

---

## SWOT Analizi: YETİM SEANS (Stop gelmeden fiş çıkışma)

Kategori	Açıklama
Güçlü Yonler (Strengths)	<ul style="list-style-type: none"><li>- Anomali durumu net tanımlanmıştır: <i>fiş çekildiği hâlde StopTx gelmemesi, status alanının hâlâ "Charging/Busy" kalması, session_active'in kapanmaması</i> gibi açık kriterler vardır.</li><li>- İzlenecek veri alanları (plug_state, status, start_tx_id, stop_tx_id, meter_total_kWh vs.) önceden belirlenmiştir; bu da kural yazmayı ve model geliştirmeyi kolaylaştırır.</li><li>- Basit IF/THEN kurallarıyla (ör. plug_state=false olduktan sonra 30 sn içinde StopTx gelmezse ALARM) yüksek tespit oranına ulaşmak mümkündür.</li><li>- Tespit edilen yetim seansların hem <b>güvenlik</b>, hem <b>faturalama</b>, hem de <b>operasyonel verimlilik</b> açısından somut etkisi olduğu için, iş birimleri tarafından önemi kolayca kabul edilir.</li></ul>
Zayıf Yonler (Weaknesses)	<ul style="list-style-type: none"><li>- Senaryo, zaman eşiklerine (ör. 30 sn) hassastır; farklı istasyon modelleri veya ağ koşulları için yanlış alarm (false positive) veya kaçırma (false negative) riski vardır.</li><li>- plug_state ve kilit sensörlerine fazla bağımlılık, bu sensörlerde arıza veya kalibrasyon problemi olduğunda sistemin güvenilirliğini düşürebilir.</li><li>- Bazı istasyonlarda olay/telemetri log'ları eksik, düzensiz veya standarda uygun olmayabilir; bu da tespit modelini genelleştirmeyi zorlaştırır.</li><li>- Yalnızca kural tabanlı yaklaşım kullanılırsa, saldırganlar veya hatalı konfigürasyonlar bu kuralları "dolandıracak" alternatif akışlar üretebilir (ör. sahte StopTx gönderimi).</li><li>- Operasyon ekiplerinin anomali loglarını düzenli incelememesi durumunda, üretilenalar sahada gerçek aksiyona dönüşmeyebilir.</li></ul>

<b>Fırsatlar (Opportunities)</b>	<ul style="list-style-type: none"> <li>- Yetim seansları azaltmak, <b>müşteri memnuniyetini</b> ve <b>faturalama doğruluğunu</b> artırarak markaya güven kazandırır.</li> <li>- Bu senaryoya özel geliştirilen tespit ve otomatik kapanış mekanizmaları, diğer OCPP anomali senaryoları için de yeniden kullanılabilir (genişletilebilir kural/motor altyapısı).</li> <li>- Yapay zekâ ve istatistiksel modeller, kural temelli yapıyı tamamlayarak dinamik eşik belirleme (station type, saat, trafik yoğunluğu vb.) imkânı sunar.</li> <li>- Mevzuat/sertifikasyon tarafında “güvenli işletim” ve “doğru faturalama” şartlarını kanıtlarken önemli bir artı değer sağlar.</li> <li>- Pilot uygulamalarda başarı gösterilmesi, çözümün farklı operatör/ülkelere ürünleştirilip sunulmasına imkân sağlayabilir.</li> </ul>
<b>Tehditler (Threats)</b>	<ul style="list-style-type: none"> <li>- Ağ kesintileri, paket kayıpları veya yüksek gecikme, StopTx mesajlarının kaybolması ya da çok geç gelmesine neden olarak sistemi zorlayabilir.</li> <li>- Donanım üreticilerinin firmware hataları veya protokolü tam uygulamaması, beklenmeyen durum makineleri (state machine bug'ları) üretebilir.</li> <li>- Kötü niyetli kullanıcılar veya saldırganlar, enerji hırsızlığı veya faturalama manipülasyonu için bu zafiyeti hedef alabilir.</li> <li>- Farklı OCPP sürümleri ve istasyon markaları arasında standart dışı alan adları, statü kodları veya log formatları bulunması, tespit sistemini karmaşıklaştırır.</li> <li>- Operatörlerin güvenlik yatırımlarını maliyet nedeniyle ertelemesi, çözümün sahada tam uygulanmaması riskini doğurur.</li> </ul>

---

## SMART Hedefler: YETİM SEANS Anomali Senaryosu

No	Hedef Başlığı	SMART Tanımı
1	<b>Yetim Seans Tespit Modeli Geliştirme</b>	YETİM SEANS senaryosunda; plug_state, status, timestamp, meter_total_kWh ve session_active gibi alanları kullanarak <b>en az %95 tespit oranına</b> ve <b>en fazla %2 yanlış alarma</b> sahip, kural tabanlı ve/veya yapay zekâ destekli bir tespit modeli geliştirmek. Model; Kural-1, Kural-2 ve Kural-3'te tanımlanan durumları eksiksiz yakalayacak şekilde tasarlanacaktır.
2	<b>StopTx Yedek Kapanış Mekanizması Kurulması</b>	plug_state=false olduktan sonra <b>konfigüre edilebilir bir süre</b> (ör. 15–45 sn) içinde StopTx mesajı alınmadığında, istasyon tarafından <b>otomatik yerel seans kapanışı</b> ve “yetim seans” olay kaydı yapan bir yedek kapanış mekanizması geliştirmek; bu mekanizmanın tüm test senaryolarında (ağ kesintisi, mesaj geciktirme vb.) tutarlı çalıştığını doğrulamak.

3	<b>Alarm Gecikme Süresini Azaltma</b>	YETİM SEANS tespiti için kurulan alarm sisteminde, anomali gerçekleştiği andan itibaren <b>en fazla 5 saniye içinde</b> merkez veya izleme paneline uyarı düşmesini sağlamak; bu hedefi, test senaryolarının en az %95'inde gerçekleştirecek şekilde olay işleme ve log akışı mimarisini optimize etmek.
4	<b>Eşik Değer (Timeout) Optimizasyonu</b>	Farklı istasyon modelleri ve ağ koşullarında, plug_state=false sonrası StopTx gecikme sürelerini istatistiksel olarak analiz ederek, <b>en az 3 farklı profil</b> (ör. "şehir içi hızlı şarj", "otayol istasyonu", "AC yavaş şarj") için optimum timeout aralıklarını (15–120 sn bandında) belirlemek; her profil için hem tespit oranı hem yanlış alarm oranını raporlayarak yapılandırma rehberi oluşturmak.
5	<b>Sensör Doğrulama ve Çapraz Kontrol Mekanizması</b>	Fiş/kilit sensörleri ile yazılım durumu (status, session_active) arasında <b>otomatik çapraz doğrulama</b> yapan bir kontrol seti tasarlamak; sensör arızası veya tutarsızlık tespit edildiğinde istasyonu <b>güvenli moda</b> (charging'i durdurma, seansı kapatma, bakım uyarısı) alacak bir prosedürü devreye almak ve bu mekanizmayı <b>en az 3 farklı arıza senaryosunda</b> test etmek.
6	<b>Yetim Seans İzleme ve Raporlama Paneli</b>	Operasyon ve güvenlik ekiplerinin kullanacağı, günlük/haftalık bazda <b>yetim seans sayısını, tespit oranını, yanlış alarm oranını ve alarm gecikme sürelerini</b> gösteren bir izleme paneli oluşturmak; bu panelin üzerinden gelen verilerle 3 aylık periyotlarda iyileştirme aksyonları çıkarılmasını sağlayacak raporlama şablonları hazırlamak.
7	<b>Pilot Uygulama ve Sahada Doğrulama</b>	Geliştirilen tespit kuralları, yerel kapanış mekanizması ve alarm altyapısını <b>en az bir pilot istasyonda veya test ortamında</b> koşturup; S1 (ağ keserek yetim bırakma), S2 (mesaj geciktirme) ve S3 (sensör tutarsızlığı) senaryolarının her birinde <b>%95'in üzerinde tespit, %2'nin altında yanlış alarm ve ≤5 saniye alarm gecikmesi</b> sağlandığını ölçmek ve raporlamak.