksel Etkiler:

- Kritik altyapıya yönelik güven kaybı; saldırıların eskalasyonu ve daha büyük sabotajlara zemin hazırlanması.
- Adli inceleme süreçlerinin zorlaşması (logların değiştirilmesi, izlerin silinmesi).

- Toplumsal Etkiler:

- Geniş çaplı etkilenme durumunda (ör. büyük bir bölgede koordineli saldırı) ekonomik faaliyet ve kamu hizmetlerinde aksamalar yaşanabilir.

- Kamu güveninin zedelenmesi ve düzenleyici kurum müdahaleleri.

8. **Önlemler ve Azaltma Stratejileri (Defense-in-Depth)**
   Aşağıdaki stratejiler, hem önleyici hem de tespit/telafi edici kontrolleri içeren derinlemesine savunma yaklaşımını temsil eder:

1. Kimlik Doğrulama ve Şifreleme:

- Karşılıklı kimlik doğrulama (mutual TLS) ve sertifika tabanlı erişim kontrolleri.

- Veri paketleri için dijital imzalama ve MAC (örn. HMAC) kullanımı; iletim sırasında bütünlük doğrulaması.

2. Zaman/GNSS Güvenliği:

- GNSS spoofing/jamming tespitleri ve alternatif zaman kaynakları (PTP, NTP fallback) kullanımı.

- Zaman damgası imzalama ve zaman senkronizasyonu için güvenli protokoller.

3. Cihaz Bütünlüğü ve Firmware Güvenliği:

- Secure Boot, imzalı firmware güncellemeleri ve üretici tarafından doğrulanmış yazılım zinciri.

- Uzaktan periyodik firmware hash doğrulama ve anomali halinde otomatik karantina.

4. Çoklu Sensör ve Sensor Fusion:

- Aynı coğrafi bölgedeki birden fazla bağımsız sensörin verilerinin karşılaştırılması.

- Trust scoring ve weighted consensus mekanizmaları; güvenilmeyen sensörlerin ağırlığının azaltılması.

5. Anomali Tespit ve Olay Müdahalesi:

- Real-time anomaly detection pipeline (stream processing) ve önceden tanımlı playbook'lar.

- Olay sırasında otomatik olarak devreye giren izole etme ve fallback modları (ör. local control mode'a düşme).

6. Ağ Segmentasyonu ve Erişim Kontrolleri:

- Kritik saha ekipmanlarının fiziksel olarak ayrı ağ segmentlerinde tutulması; yönetim ağlarına sıkı erişim politikaları.

- VPN, bastion host ve role-based access control (RBAC) uygulamaları.

7. İzleme, Logging ve Forensics:

- Değiştirilemez loglama (append-only, secure logging) ve merkezi SIEM entegrasyonu.

- Olay sonrası adli inceleme için time-synced logs ve immutable snapshots.

8. Operasyonel Önlemler ve Eğitim:

- Operatör/teknik ekipler için düzenli tatbikatlar, kırmızı ekip (red-team) testleri ve senaryo bazlı eğitimler.

- Playbook'lar: "Eğer frekans anomali uyarısı ve sensor fusion tutarsızlığı varsa yapılacaklar" adım adım hazırlanmalı.

9. **Ek Varyantlar ve İleri Düzey Senaryolar**
   - Koordine Edilmiş Coğrafi Saldırı:

- Birden fazla bölgede aynı anda benzer manipülasyonlar yapılarak merkezi regülasyonun çökertilmesi.
   - Zaman Bazlı Uyarlanabilir Saldırı:

- Saldırgan, gerçek zamanlı olarak sistem tepkisini gözlemler ve adaptif olarak bias/gürültü seviyesini değiştirir.
   - Karma Saldırı (DoS + Tampering):

- DoS ile bazı sensörlerin verisini kesip, kalan sensörlere müdahale ederek sistemde yanıltıcı bir "görünürlük boşluğu" yaratılır.

10. **Kapanış - Ders Çıkarımları ve Öneriler**
    Bu senaryo, dağıtık ve inverter ağırlıklı modern güç sistemlerinde sensör güvenliğinin temel bir gereklilik olduğunu göstermektedir.
    Frekans gibi merkezi kontrol kararlarına doğrudan etki eden telemetri verilerinin güvenliği sağlanmadan, kontrol algoritmaları
    hatta iyi tasarlanmış adaptif mekanizmalar bile sistem kararlılığını tehlikeye atacaktır. Dolayısıyla hem siber hem de fiziksel güvenlik,
    operasyonel prosedürler ve güçlü tespit mekanizmaları birlikte ele alınmalıdır.

EK — Protokoller ve Hızlı Güvenlik Notları

1. **IEC 61850 (GOOSE / SV / MMS)**

- Risk: GOOSE/SV ile sahte veya tekrar oynatılan mesajlarla yanlış koruma tetiklenmesi.

- Hızlı önlem: VLAN/segmentasyon, GOOSE/SV için bütünlük/MAC, PTP güvenliği.

2. **IEEE C37.118 (PMU)**

- Risk: GPS spoofing ile zaman bozulması, faz/korrelasyon hataları.

- Hızlı önlem: Çoklu zaman kaynağı (GNSS+PTP), PMU veri bütünlüğü ve korelasyon kontrolleri.

3. **IEC 60870-5-104 / DNP3 / Modbus TCP**

- Risk: Auth/bütünlük eksikliğinden komut enjeksiyonu ve veri manipülasyonu.

- Hızlı önlem: VPN/IPsec, Secure DNP3 veya protokol gateway; kritik cihazlara doğrudan internet erişimi yok.

4. **MQTT / IoT Broker'lar**

- Risk: Açık broker veya eksik kimlik doğrulama ile topic spoofing.

- Hızlı önlem: TLS + istemci sertifikası, ACL’ler, broker izleme.

5. **PTP / NTP (Zaman Senkronizasyonu)**

- Risk: Zaman sapması → yanlış korelasyon/anomali tespiti.
- Hızlı önlem: Güvenli NTP/PTP yapılandırması, GNSS izleme ve fallback kaynakları.

6. **OPC UA / HTTPS (Üst Katman Entegrasyonları)**

- Risk: API açıkları, yetkisiz erişim.
- Hızlı önlem: mTLS, API gateway ve rate limiting.