Elektrikli Araçlardaki Kablo Yönlendirmeli Direksiyon Sistemleri için Tehlike Analizi ve Risk Değerlendirmesi

Threat Analysis and Risk Assessment for Electric Vehicle Steer-by Wire Systems

Okan Özçetin[1,2], *Mümin Tolga Emirler*[1,3]

[1]Kontrol ve Otomasyon Mühendisliği Bölümü
Yıldız Teknik Üniversitesi, İstanbul
okan.ozcetin@std.yildiz.edu.tr, emirler@yildiz.edu.tr

[2]Fonksiyonel Emniyet ve Siber Güvenlik Takımı
FEV Türkiye, İstanbul
ozcetin@fev.com

[3]Havacılık Elektrik ve Elektroniği Bölümü
Yıldız Teknik Üniversitesi, İstanbul

Özetçe

Bu bildiride, elektrikli araçlardaki kablo yönlendirmeli direksiyon sistemine saldırganlar tarafından gelebilecek siber saldırıların tehlike analizi ve risk değerlendirmesi sunulmuştur. Tehlike analizi ve risk değerlendirmesinde, kablolu direksiyon sistemi için varlık (asset) ve fonksiyonlar tanımlanmıştır. Ardından ilgili fonksiyonlar için tehlike senaryoları ve tehlike tipleri belirlenmiştir. Hasar senaryoları ve hasar tipleri de tehlike senaryolarının ve tehlike tiplerinin sonuçlarına göre tespit edilmiştir. Hasar senaryosunun yarattığı etki ve siber saldırganın hangi yol ile siber fiziksel sistemlere sızdığının belirlenmesi ile atak fizibilitesi değerlendirmesi ortaya çıkmıştır. Bu değerlendirmeye istinaden tehlike analizi ve risk değerlendirmesi sonucunda siber güvenlik güvence seviyesi belirlenmektedir. Tehlike analizi ve risk değerlendirmesi ile kablo yönlendirmeli direksiyon sistemlerine yapılacak siber tehditlere karşı hangi seviyede nasıl önlemler alınması gerekliliği konusu ortaya konmuştur.

Abstract

This paper presents the threat analysis and risk assessment of cyber attacks by attackers on the steer-by wire system in electric vehicles. In the threat analysis and risk assessment, the asset and functions of the steer-by-wire system have been identified. Then, the threat scenarios and threat types have been determined for the relevant functions. Damage scenarios and damage types have been also determined based on the results of the threat scenarios and threat types. The attack feasibility assessment emerged with the determination of the effect of the damage scenario and the way in which the cyber attacker infiltrated the cyber physical systems. Based on this assessment, the cyber security assurance level is determined as a result of the threat analysis and risk assessment. With the threat analysis and risk assessment, the issue of what level of precautions should be taken against cyber threats by steer-by-wire systems has been revealed.

1. Giriş

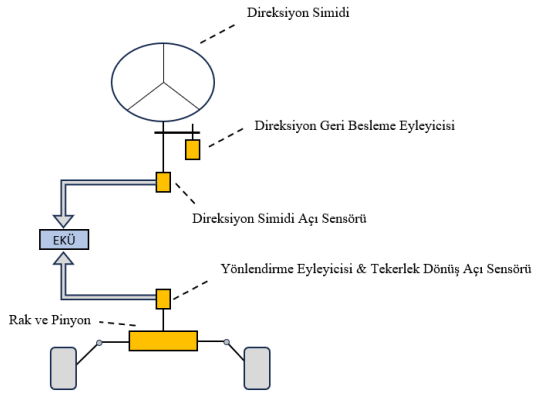
Araçların daha akıllı ve bağlantılı hale gelmesiyle, otomotiv sistemleri de giderek daha karmaşık hale gelmektedir [1-4]. Elektrik-elektronik sistemlerdeki karmaşıklığın artması ve otomotiv haberleşme ağlarının gelişmesiyle birlikte araçlara kablosuz erişim mümkün olmaktadır. Upstream Security'e [5] göre, 2025 yılına kadar, yalnızca internet veya yerelleştirme hizmetlerinden yararlanma olasılığı değil, aynı zamanda V2X (Araçtan X'e) paradigmasının benimsenmesi ile birlikte, yeni arabaların tamamı bağlantılı olarak sevk edilecektir. Bağlantılılık ifadesi, aracın diğer araçlarla (V2V, Araçtan Araca), genel bir altyapıyla (V2I) veya yayalarla (V2P) iletişim kurma ve veri alışverişi yapma kabiliyetini ifade etmektedir [6].

Araçlardaki özelliklerin, bağlanabilirliğin ve karmaşıklığın artması verilerde çok sayıda etkileşime yol açarak bilgisayar korsanları, suçlular ve casuslar tarafından yararlanılabilecek güvenlik açıklarına neden olabilir [7]. Akıllı araçların karşılaştığı dinamik, çeşitlendirilmiş ve üst düzey saldırılar; kişisel mahremiyeti ve güvenliği ve hatta toplumsal güvenliği ilgilendiren sorunlara yol açabilir [8-9].

Kablo yönlendirmeli direksiyon sistemi günümüzdeki direksiyon kavramının çehresini değiştiren teknolojik bir gelişmedir [10]. Kablo yönlendirmeli direksiyon sisteminin başlıca işlevi aracın dümenlenmesi olarak belirtilebilir. Direksiyon simidinden direksiyon rakına mekanik bir bağlantının ve hidrolik direksiyonda hidroliğin kullanılması yerine, bağlantısız kablolu direksiyon sistemi hem direksiyon simidinde hem de direksiyon kremayerinde elektrik motorları kullanır [10]. Şekil 1'de kablo yönlendirmeli direksiyon sisteminin yapısı gösterilmektedir.

Geleneksel direksiyon sisteminde kullanılan mekanik bağlantının yerine kablo yönlendirmeli direksiyon sisteminde elektronik kontrol ünitesi, direksiyon eyleyicisi, direksiyon açı sensörü, geri besleme eyleyicisi gibi elektronik bileşenler kullanabilmektedir. Elektronik kontrol ünitesi sensörlerden ve

sürücüden gelen bilgileri alır, değerlendirir ve direksiyonun nasıl aksiyon alması gerektiği bilgisini direksiyon eyleyicisine iletir. Elektronik kontrol ünitesi bu bilgileri gerektiğinde CAN bağlantısı yolu ile araçtaki diğer kontrol ünitelerine ve birimlere gönderebilmektedir. Böylelikle direksiyon sisteminde artan karmaşıklık ve haberleşme yapısı ile birlikte önlem alınmadığı takdirde güvenlik açıklarının bulunduğu siber saldırganlar tarafından sızılabilecek bir sistem haline gelmiştir. Bu bildiride, kablolu direksiyon sistemi için tehlike ve hasar senaryoları belirtilmiştir. Bununla birlikte sürücünün bu senaryolardan nasıl etkilenebileceğini belirlemeye yönelik yöntemlerin açıklandığı tehlike analizi ve risk değerlendirmesi süreci sunulmuştur.

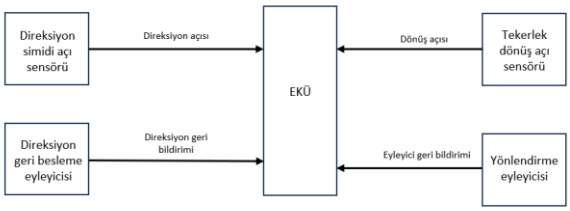


Şekil 1: Kablo yönlendirmeli direksiyon sistemi [10].

Bildirinin bundan sonraki bölümleri şu şekilde düzenlenmiştir. Bölüm 2'de tehlike analizi ve risk değerlendirmesi öncesi öğe tanımı yapılmıştır. Bölüm 3'te elektrikli araçlardaki kablo yönlendirmeli direksiyon sistemi için siber saldırılara karşı tehlike analizi ve risk değerlendirmesi yapılmıştır. Bildiri Bölüm 4'te verilen sonuçlarla sonlandırılmıştır.

2. Öğe Tanımı

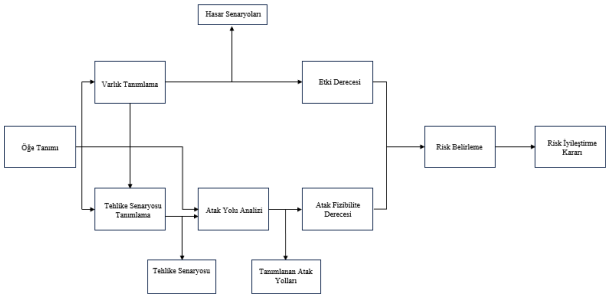
Tehlike analizi ve risk değerlendirmesi yapılmadan önce öğe tanımı yapılmaktadır. Öğe tanımında; öğe sınırları, öğe fonksiyonları ve ön mimari tanımlanmaktadır. Kablo yönlendirmeli direksiyon sisteminin ön mimarisi Şekil 2'de gösterilmiştir.



Şekil 2: Kablo yönlendirmeli direksiyon sistemi ön mimarisi.

3. Tehlike Analizi ve Risk Değerlendirmesi

Bir yol kullanıcısının bir tehlike senaryosundan ne ölçüde etkilenebileceğini belirlemeye yönelik yöntemlerin açıklandığı çıktı Tehlike Analizi ve Risk Değerlendirmesi (TARD) olarak bilinmektedir. Tehlike analizi ve risk değerlendirmesi Şekil 3'te verilen akışa uygun olarak işlemektedir.



Şekil 3: Tehlike analizi ve risk değerlendirmesi akış diyagramı.

3.1. Varlık Tanımlaması

Varlık, değeri olan veya değere katkıda bulunan nesnedir. Varlık tanımlanmasında hasar senaryoları ve siber güvenlik özellikleri için varlıklar tanımlanmalıdır [11]. Kablo yönlendirmeli direksiyon sistemi için belirlenen varlıklar Tablo 1'de gösterilmiştir.

Tablo 1: Kablo yönlendirmeli direksiyon sistemi için varlıklar

Varlıklar
Kablo yönlendirmeli direksiyonun elektronik kontrol ünitesi
Direksiyon geri besleme eyleyicisi
Yönlendirme eyleyicisi

3.2. Tehlike Senaryoları

Bir hasar senaryosunu gerçekleştirmek için bir veya daha fazla varlığın siber güvenlik özelliklerinin tehlikeye atılmasının potansiyel nedenidir [11]

Tehlike senaryosu aşağıdaki öğeleri tanımlamalı ve içermelidir [3]:

- Tehlike senaryosu hedef varlığı
- Varlığın ödün verilen siber güvenlik özelliği
- Ödün verilen siber güvenlik özelliklerinin nedeni

Kablo yönlendirmeli direksiyon sistemi için belirlenen tehlike senaryoları Tablo 2'de gösterilmiştir.

Tablo 2: Kablo yönlendirmeli direksiyon sistemi için tehlike senaryoları

Tehlike Senaryosu No:	Tehlike Senaryosu	Tehlike Tipi	Hasar Senaryosu No:
TSR1	Saldırgan, kablo yönlendirmeli direksiyon sistemine giden direksiyon simidi açı sensörü kablo bağlantısını fiziksel olarak keserek veya hasar vererek iletişim veya kontrol kaybına yol açar.	Kurcalama	D3
TSR2	Saldırgan pinyon açı sensörü kablo bağlantısını fiziksel olarak keserek veya hasar vererek iletişim veya kontrol	Kurcalama	D3

	kaybına yol açar.		
TSR3	Bir saldırgan, uygun yetkilendirme olmadan direksiyon sistemini kendi çıkarları için kullanmaya veya kontrol etmeye çalışan kablo yönlendirmeli direksiyon sistemine sistemine erişebilir.	Bilgi ifşası	D3
TSR4	Bir saldırgan, yönlendirme kontrolünün kaybedilmesine neden olabilecek virüsler, solucanlar veya fidye yazılımı gönderebilir.	Hizmet reddi	D1
TSR5	Bir saldırgan, direksiyon simidi açısı sensörünü kendi çıkarları için kullanabilir, bu da sisteme yanlış bilgilerin beslenmesine neden olabilir ve geri besleme direksiyon torkunda kayba neden olabilir.	Sahtekarlık	D4
TSR6	Bir saldırgan rak konum sensörünü kendi çıkarlı için kullanarak sisteme yanlış bilgilerin beslenmesine neden olabilir.	Sahtekarlık	D5
TSR7	Bir saldırgan, yönlendirme eyleyicisinin işlevselliğini bozabilecek veya tehlikeye atabilecek kötü amaçlı yazılımı yönlendirmeli direksiyon sistemine gönderebilir.	Hizmet reddi	D6
TSR8	Bir saldırgan, kablolu direksiyon sisteminde yer alan bileşenler arasındaki iletişimi engelleyerek yönlendirme eyleyecesi özelliklerini potansiyel olarak değiştirebilir.	Hizmet reddi	D6
TSR9	Saldırgan, kablo yönlendirmeli direksiyon sisteminin EKÜ'süne yetkisiz erişim elde eder ve bellenimi kendi çıkarları için kullanabilir.	Bilgi ifşası	D2
TSR10	Saldırgan, direksiyon simidi üzerindeki geri besleme torkunu yönlendirerek sürücüyü etkileyecek bir güvenlik açığından yararlanan kötü amaçlı bir girdi gönderebilir.	Sahtekarlık	D7

3.3. Hasar Senaryoları

Hasar senaryoları sırasıyla emniyet, finansal, operasyonel ve mahremiyet (E,F,O,M) etki kategorilerinde olası potansiyel olumsuzluklara göre değerlendirilmelidir.

Bir hasar senaryosunun etki derecesi her etki kategorisi için aşağıdakilerden biri olarak karar verilmelidir:

- Şiddetli
- Büyük
- Orta
- İhmal edilebilir

3.4. Etki Derecesi

Eki derecesi, bir hasar senaryosundan fiziksel hasarın veya hasarın büyüklüğünün tahmininin derecesidir [11].

Kablo yönlendirmeli direksiyon sistemi için belirlenen hasar senaryoları Tablo 3'te, hasar senaryolarının kategorileri ve etki dereceleri Tablo 4'te gösterilmiştir. Tablo 4'te güvenlik özelliği olarak belirtilen G: Gizlilik, B: Bütünlük, U: Uygunluk, Y: Yetki'yi göstermektedir.

Tablo 3: Kablo yönlendirmeli direksiyon sistemi için hasar senaryoları

	Güvenlik Özelliği				
Hasar No:	G	B	U	Y	Hasar Senaryosu
D1		x			Sürücü, direksiyon hakimiyetini kaybettiği için aracı yönlendiremez
D2			x	x	Kablo yönlendirmeli direksiyon sisteminin kalıcı olarak kullanılamaması nedeniyle yönlendirme istenmeden etkinleştirilebilir
D3			x	x	Kablo yönlendirmeli direksiyon sisteminin kalıcı olarak kullanılamaması nedeniyle direksiyon kontrolünün kaybı gerçekleşebilir
D4		x			Geri bildirim torkunun belirlenmesi için kullanılan sensörlere yanlış bilgiler gelmesi nedeniyle geri bildirim torku kaybolur.
D5		x			Sensörler ile belirlenen rak pozisyonunun yanlış bilgiler gelmesi nedeniyle aracın yanal kontrolü kaybedilir.
D6			x	x	Kablo yönlendirmeli direksiyon sistemine gönderilen kötü amaçlı yazılım nedeniyle beklenmedik yanal hareket gerçekleşir.
D7		x			Sömürü ve güvenlik açığı nedeniyle daha az veya daha fazla direksiyon torku geri bildirimi alınır.

Tablo 4: Kablo yönlendirmeli direksiyon sistemi için hasar senaryolarının kategorileri ve etki dereceleri

	Hasar Kategorisi					
Hasar No:	E	F	O	G	Etki Tanımı	Etki derecesi
D1	x				Yol kullanıcılarına ölümcül yaralanma	Şiddetli
D2	x	x			Yol kullanıcılarına ölümcül yaralanma	Şiddetli
D3	x	x			Yol kullanıcılarına ölümcül yaralanma	Şiddetli
D4	x				Yol kullanıcılarına ölümcül yaralanma	Şiddetli
D5	x				Yol kullanıcılarına ölümcül yaralanma	Şiddetli
D6	x				Yol kullanıcılarına ölümcül yaralanma	Şiddetli
D7	x			x	Yol kullanıcılarına ölümcül yaralanma	Şiddetli

3.5. Atak Yolu Analizi

Tehlike senaryoları atak yollarını tanımlamak için analiz edilmelidir. Atak yolu, atak yolu tarafından gerçekleştirilebilen tehlike senaryoları ile ilişkilidir [11].

Kablo yönlendirmeli direksiyon sistemi için 5 farklı tehlike tipine göre belirlenen atak yolu analizi Tablo 5'te gösterilmiştir.

Tablo 5: 5 adet tehlike senaryosu için atak yolu analizi

Tehlike Senaryosu No:	Tehlike Senaryosu	Atak Yolu
TS5	Bir saldırgan, direksiyon simidi açısı sensörünü kendi çıkarları için kullanabilir, bu da sisteme yanlış bilgilerin gelmesine ve geri besleme direksiyon torkunda kayba neden olabilir.	Kötü niyetli sinyaller direksiyon açı sensörünü yanıltır.
		EKÜ, direksiyon geri besleme eyleyecisinden kötü amaçlı sinyaller alır.
TS7	Bir saldırgan, geri besleme eyleyicisinin işlevselliğini bozabilecek veya tehlikeye atabilecek kötü amaçlı yazılımı kablo yönlendirmeli direksiyon sistemine gönderebilir.	Saldırgan, iletişim veri yolunu çok sayıda mesajla doldurur.
		Saldırgan, sürücünün akıllı telefonunu Bluetooth arabirimiyle tehlikeye atar.
TS6	Bir saldırgan rak konum sensörünü manipüle ederek sisteme yanlış bilgilerin beslenmesine neden olabilir.	Kötü niyetli sinyaller rak açı sensörünü yanıltır.
TS9	Saldırgan, kablo yönlendirmeli direksiyon sisteminin EKÜ'süne yetkisiz erişim elde eder ve bellenimi manipüle edebilir.	Saldırgan, Bluetooth arayüzünden navigasyon EKÜ'sünü ele geçirir.
TS8	Bir saldırgan, kablo yönlendirmeli direksiyon sisteminde yer alan bileşenler arasındaki iletişimi engelleyerek geri besleme eyleyicisinin özelliklerini potansiyel olarak değiştirebilir.	Saldırgan, iletişim veri yolunu çok sayıda mesajla doldurur.

3.6. Atak Fizibilite Derecesi

Atak fizibilite derecelendirme metodu; atak potansiyel bazlı yaklaşımı, OGAPS (Ortak Güvenlik Açığı Puanlama Sistemi) ve atak vektör bazlı yaklaşım gibi çeşitli yaklaşımlara göre tanımlanabilir [11]. Bu bildiride atak vektör bazlı yaklaşım kullanılarak atak fizibilite derecelendirmesi yapılmıştır.

Atak vektörü tabanlı yaklaşım, saldırı yolu kullanımının mümkün olduğu bağlamı yansıtır. Atak fizibilite derecesi, bir saldırgan saldırı yolundan yararlanmak için ne kadar uzak olabilirse (mantıksal ve fiziksel olarak) o kadar yüksek olacaktır [11]. ISO 21434 standardına göre atak vektör bazlı yaklaşım Tablo 6'da gösterilmiştir.

Tablo 6: Atak vektör bazlı yaklaşım[11]

Atak fizibilite derecesi	Kriter
Yüksek	Ağ: Potansiyel saldırı yolu, herhangi bir sınırlama olmaksızın ağ yığınına bağlıdır. ÖRNEK 1: EKÜ'ye doğrudan bağlı kılan hücresel ağ bağlantısı ve internetten erişilebilir
Orta	Bitişik: Potansiyel saldırı yolu, ağ yığınına bağlıdır; ancak bağlantı fiziksel veya mantıksal olarak sınırlıdır. ÖRNEK 2: Bluetooth arabirimi, sanal özel ağ bağlantısı.
Düşük	Yerel: Potansiyel saldırı yolu, ağ yığınına ve tehdit ajanlarına bağlı değildir saldırı yolunu gerçekleştirmek için öğeye doğrudan erişim gerektirir. ÖRNEK 3: Evrensel seri veri yolu yığın depolama cihazı, hafıza kartı.
Çok düşük	Fiziksel: Tehdit ajanları, saldırı yolunu gerçekleştirmek için fiziksel erişim gerektirir.

Kablo yönlendirmeli direksiyon sistemi için atak vektörü yaklaşımıyla belirlenen atak fizibilite derecelendirmesi Tablo 7'de verilmiştir.

Tablo 7: Kablo yönlendirmeli direksiyon sistemi için atak fizibilite derecelendirmesi

Tehlike Senaryosu No:	Tehlike Tipi	Atak vektörü	Atak Fizibilite Derecesi
TSR1	Kurcalama	Fiziksel	Çok düşük
TSR2	Kurcalama	Fiziksel	Çok düşük
TSR3	Bilgi ifşası	Ağ	Yüksek
TSR4	Hizmet reddi	Ağ	Yüksek
TSR5	Sahtekarlık	Yerel	Düşük
TSR6	Sahtekarlık	Yerel	Düşük
TSR7	Hizmet reddi	Ağ	Yüksek
TSR8	Hizmet reddi	Ağ	Yüksek
TSR9	Bilgi ifşası	Ağ	Yüksek
TSR10	Sahtekarlık	Yerel	Düşük

3.7. Siber Güvenlik Güvence Seviyesi ve Siber Güvenlik Hedefleri

Bir siber güvenlik güvence seviyesi(SGS) dolaylı olarak riskle ilişkilidir; ancak doğrudan bir risk değerinden belirlenemez. Bunun nedeni, risk değerinin dinamik olması, öğenin veya bileşenin gelişen spesifikasyonuna, tasarımına, uygulamasına ve işletim ortamına bağlı olarak zaman içinde değişmesidir; oysa SGS zaman içinde sabit kalacak bir güvence düzeyini ifade eder [11].

Siber güvenlik hedefi bir veya daha fazla tehdit senaryosuyla ilişkili konsept düzeyinde siber güvenlik gereksinimidir [11]. Siber güvenlik hedefi en yüksek seviye gereksinimlerdir.

Atak vektör yaklaşımı ile belirlenen atak fizibilite derecelendirmesi ve etki derecesine göre belirlenen siber güvenlik güvence seviyeleri sırasıyla Tablo 8 ve Tablo 9'da gösterilmiştir.

Tablo 8: Etki ve atak vektörü parametrelerine dayalı örnek SGS belirlemesi [11]

Etki değeri	Atak vektörü(b)			
	Fiziksel	Yerel	Bitişik	Ağ
Şiddetli	SGS2	SGS3	SGS4	SGS4
Büyük	SGS1	SGS2	SGS3	SGS4
Orta	SGS1	SGS1	SGS2	SGS3
İhmal edilebilir	--a	--a	--a	--a

--a: Risk değeri belirlemeye göre yapılan bir analizden belirlenen risk değeri 1 olan tehdit senaryoları için, siber güvenlik konsepti, ürün geliştirme ve siber güvenlik doğrulamasına uygunluk atlanabilir.

b: Atak vektörü, atak fizibilitesinin statik bir parametresidir.

Tablo 9: Tehlike senaryoları için siber güvenlik güvence seviyesi ve siber güvenlik hedefleri

Tehlike Senaryosu No:	Atak vektörü	Atak fizibilite derecesi	SGS	Siber güvenlik hedefleri
TS1	Fiziksel	Çok düşük	SGS 2	Kablo yönlendirmeli direksiyon sistemi EKÜ'sünün bütünlüğü sağlanmalıdır.
TS2	Fiziksel	Çok düşük	SGS 2	Kablo yönlendirmeli direksiyon sistemi EKÜ'sünün bütünlüğü sağlanmalıdır.
TS3	Ağ	Yüksek	SGS 4	Kablo yönlendirmeli direksiyon sistemi EKÜ'sünün gizliliği ve kimlik doğrulaması sağlanmalıdır.
TS4	Ağ	Yüksek	SGS 4	Kablo yönlendirmeli direksiyon sistemi EKÜ'sünün uygunluğu ve kimlik doğrulaması sağlanmalıdır.
TS5	Yerel	Düşük	SGS 3	Direksiyon geri besleme eyleyicisinin bütünlüğü sağlanmalıdır.
TS6	Yerel	Düşük	SGS 3	Yol tekerleği eyleyicisinin bütünlüğü sağlanmalıdır
TS7	Ağ	Yüksek	SGS 4	Yol tekerleği eyleyicisinin uygunluğu ve kimlik doğrulaması sağlanmalıdır.
TS8	Ağ	Yüksek	SGS 4	Kablo yönlendirmeli direksiyon sistemi EKÜ'sünün uygunluğu ve kimlik doğrulaması sağlanmalıdır.
TS9	Ağ	Yüksek	SGS 4	Kablo yönlendirmeli direksiyon sistemi EKÜ'sünün gizliliği ve kimlik doğrulaması sağlanmalıdır.

TS10	Yerel	Düşük	SGS 3	Direksiyon geri besleme eyleyicisinin bütünlüğü sağlanmalıdır.

3.8. Risk Değeri Belirleme

Her tehlike senaryosu için risk değeri, ilişkili hasar senaryolarının etkisinden ve ilişkili saldırı yollarının saldırı fizibilitesinden belirlenmelidir.[11]. Risk matrisi örneği Tablo 10'da gösterilmiştir.

Kablo yönlendirmeli direksiyon sistemi için belirlenen risk değerleri Tablo 11'de gösterilmiştir.

Tablo 10: Risk matrisi örneği[11]

		Atak fizibilite derecesi			
		Çok düşük	Düşük	Orta	Yüksek
Etki değeri	Şiddetli	2	3	4	5
	Büyük	1	2	3	4
	Orta	1	2	2	3
	İhmal edilebilir	1	1	1	1

Tablo 11: Kablo yönlendirmeli direksiyon sistemi için risk değerleri

Tehlike Senaryosu No:	Etki değeri	Atak fizibilite derecesi	Risk değeri
TS1	Şiddetli	Çok düşük	2
TS2	Şiddetli	Çok düşük	2
TS3	Şiddetli	Yüksek	5
TS4	Şiddetli	Yüksek	5
TS5	Şiddetli	Düşük	3
TS6	Şiddetli	Düşük	3
TS7	Şiddetli	Yüksek	5
TS8	Şiddetli	Yüksek	5
TS9	Şiddetli	Yüksek	5
TS10	Şiddetli	Düşük	3

3.9. Risk İyileştirme Kararı

Her bir tehlike senaryosu için, risk değerleri dikkate alınarak aşağıdaki risk iyileştirme seçeneklerinden biri veya birkaçı belirlenmelidir [11]:

- Riskten kaçınmak
- Riskin azaltılması
- Riskin paylaşılması
- Riskin elde tutulması

Kablo yönlendirmeli direksiyon sistemi için belirlenen risk iyileştirme kararı Tablo 12'de gösterilmiştir.

Tablo 12: Kablo yönlendirmeli direksiyon sistemi için risk iyileştirme kararları

Tehlike Senaryosu No:	Risk değeri	Risk iyileştirme kararı
TS1	2	Riskin azaltılması
TS2	2	Riskin azaltılması
TS3	5	Riskten kaçınmak
TS4	5	Riskten kaçınmak
TS5	3	Riskin azaltılması
TS6	3	Riskin azaltılması
TS7	5	Riskten kaçınmak
TS8	5	Riskten kaçınmak
TS9	5	Riskten kaçınmak
TS10	3	Riskin azaltılması

4. Sonuçlar

Bu bildiride, kablo yönlendirmeli direksiyon sistemi için Tehlike Analizi ve Risk Değerlendirmesi çalışması gerçekleştirilmiştir. TARD'dan önce sistemin sınırları ve fonksiyonları belirlenmiş olup saldırganların ilgili direksiyon sistemine erişebilmek için kullanabileceği varlıklar belirlenmiştir. Bu varlıklara erişebilen saldırganların yaratabileceği tehlikeler ve hasar senaryoları ile birlikte etki derecesi, siber güvenlik güvence seviyesi ve atak fizibilite derecesi belirlenmiştir. Atak fizibilite derecesi ve etki değerine istinaden risk değerleri ve risk değerlerini düşürmek için de risk iyileştirme kararları belirtilmiştir. İlgili TARD'ta siber güvenlik özelliklerine göre en yüksek seviye gereksinim olan siber güvenlik hedefleri belirlenmiştir. Gelecek çalışmalarda, TARD çalışmasından sonra gerçekleştirilecek siber güvenlik konsept çalışması ile siber güvenlik hedeflerine dayanarak siber güvenlik gereksinimleri geliştirilecektir.

Teşekkür

Bu bildiriyi hazırlarken desteklerini ve yardımı esirgemeyen FEV Türkiye'den Kıdemli Otomotiv Fonksiyonel Emniyet Mühendisi Gökhan Mersin'e teşekkür ederim.

Kaynakça

[1] M. Steger, M. Karner, J. Hillebrand, W. Rom ve K. Römer, "A Security Metric for Structured Security Analysis of Cyber-Physical Systems Supporting SAE J3061," 2nd International Workshop on Modelling, Analysis, and Control of Complex CPS (CPS Data), Viyana, Avusturya, 2016.

[2] G. Xie, G. Zeng, Z. Li, R. Li ve K. Li, "Adaptive Dynamic Scheduling on Multi-Functional Mixed-Critically Automotive Cyber-physical systems," *IEEE Trans. on Vehicular Technology*, 66(8), s: 6676-6692, 2017.

[3] G. Xie, H. Peng, Z. Li, J. Song, Y. Xie, R. Li ve K. Li. "Reliability Enhancement Towards Functional Safety Goal Assurance in Energy-Aware Automotive Cyber-Physical systems," *IEEE Trans. on Industrial Informatics*, 14(12), s: 5447–5462, 2018.

[4] G. Xie, H. Peng, J. Huang, R. Li ve K. Li, "Energy-Efficient Functional Safety Design Methodology using ASIL Decomposition for Automotive Cyber-Physical Systems," *IEEE Trans. on Reliability*, 99, s: 1–23, 2019.

[5] "Global Automotive Cybersecurity Report," Upstream Security, Technical Report 2018, 2019.

[6] M. Sicalas ve G. Giacinto, "Automotive Cybersecurity: Foundations for Next-Generation Vehicles," 2nd International Conference on New Trends in Computing Sciences (ICTCS), Amman, Ürdün.

[7] Y. Wang, Y. Wang, H. Qin, H. Ji, Y. Zhang ve J. Wang, " A Systematic Risk Assessment Framework of Automotive Cybersecurity," *Automotive Innovation*, 4, s: 253-261, 2021.

[8] C. Miller ve C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," Black Hat ABD, Las Vegas, ABD, 2015.

[9] J. Petit, B. Stottelaar, M. Feiri ve F. Kargl, "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and Lidar," Black Hat Avrupa, Amsterdam, Hollanda, 2015.

[10] M. F. Westlund ve X. Song, "Steer-by-wire system safety aspects,", Bitirme Tezi, KTH Royal Institute of Technology, Vehicle Engineering, Stokholm, İsveç, 2022.

[11] ISO/SAE 21434:2021 Standardı: Road Vehicles – Cybersecurity Engineering, 2021.