FORD TRUCKS
ÜSTYAPICI FIRMALAR IÇIN
SIBER GÜVENLİK UYUM REHBERİ
R155 REGÜLASYONU KAPSAMINDA TEKNİK GEREKLİLİLER

Rev00 22.04.2025

TRUCKS

Sharing the Load

Ford Trucks

Üstyapıcı Firmalar için Siber Güvenlik Uyum Rehberi R155 Regülasyonu Kapsamında Teknik Gereklilikler

22.04.2025

Versiyon Geçmişi

QDMS Yayınlı Versiyon	Draft Version	Değişiklik Bilgisi	Tarih	Sayfa	Oluşturan	Onaylayan
V0.0	V0.0	İlk Versiyon	07.04.2025	-	Özlem Menteş	İbrahim Kalaycı
V0.0	V0.1	Doküman genelinde geçen 'üstyapı soketi' ifadesi, terminolojik bütünlüğün sağlanması amacıyla 'üstyapı konnektörü' olarak güncellenmiştir.	21.04.2025	-	Özlem Menteş	İbrahim Kalaycı
V0.0	V0.2	QDMS yayın versiyonu eklenmiştir.	22.04.2025	1	Özlem Menteş	İbrahim Kalaycı

Table 1 – Versiyon Geçmişi

İçerik

Giriş

Bu doküman, Ford Otosan tarafından üretilen araçlara üst yapı (örneğin: kasa, vinç, çöp konteyneri vb.) ekleyen üstyapıcıların, uymaları gereken teknik ve siber güvenlik gereksinimlerini tanımlar. Dokümanın temel amacı, araçların siber güvenlik bütünlüğünü korumak, yetkisiz müdahaleleri önlemek ve tip onay süreçleri hakkında üstyapıcı firmaları bilgilendirmektir.

Kısaltmalar & Teknik Açıklamalar

BBI: Üst Yapı Konnektörü

CAN: Denetleyici Alan Ağı

CSMS: Siber güvenlik Yönetim Sistemi

ECU: Elektronik Kontrol Ünitesi

E/E: Elektrik/Elektronik

GSM: Mobil İletişim İçin Küresel Ağ

LIN: Lokal Alan Ağları

OEM: Orjinal Araç Üreticisi

TARA: Tehdit Analizi ve Risk Değerlendirmesi

Wi-Fi: Wireless Bağlantı

1. Giriş

Bu doküman, Ford Otosan ile iş birliği içerisinde çalışan üstyapıcı firmaların, araçlar üzerinde gerçekleştirecekleri bağlantı ve modifikasyonlarda siber güvenlik gerekliliklerine uygun hareket etmeleri amacıyla hazırlanmıştır.

2. Amaç

Dokümanın amacı, Ford Otosan tarafından üretilen araçlar üzerinde değişiklik gerçekleştiren üstyapıcıların;

- Siber güvenlik risklerini tanımlaması ve yönetmesi,
- Araçlara yapılan yetkisiz bağlantıların önlenmesi,
- R155 regülasyonuna uygunluğun sağlanması,

Üstyapı konnektörü (BBI) üzerinden gerçekleştirilen bağlantıların güvenli kullanımının sağlanması
hususlarında gerekli bilgi ve yönlendirmeleri sunmaktır.

3. Kapsam

Ford Otosan tarafından üretilmiş araçların üzerine üstyapı uygulayan tüm üstyapıcı firmaları kapsamaktadır.

Kapsam dahilindeki faaliyetler:

- Üstyapı konnektörü veya diğer yollarla araç ağına bağlantı kurulması,
- Yeni ECU veya elektronik bileşenlerin eklenmesi,
- Kablosuz iletişim sağlayan cihazların (Wi-Fi, GSM, Bluetooth vb.) entegrasyonu,
- Siber güvenliği etkileyebilecek tüm mekanik ve elektronik değişiklikler,

kapsam dahilinde değerlendirilmektedir.

4. Araç Bağlantıları

4.1. Üstyapı Konnektörü (BBI)

Üstyapı konnektörü (Body Builder Interface – BBI), araç ağlarına kontrollü ve güvenli erişim sağlamak amacıyla tasarlanmış özel bir konektördür. Bu konnektor Ford Otosan tarafından tasarlanmış siber güvenlik gerekliliklerine uyumluluğu teyit edilmiş konnektördür.

Bu konnektörün kullanımına ilişkin teknik esaslar aşağıda belirtilmiştir:

- Üstyapı konnektöründeki CAN hatları yalnızca okunabilir (Read-Only) yapıdadır. Üstyapıcı sistemlerinden araç sistemlerine mesaj iletilmesi mümkün değildir.
- Araç ile üstyapıcı sistemleri arasındaki iletişim, önceden tanımlanmış fonksiyonlara sahip 24V dijital sinyal pinleri üzerinden sağlanır.

- Bu sinyal pinleri yalnızca belirli ve kontrol altındaki bilgi akışına izin verir; araç sistemlerinin haberleştiği CAN hattına doğrudan müdahale edilemez.

5. Siber Güvenlik Açısından Bileşenlerin Değerlendirilmesi

Bir üstyapıcı tarafından araca eklenen herhangi bir bileşen, aşağıdaki özelliklerden bir veya birkaçına sahipse siber güvenlik açısından ilgili (cyber-relevant) olarak değerlendirilir:

- Üst yapı konnektörü üzerinden araç ağına bağlıysa,
- Uzak bağlantı özelliğine sahipse (örneğin: Wi-Fi, GSM, 4G, 5G, LTE, Bluetooth, NFC gibi),

Yukarıdaki durumlardan birini sağlayan bileşenler, R155 regülasyonu kapsamında değerlendirilmelidir.

İlave olarak;

- Eğer bir bileşen, aracın güvenli olmayan bir durumda çalışmasına neden oluyorsa, bu bileşen mutlaka R155 kapsamına girer.

Örnek Durumlar:

- Hareket halindeki bir aracın üzerine entegre edilmiş kablosuz kontrollü vinç sistemi aktif hale gelirse, bu durum güvenli değildir ve R155 kapsamındadır.
- 9 km/s hızın altında "boşaltım modu"na alınmış bir çöp kamyonunun arka kapağının açılması ise güvenlidir ve R155 kapsamı dışındadır.

Siber Güvenlik Risklerini Azaltıcı Önlemlere Örnekler

- Aracın durumu "güvenli"den "güvensiz"e geçtiğinde, sistemin otomatik olarak devre dışı kalmasını sağlayan interlock sistemleri, geçerli birer siber güvenlik önlemidir.
- Bu tür interlock sistemleri, operatör müdahalesine gerek kalmadan devreye girmelidir.
- Manuel olarak devre dışı bırakılması gereken sistemler, etkin bir siber güvenlik önlemi olarak kabul edilmez.

6. Üstyapıcı Firmaların Sorumlulukları

Siber güvenlik gereksinimlerinin karşılanması kapsamında üstyapıcı firmaların sorumlulukları üç ana modifikasyon tipine göre sınıflandırılmıştır.

6.1. Tip A – Siber Güvenlikle İlgili Olmayan Değişiklikler

E/E mimarisiyle bağlantısı olmayan ve siber güvenlik açısından risk teşkil etmeyen fiziksel modifikasyonlardır.

Sorumluluklar:

- **E/E Mimari Değerlendirmesi**: Eklenen bileşenlerin araç E/E mimarisiyle etkileşimi olup olmadığı belirlenmeli, gerekirse teknik dokümantasyon hazırlanmalıdır.

- **Siber Güvenlik Değerlendirmesi**: Bileşenlerin herhangi bir siber güvenlik etkisi bulunmadığı teyit edilmelidir.
- **Uyum Belgelendirmesi**: Modifikasyonların araç E/E ağına müdahalesi yoksa ve risk içermiyorsa aracın mevcut R155 onayı geçerliliğini korur.

Tip A Kategorisinin Özellikleri:

- Araçtaki E/E ağına (CAN, Üstyapı konnektör, Ethernet vb.) bağlantı yapılmaz.
- Genellikle sadece fiziksel ekipman eklenir.

6.2. Tip B – Siber Güvenlikle İlgili Değişiklikler (Temel Araç E/E Mimarisi Değişmeden)

Araç E/E mimarisi ile sınırlı ve kontrollü etkileşim içeren, OEM arayüzleri (CAN, üstyapı konnektörü. Vb) üzerinden bağlantı kurularak yapılan modifikasyonlardır.

Sorumluluklar:

- **E/E Mimari Entegrasyonu**: Kullanılan donanım/yazılım bileşenleri, OEM arayüzleri üzerinden sisteme entegre edilmelidir.
- **Siber Güvenlik Risk Değerlendirmesi**: Değişikliklerin siber güvenlik etkileri analiz edilerek uygunluk dokümantasyonu hazırlanmalıdır.
- **OEM Talimatlarına Uyum**: Modifikasyonlar, temel araç üreticisinin teknik yönergelerine uygun olarak gerçekleştirilmelidir.
- **Uyum Belgelendirmesi**: Tüm işlemler OEM yönergelerine uygun olduğu sürece, aracın mevcut R155 onayı geçerliliğini korur.

Tip B Kategorisinin Özellikler:

- Üstyapicilarin eriştiği CAN hattı, yalnızca bilgi okuma amacıyla tek yönlü haberleşmeye olanak sağlar.
- Siber güvenlik etki değerlendirmesi sonucunda, ilgili sistemin güvenlik etkisi "düşük" seviyede sınıflandırılmışsa veya riskler yeterli teknik kanıtlarla kontrol altına alındığı şekilde doğrulanabiliyorsa, baz araç için mevcut tip onayı geçerliliğini korur.
- Söz konusu sistem, her ne kadar yalnızca tek yönlü haberleşme (veri okuma) gerçekleştirse de, dijital girişler aracılığıyla ağırlık bilgisi gibi verileri alarak işlem yapmaktadır. Bu bağlamda, dijital girişlerde veya bağlı sensörlerde meydana gelebilecek herhangi bir arıza ya da manipülasyon, potansiyel bir güvenlik riski teşkil edebilir.

6.3. Tip C – Siber Güvenlikle İlgili Değişiklikler (Temel Araç E/E Mimarisi Üzerinde Değişiklik Yapılır)

Aracın orijinal E/E mimarisine doğrudan müdahale edilen, yeni ECU montajı, yazılım geliştirme veya kapsamlı dönüşüm işlemlerini kapsayan modifikasyonlardır.

Sorumluluklar:

- E/E Mimari Değişiklik Analizi: Yapılan tüm yazılım ve donanım değişikliklerinin araç mimarisi üzerindeki etkileri detaylandırılmalıdır.

- TARA (Tehdit Analizi ve Risk Değerlendirmesi): Değişiklikler hem temel araç hem de eklenen üstyapı bileşenleri açısından analiz edilmelidir.

- Üstyapıcı firmanın geçerli bir Siber Güvenlik Yönetim Sistemi (CSMS) sertifikasına sahip olması zorunludur. Bu sistem, OEM'in CSMS'i ile siber güvenlik açısından uyumlu olmalı ve iki taraf arasında gerçekleşecek veri alışverişini kapsayan teknik bir arayüz tanımı hazırlanmalıdır.

  Bu arayüz tanımı;

  - kullanılacak iletişim protokolü,
  - veri formatı ve içerikleri,
  - veri iletim yönü (tek yönlü/çift yönlü),
  - kimlik doğrulama ve yetkilendirme mekanizmaları,
  - güvenli haberleşme yöntemleri (örneğin şifreleme, sertifika doğrulama),
  - hata yönetimi ve geri bildirim süreçleri gibi teknik detayları içermelidir.

- Arayüz tanımı, her iki tarafın siber güvenlik sorumluluklarının sınırlarını net şekilde belirlemeli ve ISO/SAE 21434 ile UNECE R155 kapsamındaki gerekliliklerle uyumlu olacak şekilde dokümante edilmelidir.

- Değişiklikler nedeniyle aracın yeni bir R155 sistem tipi onayı alması zorunludur.

Tip C Kategorisinin Durumlar:

- Üstyapıcı tarafından araca yeni bir ECU entegre edilmişse ve bu ECU, OEM tarafından başlangıçta tanımlanmamış bir bileşense veya yeni bir fonksiyon içeriyorsa, entegrasyon teknik ve siber güvenlik yönleriyle değerlendirilmelidir.

- Yeni bileşen, aracın Elektrik/Elektronik (E/E) ağına doğrudan bağlantı sağlıyorsa (örneğin CAN, LIN, Ethernet üzerinden), bağlantının güvenli olup olmadığı kontrol edilmeli ve yetkisiz erişimlerin önüne geçilmelidir.

- Eklenen ECU, araç CAN hattına bağlıysa ve aktif şekilde mesaj alışverişi yapıyorsa, bu durumda sistemin E/E mimari üzerindeki etkisi değerlendirilmelidir. OEM tarafından izin verilmiş arayüzler dışında herhangi bir bağlantı yapılmamalıdır.

Gerekli Belgeler:

- Üstyapıcının CSMS sertifikası

- Pentest raporları ve ilgili TARA analizleri

- Yeni R155 sistem tip onayı belgesi

Örnekler:

- Elektrikli araç dönüşümleri

- Otonom sürüş modülleri

- Araç dönüşümleri

İlave olarak;

- Modifikasyon tipi doğru şekilde belirlenmelidir.
- Tür C değişikliklerde, hem CSMS hem de R155 onay süreçleri ayrı ayrı yürütülmelidir.
- Ulusal veya AB düzeyinde geçerli siber güvenlik sertifikaları (örn. CSMS) edinilmelidir.

7. Üstyapıcı Tip Onay Süreçleri

Üstyapıcı, baz araç üzerinde gerçekleştirdiği değişikliklerin detaylarını sağlamalıdır. Bu detaylar aşağıdaki unsurları içermelidir:

1. Mekanik değişiklikler
2. Elektriksel bağlantılar
3. Eklenen ECU'lar
4. Baz araçla gönderilen ve alınan mesajlar
5. Kablosuz ve uzaktan bağlantılar

Tip Onay Otoritesi, bu değişikliklerin siber güvenliği etkileyip etkilemediğini değerlendirir. Eğer etkiliyorsa, üstyapıcının baz aracı da dikkate alarak bir Tehdit Analizi ve Risk Değerlendirmesi (TARA) yapması gerekecektir. TARA sonuçları, üstyapıcı sistemlerinde uygulanması gereken önleyici kontrollerin belirlenmesinde kullanılacaktır.