Amaçlanan Fonksiyonelliğin Güvenliği için Sistem Teorik Süreç Analizinin Yorumlanarak Risk Analizinde Kullanımı

Interpretation and utilization of Systems Theoretic Process Analysis in Risk Analysis of Safety of the Intended Functionality

Tibet İşkesen[1], *Mertcan Tezcan*[2], *Barış İşman*[3], *Serhat Karaayak*[4]

[1]AVL Türkiye Araştırma ve Mühendislik, İstanbul
Tibet.Iskesen@avl.com

[2]AVL Türkiye Araştırma ve Mühendislik, İstanbul
Mertcan.Tezcan@avl.com

[3]AVL Türkiye Araştırma ve Mühendislik, İstanbul
Baris.Isman@avl.com

[4]SerhatKaraayak@gmail.com

Özetçe

Otonom sürüş teknolojilerindeki önemli ilerlemeler, dinamik sürüş görevinin insan sürücülerden araçlara çeşitli seviyelerde devredilmesine olanak tanır. Fonksiyonel güvenliğin sağlanması, ISO26262 sayesinde araçların geliştirilmesinde uzun süredir alışılagelmiş bir adımdır. Ancak, otonom araçların kontrolcüleri giderek karmaşık ve birbirine bağımlı hale geldikçe, elektronik arızalardan kaynaklanmayan tehlikeleri ele almak için ek bir standart oluşturulmasını gerektirdi. Bu, ISO21448: Amaçlanan Fonksiyonelliğin Güvenliği (SOTIF) adlı ayrı bir standart şeklinde sunulmuştur. Bu makale, SOTIF'e yönelik Sistem Teorik Süreç Analizi'nin (STPA) bir yorumunu önermekte ve mevcut literatürdeki yaygın kavram kargaşalarını tartışarak gelecekteki çalışmaların daha iyi bir uyum içinde yapılması için öneriler sunmaktadır.

Abstract

Significant advancements in autonomous driving technologies leads the way for dynamic driving task to be handed over from human drivers to the vehicles in a variety of different levels. Ensuring the functional safety has been an ordinary step of the development of vehicles for a while now thanks to ISO26262. However, as the controllers of AVs (Autonomous Vehicles) got more and more complex and interdependent, there had to be an additional standard to address the hazards that are not caused by electronic failures. This was delivered in the form of a separate standard, ISO21448: SOTIF (Safety of the Intended Functionality). This paper proposes an interpretation of Systems Theoretic Processes Analysis (STPA) to SOTIF and discusses common misconceptions in the current state of literature along with recommendations for a better harmonization of future works.

1. Giriş

Otonom sürüş teknolojisi ilerledikçe, araçlar karmaşık çevre algılama, işbirlikçi kontrol ve akıllı karar verme işlevlerine sahip daha karmaşık sensörler, kontrol mekanizmaları ve hareket düzenleyicilerle donatılmaktadır. Bu gelişmelerin amacı, dinamik sürüş görevini tamamlamak için insan sürücünün payını azaltmak veya ortadan kaldırmaktır. Ancak, bu işlevler, arıza olmamasına rağmen amaçlanan fonksiyonlarda tehlikeli durumlar yaratabilir. Performans kısıtlamaları ve isterlerin yetersizliklerinden kaynaklanan potansiyel riskler, Amaçlanan Fonksiyonelliğin Güvenliği (SOTIF) kapsamında sınıflandırılır. Bu nedenle, otomobil tedarikçileri ve üreticileri tarafından kullanılan test ve geliştirme süreçlerini uyumlu hale getirmek ve böylece SOTIF sorunlarıyla ilişkili riskleri azaltmak için ISO 21448 [1] standardı öne sürülmüştür.

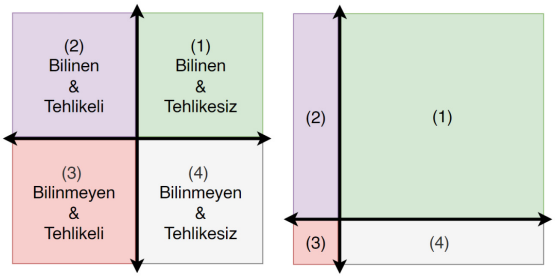
ISO 21448'in kardeşi olan ISO 26262'den bazı uygulamaları ve deneyimleri devşirerek benzerlikler kurmak mümkündür. Her ikisinde de bulunmasına rağmen SOTIF'in eklediği terimler ve bağlantılardan sebepli "Risk Analizi" basamağı daha fazla önem teşkil etmektedir. Eğer her iki standardın V-döngüleri üst üste oturtulursa, bu basamağın ISO 26262'nin "Tehlike Analizi ve Risk Değerlendirmesi (HARA)" ile örtüştüğü görülecektir. Bu kapsamlı analiz yapılırken, her faktörü barındırabilecek bir yöntemin eksikliği durumunda tehlikeleri belirlemek, riskleri değerlendirmek ve tetikleyici koşulları tespit etmek oldukça zorlaşacaktır. Bu nedenle SOTIF için geliştirilecek yöntem, hem geleneksel yaklaşımlar ile açığa çıkarılabilen hem de bu tekniklerin tespit edemediği tasarım hataları, insan hataları ve bileşen etkileşimlerinden ortaya çıkan risklerin de keşfine olanak sağlamalıdır.

Bu makale, Şerit Takip Yardımcısı (LKA) ve Şerit Değiştirme Yardımcısı (LCA) örnekleri üzerinden, fonksiyonel yetersizlikleri ve tetikleyici koşulları sistemli olarak analiz ederken karşılaşılan zorlukları ele alacak ve SOTIF'in Risk Analizi basamağında kullanılmak üzere özgün bir STPA yorumu önermektedir.

2. SOTIF

SOTIF'in ilk aşaması, fonksiyon ve sistem özelliklerinin tanımlanmasıdır. Daha sonra tehlikeler belirlenir. Bu tehlikeler en kötü olası sonuçlar için bağlamlandırılır ve bu bilgi ile tehlike tanımlama ve risk değerlendirmesi yapılır.

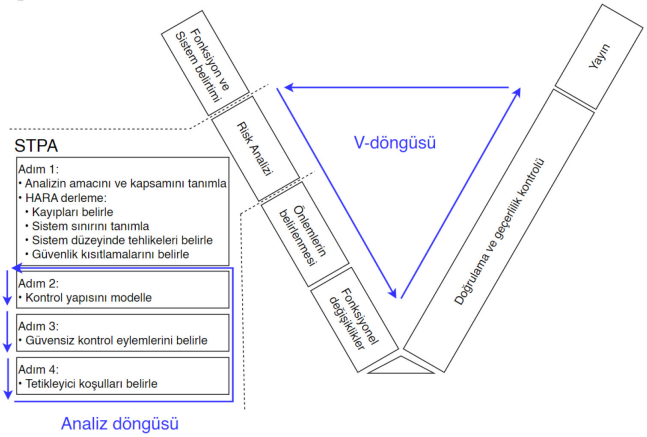
Eğer bir tehlikenin riski kabul edilebilir değilse; tehlikeli olaya neden olabilecek tetikleyici koşullar araştırılır. Bu aşamada SOTIF süreçlerinin mantığını anlatmak, senaryo çizelgesi (Şekil 1) ile daha basit hale gelir. [1]'e uygun olarak, aracın karşılaşabileceği tüm senaryolar dört alana ayrılır:



Şekil 1: ISO 21448 etkinliklerinin sonucunda elde edilen senaryo kategorilerinin değerlendirilmesi.

Bu noktada amaç; 3. alandan mümkün olduğunca çok senaryoyu keşfetmek ve onları artık SOTIF terimleriyle net bir şekilde tanımlanabilecekleri 2. alana aktarmaktır. Bu senaryolar daha sonra riskleri için değerlendirilmek üzere incelenir.

Sonrasında, tetikleyici koşullar incelenir ve eğer kabul edilemez bir risk taşıyorlarsa, ilgili fonksiyonlarda geliştirmeler yapılır. Geliştirmelerin etkileri ve geride bırakılan riskin kabul edilebilirliği doğrulanarak senaryolar 2. alandan 1. alana transfer edilir. Tespit edilen tüm tetikleyici koşullar için araç seviyesinde geriye kalan risklerin kabul edilebilirliği de onaylandıktan sonra SOTIF yayını yapılabilir.



Şekil 2: SOTIF V-döngüsü ve risk analizi alt adımlarının detaylı görünümü.

Bu çalışmanın metoduna göre, SOTIF'in V-döngüsünde (Şekil 2), Risk Analizi'nin alt kırılımları, tercih edilen yöntem olan STPA'nın basamakları ile doldurulmuştur. STPA basamaklarının, V-döngüsünden bağımsız bir şekilde süreç boyunca kendi içinde döngüsel çalışabileceği de tanınmalıdır. Bu ayrım, Risk Analizi adımının daha sık ve daha hızlı tekrarlara olan ihtiyacını vurgulamak için faydalıdır.

3. STPA

Hata Türü Etki Analizi (FMEA), Hata Ağacı Analizi (FTA) gibi geleneksel tehlike analiz teknikleri, güvenilirlik teorisine dayanır ve potansiyel bileşen arızalarına odaklanır. Bu nedenle bazen sistemin tüm yönlerini ve özellikle insan hatasını içermekte yetersiz kalırlar. 2004 yılında Leveson, FMEA ve FTA ile karşılaştırıldığında daha fazla türde tehdit ve tehlikeyi ele alabilen bütünsel bir sistem güvenliği yaklaşımı olan STPA'yı geliştirmiştir. STPA, geleneksel güvenlik analizlerinde olduğu gibi tekil bileşen arızalarını değil, kontrol yapısındaki bileşenler arasındaki Güvensiz Kontrol Eylemlerini (UCA) belirlemeye odaklanan daha kapsamlı bir tehlike analizi tekniğidir.

STPA analizlerinin temel amacı, üstten aşağı yaklaşımı göz önünde bulundurarak, kazalara yol açabilecek güvensiz senaryoları ortadan kaldırmak için güvenlik kısıtlamalarını belirlemektir.

Güvenlik yöneticisi, STPA adımlarını birden fazla işlem aşamasına yaymak veya sadece bazı temel STPA süreçlerini izole bir analitik yaklaşım olarak kullanmak arasında seçim yapabilir. Bu çalışmada, STPA'nın tüm basamakları ile kullanımı tercih edilmiştir.

Bu çalışma akışı içinde HARA'nın nasıl yerleştirileceği konusunda farklı yaklaşımlar görülmektedir, [9] tarafından yorumlandığı gibi; analizin hazırlık faaliyetleri olarak sayılabilir. Benzer şekilde, bu çalışmada da HARA, üst düzey bir belge olarak bırakılmış ancak ilk STPA döngüsünün bir çalışma ürünü olarak düşünülmüştür, süreçten tamamıyla soyutlanmamıştır.

3.1. Analizin Amacının ve Kapsamının Tanımlanması

Önemli bir not olarak belirtilmelidir ki, STPA literatürü, kayıpların ve tehlikelerin belirlenmesini iki ayrı adım olarak değerlendirirken, otomotiv sektöründe genellikle birlikte gerçekleştirilirler.

Bu aşamada, paydaşların kayıpları ve tehlikeleri araç düzeyinde belirlenir. LKA/LCA sistemleri için olası paydaşların kayıpları ve bunlara karşılık gelen tehlikeler tespit edilebilir. [1]

"<Güvensiz Durum>"un nasıl elde edileceği konusunda çelişen görüşler vardır. [7], sadece tehlikeleri tanımlayabilmek için senaryoların "kalıcı bölgesel unsurları"nı buraya yerleştirir. Ancak bu çalışma için, bir "kullanım durumu"nun oluşturulmasına katkıda bulunan tüm unsurların dahil edilmesi desteklenmektedir. Otonom Acil Frenleme (AEB) için tanımlanmış bir kullanım durumuna örnek [8] içinde bulunabilir.

[9]'un HARA tablosu, mantığı şu şekilde yansıtmaktadır. <Tehlikeli Olay>'ın yer aldığı <Senaryo/Durum> , <Kaza>'ya sebebiyet vererek <Zarar> meydana getirir. Ancak <Tehlikeli Olay> bir <Tehlike> nin eşanlamlısı olarak alınmamalıdır çünkü hem STPA sınıflandırması hem de SOTIF, <Tehlikeli Olay> ın bir <Tehlike> + <Senaryo> sonucu olduğunu ima etmektedir [10][1]. [11] açıklandığı üzere <Durum> da <Senaryo> dan ayrılmalıdır. Test yapılmadan veya herhangi bir derecelendirme almadan, <Tehlikeli Olaylar> da <Potansiyel Tehlikeli Olaylar> olarak kabul edilmelidir, çünkü bunların <Zarar> meydana getirecekleri garanti edilemeyecektir. <Kaza> da sınıflandırmada ihmal edilmiş bir ara basamak olarak anlaşılmaktadır, [1] <Tehlikeli Olay>ı ve <İlgili Kişilerin Tepkileri>ni birleştirerek <Zarar> sonucuna varmaktadır. Bu

durumda, <Kaza> sütunu olduğu gibi bırakılabilir çünkü bir kazanın sözlü açıklaması, satırları inceleyecek olan uzmana <Ağırlık> ve <Kontrol Edilebilirlik> değerlerini elle tayin etmede bazı kolaylıklar sağlayabilir. Ancak aksi takdirde değerlendirmeye çok fazla değer katmayan bir ara basamak olarak görülmelidir.

Tespit edilen kayıplar ve tehlikeler sonrasında, araç düzeyindeki Güvenlik Kısıtlamaları (SC) tanımlanmalıdır. Bu noktada <Tehlike>nin zıttını alarak, Güvenlik Kısıtlamalarını düz ve anlaşılır ifadelerle yazmak mümkündür.

[SC1]: Araç, kendisini şerit içinde tutmak için gerekli önlemleri almalıdır.

Analizlerin amacını ve kapsamını tanımlamak için, araç düzeyinde SOTIF gereksinimleri belirlenmelidir. LCA ve LKA sistem düzeyindeki gereksinimler, UN ECE düzenlemeleri #79, #130 ve #157 göz önünde bulundurularak belirlenebilir. Örneğin, UN ECE R157, ego aracın en ön üst yüzeyinin karşısındaki 46 metrelik mesafeyi algılaması gerektiğini tanımlar. [6] Ayrıca, sistem tasarım gereksinimleri bir araya getirilerek bu güvenlik kısıtlamaları daha hızlı bir şekilde belirlenebilir.

3.2. Kontrol Yapısının Modellenmesi

Kontrol yapısında, bileşen arayüzleri ve sistem elemanları arasındaki hiyerarşi belirlenir. Sistem elemanları birbirleriyle bilgi iletimi yapar (yatay oklar). Kontrol eylemleri ilgili denetleyiciler tarafından komuta edilir (aşağı yönlü oklar) ve geri bildirimler alınır (yukarı yönlü oklar).

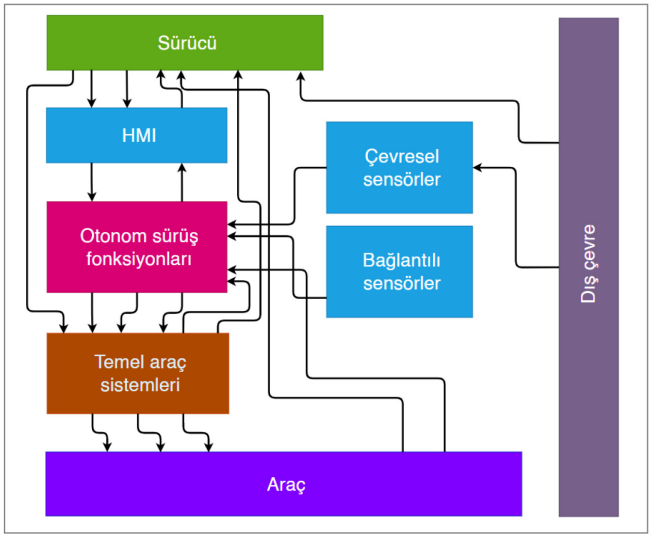
Bu aşamaya kadar, her şey araç seviyesinde tutulabilir. Ancak STPA'nın bir sonraki adımına geçmek için en azından başlangıç düzeyinde bir kontrol yapı modeli hazırlanmalıdır. SOTIF çok erken bir geliştirme aşamasında başlatılabileceğinden; bileşen veya sistem düzeyi ayrıntıları henüz tanımlanamasa bile bir kontrol yapısı hazırlamak faydalı olacaktır. Sadece araç seviyesi yapı ile başlanabilir ve bu yapı üzerinde "analiz döngüsü" içinde aşama aşama ilerlenebilir.

[12], STPA'nın farklı mimari seviyelerinde bir bütün olarak uygulanabileceğini tartışmaktadır.

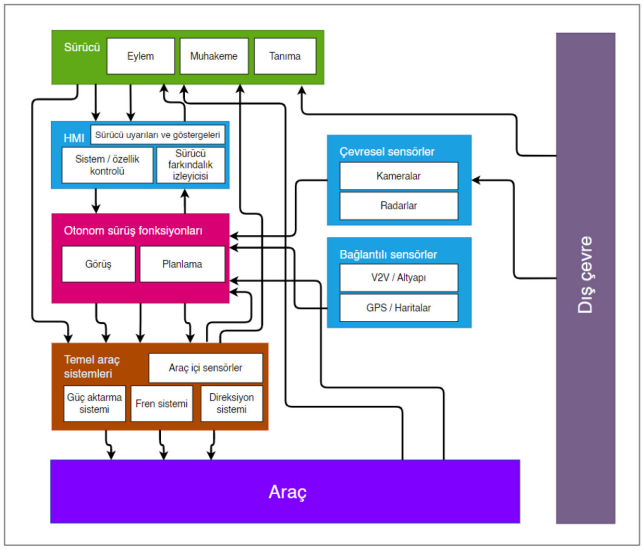
Bu çalışmayla karma mimari seviye modellemesinin kullanımı önerilmektedir. İncelenmesi hedeflenen çekirdek bir blok seçilmelidir, bu çalışmada çekirdek; "Otonom sürüş fonksiyonları" bloğudur. Bu çekirdek ile etkileşim halindeki blokların detay seviyeleri bileşen düzeyine kadar indirilebilir. Ancak sistemin kalan blokları araç seviyesi detaylarda bırakılabilir.

Geliştirme sürecinin olgunluğuna bağlı olarak mimari seviyeleri arasında geçiş yapabilen iterasyon anahtar noktaları aşağıda sıralanmıştır. Bu geçişler, önceki bir bölümde belirtildiği gibi analiz döngüsü içinde yönetilebilir.

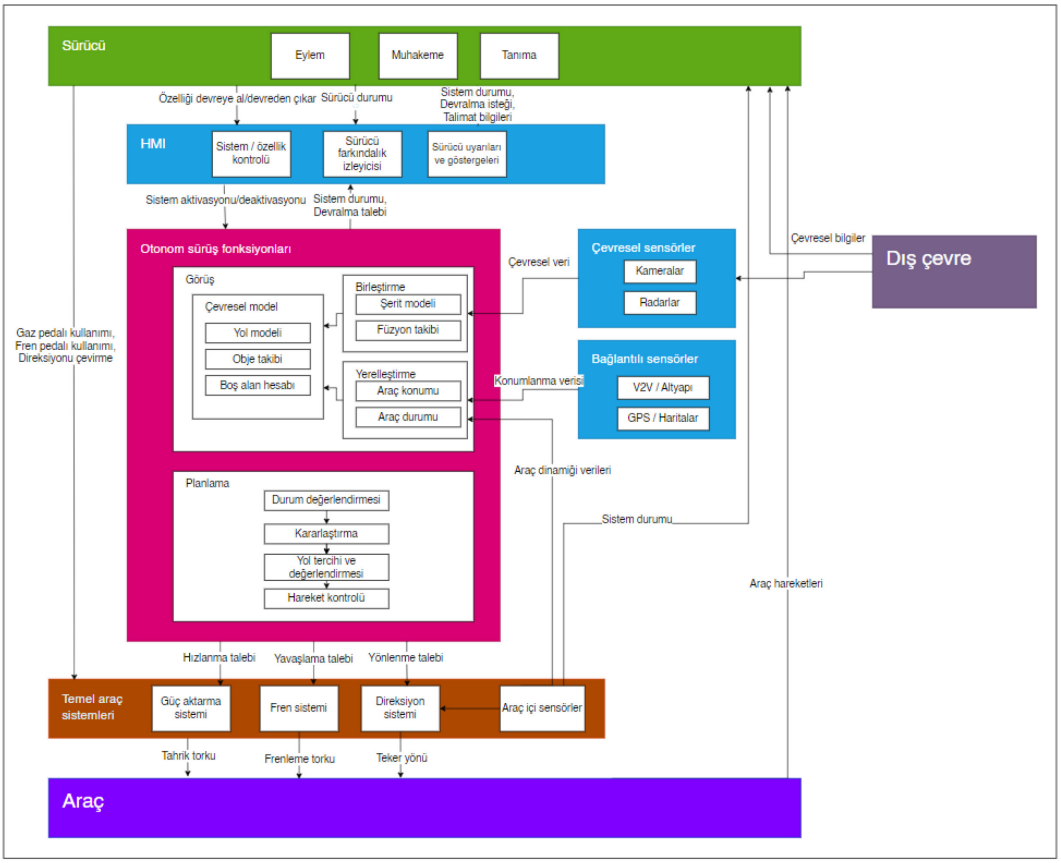
• Eğer kontrol yapısı yalnızca araç düzeyinde oluşturulabilirse; bu yüksek seviyedeki görüşte, otomatik sürüş işlev platformu, sensörlerden veri alır ve eyleyicilere kontrol komutları gönderen tek bir kontrol bileşeni olarak kabul edilir (Şekil 3).



Şekil 3: Sadece araç düzeyindeki bloklardan oluşan kontrol yapısı (ok tanımları, okunabilirlik için çıkarılmıştır)



Şekil 4: Kontrol yapısı, araç ve sistem düzeyinde bloklarla oluşturulmuştur (ok tanımları, okunabilirlik için çıkarılmıştır).



Şekil 5: Araç, sistem ve bileşen düzeyinde bloklarla oluşturulan kontrol yapısı.

• Proje yeterince olgunlaştığında, sistem seviyesine geçilir. Ancak tüm mimariyi bu seviyeye dönüştürmek gerekmez. Daha düşük seviyelere inerken önemli olan, SOTIF'in odaklandığı kontrol bileşenlerini seçmek ve sadece onları daha düşük seviyede incelemektir. Odak dışı bloklar (dikkate alınmayan fonksiyonlar) daha yüksek seviye ayrıntıda (soyutlanmış) bırakılabilir (Şekil 4). Eğer SOTIF, bir LKA sistemi üzerine odaklanıyorsa, güç aktarma organı veya fren sistemlerinin sistem seviyesi detayları önemli olmayabilir. Aslında, bu detayların varlığı proje karmaşıklığını istenmeyen bir şekilde artırabilir. Odaklanılan blokların birden çok birbirine bağlı alt bileşene çözümlenmesiyle, bu seviyenin her yeni bloğunun güvenli olmayan kontrol eylemleri türetilir. Belirli bir soyutlama düzeyi gerekecektir, çünkü tüm işlevler SOTIF değerlendirmesinin odağında olmayacaktır. Örneğin bu çalışmada, Otonom Hız Sabitleyici (ACC) işlevi soyutlanmış ve STPA adımlarına dahil edilmemiştir. Benzer şekilde sistemde bulunan bazı işlevler de çatı karşılıklarıyla birleştirilir. Örneğin gösterge paneli, basitlik açısından İnsan-Makine Arayüzü (HMI) bloğu ile birleştirilmiştir. [9], benzer bir mantığı izleyerek "Otoyol Pilotu" bloğunu çekirdek işlev olarak belirlemiş ve STPA'yı onun etrafında uygulamıştır.

• Bileşen düzeyi ayrıntıları da hazır olduğunda, önceki adımda olduğu gibi seviye ayrışımını uygulayarak "odaklanılan" her yazılım sistem bileşeninin kontrol eylemleri bulunur (Şekil 5).

[12] çalışmasındaki gibi, kontrol eylemlerine seviye göstergesi değerleri atanacak, böylece daha düşük seviye kontrol eylemlerini, daha yüksek seviye güvensiz kontrol eyleminin katkıda bulunanları olarak bağlantılandırmak mümkün olacaktır. n seviyesindeki tehlikeler HAn.x olarak kodlanacaktır. Burada 'n'; seviyenin numarasını, 'x' ise tehlikenin numarasını temsil eder.

Örnek: CA1.23, CA0.23, CA2.5

3.3. Güvensiz Kontrol Eylemlerinin Tanımlanması

Araç seviyesindeki tehlikeler temel olarak belirli bir bağlam ve/veya en kötü senaryolar altında meydana gelen güvensiz kontrol eylemlerinin sonucudur. [1]. UCAlar tanımlandığında, hepsi adım 2'de belirtilmiş ilişkili araç seviyesi tehlikelerine bağlanır. Her bir UCA, en az bir araç seviyesi tehlike oluşturmak zorundadır.

Kontrol yapısı oluşturulduktan sonra, ilk olarak kontrol eylemleri elde edilir. Şerit değiştirme ve şerit tutma asistanı için bazı kontrol eylemleri aşağıdaki gibi belirlenebilir:

• Yanal konumu koru - Bu kontrol eyleminin ana önceliği, ego aracı ve şeritler arasındaki mesafeyi ayarlamaktır.
• Şerit değiştirme sırasında hızı sabit tut - Şerit değiştirme işlemleri sırasında, ego aracın kendi hızını koruması gerekir.
• Direksiyon komutu gir - Sürücü, LCA/LKA fonksiyonunu komuta etmek için HMI kullanır.

UCA formülü: <Güvensiz Kontrol Eylemi> = <Kaynak> <Tür> <Kontrol Eylemi> <Bağlam> <Tehlikelerle Bağlantı>

Her bir kontrol eylemi doğrudan UCA senaryolarıyla ilişkilidir. LCA/LKA'nın kontrol eylemlerinden biri, bir direksiyon komutudur.

Daha iyi ifade edilebilmesi için, [9] tarafından önerilen kelimeler şunlar şekilde kullanılabilir: "ne zaman", "sırasında", "esnasında", "rağmen", "ile", "bu nedenle" gibi bağlaçlar, bağlamları kontrol eylemleri ile bağlayarak Güvensiz Kontrol Eylemleri elde etmek için kullanılabilir.

STPA'nın kritik adımlarından biri, tanımlanan kontrol eylemlerine bağlamsallaştırma sağlayacak kaynakları seçmektir ve bazı kaynak örnekleri listelenen gibidir:
• Uzman incelemeleri; eylem dizilerinin gözden geçirilmesi
• Tehlike oluşumunun tipik şemaları için kontrol listeleri (örneğin [2] tarafından önerilenler)
• Sanal simülasyon
• [9] tarafından önerildiği gibi (sistem etkileşimlerinde) Hata Ağacı Analizi
• [12]'de yapıldığı gibi bağlam tablolarını oluşturmak için XSTAMPP (eXtensible STAMP Platform) [13]

3.4. Tetikleyici Koşulların Tanımlanması

Nedensel senaryolar (causal scenarios), STPA analizinin nihai çıktılarıdır. Güvensiz kontrol eylemleri, şerit değiştirme ve şerit tutma asistanının fonksiyonel yetersizlikleri ve tetikleyici koşullarının birleşmesi ile oluşturulurlar. Ayrıca, sistemin öngörülebilir yanlış kullanımları da bu senaryolara yol açar [4].

Bazı örnekler aşağıda verilmiştir:

[CS1]: Sürücü, sistemi istemeden devre dışı bırakıyor (refleksif ve/veya kazara)
[CS3.1]: Pozisyon sensörü, olumsuz hava koşullarından dolayı ego aracının önündeki mesafeyi yanlış ölçüyor.
[CS3.2]: Pozisyon sensörü yanlış monte/kalibre edilmiş.

Önemli bir nokta, tehlikelere yol açan neden-sonuç senaryolarının, aynı zamanda "tetikleyici koşullar" olarak da adlandırılan nedensel faktörlerden oluştuğudur. Bu noktada, deneyim önemlidir, [14] tarafından belirtildiği gibi. Bir uzman, teknik tasarımı analiz edebilir ve bir bileşenin potansiyel tetikleyici koşullarını, önceki deneyimlerine ve alandaki genel bilgisine dayanarak belirleyebilir. Kolaylık sağlamak için [1]'in Tablo 4'ünde bazı yöntemler listelenmiştir.

Uzmanların listesi, konuyla ilgili hayal güçleri veya hafızalarının sınırlarında sona erer ve “bilinmeyen ve güvensiz” havuzunda keşfedilecek çok senaryo bırakabilir.

Bu noktada, yol testleri devreye girebilir, ancak tek başına yeterli olamaz. [15]'e göre, otomatik araçların güvenliğini %95 düzeyinde doğrulamak için 10 milyar kilometrelik yol testi tamamlanmalıdır. Geleneksel testlerin uzun döngü süreleri ve yüksek maliyetleri gibi dezavantajları bulunmaktadır; bu da hızlı güncelleme döngüsüne sahip otonom teknolojilerle donatılan araçların test ihtiyaçlarını karşılamayı zorlaştırır.

Sanal simülasyon ortamları gerçek dünya sürüşünü taklit edebilir ve testlerin zaman ve maliyet isterlerini azaltabilir. Bu nedenle, tetikleyici koşulların bulunduğu “bilinmeyen ve güvensiz” senaryoları keşfetmek için sanal simülasyonların kullanımı faydalı olacaktır.

[16], yöntemleri "bilgi temelli" olarak adlandırılan, daha çok beyaz kutu sistemler için uygun olan ve "veri temelli" olarak adlandırılan, daha çok siyah kutu sistemler için uygun olan iki kategoriye ayırmayı tercih eder. SOTIF çabasının büyük bir kısmı bir ara aşamada harcanacağından, bu iki yöntemi birbirini tamamlayıcı olarak birleştirmek en iyisidir.

Tamamen uzman görüşünden veya yol testlerinden feragat etmek önerilmez, çünkü tüm yöntemlerin kendi kapsama alanları vardır. Bir uzman tarafından önerilen veya yol testi sırasında ortaya çıkan "Sensör düzgün bir şekilde kurulmamıştır" gibi bazı tetikleyici koşullar vardır ki bu, herhangi bir set parametrenin kombinasyonuyla üretilemeyebilir (siyah kuğu durumları).

Ayrıca dikkat edilmesi gereken bir başka konu ise: Simülasyon ve yol testi, aracı çevresel koşullara maruz bırakır ve bir yetersizliğin ortaya çıkmasını bekler. Ancak bir uzman, çevresel koşullardan bağımsız olarak tanımlanan bir tetikleyici koşulu doğrudan önermeyi tercih edebilir. Dolayısıyla, uzmanların tetikleyici koşulları, daha sonra risk değerlendirme puanlamalarında kullanılacak aynı arka plan verilerini taşımayabilir. Bu nedenle, çerçevenin farklı girdi kaynaklarını işleyebilmesi ve onları güvenilir bir puanlama mantığı ve kabul kriterine entegre edebilmesi gerekmektedir; ancak bu entegrasyon uyumluluğu gelecek çalışmalara bırakılmıştır.

Yukarıda bahsedilen tüm neden-sonuç senaryoları "Tip 1" olarak sayılabilir. Bu neden-sonuç senaryoları, sistem ve bileşenlerin performans sınırlarını aşan koşulları içerir. Bunlar, işlevsel ve sistem spesifikasyonlarda tanımlanan teknolojilere, ana araç tabanlı sensörlere (kamera ve radar), GPS ve haritalara, algılama ve karar verme algoritmalarına özgüdür. Ayrıca, "Tip 2" olarak adlandırılan, insan faktörü kısıtlamaları tarafından oluşturulan neden-sonuç senaryoları vardır. Bu türde, HMI'daki kısıtlamalar ve potansiyel öngörülebilir yanlış kullanım senaryoları yer alır.

İnsan hatalarıyla ilgili olarak, ISO 21448 “rehber kelimeleri”ne dayanarak birçok tetikleyici olay bulunabilir. İnsanın zihinsel modeli; tanıma, değerlendirme ve eylem olmak üzere üç bölüme ayrılır. Tanıma için kullanılacak bazı kılavuz kelimeler; "Anlamama", "Yanlış anlama"; değerlendirme için: "Değerlendirme hatası / Yanlış değerlendirme", "Kayma/Hata"; eylem için ise: "Kasten", "Yapamama" [1]. Tüm potansiyel insan hataları, çeşitli insan-araç etkileşim tipleriyle birleştirilerek elde edilebilir ve ardından bu insan hataları neden-sonuç senaryolarının bir parçası olarak kabul edilir.

Bilinmeyen güvensiz senaryolarda tatmin edici bir kapsama düzeyine sahip olmak için, Operasyon Tasarım Kümesi (ODD) [18] koşullarından uyarlanmış, simülasyon için senaryolar oluşturulması gerekecektir. Çok sayıda durumla uğraşılacağından, hangi durumların öncelikli olacağının veya ihmal edileceğinin seçileceği bir strateji belirlenmeli ve bu bilgi sonraki STPA iterasyonlarına taşınmalıdır, böylece otonom sistemi daha da zorlayıcı senaryolar oluşturulabilir. Son olarak; SOTIF'in "gerçekleşme", "kontrol edilebilirlik" ve "şiddet" gibi derecelendirme terimleri arasında veri ve matematiksel ilişkiler kurulması gerekmektedir.

[7]’de bir çerçeve önerilmektedir ancak senaryonun araç dışındaki yönlerini belirlemeye çalışır ve bu nedenle "sistem hedefleri ve değerleri" terimini içermez. Bu eksiklik, senaryoların bir dizi “sahne”den filtrelenebilmesinde gereken ayırıcıdır. Yine de, öne sürülen çerçeve [17], [1] ve Ölümlü Kaza Analiz Raporlama Sistemi (FARS) olmak üzere üç kaynaktan türetilen değişkenleri birleştirebilmektedir.

4. Sonuç

Bu makalede yazarlar, SOTIF analizinin STPA tarafından yönetilen adımlarını tartışmış, yoğun efor gerektiren çalışma ürünlerini ve noksanlıkları işaret etmiş, V-döngüsüne ek olarak ikincil bir iterasyon döngüsü belirlemişlerdir. SOTIF zorluklarını

kucaklamak için çalışma çerçevelerinde yapılabilecek değişiklikler önerilmiş, tehlikeleri tanımlarken, güvensiz kontrol eylemlerini bağlamsallaştırırken ve tetikleyici koşulları incelemek için nedensel senaryolar oluştururken farklı yaklaşımlar karşılaştırılmıştır. Konvansiyonel yaklaşımların yetersizlikleri ve önceki çalışmaların hataları da ele alınmıştır.

5. Gelecek Çalışmalar

Önerilen yöntemler test edilmelidir. Analiz kapsamı, bir otonom aracın diğer alt sistemlerini de içerecek şekilde genişletilebilir, böylece etkileşimler daha ayrıntılı bir şekilde incelenebilir ve SOTIF'in risk analizi daha kapsamlı bir şekilde gerçekleştirilebilir.

Kaynakça

[1] International Organization for Standardization. (2022). Road vehicles — Safety of the intended functionality (ISO 21448:2022)

[2] International Organization for Standardization. (2018). Road vehicles — Functional safety (ISO 26262:2018)

[3] Jung S., Heo Y., Yoo J., (2021 July, 19) A formal approach to support the identification of unsafe control actions of STPA for nuclear protection systems. [Article, ScienceDirect].

[4] Asım A., Daniel L., Stefan W., Jürgen R., Norbert B., Ludwig R., Thomas R., Hagen B., (2016) A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles [4th European STAMP Workshop, ScienceDirect].

[5] Asım A., Daniel L., Stefan W., Hagen B., Pierre B (2017) Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles.

[6] United Nations Addendum 156 – UN Regulation No. 157 (2021) Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems. Retrieved from: https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-141-160

[7] Rau P., Becker C. (2019). Approach for deriving scenarios for safety of the intended functionality

[8] Kirovskii, O. M., & Gorelov, V. A. (2019). Driver Assistance Systems: Analysis, tests and the safety case. ISO 26262 and ISO PAS 21448. IOP Conference Series: Materials Science and Engineering, 534(1), 012019. https://doi.org/10.1088/1757-899x/534/1/012019

[9] Kaiser, Bernhard. (2019). Applying STPA in the Context of SOTIF for ADAS and Automated Vehicles. 10.13140/RG.2.2.31689.67682.

[10] Leveson, N., Thomas, J.: STPA-Handbook. 2018. Available for download at psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[11] Schuldt, Fabian & Ulbrich, Simon & Menzel, Till & Reschka, Andreas & Maurer, Markus. (2015). Defining and Substantiating the Terms Scene, Situation, and Scenario for Automated Driving. 10.1109/ITSC.2015.164.

[12] Abdulkhaleq, Asim & Wagner, Stefan & Lammering, Daniel & Röder, Jürgen & Balbierer, Norbert & Ramsauer, Ludwig & Raste, Thomas & Beohmert, Hagen. (2017). A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles. Procedia Engineering. 179. 51. 10.1016/j.proeng.2017.03.094.

[13] A. Abdulkhaleq, S.Wagner, XSTAMPP 2.0: New Improvements to XSTAMPP including CAST Accident analysis and an extended approach to STPA . 2016 STAMP Conference at Massachusetts Institute of Technology (MIT), 21 March 2016, Boston, USA

[14] Krishnan, S. and Venkatesh, P., "Validation Challenges of Safety of the Intended Functionalities (SOTIF) Risks/Hazards," SAE Technical Paper 2022-28-0005, 2022, https://doi.org/10.4271/2022-28-0005.

[15] H.Winner, S. Hakuli, F. Lotz et al. Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort[M]. Amsterdam: Springer International Publishing, 2015.

[16] Huang, A., Xing, X., Zhou, T., and Chen, J., "A Safety Analysis and Verification Framework for Autonomous Vehicles Based on the Identification of Triggering Events," SAE Technical Paper 2021-01-5010, 2021, https://doi.org/10.4271/2021-01-5010.

[17] E. Thorn, S. Kimmel and M. Chaka, "A Framework for Automated Driving System Testable Cases and Scenarios," NHTSA, Washington, D.C., 2018.

[18] Operational Design Domain (ODD) taxonomy for an automated driving system (ADS) — Specification PAS 1883:2020: