SigintOS™

ANALİZ RAPORU

Kritik Tesislere Yönelik RF Tehditleri ve Savunma Tedbirleri

Sinyal güvenliği • Elektronik koruma • Operasyonel dayanıklılık

RAPOR TARİHİ	Ekim 2026
KAPSAM	Kritik altyapılarda RF kaynaklı tehditler ve savunma
NİTELİK	Genel tehdit değerlendirmesi; saha incelemesinin yerine geçmez

YÖNETİCİ NOTU

RF güvenliği yalnızca kablosuz iletişimi korumak değildir. Konum, zamanlama, sensör verisi, endüstriyel kontrol ve operasyonel süreklilik üzerindeki etkiler birlikte ele alınmalıdır. En etkili yaklaşım; algılama, doğrulama, yedeklilik ve müdahale süreçlerini katmanlı bir mimaride birleştirmektir.

İçindekiler

- 1. Yönetici özeti
- 2. Kapsam ve kritik tesisler
- 3. Başlıca RF tehdit türleri
- 4. Operasyonel etkiler
- 5. Katmanlı savunma mimarisi
- 6. Tespit ve olay sınıflandırma
- 7. Yapay zekâ destekli analiz
- 8. 90 günlük uygulama yol haritası
- 9. Başarı göstergeleri
- 10. Hukuki ve operasyonel sınırlar
- 11. Sonuç ve stratejik öneriler
- Kaynaklar ve ileri okuma

1. Yönetici özeti

Kritik tesisler; enerji santralleri, elektrik iletim merkezleri, havaalanları, limanlar, savunma sanayii tesisleri, telekomünikasyon altyapıları, su arıtma tesisleri ve veri merkezleri gibi fiziksel ve dijital güvenliğin birlikte ele alınması gereken varlıklardır.

RF (radyo frekansı) tehditleri yalnızca haberleşmenin kesilmesiyle sınırlı değildir. Kablosuz sistemlerin yanıltılması, uzaktan kontrol bağlantılarının bozulması, elektromanyetik girişim, izinsiz verici faaliyetleri ve kablosuz iletişim üzerinden yürütülen siber saldırılar operasyonel risk oluşturabilir.

Temel değerlendirme: RF güvenliği, çevre güvenliği ve siber güvenlikten ayrı düşünülemez. Etkili bir koruma programı; RF spektrumunun izlenmesini, olayların doğrulanmasını, kritik sistemlerin yedekli çalışmasını ve fiziksel müdahale kapasitesini birlikte içermelidir.

Bu rapor, saldırıların uygulanmasına ilişkin operasyonel talimatlar yerine tehdit türlerini, olası etkileri, erken uyarı işaretlerini ve savunma tedbirlerini ele alır.

2. Kapsam ve kritik tesisler

Enerji altyapısı

SCADA/telemetri bağlantıları, kablosuz saha haberleşmesi, GNSS zaman senkronizasyonu ve uzaktan bakım sistemleri. Olası sonuçlar: görünürlük kaybı, hatalı ölçüm veya işletme sürekliliğinin bozulması.

Havaalanları ve ulaşım

GNSS, radar, hava-yer haberleşmesi, liman operasyonları ve kablosuz takip sistemleri. Olası sonuçlar: konum/zaman tutarsızlığı, haberleşme sorunları ve emniyet süreçlerinde gecikme.

Telekomünikasyon ve veri merkezleri

Hücresel ağlar, mikrodalga bağlantılar, Wi-Fi, kablosuz yönetim arayüzleri ve hassas zamanlama kaynakları. Olası sonuçlar: bağlantı kaybı, hizmet kesintisi veya güvenlik kontrollerinin zayıflaması.

Su, sağlık ve endüstriyel tesisler

Uzaktan ölçüm, sensör ağları, telsiz sistemleri ve kablosuz saha kontrolü. Olası sonuçlar: izleme eksikliği, yanlış alarm, manuel işletmeye geçiş veya proses güvenliği riski.

3. Başlıca RF tehdit türleri

3.1 RF karıştırma (Jamming)

Risk düzeyi: Yüksek–Kritik

Alıcının arzu edilen sinyali güvenilir biçimde alamamasına veya işleyememesine neden olan girişimdir. GNSS, telsiz haberleşmesi ve kablosuz telemetri etkilenebilir.

Belirtiler: ani bağlantı kaybı, hata oranlarında artış, sinyal-gürültü oranında düşüş ve birden fazla sistemde eşzamanlı bozulma.

Savunma: spektrum izleme, yedek haberleşme kanalları, kablolu alternatifler, alıcı dayanıklılığı değerlendirmeleri ve emniyetli çalışma prosedürleri.

3.2 Sinyal yanıltma (Spoofing)

Risk düzeyi: Yüksek–Kritik

Alıcıya gerçekmiş gibi görünen ancak yanlış konum, zaman veya ölçüm bilgisi üreten sinyaller söz konusudur. GNSS kaynaklı yanlış zaman bilgisi diğer sistemlere yayılabilir.

Belirtiler: fiziksel gerçeklikle uyuşmayan konum, bağımsız saatler arasında sapma, tutarsız hız veya zaman damgaları.

Savunma: bağımsız konum ve zaman kaynakları, çoklu sensör doğrulaması, fiziksel olarak mümkün olmayan değişimleri algılama ve kaynak bütünlüğü kontrolleri.

3.3 İstenmeyen elektromanyetik girişim

Risk düzeyi: Orta–Yüksek

Arızalı vericiler, hatalı anten sistemleri, endüstriyel ekipmanlar veya uygunsuz kurulumlar, kasıtlı saldırı olmadan haberleşme ve ölçüm performansını bozabilir.

Belirtiler: belirli bölgelerde kalite düşüşü, tekrarlayan hata veya ekipmanlar devreye girdiğinde ortaya çıkan bozulma.

Savunma: EMC incelemeleri, kablolama ve topraklama kontrolleri, filtreleme, ekranlama ve girişim kaynağının kontrollü tespiti.

3.4 Sahte kablosuz erişim noktası veya baz istasyonu

Risk düzeyi: Yüksek

Sahte veya yetkisiz kablosuz altyapı, cihazların güvenilmeyen ağa bağlanmasına veya kimlik doğrulama risklerine yol açabilir.

Belirtiler: envanterde bulunmayan erişim noktaları, beklenmeyen kimlik doğrulama istemleri veya cihaz/ağ günlüklerinde olağan dışı değişiklikler.

Savunma: sertifika doğrulaması, karşılıklı kimlik doğrulama, yönetilen cihaz politikaları, yetkisiz erişim noktası tespiti ve ağ segmentasyonu.

3.5 Kablosuz protokol ve uygulama saldırıları

Risk düzeyi: Yüksek

Zayıf kimlik doğrulama, tekrar oynatma riskleri veya hatalı yapılandırmalar kablosuz sistemlerin güvenliğini tehlikeye sokabilir.

Belirtiler: olağan dışı oturumlar, kimlik doğrulama hataları, tekrarlanan mesajlar veya cihaz günlüklerinde tutarsızlık.

Savunma: karşılıklı kimlik doğrulama, mesaj bütünlüğü ve güncellik kontrolleri, anahtar yönetimi, güvenli yazılım ve erişim kısıtlamaları.

3.6 Zamanlama ve senkronizasyon bozulması

Risk düzeyi: Yüksek–Kritik

GNSS tabanlı zamanlamaya bağımlı enerji, telekomünikasyon veya dağıtık ölçüm sistemleri, zaman bilgisinin kaybolması ya da yanlışlaşması durumunda beklenmedik davranabilir.

Belirtiler: zaman damgalarında sapma, saatler arasında uyuşmazlık veya senkronizasyon alarmları.

Savunma: yerel osilatörler, holdover kapasitesi, bağımsız zaman kaynakları, sapma alarmları ve zaman doğrulama mekanizmaları.

3.7 RF keşif ve pasif sinyal analizi

Risk düzeyi: Bağlama bağlı

Pasif alıcılarla yayınların varlığı, zamanlaması veya bazı teknik özellikleri incelenebilir. Zayıf korunan iletişimler operasyonel bilgi açığa çıkarabilir.

Belirtiler: tek başına kesin saldırı göstergesi yoktur; beklenmedik yayınlar veya yayın düzenindeki değişimler araştırılabilir.

Savunma: gereksiz yayınları azaltma, güçlü şifreleme ve kimlik doğrulama, yönetim trafiğini ayırma ve yayın politikalarını denetleme.

4. Operasyonel etkiler

Kritik fonksiyon	Olası sonuç	Öncelikli savunma
Komuta ve haberleşme	İletişim kaybı veya gecikme	Bağımsız yedek haberleşme
Konum ve navigasyon	Yanlış veya kullanılamayan konum	Bağımsız sensör doğrulaması
Zaman senkronizasyonu	Zaman damgası ve ölçüm tutarsızlığı	Holdover ve alternatif zaman kaynağı
Endüstriyel kontrol	Telemetri kaybı, güvensiz işletme durumu	Güvenli varsayılan durum ve yerel kontrol
Fiziksel güvenlik	Kablosuz sensörlerde kör nokta	Yedek sensörler ve çapraz doğrulama
Kurumsal kablosuz ağ	Yetkisiz bağlantı veya veri riski	Kimlik doğrulama ve ağ segmentasyonu

RF olayları birden fazla sistemi aynı anda etkileyebilir. Bir bağlantıdaki arıza yerel kalabilir; ancak ortak zaman kaynağına, haberleşme altyapısına veya aynı RF ortamına bağlı sistemlerde zincirleme sonuçlar doğurabilir.

Havacılıkta GNSS karıştırma ve yanıltma olayları haberleşme, navigasyon ve gözetim işlevlerine yansıyabilir. Alternatif seyrüsefer yöntemleri ve önceden tanımlı prosedürler bu nedenle önemlidir.

5. Katmanlı savunma mimarisi

Katman 1 — RF algılama ve spektrum görünürlüğü

Yetkili frekans planına göre ölçüm, anormal yayın tespiti, sinyal kalitesi ve spektrum kullanımının izlenmesi.

Katman 2 — Korelasyon ve tehdit analizi

RF olaylarının zaman, konum, cihaz telemetrisi ve sistem günlükleriyle karşılaştırılması.

Katman 3 — Dayanıklılık ve yedeklilik

Alternatif iletişim, bağımsız zaman kaynakları, kablolu yedekler ve emniyetli yerel çalışma.

Katman 4 — Müdahale ve iyileştirme

Alarm doğrulama, olay kaydı, sorumlu ekiplere bildirim, güvenli işletme prosedürleri ve olay sonrası inceleme.

5.1 Algılama ve izleme

- Spektrum izleme: Yetkilendirilmiş frekans aralıklarında gürültü tabanı, sinyal seviyesi ve beklenmedik yayınların gözlenmesi.
- Zaman serisi analizi: Sinyal kalitesindeki ani veya kademeli değişimlerin geçmiş ölçümlerle karşılaştırılması.

- Çoklu sensör korelasyonu: Birden fazla alıcıda görülen olayların karşılaştırılması.
- RF dışı doğrulama: Spektrum anomalisinin ağ günlükleri, cihaz hata kayıtları ve fiziksel süreç alarmlarıyla birlikte incelenmesi.
- Denetlenebilir kayıtlar: Ölçüm zamanı, sensör kimliği, kalibrasyon durumu, alarm nedeni ve analist kararının kaydedilmesi.

Teknik not: Yüksek RF enerji seviyesi tek başına saldırı kanıtı değildir. Düşük enerji seviyesi de yanıltma veya protokol kaynaklı saldırıları dışlamaz.

5.2 Koruma ve dayanıklılık

Tedbir	Koruduğu özellik	Öncelik
Alternatif haberleşme	Kullanılabilirlik	Çok yüksek
GNSS dışı zaman kaynağı ve holdover	Zaman sürekliliği	Bağımlılığa göre yüksek–çok yüksek
Karşılıklı kimlik doğrulama ve şifreleme	Kimlik ve veri güvenliği	Çok yüksek
EMC ve ekranlama değerlendirmesi	Elektronik dayanıklılık	Yüksek
Kablolu ve bağımsız sensörler	Algılama sürekliliği	Yüksek
Güvenli yerel kontrol modu	Operasyonel emniyet	Kritik proseslerde çok yüksek
Yedek güç ve ağ ayrıştırması	Ortak arıza riskini azaltma	Çok yüksek

Savunma tasarımı tesisin risk değerlendirmesine dayanmalıdır. RF bağlantısının kaybında tamamen durması gereken bir proses ile kontrollü biçimde yerel çalışmayı sürdürebilen bir proses aynı şekilde tasarlanmamalıdır.

6. Tespit ve olay sınıflandırma

1. Anomali tespiti

Bir alıcıda sinyal kaybı, beklenmedik spektrum değişimi veya zamanlama alarmı meydana gelir.

2. Ölçümün doğrulanması

Sensör arızası, anten bağlantısı, kalibrasyon, güç kaynağı ve bilinen meşru yayınlar kontrol edilir.

3. Bağımsız kanıtların karşılaştırılması

Farklı alıcılar, kablolu telemetri, ağ günlükleri ve fiziksel süreç ölçümleri incelenir.

4. Risk ve etki değerlendirmesi

Etkilenen hizmetler, emniyet sonuçları ve alternatif işletme kapasitesi belirlenir.

5. Müdahale ve raporlama

Yetkili ekipler bilgilendirilir; gerektiğinde güvenli işletme moduna geçilir ve olay kayıt altına alınır.

Gösterge	Olası açıklamalar	Doğrulama yöntemi
Gürültü tabanında artış	Girişim, yerel verici, sensör sorunu	Bağımsız alıcı karşılaştırması
GNSS konumunda ani sapma	Yanıltma, alıcı arızası, yansıma	Bağımsız konum kaynağı
Birden fazla telsizde bağlantı kaybı	Ortak RF, güç veya ağ arızası	Alternatif haberleşme testi
Zaman damgalarında sapma	GNSS sorunu, saat veya ağ hatası	Bağımsız zaman referansı
Bilinmeyen kablosuz ağ	Yetkisiz erişim noktası veya meşru komşu ağ	Envanter ve kimlik doğrulama kayıtları

RF sensörlerinin konum belirleme kabiliyeti varsa sonuçlar ölçüm belirsizliğiyle sunulmalıdır. Birden fazla sensörün aynı olayı görmesi güveni artırabilir; ancak sensörlerin ortak bir arızadan etkilenmediği ayrıca değerlendirilmelidir.

7. Yapay zekâ destekli RF tehdit analizi

Yapay zekâ, çok sayıda ölçümün anlamlandırılması ve olayların önceliklendirilmesi için değerlidir. Bununla birlikte, yapay zekâ çıktıları tek başına saldırı doğrulaması olarak kabul edilmemelidir.

Anomali tespiti

Her frekans aralığının ve sensörün normal davranışını öğrenerek olağan dışı enerji, süre, değişkenlik veya bağlantı kalitesi örüntülerini işaretler.

Olay korelasyonu

RF ölçümlerini ağ günlükleri, zaman senkronizasyonu kayıtları ve tesis alarm sistemleriyle eşleştirir.

Risk önceliklendirmesi

Bir olayın sinyal seviyesinin yanı sıra hizmet kritikliğine, bağımsız doğrulama sonuçlarına ve yedeklerin durumuna göre öncelik kazanmasını sağlar.

Adli inceleme desteği

Olay öncesi ve sonrası ölçümleri zaman çizelgesinde birleştirerek analistin kararını destekler.

Önerilen teknik yaklaşım

1. Sentetik sinyaller ve izinli SDR ölçümleriyle kontrollü veri kümesi oluşturmak.
2. Normal çalışma, doğal girişim, cihaz arızası ve kontrollü bozulma senaryolarını ayrı etiketlemek.
3. Kural tabanlı alarm sistemiyle makine öğrenmesi sonuçlarını birleştirmek.
4. Yanlış pozitif oranı, tespit gecikmesi ve kaçırılan olayları ölçmek.
5. Model değişikliklerini sürümlemek ve insan onayını korumak.

Bir RF sınıflandırma modeli yalnızca spektrum görüntüsünden hareketle niyeti kesin olarak belirleyemez. Aynı örüntü kasıtsız girişim, arıza veya kasıtlı bir olayla ilişkili olabilir.

8. 90 günlük uygulama yol haritası

Aşama 1 — Envanter ve risk analizi (0–30 gün)

- Kritik RF bağımlılıklarının envanterini çıkarmak.
- Tesisin frekans ve haberleşme mimarisini belgelemek.
- Tek hata noktalarını ve yedeksiz sistemleri belirlemek.
- Mevcut olay müdahale prosedürlerini incelemek.

Aşama 2 — İzleme ve doğrulama (31–60 gün)

- Yetkili noktalarda pasif RF ölçüm sistemi kurmak.
- Referans spektrum ve normal çalışma profilleri oluşturmak.
- Alarm ve kayıt mekanizmalarını devreye almak.
- Kontrollü testlerle sensör ve prosedürleri doğrulamak.

Aşama 3 — Dayanıklılık ve operasyonel hazırlık (61–90 gün)

- Alternatif haberleşme ve zamanlama çözümlerini test etmek.
- Güvenli yerel çalışma senaryolarını uygulamak.
- Yapay zekâ destekli olay korelasyonu için pilot çalışma yürütmek.
- Personel eğitimi, olay tatbikatı ve yönetim raporlaması yapmak.

9. Başarı göstergeleri

Gösterge	Ölçtüğü unsur
Ortalama tespit süresi	Anomalinin fark edilmesine kadar geçen süre
Doğrulama süresi	Alarmın gerçek bir olay olup olmadığının belirlenmesi
Yanlış alarm oranı	Operasyonel ekip üzerindeki gereksiz yük
Yedek sisteme geçiş süresi	Hizmet sürekliliğinin sağlanma hızı
Yedek çalışma başarısı	Kesinti sırasında kritik fonksiyonların devam edebilmesi
Kayıt bütünlüğü	Olayın sonradan incelenebilmesi
Tatbikat başarı oranı	Personelin ve prosedürlerin etkinliği

Sayısal hedefler tesisin başlangıç performansı ve emniyet gereksinimleri belirlendikten sonra atanmalıdır. Kabul edilebilir kesinti süresi ve güvenli duruma geçiş kriterleri, işletme ve emniyet sorumluları tarafından onaylanmalıdır.

10. Hukuki ve operasyonel sınırlar

RF izleme, frekans kullanımı ve elektromanyetik müdahale uygulamaları ülkeye ve kullanım alanına göre değişen hukuki yükümlülüklere tabidir. Türkiye'de proje kapsamı belirlenirken BTK'nın frekans tahsisi ve elektronik haberleşme düzenlemeleri ile tesisin sektörel yükümlülükleri değerlendirilmelidir.

- Yetkisiz yayın veya karıştırma yapılmamalıdır.
- Başka kurumların haberleşmesine müdahale edecek testler gerçek operasyonel ortamlarda yürütülmemelidir.
- RF ölçümü, iletişim içeriğinin kaydedilmesi ve kişisel verilerin işlenmesi ayrı hukuki değerlendirmelere tabi olabilir.
- Aktif müdahale veya karşı tedbir uygulaması yalnızca açık yetki ve uygun güvenlik prosedürleri çerçevesinde değerlendirilmelidir.

11. Sonuç ve stratejik öneriler

Kritik tesislere yönelik RF savunmasında en önemli yaklaşım, bir saldırı türüne karşı tek bir cihaz satın almak değil; algılama, doğrulama, dayanıklılık ve müdahale yeteneklerini bütünleştiren bir sistem kurmaktır.

6. Kritik hizmetlerin RF ve zamanlama bağımlılıklarını belirlemek.
7. Pasif RF izleme ve çoklu kaynak korelasyonunu devreye almak.
8. Kritik işlevler için bağımsız haberleşme ve zamanlama alternatifleri sağlamak.
9. Güvenli yerel işletme ve olay müdahale prosedürlerini test etmek.
10. Yapay zekâyı analist kararını destekleyen, ölçülebilir bir araç olarak uygulamak.

Bu model, RF kaynaklı kesintilerin etkisini azaltmaya ve tesisin olağan dışı koşullarda çalışmaya devam etmesine yardımcı olur.

Kaynaklar ve ileri okuma

EASA — GNSS Outages and Alterations

https://www.easa.europa.eu/en/domains/air-operations/global-navigation-satellite-system-outages-and-alterations

GNSS karıştırma ve yanıltma olayları, belirtileri ve azaltım tedbirleri.

CISA — Improving the Operation and Development of GPS Equipment Used by Critical Infrastructure

https://www.cisa.gov/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf

Kritik altyapılarda GPS bağımlılığı ve dayanıklılık.

NIST — Jamming glossary

https://csrc.nist.gov/glossary/term/jamming

Karıştırma kavramı.

NIST — Spoofing glossary

https://csrc.nist.gov/glossary/term/spoofing

Yanıltma kavramı.

ICAO — GNSS RFI publications

https://www.icao.int/air-navigation-bureau/gnss-rfi/publications

Havacılıkta GNSS girişimi ve dayanıklılık kaynakları.

ITU — Harmful interference in radionavigation-satellite services

https://www.itu.int/en/mediacentre/Pages/PR-2025-03-25-radio-navigation-satellite-service-harmful-interference.aspx

Frekans kullanımının ve zararlı girişimin uluslararası boyutu.

SigintOS — Yüksek Teknoloji ve Savunma Ürünleri AŞ.

https://www.sigintos.com

RF Intelligence Dashboard. Yapay Zeka Destekli RF tehdit Analizi

Not: Bu rapor genel bir tehdit ve savunma değerlendirmesidir. Belirli bir tesisin saha incelemesi, RF ölçümleri ve mühendislik doğrulaması yerine geçmez.

SigintOS™

www.sigintos.com