Journal of the Faculty of Engineering and Architecture of Gazi University 40:3 (2025) 1951-1966

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University
Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

A comparative evaluation of the prominent methods in autonomous vehicle certification

Mustafa Erdem Kırmızıgül[1,3,4]*, Hasan Feyzi Doğruyol[2], Haluk Bayram[3,4]

[1]Transportation and Infrastructure Ministry, DG for Regulation of Transport Services, 06338, Çankaya, Ankara, Türkiye
[2]Havelsan, Bilişim Vadisi, 41400, Gebze, Kocaeli, Türkiye
[3]Field Robotics Laboratory, Science and Advanced Technologies Research Center (BILTAM), Istanbul Medeniyet University, 34700, Üsküdar, İstanbul, Türkiye
[4]Field Robotics Laboratory, Robotics and Artificial Intelligence Laboratories (ROYAL), Bogazici University, 34342, Bebek, Istanbul, Türkiye

Highlights:

- Comparative analysis of RSS, PEGASUS and STPA methods
- Evaluation of these methods and their roles in the certification process of autonomous vehicles
- Incorporating these methods into the certification process and developing a flow-chart

Keywords:

- Certification of Autonomous Vehicles
- RSS
- STPA
- PEGASUS
- Vision Zero

Article Info:

Research Article
Received: 06.07.2023
Accepted: 08.03.2025

DOI:

10.17341/gazimmfd.1323360

Acknowledgement:

The work was partially supported by "ROYAL CB SBB 2019K12-149250"

Correspondence:

Author: Mustafa Erdem Kırmızıgül
e-mail: mustafa.kirmizigul@uab.gov.tr
phone: +90 530 422 5580

Graphical/Tabular Abstract

The "Vision Zero" policy, introduced by the Swedish Parliament in 1997, aims to eliminate fatalities and serious injuries resulting from traffic accidents. To achieve this goal, the use of self-driving vehicles in traffic is envisioned and a roadmap for the certification of self-driving vehicles is aimed to be determined. However, it is still unclear how the basic safety requirements that autonomous vehicles must meet will be verified and certified, and which methods will be used. This paper focuses on the comparative evaluation of the prominent methods planned to be used in the certification process of autonomous vehicles. It examines the prominent methods used in the certification process, develops a pipeline for the certification process of autonomous vehicles, and determines the stages, actors, and areas where the addressed methods can be applied. Figure A illustrates a general view of a certification process.

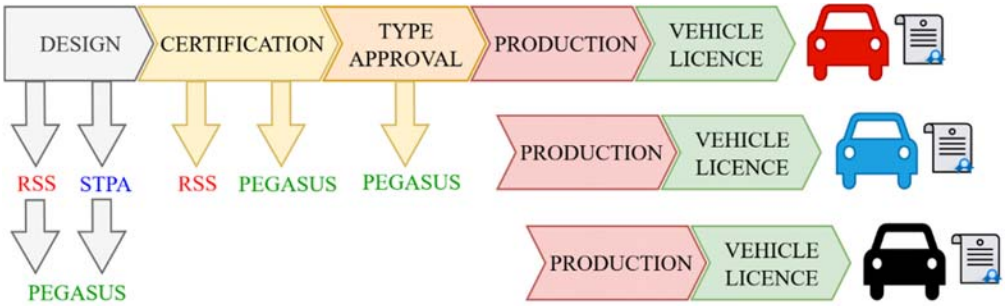


Figure A. Pipeline in the Certification Process of Autonomous Vehicles

Purpose: The paper aims to provide a comparative evaluation of the certification methods for autonomous vehicles and determine which method should be used at which stages, by which actors, and for which purposes in the certification process.

Theory and Methods: Our study adopts a comprehensive and comparative approach to evaluate the certification methods for autonomous vehicles. Grounded in the critical aspects of safety assessment, validation, and certification, we examine and compare prominent methods, including RSS, STPA, and PEGASUS. Through a rigorous evaluation, we assess the strengths and limitations of each method, considering their applicability at different stages, by diverse actors, and for specific purposes within the certification process. Furthermore, we establish a structured pipeline model that depicts the sequential steps involved in the certification process of autonomous vehicles.

Results: After conducting the study, we evaluate the certification process of autonomous vehicles and examine the roles of various methods in a comparative manner. All these methods are situated within the pipeline of the autonomous vehicle certification process.

Conclusion: In this paper, we have addressed the critical aspects of safety assessment, validation, and certification for autonomous vehicles. Specifically, we have conducted a comparative examination of prominent methods such as RSS, STPA, and PEGASUS in the context of autonomous vehicle certification. Furthermore, we have established a structured pipeline for the certification process of autonomous vehicles, as depicted in Figure A. Additionally, we have identified the appropriate method to be employed at different stages, by various actors, and for specific purposes within the process.

Journal of the Faculty of Engineering and Architecture of Gazi University 40:3 (2025) 1951-1966

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Otonom araç sertifikasyonunda öne çıkan metotların karşılaştırmalı değerlendirilmesi

Mustafa Erdem Kırmızıgül[1,3,4]*, Hasan Feyzi Doğruyol[2], Haluk Bayram[3,4]

[1]Ulaştırma ve Altyapı Bakanlığı, Ulaştırma Hizmetleri Düzenleme Genel Müdürlüğü, 06338, Çankaya, Ankara, Türkiye
[2]Havelsan, Bilişim Vadisi, 41400, Gebze/Kocaeli
[3]Saha Robotik Laboratuvarı, Bilim ve İleri Teknoloji Uygulama ve Araştırma Merkezi (BİLTAM), İstanbul Medeniyet Üniversitesi, 34700, Üsküdar, İstanbul, Türkiye
[4]Saha Robotik Laboratuvarı, Robotik ve Yapay Akıl Laboratuvarları (ROYAL), Boğaziçi Üniversitesi, 34342, Bebek, İstanbul, Türkiye

ÖNEÇIKANLAR

- RSS, STPA ve PEGASUS metotlarının karşılaştırmalı analizi
- Otonom araçların sertifikasyon sürecinde kullanılacak metotların ve rollerinin değerlendirilmesi
- Bu metotların sertifikasyon süreciyle bütünleştirilerek, akış diyagramı haline getirilmesi

Makale Bilgileri
Araştırma Makalesi
Geliş: 06.07.2023
Kabul: 08.03.2025

DOI:
10.17341/gazimmfd.1323360

Anahtar Kelimeler:
Otonom Araçların Sertifikasyonu, RSS, STPA, PEGASUS, Vizyon Sıfır

ÖZ

1997'de İsveç Parlamentosu'nun kabul etmiş olduğu "Vizyon Sıfır" politikası, trafik kazalarından kaynaklanan ölümlerin ve ciddi yaralanmaların azaltılmasını hedeflemektedir. Bu hedefe ulaşmak için trafikte otonom araçların kullanılması öngörülmüş ve otonom araçların sertifikasyonu için bir yol haritasının belirlenmesi amaçlanmıştır. Bununla birlikte otonom bir aracın sahip olması gereken temel emniyet gereksinimlerinin nasıl doğrulanarak sertifikalandırılacağı ve hangi metotların kullanılacağı konuları hala açıklığa kavuşmuş değildir. Bu makalede otonom araçların sertifikasyonunda öne çıkan metotlar karşılaştırmalı olarak değerlendirilmiş, aracın sertifikasyon süreci bir akış diyagramı haline getirilerek ele alınan metotların bu süreçte hangi aşamalarda, hangi aktörler tarafından ve ne amaçla kullanılabileceği belirlenmiştir.

A comparative evaluation of the prominent methods in autonomous vehicle certification

HIGHLIGHTS

- Comparative analysis of RSS, PEGASUS and STPA methods
- Evaluation of these methods and their roles in the certification process of autonomous vehicles
- Incorporating these methods into the certification process and developing a flow-chart

Article Info
Research Article
Received: 06.07.2023
Accepted: 08.03.2025

DOI:
10.17341/gazimmfd.1323360

Keywords:
Certification of Autonomous Vehicles, RSS, STPA, PEGASUS, Vision Zero

ABSTRACT

The "Vision Zero" policy, introduced by the Swedish Parliament in 1997, aims to eliminate fatalities and serious injuries resulting from traffic accidents. To achieve this goal, the use of self-driving vehicles in traffic is envisioned and a roadmap for the certification of self-driving vehicles is aimed to be determined. However, it is still unclear how the basic safety requirements that autonomous vehicles must meet will be verified and certified, and which methods will be used. This paper focuses on the comparative evaluation of the prominent methods planned to be used in the certification process of autonomous vehicles. It examines the prominent methods used in the certification process, develops a pipeline for the certification process of autonomous vehicles, and determines the stages, actors, and areas where the addressed methods can be applied.

*Sorumlu Yazar/Yazarlar / *Corresponding Author/Authors: *mustafa.kirmizigul@uab.gov.tr, hfdogruyol@havelsan.com.tr, haluk.bayram@medeniyet.edu.tr / Tel: +90 530 422 5580

1. Giriş (Introduction)

Genel olarak otonom araç, çevresini algılama ve insan müdahalesi olmaksızın seyahat etme kabiliyetlerine sahip araç olarak tanımlanır [1]. Otomotiv Mühendisleri Derneği (Society of Automotive Engineers - SAE) tarafından, günümüzde üçüncü revizyonu yayımlanmakta olan J3016 standardında araçların otonomi kabiliyetlerine göre altı otonomi seviyesine ayrıldığı bir taksonomi tanımlanmaktadır. Bu taksonomi ile araçlar 0'ıncı seviyeden 5'inci seviyeye kadar; otonom sürüş olmayan, sürücü destek, kısmen otonom sürüş, şartlı otonom sürüş, yüksek otonom sürüş ve tam otonom sürüş seviyelerine ayrılmıştır [2].

Amerika Birleşik Devletleri'nin Ulusal Karayolu Trafik Emniyeti Otoritesi (National Highway Traffic Safety Administration - NHTSA) tarafından yayımlanan verilere göre 2021 yılında Amerika Birleşik Devletleri'nde yaşanan karayolu kazalarında 42,939 kişinin hayatını kaybettiği bildirilmektedir [3]. Bu dikkat çekici veriler dikkate alındığında, insan hatasından kaynaklanan kazaları sıfıra indirebilmek için, insan kontrolünden bağımsız tam otonom araçların kullanımı oldukça önemli hale gelmektedir. Günümüzde otonom araçların kullanıma sunulabilmesi için kimi ülkelerde halihazırda gerekli test senaryolarının belirlenmesi, test merkezi kurulması [4] ve doğrulama protokollerinin hazırlanması [5] gibi çalışmaların tamamlanarak 3'üncü ve 4'üncü otonomi seviyelerindeki araçların kullanıma sunulduğu göz önüne alındığında, 5'inci seviye otonom araçlara trafikte rastlamak üzere olduğumuz açıktır. Teknik gelişimlerini, yeterli düzeyde tamamladıkları değerlendirilen otonom araçların kullanıma sunulabilmesi için üstesinden gelinmesi gereken önemli problemlerden biri karayolu altyapısının uyumlu hale getirilmesidir [6]. Bir diğeri ise otonom araçların trafik davranışları dikkate alınarak trafik emniyetini garanti altına alacak yeni trafik düzenlemelerinin yapılmasıdır [7, 8]. Bir başka problem ise aracın sahip olması gereken teknik ve fonksiyonel asgari gereksinimlerin belirlenmesi, test, sertifikalandırma ve tip onay için uygunluk değerlendirmelerinin nasıl bir süreç dahilinde, hangi metotlarla yapılacağının netleştirilmesi gerektiğidir.

Bu problemin en temel biçimde tanımını 2016 yılında yapan Schöner otonom araçların emniyetli kabul edilebilmesi için test senaryolarına ve prosedürlerine ihtiyaç olduğunu ifade etmiştir [9]. Junietz vd. ise otonom aracın sınanmasında, araç endüstrisinin yanı sıra tip onay için yetkilendirecek resmi makamların da konunun paydaşı olduğunu ve kabul edilecek test metodunun hem endüstri hem de resmi makamlarca kabul edilir bulunması gereğini vurgulamış ve senaryo temelli test yaklaşımını öne sürmüştür [10]. Koopman vd. otonom aracın emniyet standardının hazırlanmasında esas alınmak üzere halihazırda konvansiyonel araçların veya demiryolu sinyalizasyon sistemlerinin emniyeti gibi farklı konularda geçerli olan fakat temelde emniyeti garanti altına almak üzere geliştirilen farklı standartları inceleyerek otonom araçların emniyet standardının çerçevesini çizmiştir [11]. Öte yandan Baldini'nin hazırladığı Avrupa Komisyonu raporunda, otonom araçların test ve sertifikasyonu kavramı resmi olarak ele alınmış, aracın emniyetinin test edilmesi için otonomi fonksiyonlarını yönetecek yazılımın emniyetinin de test edilmesi, ayrıca siber güvenlik konularının da açıklığa kavuşturulması gerektiği yönünde önerilerde bulunulmuştur [12].

Hukuki tarafta gelinen aşamada Avrupa Komisyonu ve Birleşmiş Milletler Avrupa Ekonomi Komisyonu (United Nations Economic Commission for Europe - UNECE) nezdinde araçların otonomi fonksiyonlarının belirli alanlar ve rotalarla sınırlı kalmak kaydıyla kullanılabilmesi için tip onay değerlendirmelerinde esas alınacak prosedürlere ilişkin sınırlı düzenlemeler yapılmıştır [13-15]. Buna rağmen şimdiye kadar yapılan düzenlemeler, otonom araçların uluslararası trafikte engelsizce kullanılabilmesi için uluslararası boyutta kabul görecek bir sertifikasyon sürecine yönelik gereksinimleri karşılamamaktadır. Bu sebeple konu ile ilgili kamu otoriteleri başta olmak üzere, karayolu araç ve altyapı sektöründe yer alan paydaşlar tarafından, düzenleyici kurumların yürüttüğü çalışmalar takip edilmekte ve uluslararası düzeyde ihtiyaçları karşılayacak test metotlarının geliştirilerek kabul edilmesi beklenmektedir. Bu süreçte İsveç "Vizyon Sıfır" politikası ile trafikte insan hatasından kaynaklanan kazaların sıfıra indirilmesi adına otonom araçların kullanımı için bir yol haritasının belirlenmesine karar vermiştir [16]. Fransa yerel mevzuatlarını hazırlama çalışmalarına devam etmektedir [17]. Almanya ise otomobil ve otomobil malzemeleri üreten firmalarla bilim insanlarını bir araya getirerek bu ihtiyacın karşılanmasını teşvik etmektedir [18].

Bugüne kadar otonom araçların emniyet gereksinimlerinin belirlenmesi ve sınanmasında kullanılacak metotların geliştirilmesi için pek çok akademik çalışma yapılmıştır. Bununla birlikte, halihazırda geliştirilen metotların otonom aracın tasarımından tip onayına kadar, sertifikasyon sürecinde rol oynayan aktörlerden hangilerinin kullanımına sunulacağının ve ne amaçla kullanılacağının açıklandığı bütüncül bir çalışma yapılmamıştır. Öte yandan, Avrupa Komisyonunun 2020 yılında yayınladığı, "Otonom Araçların Sertifikasyonu için Yeni Yaklaşımlar" raporunda açıklanan RSS, STPA ve PEGASUS metotları ile [19] sertifikasyon sürecinde rol oynayan tüm paydaşların ihtiyaçlarına cevap verecek şekilde öne çıkan metotlar bir araya getirilmiştir. Makalemizde temel olarak bu metotlar ele alınarak detaylıca incelenmiş, daha sonra aracın tasarımından tip onayına kadar, süreçte rol oynayan aktörlerin bu metotlardan hangisini, hangi amaçla kullanılacağına dair bir taksonomi yapılmış, böylelikle tüm süreç hiyerarşik bir model halinde ortaya koyulmuştur.

2. Otonom Araçların Sertifikasyonunda Öne Çıkan Metotlar (The Prominent Methods For Certification Of Autonomous Vehicles)

Bu bölümde otonom araçların sağlaması gereken emniyet gereksinimlerinin belirlenmesi, doğrulanması ve sertifikasyonu için Avrupa Birliği'nin "Otonom Araçların Sertifikasyonu için Yeni Yaklaşımlar" raporunda ele alınan RSS, PEGASUS ve STPA metotları incelenerek değerlendirilmiştir [19].

2.1. Responsibility Sensitive Safety (RSS)

RSS metodu Mobileye firması tarafından ilk kez 2017 yılında, otonom araçların emniyetinin garanti altına alınabilmesi için temel iki probleme cevap bulmak üzere geliştirilmiştir [20]. Bunlardan ilki, otonom bir aracın sağlaması gereken temel emniyet gereksinimlerinin neler olduğudur. İkincisi ise, otonom aracın temel emniyet gereksinimlerini sağladığının nasıl doğrulanabileceğidir. RSS'in geliştiricilerinin dikkat çeken vaadi ise bu sorulara cevap verirken, net matematiksel modeller önerilmesidir. RSS metodunda önerilen matematiksel modeller Newton mekaniğine dayanmaktadır [21]. Bu matematiksel modeller otonom aracın temel emniyet gereksinimlerinin doğrulanmasının yanı sıra, bu gereksinimlerin sağlanabilme kabiliyetinin derecelendirilmesine de imkân sağlayacaktır. RSS metodu ile açıklanan bu matematiksel modeller, trafik emniyetinin temel unsurlarından olan doğrusal ve yanal emniyet mesafelerinin belirlenmesinde esas alınacaktır.

Trafikte her sürücünün uyması gereken yazılı ve yazılı olmayan kurallar bulunmaktadır. Bu kurallar açık kurallar ve örtülü kurallar olarak sınıflandırılabilir [22]. Açık kurallar; resmi makamlar tarafından hukuki düzenlemelerle belirlenmiş olan kurallardır. Hız limitleri veya trafik işaretleri bunlara örnek olarak verilebilir. Örtülü

kurallar ise herhangi bir yazılı kaynakla belirlenmemiş olan, kültürel olarak değişiklik gösterebilen, trafikteki araç kullanıcılarının alışkanlıklarına ve sürüş davranışlarına göre şekillenerek genel kabullere göre zamanla ortaya çıkmış olan kurallardır. Örtülü kurallar her ne kadar hukuki düzenlemeler gibi kesin ve uyulması kati suretle şart koşulmuş olmamakla birlikte trafikteki araçların sürüş emniyetlerinin sağlanması açısından önemli bir rol oynamaktadır. Özünde bir robot olan otonom aracın açık kurallara uyacak şekilde tasarlanması ve bu kurallara uyduğunun test edilerek garanti altına alınması daha kolay olarak değerlendirilebilir. Fakat yazılı olmayan örtülü kurallara göre test edilmesi, üstesinden gelinmesi gereken çok daha fazla problemi beraberinde getirecektir. Bu problemlerin üstesinden gelmek için öncelikle örtülü kuralların da genelleştirilmesi ve belirgin hale getirilmesi gerekmektedir.

Öte yandan RSS metodu, yalnızca yanal ve doğrusal emniyet mesafelerinin matematiksel modeller haline getirilerek formüle edilmesinin emniyeti garantiye almada yetersiz kalacağı yönünde eleştirilere maruz kalmıştır. Buna göre bir robot olan otonom araç, yalnızca tasarımında esas alınan kurallara uyabilir. Oysa bir insan sürücü, kimi durumlarda kurallara uymanın tehlikeyle sonuçlanabileceğini öngörerek, kurallara uymama inisiyatifini alabilmektedir [23]. Örneğin bir insan sürücü, kendisi ile çarpışma ihtimali olan bir başka aracı veya yola düşen bir nesneyi fark ettiğinde, çarpışmadan kurtulmak için hız sınırlarının aşılmasını göze alarak hızlanabilir veya emniyeti tehlikeye düşürmeden birden fazla şerit değiştirmek gibi reaksiyonlar gösterebilir.

Tüm bu farklı yaklaşımlara cevap verebilmek için Mobileye firması Responsibility Sensitive Safety (RSS) metodu ile yalnızca yanal ve doğrusal emniyet mesafelerini formüle etmekle kalmamış, aynı zamanda örtülü kuralları da genelleştirerek otonom aracın uyması gereken beş kural öne sürmüş ve otonom aracın bu kurallara uyabilme becerilerinin sınanacağı kıstasları açıklamıştır. RSS metodunun otonom araçların tasarımında ve test edilmesinde kullanımı ele alınmakla birlikte, halihazırda konvansiyonel araçların sürüş destek sistemlerinin tasarımında da kullanılmaktadır. Örneğin Chai v.d. RSS metodunu adaptif hız sabitleme sisteminin geliştirilmesinde kullanmıştır [24]. Koopman v.d. ile Liu v.d. ise çalışmalarında metodun otonom araçların yanal ve doğrusal emniyet mesafelerinin hesaplanması için nasıl kullanılacağını net bir şekilde açıklamaktadır [21, 25].

2.1.1. Otonom araç için beş emniyet kuralı
(Five safety rules of autonomous vehicle)

RSS metodunda otonom bir aracın emniyetinin garanti altına alınması için, senaryo bazlı beş kural geliştirilmiştir. Bu bölümde söz konusu kurallar açıklanacaktır.

Kural 1: Öndeki araca çarpma (Rule 1: Do not hit the vehicle in front)

RSS metodunun ilk prensibi takip halindeki iki aracın birbirine çarpmadan seyrini garanti altına alabilmek için araçların arasındaki emniyetli takip mesafesini korumaktır. RSS metodunun geliştiricileri emniyetli takip mesafesini; öndeki aracın ani bir frenle durması durumunda, takip eden aracın öndekine çarpmadan durabileceği minimum mesafe olarak tanımlamaktadır [22]. Şekil 1'de tepki süresi ile durma süresinin toplamı ile belirlenen emniyetli takip mesafesi gösterilmektedir.

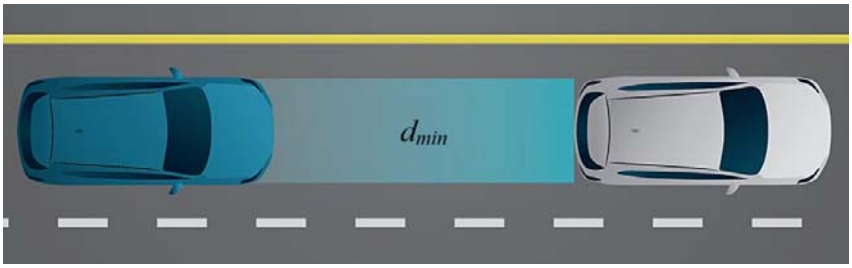
Araç kullanıcılarının genel kabulüyle iki araç arasındaki emniyetli takip mesafesi iki saniye kuralı ile belirlenmektedir. Buna göre takip eden aracın sürücüsü önündeki araçla arasındaki emniyetli takip mesafesini belirlerken, önündeki aracın geçtiği bir noktaya 2-3 sn sonra ulaşacağı şekilde aracının hızını ayarlar. Şekil 2'de emniyetli takip mesafesi, tepki süresi ve fren mesafesinin toplamından oluşan d_{min} ile gösterilmektedir. Bu pratik RSS metodunda Eş. 1'deki gibi formüle edilmiştir [22].

$$d_{min} = [V_a P + \frac{1}{2}\alpha_{maks} P^2 + \frac{(V_a + P\ \alpha_{maks})^2}{2\beta_{min}} - \frac{V_ö^2}{2\beta_{maks}}]_+ \quad (1)$$

- α_{maks} tepki süresi içerisinde arkadaki araç için izin verilen maksimum hızlanma
- β_{maks} öndeki araç için izin verilen maksimum yavaşlama
- β_{min} öndeki araç için izin verilen minimum yavaşlama
- d_{min} minimum emniyetli takip mesafesi
- P arkadaki aracın tepki süresi
- v_a arkadaki aracın hızı
- $v_ö$ öndeki aracın hızı

Eş. 1'e göre otonom aracın önündeki araçla olan mesafesi d_{min} ile hesaplanan mesafeden düşük olduğu anda, araç gereken tepkiyi göstererek yavaşlayacak, aradaki mesafenin tekrar d_{min} mesafesinin üzerine çıkması sağlanacaktır.

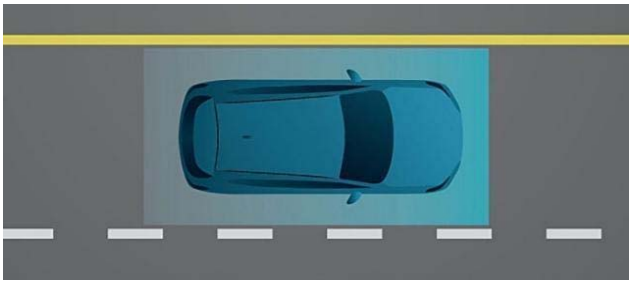
Şekil 1. Tepki Süresi ve Fren Mesafesi [22] (Response Time and Braking Distance)



Şekil 2. Boyuna Güvenli Mesafe [22] (Safe Longitudinal Distance)

Kural 2: Yanal mesafelerini koru (Rule 2: Do not cut in recklessly)

Araç gerek şeridinde seyrederken gerekse şerit değiştirirken tanımlanmış olan emniyetli yanal mesafelerini ihlal etmemelidir. Örneğin şerit içerisinde seyrederken şerit çizgilerine yaklaşmamalı, şeridi mümkün olduğunca ortalamalıdır. Sollama durumunda ise solladığı araca yaklaşırken veya solladığı sırada yanındayken emniyetli yanal mesafelerini korumalı, daha fazla yaklaşmamalıdır. Aynı şekilde şeridinde seyrederken öndeki aracı sollayan bir aracın sollanan araca solundan yaklaşması durumunda sollanan araç olası bir çarpışmayı önlemek için direksiyonunu hafifçe sağa doğru kırarak şeridi içerisinde sağa yaklaşmalı ve sollayan araçtan uzaklaşacak şekilde frenleme yaparak hızını düşürmeli ve sollayan araçtan emniyetli bir şekilde uzaklaşmalıdır. O halde emniyetli yanal mesafelerin nasıl hesaplanacağının belirlenmesi gerekmektedir. RSS metodunun geliştiricileri Şekil 3'te gösterilen emniyetli yanal mesafelerin Eş. 2 ve 3'teki gibi hesaplanacağını açıklamaktadır [22].



Şekil 3. Güvenli Yanal Mesafe [22] (Safe Lateral Distance)

$$v_{1,p} = v_1 + P\,\alpha_{yanal,maks,hızlanma},\ v_{2,p} = v_2 - P\,\alpha_{yanal,maks,hızlanma} \quad (2)$$

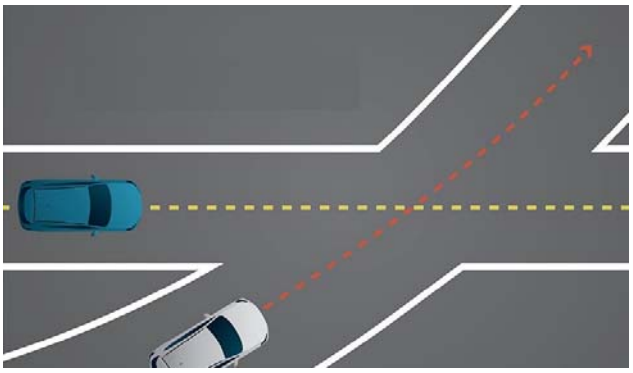
$$d_{yanal,min} = \mu + \left[\frac{(V_1 + V_{1,P})}{2}P + \frac{V_{1,P}^2}{2\beta_{1,yanal,min}} - \left(\left(\frac{V_2 + + V_{1,P}}{2}\right)P + \frac{V_{2,P}^2}{2\beta_{2,yanal,min}}\right)\right]_+ \quad (3)$$

- $\alpha_{yanal,}$maks,hızlanma aracın yanal maksimum hızlanması
- β1,yanal,min ve β2,yanal,min aracın sağa ve sola minimum yavaşlama
- μ emniyetli asgari yanal mesafe
- dyanal,min minimum emniyetli yanal mesafe
- v1 ve v2 aracın sağa ve sola yanal hızları
- v1,p ve v2,p tepki süresi içerisinde aracın yanal hızları
- P aracın tepki süresi

Kural 3: Yol hakkı verilir, alınmaz
(Rule 3: Right of way is given, not taken)

Yol çizgileri belirgin ve trafik işaret, işaretçileri tam olan yollar için kavşaklarda ve bağlantı noktalarında geçiş öncelikleri net bir şekilde belirlenmiştir. Sürücüler bu işaret ve işaretçilerin yönlendirmeleri doğrultusunda yol hakkının hangi araçta olduğunu bilirler. Fakat tüm yollar yol hakkının hangi araca ait olduğunu kesin bir şekilde belirleyecek yol çizgilerine, trafik işaret ve işaretçilere sahip değildir. Örneğin Şekil 4'te tali yoldan ana yola çıkmakta olan sürücü için dur işareti olması gerektiği halde her iki araç sürücüsü için böyle bir işaret bulunmamaktadır.

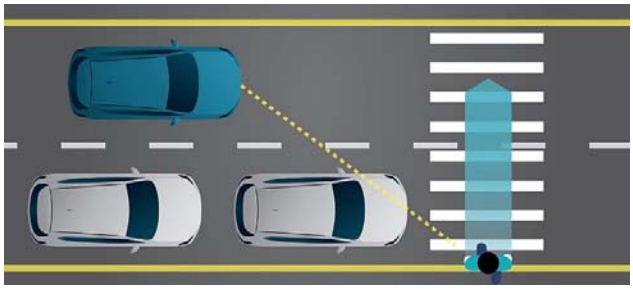
Her iki yolun eşit statüde olması durumunda yol hakkı sağdaki araca ait olacaktır. Fakat soldaki aracın kullandığı yol ana yol ise, bu defa yol hakkı soldaki araca ait olmalıdır. Şu halde yol hakkının hangi araca ait olduğu kesin bir şekilde anlaşılamamaktadır. Pratikte bu gibi yollarda yol hakkı, kesişime yaklaşan iki aracın sürücüsü arasında anlaşma yolu ile belirlenmektedir. Oysa bir otonom araç, araç sürücüsü ile böyle bir anlaşma yapamayacaktır. Bu durumda yol hakkının hangi araçta olacağının bir metot ile belirlenmesi gerekmektedir. Diğer bir taraftan yol hakkı otonom araca ait olsa bile, diğer araç trafik kurallarına aykırı hareket edip yola çıkabilir. Bu durumda otonom aracın yola devam ederek bir kazaya sebebiyet vermesi kabul edilebilir değildir. RSS metoduna göre böyle durumlarda trafiğin emniyeti için "yol hakkı verilir, alınmaz" prensibinin geçerli olacağı kabul edilmektedir.



Şekil 4. Yol Hakkı [22] (Right of Way)

Kural 4: Kısıtlı görüş şartlarında tedbirli ol
(Rule 4: Be cautious in limited visibility conditions)

Kısıtlı görüş şartları yolun topolojisinden yol kenarındaki binalara, olumsuz hava şartlarından trafikteki diğer araçlara kadar pek çok nedenden kaynaklanabilir. Bu gibi şartlarda, araç sürücüleri yolun ilerisinde riskli bir durum olduğunda bunu fark edemeyebilirler. Aynı durum otonom araçlar için de geçerlidir. Her ne kadar trafik kurallarına aykırı da olsa, yayaların yaya şeridi olmaksızın karşıdan karşıya geçmeye kalkışması çok ciddi bir tehlikedir. Örneğin şehirlerarası ana yollarda böyle bir durum olası görülmeyebilir. Fakat meskun mahallerde bu ihtimal daima göz önünde bulundurulmalıdır. Şekil 5'te gösterildiği gibi yaya şeridinin bir kısmının görülememesi de ihtimal dahilindedir.

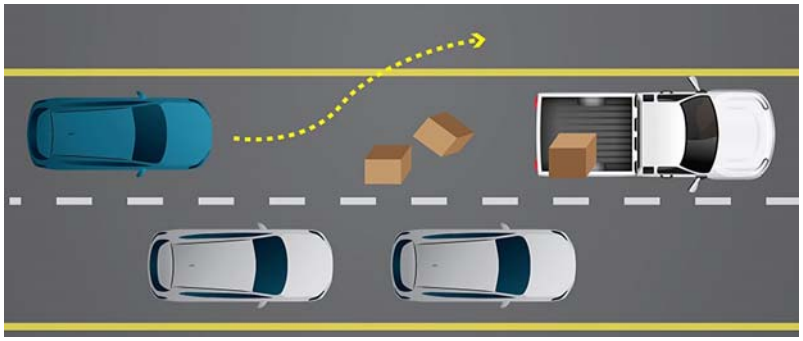


Şekil 5. Sınırlı Görüşü Olan Alanlar [22] (Areas of Limited Visibility)

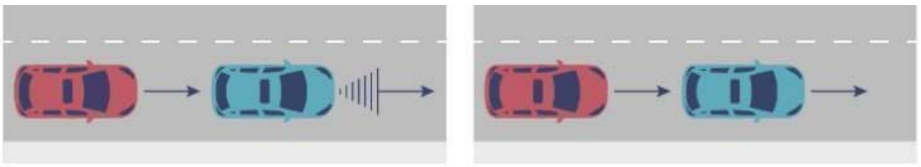
Özellikle yol kenarının görülemeyecek şekilde araçların park etmesi veya diğer araçlar hareketli halde olsa bile bir yayanın görülmesini engellemesi mümkündür. Böyle durumlarda sürücüler karşıdan karşıya geçmeye çalışacak yayaları önceden göremeyeceği için özellikle yaya şeritlerine yaklaşırken oldukça tedbirli davranmalıdırlar. Otonom araçlar da aynı kabulle hareket etmelidir.

Kural 5: Başka bir kazaya sebep olmadan kazadan kaçınabiliyorsan, kaçın (Rule 5: If you can avoid an accident without causing another accident, do so)

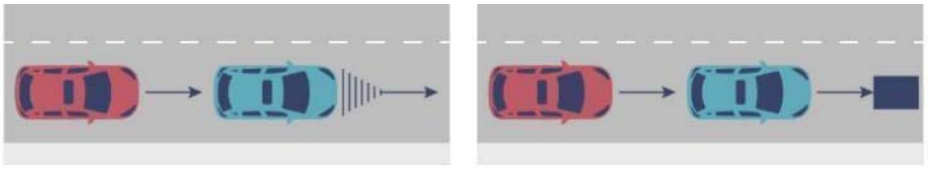
İlk dört kural tehlikeli bir durumun ortaya çıkmasına sebep olabilecek senaryoları ve bu durumlar için nasıl tedbirler alınması gerektiğini



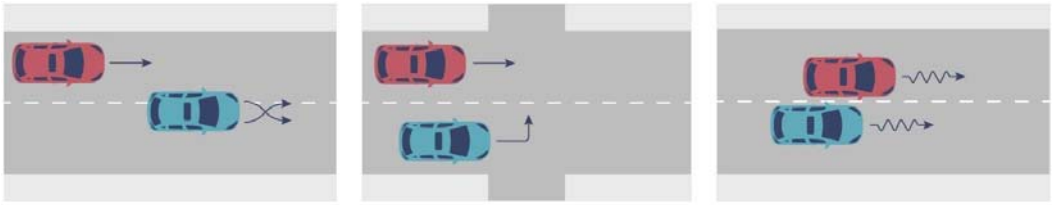
Şekil 6. Başka Bir Çarpışmaya Neden Olmadan, Çarpışmadan Kaçın [22] (Avoid Collision Without Causing Another Collision)



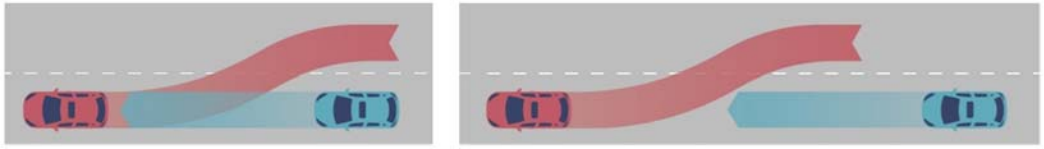
Şekil 7. Öndeki Aracın Hızlanması (Solda), Öndeki Aracın Daha Düşük Hızla Hareket Etmesi (Sağda) [26]
(Acceleration of the Front Vehicle (Left), Slower Movement of the Front Vehicle (Right))



Şekil 8. Öndeki Aracın Yavaşlaması (Solda), Öndeki Aracın Durması (Sağda) [26]
(Deceleration of the Leading Vehicle (Left), Stopping of the Leading Vehicle (Right))



Şekil 9. Şerit Değiştirme (Solda), Yanlış Şeritten Dönüş (Ortada), Drift Yapma (Sağda) [26]
(Lane Changing (Left), Wrong Lane Turning (Center), Drifting (Right))



Şekil 10. Emniyetli Olmayan Şerit Değiştirme (Solda), Emniyetli Şerit Değiştirme (Sağda) [26]
(Unsafe Lane Change (Left), Safe Lane Change (Right))

açıklamıştır. Beşinci kural ise beklenmedik bir biçimde, aniden meydana gelen tehlikeli bir durum sebebiyle kazanın kaçınılmaz olması durumunu açıklamaktadır. Beşinci kurala göre kazanın kaçınılmaz olması durumunda şayet otonom araç başka bir kazaya sebep olmadan bu kazadan kaçınabiliyorsa, kaçınmalıdır. Şekil 6'da böyle bir durum gösterilmektedir. Mavi olan otonom araç öndeki araçtan düşen objelere çarpmaktan kaçınmak için sağ şeride geçmeye kalkarsa hemen sağında duran araçla başka bir kaza yapması söz konusu olacaktır. RSS metoduna göre bu durum kabul edilebilir olmayıp, araç mümkünse kazaya sebep olmadan emniyetli bir alana geçmeli, mümkün değilse tam fren yapmalıdır.

2.1.2. RSS metodunun uygulaması (Implementation of RSS Method)

NHTSA tarafından yapılan araştırma ile, hafif araç kazalarının %99.4'üne konu olan 37 farklı kaza öncesi senaryosu belirlenmiştir [26]. Bu senaryoların bir kısmı sürücü davranışlarıyla ilgili olmakla birlikte bir kısmı ise araçların kendi arızaları veya lastik patlaması gibi sürücü kusurundan kaynaklanmayan senaryolardır. Sürücü kusurundan kaynaklanan kazaların ise bir kısmı yalnızca kazanın karıştığı aracın sürücüsünün kusuruyla meydana gelen ve farklı bir aracın rol oynamadığı kazalar olup, bir kısmı ise birden fazla araç sürücüsünün rol oynadığı kazalardır. RSS bu senaryolardan yalnızca

birden fazla sürücünün rol oynadığı kaza senaryolarını ele almaktadır. Bu nedenle RSS metodunun uygulamasının açıklanması için NHTSA'nın birden fazla sürücünün rol oynadığı kaza öncesi senaryoları ele alınmıştır. Bu senaryolar aşağıda açıklanmaktadır.

2.1.3. Tek yön trafik senaryoları (One way traffic scenarios)

Öndeki aracın hareketine göre belirlenmiş tek yön senaryoları Şekil 7 ve Şekil 8'de gösterilmektedir. RSS metodu ile ele alındığında yukarıdaki dört farklı tek yön senaryosu birbirine oldukça benzer olduğundan dört senaryo da tek bir senaryo olarak ele alınmaktadır.

2.1.4. Şerit değiştirme ve drift senaryoları
(Lane change and drift scenarios)

Araçların şerit değiştirme ve drift yapmalarına göre belirlenmiş senaryolar Şekil 9 ve Şekil 10'da gösterilmektedir. Şekil 9'da birinci ve ikinci senaryolarda şerit değiştirmenin emniyetli bir şekilde yapılıp yapılmadığının Şekil 10'daki senaryolara göre değerlendirilmesi gerekmektedir. Şekil 10'da ilk durumda şerit değiştiren kırmızı araç arkada kalan mavi aracın emniyetli durma mesafesi ile çakışacak şekilde mavi aracın şeridine geçmiştir. Böyle bir senaryoda kırmızı araç mavi aracın emniyetli durma mesafesi içerisinde ani bir duruş yaparsa kazaya sebebiyet verebilir. Bu nedenle bu şerit değiştirme emniyetli olmayan bir şerit değiştirmedir. İkinci durumda ise kırmızı araç mavi aracın emniyetli durma mesafesini geçtikten sonra mavi aracın şeridine girdiğinden ani bir duruş halinde kaza riski bulunmamaktadır. Bu şerit değiştirme ise emniyetli bir şerit değiştirmedir.

2.2. PEGASUS Metodu (PEGASUS Method)

PEGASUS metodu üzerinde ilk çalışmalara Ocak 2016 yılında başlanmış olup, Alman Federal Devletinin desteği ile ortaya çıkmıştır [18, 27]. Halihazırda geliştirilmesine devam edilen bu proje ile Alman otomobil endüstrisinin önde gelen firmalarının ve akademi dünyasının katılımı ile otonom araçların sağlaması gereken temel emniyet kriterlerinin, bu kriterlerin test edilebilmesi için gerekecek araç gereçlerin ve test metotları ile senaryolarının belirlenmesi amaçlanmaktadır. Burada üstesinden gelinmesi gereken asıl zorluk, temel emniyet gereksinimlerinin bölgesel olarak değişebilmesi sebebiyle, farklı bölgeler için farklı test senaryolarının kullanımına ihtiyaç duyulmasıdır. Uluslararası Hareketlilik, Test ve Standardizasyon Birliği (International Alliance for Mobility Testing and Standardization-IAMTS), bölgeler arasında farklılık gösteren popülasyon yoğunlukları, karayolu altyapı ağı, trafik yoğunluğu ve trafik kuralları gibi şartların, otonom araçların sınanmasında kullanılacak test senaryolarına büyük farklılıklar getireceğini işaret etmektedir [28]. PEGASUS projesinde bu husus dikkate alınarak, bölgesel şartlar doğrultusunda farklı senaryolar geliştirilmesine imkan sağlayan, tip onay süreçlerinin dinamik bir yapıyla birleştirildiği bir mekanizma tanımlanmıştır.

PEGASUS, Alman Federal Ekonomi ve Enerji Bakanlığı (Bundesministerium für Wirtschaft und Energie-BMWi) yönetiminde 2016 yılında başlatılan, otomotiv sektörünün öncü firmalarının ve otonom araç teknolojisine yönelik alanlarda çalışma yapan aktörlerin katılımlarıyla yürütülen bir projedir [27]. Bu proje SAE tarafından belirlenen otonom sürüş seviyelerine göre 3'üncü ve 4'üncü seviyelerdeki araçların emniyeti için tasarım, gerçekleme, test, doğrulama ve resmi makamlarca tip onay düzenlenmesi süreçlerini açıklamaktadır.

Projenin hayata geçirilmesi tip onay şartlarının ve sürecinin usul ve esaslarının belirleneceği düzenlemelerin yürürlüğe koyulmasına bağlıdır. Halihazırda Avrupa Birliği tarafından (AB) 2022/1426 ve (EU) 2022/2236 düzenlemeleri ile otonom araçların tip onayı için hangi alt sistemlerin değerlendirileceği ve değerlendirme kriterleri belirlenmiştir [13,14]. Bununla birlikte söz konusu düzenlemelerin kapsamı otonom araçların önceden belirlenmiş alanlarda, belirli rotalarla sınırlı kalmak koşulu ile kullanımına ve belirlenmiş park alanlarına otonom olarak park edilmelerine imkan vermektedir. Gelinen aşamada otonom araçların uluslararası trafikte kullanılabilmesi için Birleşmiş Milletler Avrupa Ekonomi Komisyonu (United Nations Economic Commission for Europe - UNECE) nezdinde yayımlanan ECE/TRANS/WP.29/2019/34/Rev.2 düzenlemesi ile uluslararası geçerlilikte trafik emniyeti, trafik kuralları ve otonom araçların sertifikasyonu konularında düzenlemeler yapılmış olmakla birlikte, komisyon dahilindeki WP.29 (World Forum for Harmonization of Vehicle Regulations) ve WP.1 (Global Forum for Road Traffic Safety) düzenleyici forumları ile yürütülen çalışmalar halen devam etmektedir [15, 29]. Öte yandan, ISO 34502:2023 standardı ile, halihazırda çalışmaları devam etmekte olan düzenlemelere uygunluğunun sınanması için gerekli senaryoların belirlenmesi ve aracın bu senaryolara göre sınanması için operasyonel tasarım alanı kavramı açıklanmış, böylece standardizasyon çalışmalarının ilk aşaması tamamlanmıştır [30]. Devam eden standardizasyon ve regülasyon çalışmalarının sonuçlandırılması ile PEGASUS projesinin çıktılarının yasal düzenlemeler dayanak alınarak uygulamaya koyulacağı değerlendirilmektedir.

PEGASUS projesi ile hedeflenen temel çıktı, otonom kullanım modunda emniyetin garanti altına alınabilmesi için gerekli standartları ve doğrulama yöntemlerini belirlemektir. Projenin amacı projenin ismini de veren PEGASUS kelimesini meydana getiren harflerin anlamlarıyla temsil edilmektedir; "*project for the establishment of generally accepted quality criteria, tools and methods as well as scenarios and situations for the release of highly-automated driving functions*". Projenin temel hedefleri maddeler halinde aşağıdaki gibi açıklanabilir [18]:

- Otonom araç sistemlerinin simülasyon, test standı ve gerçek trafik şartlarında test edilebilmesi için standartlaştırılmış bir prosedür tanımlanması,
- Otonom sürüşü korumak için sürekli ve değişken araçların geliştirilmesi,
- İlk geliştirme sürecinde testlerin entegrasyonu,
- Yüksek otonom sürüş fonksiyonlarının emniyetinin sürdürülebilmesi için üreticiler arasında bir metodoloji geliştirilmesi.

Günümüzde otonom araç teknolojisi konusunda yapılan çalışmalar sonucunda otonom fonksiyonların yerine getirilebilmesi için ihtiyaç duyulan teknik gereksinimler karşılanmış ve gerek özel kullanıma hizmet verecek otonom otomobiller, gerek toplu taşıma amacıyla kullanılacak otonom minibüsler ve hatta iş makinaları hizmete sunulabilmiştir [31]. Bununla birlikte otonom araçların trafikte kullanılabilmesi için hala cevaplanması gereken birçok soru vardır. PEGASUS projesi kapsamında otonom aracın emniyeti ile ilgili cevaplanması gereken konular, şu iki temel soru ile ele alınmaktadır: 1) Otonom araçlarda aranması gereken emniyet gereksinimleri nelerdir? 2) Bu gereksinimlerin sağlandığı nasıl ispatlanabilir?

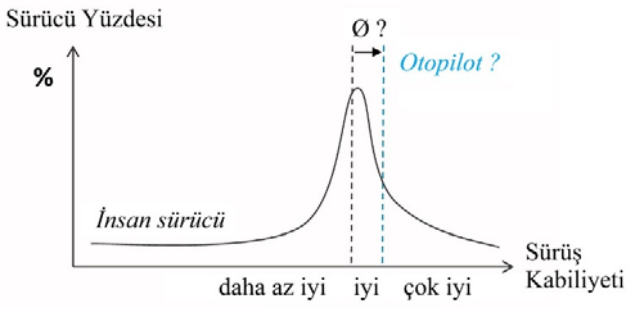
Bilindiği üzere otonomi fonksiyonu sürücünün herhangi bir süpervizyon veya müdahale etkisi olmaksızın otonom aracın kendi kendisini yönetebilmesini gerektirmektedir. Fakat artık tekerleğin arkasında herhangi bir insan yönetimi bulunmaması ve tüm sorumluluğun araca devredilmesi, bu sorumluluğun hayati niteliği sebebiyle, karşılanması gereken ağır isterleri de beraberinde getirmektedir. Peki gelecekte otonom sürüş sırasında insanın rolü ne olacaktır? Araç ve insanın görev dağılımları nasıl optimize edilebilir?

Otonom araç teknolojisinin hazır olması ve olabildiğince hızlı kullanıma sunulması yönünde beklenti olduğu dikkate alındığında bu gibi konularda günümüzde hala çok yoğun araştırma geliştirme çalışmalarını gerektiren bu gibi konuların hızlı bir şekilde tamamlanması gerekmektedir.

Otonom araçların kullanıma sunulabilmesinden önce otonomi fonksiyonlarının emniyetli olduklarının onaylanabilmesi için araştırma ve endüstri sektörlerinin bir araya gelerek yakın işbirliği ile yeni standartlar ve metotlar geliştirilmesi gerekmektedir. Uluslararası Motorlu Araç Üreticileri Örgütü (International Organization of Motor Vehicle Manufacturers-OICA) tarafından yayımlanan Global Karayolu Emniyeti Manifestosu'nda karayolu araçlarında sağlanması gereken uluslararası veya bölgesel emniyet gereksinimlerinin, UNECE WP.29 nezdinde yürütülen çalışmalarla hazırlanacak uluslararası düzenlemeler kapsamında belirlenmesi gerektiğine işaret edilmiştir [32]. PEGASUS ortak projesi tam da bu noktada uluslararası düzenleyici çalışmalara çözümler sunabilecek, tam otonom sürüş fonksiyonlarına ilişkin genel emniyet gereksinimleri ile bu gereksinimlerin sınanmasında kullanılacak araçların ve senaryoların belirlenmesini sağlayacaktır. Öte yandan bu test konularının doğrulanması için resmi makamların, üreticilerin ve toplumun kabul edeceği bir metoda ihtiyaç vardır.

PEGASUS metodunun en kritik iki özelliğinden biri aracın üretiminden hizmete sunulmasına kadar tüm tasarım, üretim ve son kontrol süreçlerini içerisine alan bir metot olmasıdır. Bu süreç analiz ve simülasyonlarla tasarımın doğrulanmasından prototip üretimine daha sonra prototip aracın senaryo bazlı testlerle emniyetli olduğunun doğrulanmasının ardından seri üretime geçilebilmesini öngören tip onay sertifikasyonuna ulaşan aşamalardan oluşmaktadır. Bu yönüyle PEGASUS metodu hem üreticinin hem de emniyet değerlendirme kuruluşlarının rollerini ve tüm aşamaların gereksinimlerinin net bir şekilde belirlemektedir.

PEGASUS metodunun ikinci kritik özelliği ise değerlendirmenin yapılacağı kriterlerin trafikteki sürücülerin kullanım kabiliyetlerinin ve tercihlerinin dikkate alınarak belirlenmesidir. PEGASUS metodunda değerlendirme sürecinin başında aşılması gereken eşik sürüş becerisi gereksinimleri belirlenmemiş, bunun yerine Şekil 11'de gösterildiği gibi trafikteki sürücülerin performansları ve davranışları bir veri havuzunda toplanarak istatistiklerle başarılı ve başarısız olarak değerlendirilecek eşik sürüş becerisi gereksinimlerinin istatistiksel verilere dayalı olarak belirlenmesi öngörülmüştür [33].



Şekil 11. Sürüş Becerileri [31] (Driving Skills)

Sürücü performans ve davranışlarının bölgesel olarak değişmesi, değerlendirme kriterlerinin aracın kullanılacağı ülkelere göre belirlenmesi ve otonom aracın daha gerçekçi bir değerlendirmeye tabi tutulabilmesi için kullanım sahasının pratiklerine uygun olarak her ülke için ayrı test senaryolarının kullanabileceğini akla getirmektedir. Bu metodun teorik gelişimi tamamlanmış olmakla birlikte, sürücü performans ve davranışlarının verilere yansıtılması ve veri havuzlarında toplanması konusunda çalışmalar halihazırda devam etmektedir.

PEGASUS metodunu yalnızca otonom aracın emniyet seviyesinin ölçülmesi için geliştirilen bir metot olarak değerlendirmek doğru değildir. Çünkü bu metot aslında otonom aracın tasarımından başlamak üzere prototip üretimine, test ve analizlere ve üretim aşamasına; başlı başına otonom aracın tasarımından kullanıcısına kadar uzanan bir süreci açıklamaktadır. Bu süreç içerisinde aracın tasarımcısının, alt sistem sağlayıcılarının, ana entegratör ve üretici firmanın, test merkezlerinin, tüm bu süreci kontrol edecek uygunluk değerlendirme kuruluşlarının, resmi makamların ve nihayet kullanıcıların rollerini içerebilecek kapsama sahip bir metottur. Bu yönüyle PEGASUS metodu yalnızca emniyet gereksinimlerini ve ölçüm parametrelerini belirlemekle kalmayıp, bunların sınanma aşamalarını da açıklayarak konuya dahil olan tüm paydaşların rollerine ve sorumluluklarına ışık tutmaktadır. BMWi, PEGASUS metodunun tam da bu amaçla geliştirilmesi için araç üretiminde rol oynayan pek çok firmayı bu sürecin içerisine dahil ederek bu metodu geliştirmektedir.

PEGASUS metodunu açıklamak için süreç Şekil 12'deki gibi detaylı bir akış şemasına dönüştürülmüştür. Burada sürecin izleyeceği yol verilerin işlenmesi, gereksinimlerin tanımlanması, veritabanının hazırlanması, otonom sürüş fonksiyonunun değerlendirilmesi ve argümantasyon kısımları olarak açıklanmaktadır.

Form'un 2018'de yayımlanan, PEGASUS metodunun çalışma mekanizmasının açıklandığı çalışmasında Şekil 12'de gösterilmekte olan adımlar aşağıdaki gibi açıklanmaktadır [33].

2.2.1. Veri işleme (Data processing)

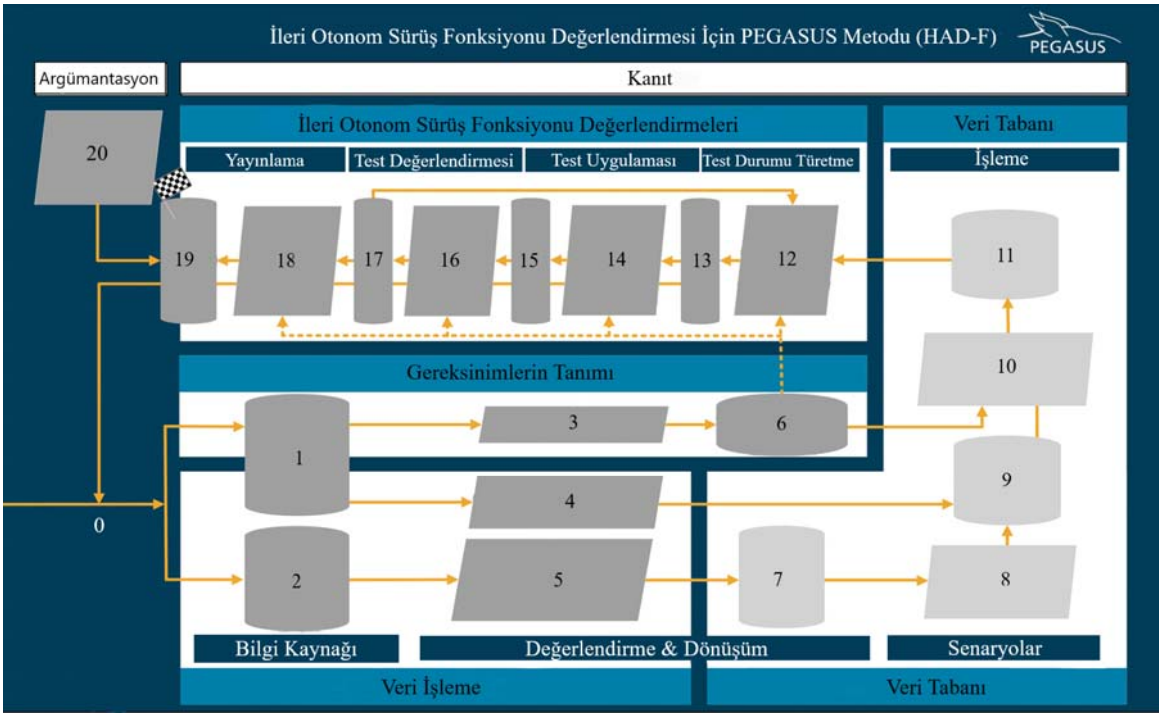
Adım 1 (Bilgi: Kanunlar, Standartlar ve Yönergeler), 2 (Veri: Test Sürüşü, Simülasyon ve Kaza), 4 (Senaryoların Sistematik Tanımlanması) ve 5 (Ön İşleme ve Yeniden Yapılandırma) ile temsil edilen süreç veri işleme aşamasıdır. Bu aşamada otonom aracın karşılaması gereken yasal gereksinimler, aracın teknik özellikleri ve fonksiyonlarının test edilmesi için referans alınacak ölçüm verileri ve testlerde kullanılacak senaryolar belirlenir. Daha sonra hazırlanan veriler, veri tabanına kaydedilmek üzere uygun formata dönüştürülerek girdi verisi haline getirilir.

2.2.2. Gereksinimlerin tanımlanması (Definition of Requirements)

Adım 1 (Bilgi: Kanunlar, Standartlar ve Yönergeler), 3 (Gereksinimlerin Analizi) ve 6 (Süreç Yönergeleri ve HAD Değerlendirmesi İçin Metrikler) ile temsil edilen süreç, gereksinimlerin tanımlanması aşamasıdır. Bu aşamada yasal gereksinimler belirlenir, veri işleme sürecinden farklı olarak bu gereksinimlerin test metotları da seçilir. Yasal gereksinimlerin yanı sıra aracın tasarımının ve prototip ürünün doğruluğunu ispat etmek üzere hangi analiz ve testlerin yapılacağı, sonuçların nasıl analiz edileceği ve kullanılacak metrik değerler açıklanarak talimatlar haline getirilir.

2.2.3. Veritabanı (Database)

Adım 7 (PEGASUS Formatındaki Veriler), 8 (Metrik Uygulaması ve Mantıksal Senaryolara Eşleme), 9 (Mantıksal Senaryolar ve Parametreler Uzayı), 10 (Geçiş Kriterlerinin Entegrasyonu) ve 11 (Mantıksal Test Durumları Uzayı) ile temsil edilen süreç, veri tabanının hazırlanması aşamasıdır. Bu aşamada girdi verisi haline getirilen veriler PEGASUS formatına dönüştürülerek analiz ve testlerde kullanılmak üzere hazırlanır. Önceden açıklanan metrik değerler, uygulanacak analiz ve testlerle eşleştirilerek ortak bir veri havuzunda toparlanır. Ayrıca tüm test senaryoları ve metrik değerler derlenerek test konsepti oluşturulur.



Şekil 12. PEGASUS Metodunun Çalışma Mekanizması. Düz çizgi, iş akışını; kesik çizgi, süreç talimatını gösterir. Açık gri, merkezde olanları; koyu gri, merkezde olmayanları gösterir. Paralel kenar, prosedürleri; silindir, veri/içerikleri gösterir [33] (Working Mechanism of the PEGASUS Method. A solid line represents the workflow, while a dashed line indicates the process instructions. Light gray denotes elements that are central, whereas dark gray denotes those that are not. A parallelogram represents procedures, and a cylinder represents data or content.)

2.2.4. Otonom sürüş fonksiyonlarının değerlendirilmesi (Evaluation of Highly Autonomous Driving Functionality)

Adım 12 (Test Konseptinin Varyasyon Yöntemi ile Uygulanması), 13 (Test Durumları), 14 (Gerçek Dünya Sürüşünü Kanıtlayan Simülasyon (Highly Automated Driving Function-HAD-F) Testi), 15 (Test Verisi), 16 (Yenileme ve Sınıflandırma), 17 (Test Sonuçları), 18 (Risk Değerlendirmesi), 19 (Güvenlik Beyanı) ile temsil edilen süreç, otonom sürüş fonksiyonunun değerlendirilmesi aşamasıdır. Bu aşamada test konseptleri ile geçiş kriterleri birleştirilerek mantıksal test vakasına dönüştürülür, test konseptlerin uygulama metotları belirlenir, test senaryoları yürütülür, elde edilen veriler veri havuzunda toplanarak önceden belirlenen metriklerle değerlendirilir ve test sonuçları düzenlenir. Ayrıca risk değerlendirmeleri de yapılır.

2.2.5. Argümantasyon (Argumentation)

Adım 20 (Güvenlik Argümantasyonu), PEGASUS metodunun son işlem adımı olup, elde edilen emniyet beyanı ve risk değerlendirme sonuçları ile birlikte emniyet argümantasyonu uygulanarak bu adımda derlenen çıktılarla birleştirilir. PEGASUS emniyet argümantasyonu; yapı, resmileştirme, tutarlılık, bütünlük ve uygunluk yoluyla beş katman olarak yapılandırılan, daha yüksek otomasyon seviyelerinin güvenliğini ve onaylanmasını destekleyen kavramsal bir çerçeve olarak anlaşılmalıdır.

2.3. STPA Metodu (STPA Method)

STPA (Systems-Theoretic Process Analysis-Sistem-Teorik Süreç Analizi) metodu ise ilk kez 2010 yılında MIT ile JAXA/JAMSS üniversitelerinden akademisyenlerin uzay araçlarının emniyet seviyelerinin tasarım aşamasında analiz edilerek uygun önlemlerin belirlenmesi ve tasarıma yansıtılması amacıyla, yazılım ve donanım bileşenlerinden oluşmakta olan sistemlerin teorik kaza analizi için geliştirilmiştir [34]. Bu analiz metodu 2013 yılında otonom araçların emniyet seviyelerinin belirlenebilmesi için otomotiv sektörüne uyarlanmıştır [35].

STPA metodunun otonom araçların emniyetine ilişkin iki farklı uygulama alanı bulunmaktadır. Bunlardan biri ISO/PAS 21448 (Safety of Intended Functionality-SOTIF) standardıdır. SOTIF, otomobil endüstrisi tarafından sürüş destek sistemlerinin emniyet standardı olarak geliştirilmiştir. Bu standart öncelikle, ele alınan fonksiyonun tam olarak tanımlanmamasından kaynaklanan veya aracın alt sistemlerinin, sensörlerin ve algoritmaların çalışmasına engel nitelikte beklenmedik koşullara maruz kalmasından doğan risklerin kabul edilebilir seviyelere azaltılmasını konu edinmektedir. SOTIF, sürüş destek sistemlerinin emniyetini konu alan bir standart olarak SAE 0, 1 ve 2 seviye araçlar için uygulanmak üzere geliştirilmiştir. STPA metodunun SOTIF ile kullanımı SAE 3 ve 4 seviyesindeki araçlar için mümkündür. Bununla birlikte SOTIF'in, ISO 26262 standardının kapsamında öngörülmemiş olan sürüş destek fonksiyonlarına ilişkin eksikliklerin tamamlanması için geliştirildiği ve ISO 26262'nin devamı niteliğinde olduğu kabul edilmektedir [36, 37].

STPA metodunun otonom araçların emniyetinde diğer uygulama alanı ise, bu çalışmada incelenen metotların seçiminde referans alınan AB raporunda da ele alındığı üzere ISO 26262 standardıdır [19]. Günümüz konvansiyonel karayolu araçlarının emniyetli olup olmadıkları ISO 26262 standardında açıklanan metotlarla doğrulanmaktadır. Bu standartla aracın fonksiyonel emniyeti açısından tehlikelere yol açabilecek hataların tespitinde FTA (Failure Tree Analysis), FMA (Failure Mode Analysis), HAZOP (Hazard and

Operability) gibi farklı metotlar kullanılmaktadır. Ancak bu metotlar yazılım hatalarından kaynaklı, insan hatasının neden olduğu veya bileşen arızasından dolayı ortaya çıkan tehlikelerin tespiti için yeterli değildir.

STPA metodu uzay araçlarından, deniz ve hava araçlarına kadar yazılım ve donanım bileşenlerinden oluşan sistemlerin analizi için halihazırda kullanılan bir metottur. STPA geleneksel tehlike analiz metotlarının sınırlarını aşmayı vadetmektedir. STPA'nın ISO 26262'nin otonom araç değerlendirmesinde eksik kalan yönlerini tamamlayabileceği öngörülerek bütünleşik bir metot önerilmiştir [37]. Böylece ISO 26262 standardında göz önünde bulundurulmamış olan otonomi fonksiyonlarına ilişkin eksiklikler tamamlanmıştır.

ISO 26262 aracın tehlike analizlerinin alt sistemler veya riskler özelinde ayrı ayrı incelendiği metotları açıklamaktadır. Öte yandan sürücü aracın seyrinde kritik bir rol oynamakla beraber fonksiyonel bütünlük anlamında aracın bir bileşeni olarak değerlendirilip değerlendirilmeyeceği hususunda net bir anlayış yoktur [37]. STPA'da ise sürücünün üstlendiği tüm görevler araca atfedildiği için STPA metodunun değerlendirme alanına net bir şekilde dahil edilmiştir.

STPA metodu ile sürücü özelinde anlayış değişiklikleri getirildiğinden, ISO 26262'de kabul edilen terminolojilere de değişiklik getirilmesi gerekmektedir. Tablo 1'de farklılık gösteren terimler karşılaştırılmıştır. Tablo 1'de yer alan terimlerin neden STPA ve ISO 26262 arasında değişiklik gösterdiği konusu açıklandığında STPA'nın ISO 26262'nin hangi yönlerini nasıl tamamladığı daha net anlaşılır olacaktır. Öncelikle tehlike terimi ISO 26262 standardında aracın alt sistemleri özelinde değerlendirilirken STPA metodunda aracın sürüş ortamı içerisinde bulunduğu çevresel şartlar, trafikte yer alan diğer aktörler ve tüm bu çevresel şartların anlık değişimleri veya trafikteki aktörlerin davranışları itibariyle çok daha geniş bir perspektifle ele alınmaktadır.

Arızalı davranış terimi ISO 26262 standardında aracın herhangi bir bileşeninin kazaya yol açabilecek nitelikte fonksiyonel kaybı veya yanlış çalışması olarak tanımlanmış olmasına rağmen STPA metodunda bu terimle ilgili net bir tanım yoktur. Aynı şekilde arıza tanımı için de aynı şeyi söylemek mümkündür. ISO 26262 arızayı; bir bileşenin yerine getirmesi gereken bir fonksiyonun yerine getirebilme kabiliyetinin sonlanması olarak tanımlanırken STPA metodunda bu terimin de net bir karşılığı bulunmamaktadır [37]. Bu iki terimin STPA metodunda net olarak tanımlanmaması, tehlike teriminde olduğu gibi ele alınan değerlendirme alanının araca ait bileşenlerin dışına çıkılarak aracın etkilendiği tüm çevresel öğeleri kapsayacak şekilde genişletilmesinden kaynaklanmaktadır. ISO 26262 standardına göre bir kazanın nedeni aracı oluşturan ekipmanlardan birinin arızalanması olarak kabul edilirken STPA kazanın nedeni olarak aracın emniyetli seyrini etkileyebilecek, çevresel etkiler dahil her şey olarak ele aldığından olası bir kazanın sebebi olarak görülen arıza kavramı da anlamını kaybetmektedir.

Kaza tanımını incelerken ISO 26262'nin odak noktasının aracı oluşturan bileşenlerin arızalanması ihtimaline dayalı tehlikeler olduğunu göz önünde bulundurduğumuzda kaza olayının gerçekleşmesi ISO 26262'nin dışında kalmaktadır. STPA'nın odak noktası ise aracın arızalanması çerçevesinin dışına çıkarak çevresel tehlikeleri kapsadığından araçtan kaynaklanmayan kazalar da ele alınmaktadır. Öte yandan STPA'daki kaza tanımı, ISO 26262'deki zarar kavramına benzemekte, fakat çok daha geniş bir kapsama dayanmaktadır. ISO 26262 kişilerin zarar görmesini ele alırken STPA ise kişilerle sınırlı kalmayıp, kişilerin veya malların zarar görmesi, çevresel kirlilik, taşımacılık ile amaçlanan görevin yerine getirilememesi dahil olmak üzere herhangi bir kayıp olarak ortaya çıkmaktadır. Tehlikeli olay kavramı ise ISO 26262'de zararla sonuçlanacak durumlar olarak açıklanırken, STPA'daki kaza tanımı ile sonuçlanacak olaylar kastedilmektedir. STPA'da ise tehlikeli olay kavramının net bir tanımı yoktur [37].

STPA ile ISO 26262'nin bir karşılaştırması da emniyet kapsamı boyutunda yapılmaktadır [38]. ISO 26262'nin emniyet kapsamı HARA metoduna dayalıdır. Bu iki metodun kapsamlarının karşılaştırıldığı bir gösterim Şekil 13'te verilmiştir.

HARA ve STPA arasındaki emniyet kapsamı karşılaştırıldığında, HARA'da tehlike kaynağı olarak bir ekipman arızasından kaynaklanan arızalı durum ele alınırken STPA'da buna ek olarak insan hatası, trafikte rol oynayan unsurlar arasında etkileşim hatası, öngörülemeyen çevresel şartlar veya yazılım hatası gibi kontrolün yitirilmesine sebep olabilecek her türlü durum olarak ele alınmaktadır.

2.3.1. STPA metodunun adımları (Steps of STPA Method)

Tüm bu açıklamalar doğrultusunda STPA'nın, ISO 26262'nin kapsamını genişleterek otonom aracın otonomi fonksiyonlarının getirdiği ilave konuların ele alınmasını sağlayan tamamlayıcı bir metot olarak değerlendirilmektedir. Böylece STPA'nın ISO 26262 kapsamında kullanılması öngörülerek, bu kullanım için izlenecek adımlar aşağıdaki gibi açıklanmaktadır [38].

Tablo 1. STPA ve ISO 26262 Terminolojilerinin Karşılaştırılması [37] (Comparison of STPA and ISO 26262 Terminologies)

Terminoloji	*STPA*	*ISO 26262*
Tehlike	Belirli bir en kötü durum ve çevresel koşullarla birlikte bir kazaya veya kayba yol açacak bir sistem durumu veya koşullar dizisi	Ögenin (item) hatalı çalışma davranışından kaynaklanan potansiyel zarar kaynağı
Arızalı Davranış	Açık bir tanım yok	Tasarım amacı ile ilgili olarak bir öğenin başarısızlığı veya istenmeyen davranışı
Arıza	Açık bir tanım yok Not: Mühendislik literatüründe arıza; bir komponentin veya sistemin tasarım amacı olan fonksiyonu yerine getirememesi veya yerine getirme performansının eksikliği olarak tanımlanmaktadır.	Bir elemanın, bir işlevi gerektiği gibi yerine getirme yeteneğinin sona ermesi Not: Hatalı ikaz bir hata kaynağıdır.
Kaza	İnsan yaşamının kaybı veya zarar görmesi, mal hasarı, çevre kirliliği, görev kaybı dahil olmak üzere kayıpla sonuçlanan istenmeyen veya planlanmamış bir olay	Açık bir tanım yok
Zarar	Açık bir tanım yok	Fiziksel yaralanma veya kişinin sağlığına zarar verme
Tehlikeli Olay	Açık bir tanım yok	Tehlike ve operasyonel durumun kombinasyonu

Şekil 13. STPA ve ISO 26262 Kapsamlarının Karşılaştırılması [38] (Comparison of STPA and ISO 26262 Scopes)

1. STPA Adım 0 (Temel Analizler)
   1.1. Kazaların ve sistem-seviyesi tehlikelerin tanımlanması.
   1.2. Yüksek-seviye sistem emniyet kısıtlarının tanımlanması.
   1.3. Sistemin kontrol yapısı diyagramının çizimi.
2. STPA Adım 0'ın sonuçlarını kullanarak öge (item) ve öğenin amacı, içeriği veya fonksiyonel gereklilikleri gibi bilgiler tanımlanır. STPA Adım 0'daki kontrol yapısı diyagramı analiz edilen sistemin ana komponentlerini gösterir. Bu diyagram, bir öğenin ve sınırlarının tanımlanması için fonksiyonel emniyet mühendisine yardımcı olacak bilgileri içermektedir.
3. HARA yaklaşımı için bir girdi olarak STPA Adım 0'da tanımlanan tehlike, kaza ve yüksek seviye sistem emniyet kısıtlama listeleri kullanılır.
4. HARA yaklaşımı uygulanır:
   4.1. Bir öğenin arızalı davranışının sebep olabileceği potansiyel tehlikeler için operasyonel durumları ve operasyon modlar belirlenir.
   4.2. Üç faktörün (Önem/vehamet (Severity), Gerçekleşme Olasılığı (Probability of Exposure) ve Kontrol Edilebilirlik (Controllability)) tahminine dayalı olarak Adım 0'da tanımlanan tehlikeleri sınıflandırılır.
      4.2.1. Farklı durumlardaki tehlikeler göz önünde bulundurularak tehlikeli olaylar tanımlanır.
   4.3. Dört ASIL (Automotive Safety Integrity Level) seviyesini (en düşük emniyet bütünlük seviyesi A'dan en yüksek emniyet bütünlük seviyesi D'ye) kullanarak her tehlikeli olay için ASIL seviyesi tanımlanır. Eğer tehlikeli olay makul değilse, bunu QM (Quality Management) olarak nitelendirilir.
   4.4. Her tehlikeli olay için emniyet hedefi formüle edilir.
5. STPA Adım 1 için girdi olarak tehlikeli olay, emniyet hedefleri, operasyonel durumlar ve modları kullanılır.
6. Öğenin emniyetli olmayan kontrol aksiyonlarını tanımlamak için STPA Adım 1 uygulanır.
7. STPA Adım 1'de tanımlanmış her emniyetsiz kontrol aksiyonunun nedensel faktörlerini ve emniyetsiz senaryolarını tanımlamak için STPA Adım 2 uygulanır.
8. Bu seviyede sistemin fonksiyonel emniyet konseptini ve emniyet gereklerini oluşturmak için STPA Adım 1 ve 2'nin sonuçları kullanılır.

STPA metodunun uygulama süreci Şekil 14'te akış diyagramı olarak görülmektedir. Hu'ya göre STPA analizi spesifik kazalardan, analiz edilen tehlikeli durumlardan ve sistemin emniyete konu davranışlarında tehlikelere sebep olacak olumsuzlukların elemine edilmesi için gerekli emniyet kısıtlamalarından başlar [39]. Daha sonra sistemin kontrol yapısında emniyetli olmayan davranışlar tespit edilmeli ve bu davranışların sebep analizleri yapılarak aracın kontrolünde gerekli güvenlik kısıtlaması elde edilir.

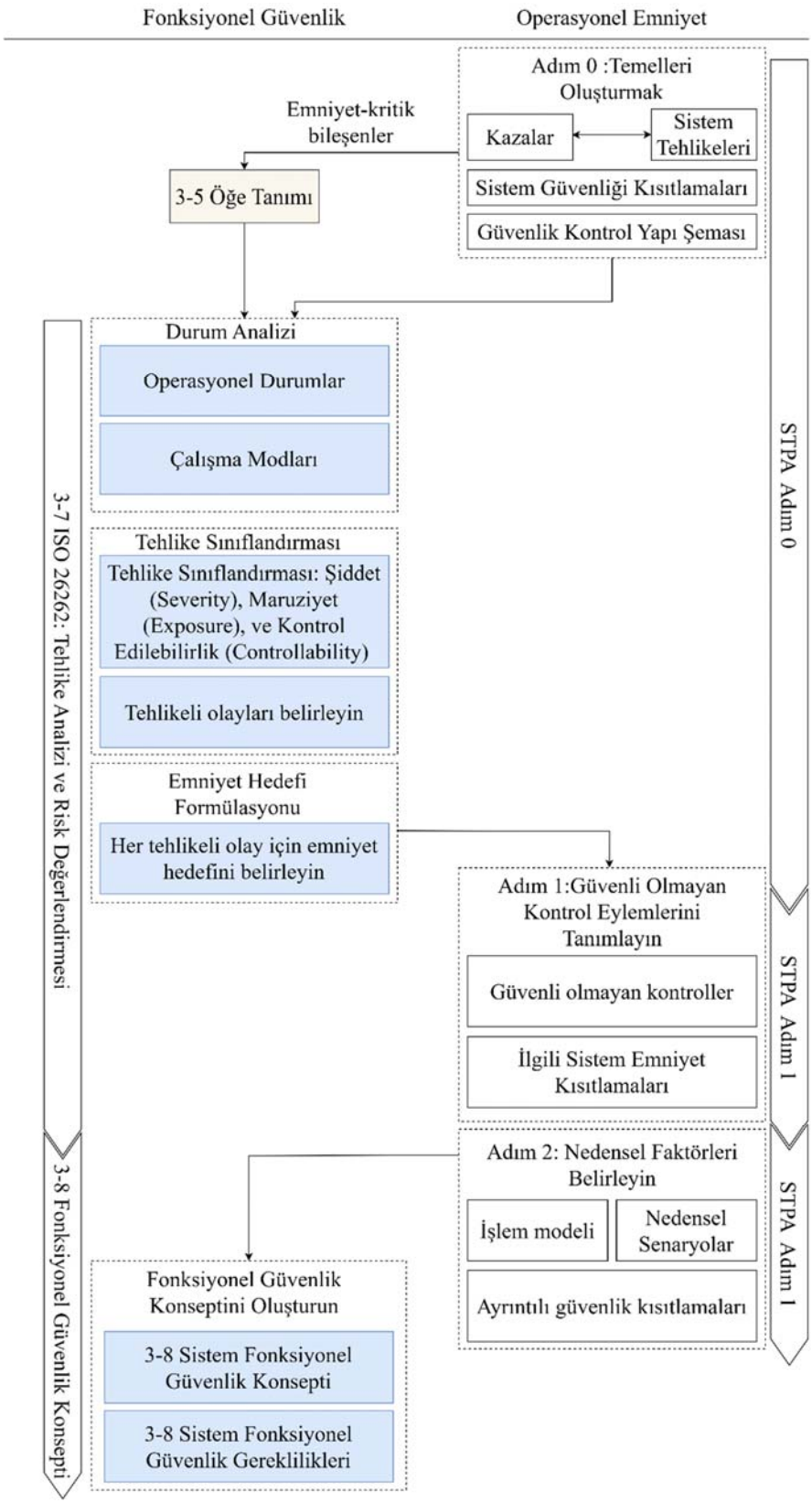
2.3.2. STPA metodunun ISO 26262 ile kullanılması
(Using STPA with ISO 26262)

STPA metodunun halihazırda araçların emniyetleri konusunda geçerli olan ISO 26262 standardı ile birlikte kullanılmak üzere geliştirildiğini açıklamıştık. STPA'nın adımlarının ISO ve STPA arasındaki dağılımı ise Şekil 14'te açıklanmaktadır [38].

ISO 26262'nin HARA (Hazard Analysis and Risk Assessment) süreci dört adımdan oluşmaktadır. Bu adımlarla tehlikelerin analizleri yapılarak tehlikeler tanımlanır, sınıflandırılır ve emniyet hedefleri belirlenir. Fakat bu adımlarda analizi yapılan riskler, aracın alt sistemlerinden kaynaklanabilecek tehlikeleri ele almaktadır. Oysa otonom bir araçta, aracın alt sistemlerinin yanı sıra sürüş yöntem ve tercihleri ile sürüşe etki edebilecek, aracın otonomi fonksiyonuna ait sürüş davranışlarının, iklim ve çevre şartlarının ayrıca sürüş ortamında rol oynayan diğer araçların davranışları gibi risk kaynaklarından doğabilecek tehlikelerin de ele alınması gerekmektedir. STPA bu ihtiyacı karşılamakta ve HARA'ya ilave olarak Adım 1 ve 2 ile bu risklerin ele alınmasını sağlamaktadır.

3. Sertifikasyon Sürecinin Modellenmesi ve Öne Çıkan Metotların Karşılaştırması
(Modeling of The Certification Process and A Comparison of Prominent Methods)

Bu bölümde otonom aracın sertifikasyon süreci hiyerarşik bir model haline getirilmiş, RSS, PEGASUS ve STPA metotlarının bu süreçte hangi aşamalarda kullanılabileceği açıklanmış ve metotlar arasında uygulama alanları, olası kullanıcı paydaşları ve uygulanabilirlikleri yönünden karşılaştırma bir taksonomi dahilinde metotlar arasındaki ilişki açıklanmıştır.



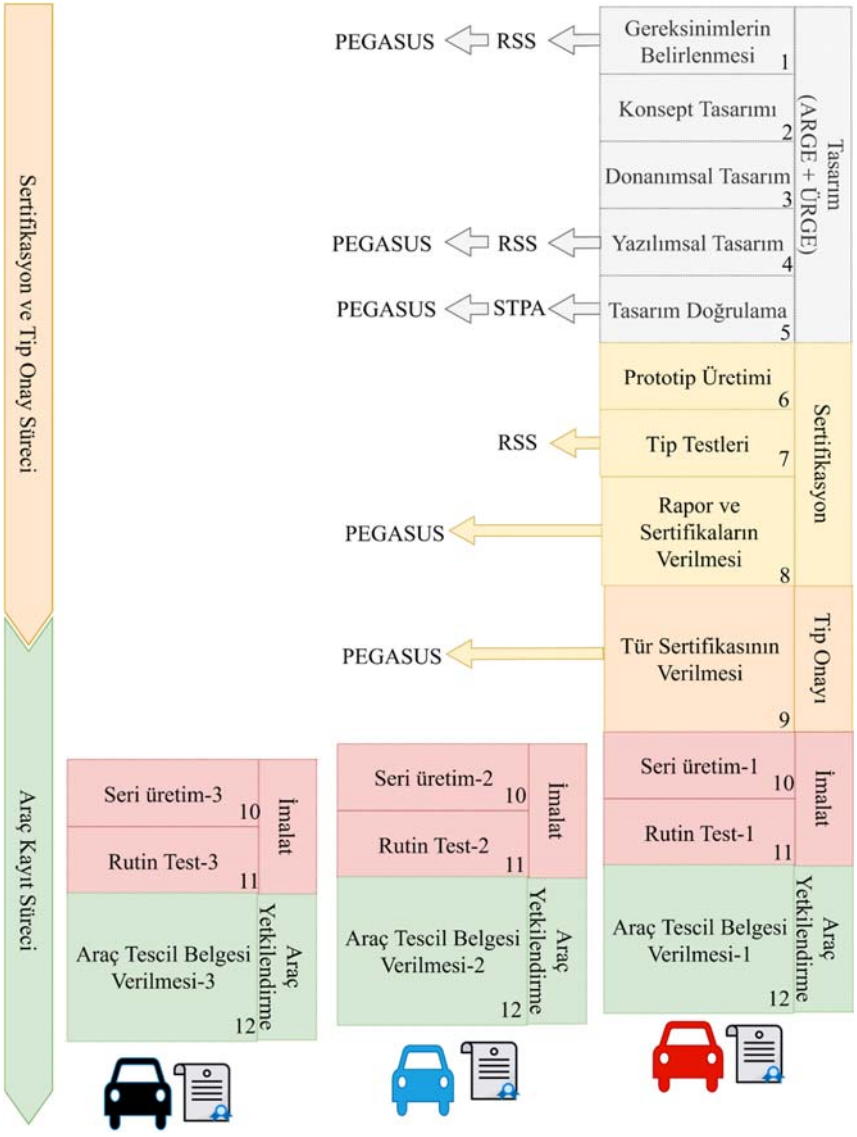
Şekil 14. STPA'nın ISO 26262'ye Entegrasyonu [38] (Integration of STPA into ISO 26262)

Şekil 15'te otonom araçların sertifikasyon, tip onay ve ruhsatlandırma aşamaları şematik olarak açıklanmaktadır. Şekildeki gösterimde demiryolu araçlarının tasarım, üretim, test, sertifikalandırma ve tip onay süreci [40] otonom araca uyarlanmıştır. Şekil 15'in 1. aşaması olan gereksinimlerin belirlenmesi aşaması, iki kaynaktan doğan ihtiyaçların bir araya getirilmesinden oluşmaktadır. Bunların ilki araç üreticisinin piyasanın beklentileri ve bu beklentilerin gerçekleştirilmesi durumunda tüketiciler tarafından ekonomik olarak kabul edilebilirliği dikkate alınarak belirlenen gereksinimlerdir. Bu gereksinimler boyut veya maksimum hız gibi aracın temel tasarım özelliklerinden meydana gelebileceği gibi iklimlendirme, direksiyon kontrol mekanizmasının türü, koltuk ısıtma, iç aydınlatma gibi konfora yönelik fonksiyonlardan veya kullanılacak malzemelerin kalitesi gibi unsurlardan da meydana gelebilmektedir. İkinci kaynak ise, ulusal ve uluslararası mevzuattır. İlk aşamada belirlenen gereksinimlerin ardından, aracın tipi itibariyle gündeme gelecek ulusal ve uluslararası kuralların getireceği gereksinimler toplanarak aracın karşılaması gereken tüm gereksinimler belirlenmelidir.

RSS metodu, aracın üstesinden gelmesi beklenen senaryolar vasıtasıyla yerine getirmesi gereken otonomi fonksiyonların neler olması gerektiği konusundaki soruların bir kısmına cevap verebilmektedir. PEGASUS metodunda ise sertifikasyon sürecinin sistematik bir model ile netleştirilmiş ve sürecin gereksinimlerin belirlenmesi aşamasıyla başlatıldığı dikkate alındığında bu metodun da gereksinimlerin belirlenmesi aşamasına cevap sunduğu görülmektedir.

2. aşamada belirlenen gereksinimlere istinaden konsept tasarımlar yapılmalıdır. Bu tasarımlar aracın yapısal tasarımından, her bir alt sisteme ilişkin sistem mimarilerine ve alt sistemlerin arayüzlerinin belirlenmesine ve sistem bütünlük tasarımlarının meydana gelmesine kadar aracın tüm detay tasarımlarında referans kabul edilecek tasarımları oluşturmaktadır.

3. aşamada konsept tasarımlarla belirlenen donanımsal gereksinimlere uygun donanım ve malzemeler belirlenerek konsept tasarımlarda



Şekil 15. Sertifikasyon Sürecinde RSS, STPA ve PEGASUS Metotlarının Rolleri
(Roles of RSS, STPA and PEGASUS Methods in Certification Process)

ortaya koyulan yapısal tasarımlar ve sistem mimarileri belirlenen donanımlarla detaylandırılarak yeniden- güncellenir. Bu aşamada sistem mimarilerinde kullanımı belirlenmiş donanımların özelliklerine, kullanım alanı ve donanımların mesafeleri dikkate alınarak haberleşme mimarileri de güncellenir. Donanım altyapısı hazırlanırken RSS ve PEGASUS metotlarında ele alınan senaryolarda yerine getirilmesi gereken otonomi fonksiyonlarının gerçekleştirilmesi için gereken uygun donanımlar belirlenmelidir.

4. aşamada ise donanım ve haberleşme detayları belirlenmiş sistem mimarilerinde her bir alt sistemin yerine getirmesi gereken fonksiyonlarını ve bu alt sistemlerin birbiri ile uyumlu ve senkron bir şekilde entegrasyonlarını sağlayacak şekilde kullanılacak yazılımlar, programlama dilleri, algoritmalar belirlenerek yazılım altyapısı hazırlanır. Yazılım altyapısı hazırlanırken RSS ve PEGASUS metotlarında ele alınan senaryolarda yerine getirilmesi gereken otonomi fonksiyonlarının gerçekleştirilmesi için gereken algoritmalar hazırlanır.

5. aşamada yapısal, donanımsal, haberleşme ve yazılım detayları ile tamamlanan tasarımların, her bir alt sistemin birbiri ile sorunsuz bir entegrasyonla, hedeflenen performans kriterlerine uygun şekilde belirlenen fonksiyonları yerine getirebildiği doğrulanır. Bu doğrulama, simülasyonlar ve her bir fonksiyon için uluslararası standartlarda belirlenen analiz metotları kullanılarak gerçekleştirilir. Simülasyon ve analiz sonuçlarının beklenen sonuçları sağladığının teyit edilmesinin ardından prototip üretimine geçilir. Tehlike analizlerinde ISO 26262'de ele alınmayan otonomi fonksiyonlarına ilişkin tehlike analizleri için STPA metodu, doğrulamanın sertifikasyon süreci içerisinde resmi makamlar dahil tüm taraflarca izlenebilirliğinin sağlanması ise PEGASUS metodu ile sağlanmış olur.

6. aşamada konsept, donanımsal, haberleşme ve yazılımsal tasarımlar doğrultusunda kullanılacak donanımların, alt sistemlerin ve bütünleşik sistemin bir prototipi üretilir.

7. aşamada üretilen donanımların, alt sistemlerin ve bütünleşik sistemin saha ve laboratuvar testleri ve incelemeler gerçekleştirilir. Gerçekleştirilen testlerin akredite laboratuvarlarda yapılması, saha testlerinin ve incelemelerinin ise mahiyetine göre yetkilendirilmiş uygunluk değerlendirme kuruluşları nezaretinde yapılarak test sonuçlarının analizlerinin uygunluk değerlendirme kuruluşlarınca teyit edilmesi gerektiği göz önünde bulundurulmalıdır.

8. aşamada ise tip test sonuçları her testin veya incelemenin mahiyetine göre uygunluk değerlendirme kuruluşları tarafından değerlendirilerek, ulusal ve uluslararası mevzuatta belirlenmiş gereksinimlerin karşılandığı doğrulanır ve ürün sertifikalandırılır.

9. aşamada ulusal ve uluslararası mevzuatta belirtilen sertifikalar piyasaya sunma için tip onay başvurusu ile resmi makamlara sunulur. Resmi makamların sunulan sertifikalar ve raporlar üzerinde yapacağı incelemeler sonucunda uygun bulunması halinde, aracın tasarımına ilişkin düzenlenecek tip onay ile seri üretime geçilmesine izin verilir.

Bu aşamadan sonra 10. ve 11. aşamalar, seri üretilen her bir araç için tekrar edilir. 10. aşamada, ulusal ve uluslararası mevzuatla belirlenmiş teknik ve idari gereksinimlere uygunluğu sertifikalandırılmış üretim tesislerinde, tip onaya uygun şekilde araç üretilir. 11. aşamada ise üretilen aracın tip onay şartlarına uygunluğu rutin testlerle doğrulanır. 12. aşamada üretilen aracın tip onay şartlarına uygunluğuna dair kanıtlarla birlikte ruhsatlandırma için ilgili resmi makama başvurularak aracın ruhsatı düzenlenir. Aracın kullanıma sunulması için gerekli olan araç yetkilendirmesi, aracın ruhsatlandırılması olarak kabul edilebilir.

3.1. Metotların Uygulama Alanları (Application Areas of the Methods)

Bu çalışma kapsamında yapılan araştırmalar sonucunda RSS metodunun aracın otonomi fonksiyonları ile ilgili temel prensiplerin belirlenmesi için geliştirildiği açıklanmıştır. Bu yönüyle ürün geliştirme (Ür-Ge) çalışmalarında esas alınması gerekmektedir. Öte yandan üretilen aracın RSS metodu ile belirlenen prensipleri karşılayıp karşılamadığı, bu prensipler doğrultusunda üretilecek senaryolarla test edilmelidir. Bu test mekanizması ise PEGASUS metodunda detaylıca açıklanmaktadır. PEGASUS metodu teker teker tüm işlem basamaklarını açıklamakta, konsept tasarım aşamasından test, sertifikasyon ve resmi makamlarca tip onay düzenlenmesine kadar olan aşamaların birbirleri ile etkileşimlerini belirleyerek tüm süreci bir mekanizma halinde ortaya koymaktadır. STPA metodunda ise otonom aracın otonomi fonksiyonları sebebiyle araçtan veya dış ortam şartlarından veya trafikteki aktörlerden kaynaklanabilecek risklerin ve bu risklerin kabul edilebilir seviyeye indirgenmesi için alınacak tedbirlerin belirlenmesi için gerekli adımlar açıklanmıştır. Böylece halihazırda konvansiyonel otomobiller için kullanılmakta olan ISO 26262 standardında tamamlanması gereken açık noktalara cevap verilmiştir.

3.2. Metotların Olası Kullanıcı Paydaşları (Possible User Stakeholders of the Methods)

RSS metodu aracın otonomi fonksiyonları ile ilgili prensipleri belirlediğinden araç üreticilerinin Ür-Ge departmanları tarafından kullanılacaktır. Öte yandan söz konusu prensipler aracın test senaryolarının belirlenmesinde de kullanılacağından tip onay için gerekli şartları belirlemek ve hukuki düzenlemeleri hazırlamakla yetkilendirilmiş resmi makamlarla bu gereksinimlere uygunluğu sınayacak olan test merkezleri de RSS metodunun muhtemel kullanıcıları arasında olacaktır.

PEGASUS metodunda ise otonom aracın tasarım, üretim, test ve sertifikasyon süreçlerini bir bütün olarak ele alındığından, alt sistem sağlayıcıları, araç üreticileri, test merkezleri ve resmi makamlar bu metodu kullanacak olan muhtemel paydaşlardır.

STPA metodu, konvansiyonel aracın sınandığı ISO 26262 standardında eksik olan otonomi fonksiyonlarının getirdiği risklerin tespiti, risklerin kabul edilebilir seviyeye indirgenebilmesi için gerekli tedbirlerin belirlenmesi konularını tamamladığından tehlike analizi otoritelerinin ve uygunluk değerlendirme kuruluşlarının muhtemel kullanıcılar olduğu değerlendirilmektedir.

3.3. Metotların Uygulanabilirliği (Applicability of the Methods)

Her üç metodun otonom aracın sertifikasyon sürecinde kullanmak için yeterli gelişimin tamamlanmış olup olmadığı konusunda bir değerlendirme yapıldığında; RSS metodunun otonom araç konusunda bugüne kadar yapılan bilimsel ve sektörel çalışmaların çoğuna referans teşkil etmiş olduğu göz önünde bulundurularak uygulanması bakımından yeterli ölçüde tamamlanmış olduğu görülmektedir. Bu sebeple RSS metodunun halihazırda uygulanabilir olduğu değerlendirilmektedir.

PEGASUS metodu ise otomobil ve alt sistem üreticileri ile bilim dünyasından araştırmacıların üzerinde çalıştığı bir projedir. Projenin amaçları, hedefleri ve konsepti açıklanmakla beraber hayata geçirilebilmesi için teknik düzenlemelerdeki eksikliklerin giderilmesi gerekmektedir. Öte yandan PEGASUS projesinin tamamlanması için ulusal ve uluslararası hukuki düzenlemelerin de tamamlanarak yürürlüğe konulması gerekmektedir. Fransa ve Almanya gibi bazı ülkelerin bu konuda ulusal ölçekte çalışmaları olduğu bilinmekle beraber, Avrupa Komisyonu ve UNECE nezdinde ise uluslararası

ölçekte düzenleyici çalışmaların sürdürülmekte olduğu bilinmektedir. Bununla birlikte otonom aracın otonomi fonksiyonlarının periyodik muayenesi veya kaza sonrası onarılan aracın otonomi fonksiyonlarının test edilmesi gibi emniyet açısından kritik önem arz eden bazı hususlara ilişkin uygulamaya yönelik düzenlemeler veya karayolu altyapısında gerekecek yapısal değişiklikler ile akıllı ulaşım sistemlerinin tesisi için gerekli düzenlemeler henüz tamamlanmamıştır. Tüm bu sebeplerle metodun uygulanabilirliği için mevzuat çalışmalarının devam ettiği görülmektedir. Resmi makamlarca otonom araçlar için tip onay düzenlenebilmesi için ulusal ve uluslararası ölçekte düzenleyici çalışmaların tamamlanması ve PEGASUS yönteminin uygulanabilir hale getirilmesi gerekmektedir.

STPA metodu ISO 26262'nin otonom araçlar için kullanımına hazırlanması için geliştirilmiş bir metot olup, özellikle alt sistemlerin değerlendirilmesi konusunda akademik çalışmalar olduğu görülmektedir. Ayrıca her ne kadar otonom araçlar için resmi otoritelerce kabul edilecek nitelikte detaylı risk değerlendirme çalışmaları henüz yapılmamış olsa da, benzer yaklaşımların benimsendiği demiryolu gibi farklı ulaştırma alanlarından örnek uygulamaların benimsenerek gerekli altyapının sağlanması mümkündür. Metodun açık olması ve benzer uygulamalarının bulunması sebebiyle uygulanabilir olduğu değerlendirilmektedir.

3.4. Metotların Sertifikasyon Sürecindeki Rolleri
(The Role of The Methods in Certification Process)

RSS, PEGASUS ve STPA otonom araçların sertifikalandırılması konusunda Avrupa Konseyi tarafından geliştirilmekte olan metotlar olarak yayınlanmış olmakla birlikte, aslında bu üç metodun birbirine alternatif metotlar olmaktan ziyade üç farklı alandaki ihtiyaca cevap veren metotlar olduğu görülmüştür. RSS tasarım ve test kriterlerinin belirlenmesi, PEGASUS tasarımdan tip onaya kadar sertifikasyon sürecinin açıklanması, STPA ise otonom fonksiyonların getirmiş olduğu tehlikelerin analizi konularına açıklık getirmekte olup birbirini tamamlayıcı metotlardır.

4. Sonuçlar (Conclusions)

Günümüzde otonom araçlar ticarileşmiş ve bazı ülkelerde yerel mevzuata dayalı olarak kullanıcıların hizmetine sunulmuş olsalar da otonom bir aracın ulusal ve uluslararası mevzuat gereksinimlerinin neler olacağı, üreticilerin araçları hangi fonksiyonel şartlara uygun tasarlayacakları, bu şartların hangi metotlarla test edileceği konularında çalışmalar henüz sonuçlandırılabilmiş değildir.

Bu çalışmada Avrupa Konseyinin 2020 yılında yayınlamış olduğu "Otonom Araçların Sertifikasyonu İçin Yeni Yaklaşımlar" raporunda ele alınan RSS, PEGASUS ve STPA metotları incelenmiş, otonom aracın sertifikasyon sürecinde bu metotların hangi aşamalarda, hangi alanlarda ve hangi aktörler tarafından kullanılması gerektiği açıklanarak otonom araçların sertifikasyon süreci bir model haline getirilmiştir.

Otonom araçların sertifikasyon sürecinde öne çıkan metotlarda gözlemlenen en önemli eksikliklerden biri, bu çalışma kapsamında incelenen metotların ele alınan senaryo temelli testlerde iklim koşulları, heyelan, bakım onarım çalışmaları veya kaza sonucu yolun zemin şartlarında meydana gelebilecek değişimlerin aracın otonomi fonksiyonlarını öngörülen performans şartlarında yerine getiremeyebileceğinin öngörülmemiş olmasıdır. Böyle bir durumda otonom aracın performans şartlarının beklenmedik koşullarla başa çıkabilecek nitelikte geliştirilmesi gerektiği değerlendirilmektedir.

Benzer şekilde aracın lastiklerinin veya fren sisteminin performans şartlarını etkileyecek sarf malzemelerinin zamana bağlı olarak yıpranması sonucu aracın fonksiyonlarının tasarımında kullanılan formüllerde esas alınan fabrika performans verilerinin zaman geçtikçe değişebileceği dikkate alınarak, araç prototipinin tip test aşamasını başarıyla tamamlamasından sonra seri üretilen araçların kullanım ömrü boyunca karşı karşıya kalacağı öngörülen senaryolarda, tip test aşamasında elde edilen performansı sağlayamayacağı göz önünde bulundurulmalıdır. Bu problemin üstesinden gelebilmek için, öngörülen performans değerleri ile sahadaki gerçekleşmelerin devamlı kıyaslanması ve aracın güncel performans değerlerinin tasarımda kullanılan formüllere yansıtılması gerekmektedir. Dolayısıyla RSS'in birinci ve ikinci kurallarında açıklanan formüllerde adezyonun da matematiksel modellemeye dahil edilmesi ve aracı yöneten yapay zeka tabanlı bilgisayarın, frenleme alt sistemine vereceği fren komutunun fiilen gerçekleşmesini ölçerek maksimum frenleme mesafesini sahadaki adezyon katsayısına göre yeniden hesaplaması ve güncellemesi gerektiği değerlendirilmektedir.

Bir başka önemli husus ise otonom araçların periyodik bakım ve muayeneleri ile kaza sonrası onarım ve muayeneleridir. Bu husus araç üreticilerinin emniyet yönetim sistemi kapsamında ele alınmakla birlikte otonomi fonksiyonların emniyetli şartlarda sürekliliğinin sağlanması, izlenmesi ve denetlenmesi kamu güvenliği açısından kritiktir. Tüm bu uygulamaların denetlenebilmesi ve otonom araçlardan trafik emniyetine beklenen faydanın temin edilebilmesi için kamu otoritelerinin gerekli düzenlemelerle birlikte ilave kurumsal kapasiteler hazırlaması gerektiği görülmektedir.

Otonom araçların otonomi fonksiyonlarının tasarımı, sertifikasyonu ve tip onayı konusunda gelecekte yapılacak çalışmalarda, yukarıda açıklandığı üzere bu çalışmada incelenen metotların eksikliklerinin tamamlanması, sertifikasyon sürecinin resmi bir model haline getirilerek ulusal ve uluslararası düzenlemelerin hazırlanması yönünde çalışmalara devam edilmesi gerekmektedir.

Teşekkürler (Acknowledgement)

Çalışma, kısmi olarak "ROYAL CB SBB 2019K12-149250" kapsamında desteklenmiştir.

Kaynaklar (References)

1. Rohr, C., Ecola, L., Zmud, J., Dunkerley, F., Black, J., Baker, E. Travel in Britain in 2035: Future scenarios and their implications for technology innovation. https://www.rand.org/pubs/research_reports/RR1377.html. Yayın tarihi Haziran 24, 2016. Erişim tarihi Aralık 28, 2023.
2. SAE International. J3016: Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. https://www.sae.org/standards/content/j3016_202104/. Yayın tarihi Nisan 30, 2021. Erişim tarihi Aralık 29, 2023.
3. Stewart, T. Overview of Motor Vehicle Traffic Crashes in 2021. https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/813435. Yayın tarihi Nisan, 2023. Erişim tarihi Aralık 28, 2023.
4. Centre of Excellence for Testing & Research of Avs. Scenario Categories for the Assessment of Automated Vehicles. https://cetran.sg/wp-content/uploads/2020/01/REP200121_Scenario_Categories_v1.7.pdf. Yayın tarihi Ocak 21, 2020. Erişim tarihi Aralık 27, 2023.
5. International Telecommunication Union. Automated driving safety data protocol - Practical demonstrators. https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-AI4AD-2022-01-PDF-E.pdf. Yayın tarihi Eylül 29, 2022. Erişim tarihi Aralık 27, 2023.
6. Liu, Y., Tight, M., Sun, Q., Kang, R., A systematic review: Road infrastructure requirement for Connected and Autonomous Vehicles (CAVs), Journal of Physics: Conference Series, 1187 (4), 042073, 2019.
7. Claybrook, J., Kildare, S. Autonomous vehicles: No driver… no regulation?. Science, 361 (6397), 36-37, 2018.

8. Yu, W., Zhao, C., Wang, H., Liu, J., Ma, X., Yang, Y., Zhao, D., Online legal driving behavior monitoring for self-driving vehicles. Nature communications, 15 (1), 408, 2024.

9. Schöner, H. P., Challenges and approaches for testing of highly automated vehicles, Energy Consumption and Autonomous Driving: Proceedings of the 3rd CESA Automotive Electronics Congress, Paris-France, 101-109, 2014.

10. Junietz, P., Wachenfeld, W., Klonecki, K., Winner, H., Evaluation of different approaches to address safety validation of automated driving, 21st International Conference on Intelligent Transportation Systems, IEEE 491-496, 2018.

11. Koopman, P., Ferrell, U., Fratrik, F., Wagner, M., A safety standard approach for fully autonomous vehicles. In Computer Safety, Reliability, and Security: SAFECOMP 2019 Workshops, ASSURE, DECSoS, SASSUR, STRIVE, and WAISE, Springer International Publishing 38, 326-332, 2019.

12. Baldini, G., Testing and certification of automated vehicles (AV) including cybersecurity and artificial intelligence aspects, EUR 30472 EN, JRC121631, 2020.

13. European Parliament And Of The Council. Commission Implementing Regulation (EU) 2022/1426. https://eur-lex.europa.eu/eli/reg_impl/2022/1426/oj. Yayın tarihi Ağustos 26, 2022. Erişim tarihi Mart 8, 2024.

14. European Parliament And Of The Council. Commission Delegated Regulation (EU) 2022/2236. https://eur-lex.europa.eu/eli/reg_del/2022/2236/oj/eng. Yayın tarihi Kasım 16, 2022. Erişim tarihi Haziran 22, 2025.

15. The United Nations Economic Commission for Europe. Framework document on automated/autonomous vehicles. https://docs.un.org/en/ECE/TRANS/WP.29/2019/34/REV.2. Yayın tarihi Aralık 31, 2019. Erişim tarihi Haziran 21, 2025.

16. Shalev-Shwartz, S., Shammah, S., Shashua, A. Vision zero: can roadway accidents be eliminated without compromising traffic throughput. https://static.mobileye.com/website/corporate/rss/vision_zero_with_map.pdf. Yayın tarihi 2018. Erişim tarihi Mart 6, 2024.

17. French Republic. Development of Autonomous Vehicles - Strategic Orientations for Public Action. https://www.ecologie.gouv.fr/sites/default/files/18029_D%C3%A9veloppement-VA_8p_EN_Pour%20BAT-3.pdf. Yayın tarihi Mayıs, 2018. Erişim tarihi Mart 3, 2024.

18. PEGASUS Research Project. https://www.PEGASUSprojekt.de/en/about-PEGASUS . Erişim tarihi Aralık 27, 2022.

19. Galassi M.C., Lagrange A., Tsakalidis, A. New approaches for automated vehicles certification: Part I - Current and upcoming methods for safety assessment. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC119345/new_approaches_for_automated_vehicles_certification.pdf. Yayın tarihi 2020. Erişim Aralık 31, 2023.

20. Shalev-Shwartz, S., Shammah, S., Shashua, A., On A Formal Model Of Safe And Scalable Self-Driving Cars, arXiv Preprint arXiv:1708.06374, 2017.

21. Koopman, P., Osyk, B., Weast, J., Autonomous vehicles meet the physical world: RSS, variability, uncertainty, and proving safety, 38th International Conference on Computer Safety, Reliability, and Security, Springer International Publishing 38, 245-253, 2019.

22. Mobileye. RSS Explained: the Five Rules for Autonomous Vehicle Safety. https://iot-automotive.news/rss-explained-the-five-rules-for-autonomous-vehicle-safety/autonomous-vehicle-safety/. Yayın tarihi 2019. Erişim tarihi Aralık 27, 2023.

23. Yoshida J., When AVs Attack, Who's at Fault?. https://www.eetimes.com/2020-when-avs-attack-whose-fault/. Yayın tarihi Şubat 1, 2020. Erişim tarihi Aralık 27, 2023.

24. Chai SC., Zeng X., Alvarez I., Elli M. S., Evaluation of Responsibility-Sensitive Safety (RSS) Model based on Human-in-the-loop Driving Simulation, IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), 1-7, 2020.

25. Liu, S., Wang, X., Hassanin, O., Xu, X., Yang, M., Hurwitz, D., Wu, X., Calibration And Evaluation Of Responsibility-Sensitive Safety (RSS) in Automated Vehicle Performance During Cut-In Scenarios, Transportation Research Part C: Emerging Technologies, 103037, 125, 2021.

26. Shashua, A. Shalev-Shwartz, S. Shammah, S. Implementing the RSS model on NHTSA pre-crash scenarios. https://static.mobileye.com/website/corporate/rss/rss_on_nhtsa.pdf. Yayın tarihi 2018. Erişim tarihi Aralık 28, 2023.

27. PEGASUS Project Consortium. Pegasus Method: An Overview. https://www.pegasusprojekt.de/files/tmpl/Pegasus-Abschlussveranstaltung/PEGASUS-Gesamtmethode.pdf. Erişim tarihi Aralık 28, 2023.

28. The International Alliance for Mobility Testing and Standardization. Worldwide Comparison of Highly Automated Vehicle Testing Scenarios Using Real Road Statistics. https://www.iamts.org/storage/app/media/Publications/IAMTS0002202301.pdf. Yayın tarihi Ocak 20, 2023. Erişim tarihi Aralık 28, 2023.

29. The United Nations Economic Commission for Europe. UNECE is driving progress on Autonomous Vehicles. https://unece.org/transport/road-transport/automated-driving-0#accordion. Erişim tarihi Aralık 27, 2023.

30. International Organization for Standardization. ISO 34503:2023 Road Vehicles-Test Scenarios for Automated Driving Systems-Specification for Operational Design Domain https://www.iso.org/standard/78952.html. Yayın tarihi Ağustos, 2023, Erişim tarihi Aralık 26, 2023.

31. The Smart Nation and Digital Government Office. Driving Into The Future. https://www.smartnation.gov.sg/initiatives/transport/autonomous-vehicles/. Erişim tarihi Aralık 28, 2023.

32. International Organization of Motor Vehicle Manufacturers. Global Road Safety OICA Manifesto. https://www.oica.net/wp-content/uploads/OICA-manifesto-on-global-road-safety-30-06-2022.pdf. Yayın tarihi Haziran 30, 2022. Erişim tarihi Aralık 27, 2023.

33. Form, T., PEGASUS Method for Assessment of Highly Automated Driving Function, SIP-adus Workshop, 13-15, 2018.

34. Ishimatsu, T., Leveson, N. G., Thomas, J., Katahira, M., Miyamoto, Y., Nakao, H., Modeling And Hazard Analysis Using STPA, Proceedings of the 4th IAASS Conference, 19-21, 2010.

35. Abdulkhaleq, A., Wagner, S., Experiences with applying STPA to software-intensive systems in the automotive domain, STAMP Workshop, 1-3, 2013.

36. Czarnecki, K., On-road safety of automated driving system (ADS)-Taxonomy and safety analysis methods, WISE Requirements Analysis Framework for Automated Driving Systems, University of Waterloo, 2018.

37. Mallya, A., Pantelic, V., Adedjouma, M., Lawford, M., Wassyng, A., Using STPA in an ISO 26262 compliant process, International Conference on Computer Safety, Reliability, and Security, Springer, 117-129, 2016.

38. Abdulkhaleq, A., Wagner, S., Lammering, D., Boehmert, H., Blueher, P., Using STPA In Compliance With ISO 26262 For Developing A Safe Architecture For Fully Automated Vehicles, arXiv preprint arXiv:1703.03657, 2017.

39. Hu, Z., Analysis Of Autonomous Vehicle Safety Constraints Based On Systems-Theoretic Process Analysis, Journal Of Physics: Conference Series 1650 (3), 032137, 2020.

40. European Union Agency For Railways. Guide fort he application of the LOC&PAS TSI Version 4.0 of 16/02/2024. https://www.era.europa.eu/system/files/2024-02/LOC-PAS_Guide-2023.pdf?t=1709711569. Yayın tarihi Şubat 16, 2024. Erişim tarihi Mart 6, 2024.