Demiryolu Mühendisliği **Railway Engineering**
Ocak 2023 Jan. 2023
Sayı:17, Sayfa: 145-160 Issue:17, Page: 145-160
Araştırma Makalesi Research Article
doi: 10.47072/demiryolu.1216606
http://dergipark.org.tr/demiryolu
e-ISSN: 2687-2463, ISSN: 2149-1607

Demiryolu Sinyalizasyon Sistemi İçin Hibrit Bir RAMS Değerlendirme Yöntemi

Özgür Turay KAYMAKÇI[*1], İsmail YAKIN[2], Mehmet Turan SÖYLEMEZ[3]

[1] *Çanakkale Onsekiz Mart Üniversitesi, Mühendislik Fakültesi, Elektrik - Elektronik Mühendisliği Bölümü, Çanakkale, Türkiye*
[2] *Alstom Transport, FAST Metro HQ, Riyadh, Saudi Arabia*
[3] *İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Kontrol ve Otomasyon Mühendisliği Bölümü, İstanbul, Türkiye*

**okaymakci@comu.edu.tr*

(Alınış/Received: 12.12.2022, Kabul/Accepted: 05.01.2023, Yayımlama/Published: 31.01.2023)

Öz: Demiryolu teknolojisinin gelişmesiyle birlikte emniyet ve konfor kavramları hiç olmadığı kadar önem kazanmıştır. Bu kapsamda yapılan sistem mühendisliği Güvenilirlik, Emre Amadelik, Bakım Yapılabilirlik ve Güvenlik (RAMS) analizleri ile işletilen sistemin güvenilir, elverişli, sürdürülebilir ve emniyetli bir şekilde işletilmesi garanti altına alınmaya çalışılmaktadır. Bu çalışmada hata modları etkileri analizi ve hata ağacı analizi olmak üzere iki farklı analiz yöntemi birlikte kullanılmıştır. İşletmesel hedefleri tehdit eden tüm tehlikeleri kabul edilebilir seviyeye çekmeyi hedefleyen bir risk değerlendirme yöntemi ortaya koyulmuştur. Önerilen bu yaklaşım İstanbul'da işletilen Mescidi Selam bölgesi sinyalizasyon sistemi üzerine uygulanmıştır. Bu çalışmanın sonucunda tramvay hatlarında kullanılan sabit blok sinyalizasyon sistemlerine ilişkin hatalar ve nedenleri açığa çıkartılmıştır. Ayrıca trenin raydan çıkması tehlikesi için yöntem detaylı bir şekilde işletilmiş ve nicel olarak riskin seviyesi ifade edilmiştir.

***Anahtar kelimeler**:* Sinyalizasyon, RAMS analizi, risk değerlendirme, FMEA, FTA

A Hybrid RAMS Evaluation Method for Railway Signalization System

Abstract: The concept of safety and comfort has become more important than ever with the development of railway technology. In this context, it is tried to guarantee that the system can be operated in a reliable, convenient, sustainable and safe way with the RAMS analysis conducted within the scope of system engineering. In this study, two different analysis methods, namely failure mode and effects analysis and fault tree analysis, were used together. A risk assessment method has been introduced that aims to reduce all hazards that threaten operational objectives to an acceptable level. This proposed approach has been applied to the Mescidi Selam signalling system operated in Istanbul. As a result of this study, the errors and their causes of fixed block signalling systems used in tram lines were expressed.

***Keywords**:* Signalling, RAMS analysis, risk assessment, FMEA, FTA

1. Giriş

Demiryolu organizasyonları diğer ulaşım metotlarına kıyasla kendine özgün kriterleri olan ve rekabet etme avantajları açısından yaygın bir araştırma konusu olmuşlardır. Bunun neticesi olarak demiryolu organizasyonları, emre âmadelik, güvenilirlik, etkin maliyet, ileri teknolojilerin uygulama ve yönetimleri konusunda yenilikçi gelişmeler için yeniden yapılandırma süreci içerisine girmişlerdir. Örneğin, taşımacılıkta kademeli olarak serbestleşme ve denetimleri azaltma, işletme ile altyapının birbirinden ayrılmasına, modlar arası rekabetin ortaya çıkmasına ve birlikte işletilebilirliğinin ortaya çıkmasına sebep olmuştur [1], [2].

Raylı ulaşım sektöründe sürdürebilirlik kavramının bir sonucu olarak güvenilirlik, emre âmadelik ve maliyet etkinlik son yıllarda kritik öneme sahip konulardan birisi gelmiştir öyle ki sektörde sisteminin yüksek güvenlik, emre âmadelik ve maliyet etkinliğinin sürekli olarak geliştirilmesi ve

Atıf için/Cite as: Ö.T. Kaymaçı, İ. Yakın, M.T. Söylemez, "Demiryolu sinyalizasyon sistemi için hibrit bir RAMS değerlendirme yöntemi," *Demiryolu Mühendisliği*, no. 17, pp. 145-160, Jan. 2023. doi: 10.47072/demiryolu.1216606

takip edilmesi beklenmektedir. Bu noktada demiryolu işletmeleri kendi demiryolu tasarım ve geliştirme projelerinde bazı özel mühendislikler ortaya koymuşlardır. Örneğin, sistem mühendisliğiyle beraber RAMS yönetimi, birçok demiryolu işletmesi tarafından ilk proje aşamasından itibaren güvenlik, emre âmadelik ve maliyet etkinlik gibi mühendislik kavramlarını yerleştirmek için kullanılmıştır.

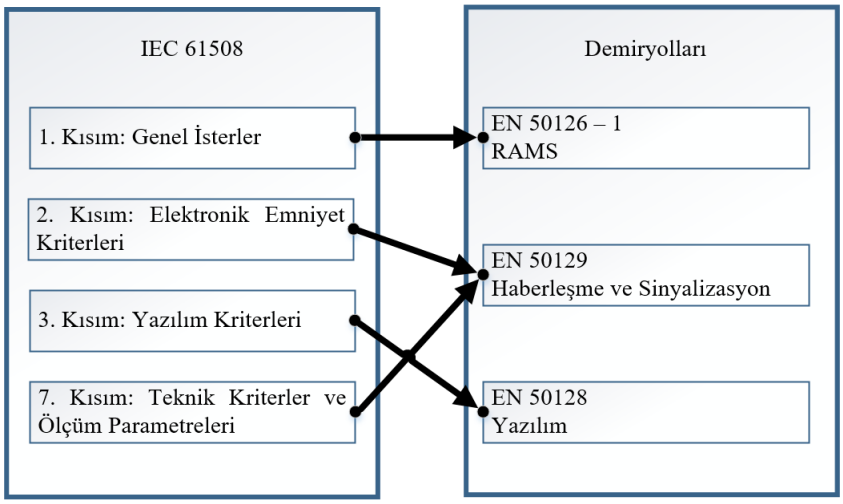
RAMS yönetimi güvenilirlik, emre âmadelik, sürdürülebilirlik ve emniyet özelliklerini sistem mühendisliği süreçleriyle birleştirerek bir öz sistem tasarım özelliği ortaya koymaya yarayan ve belirlenen demiryolu tarifesini başarıyla sağlamaya çalışan bir mühendislik alanıdır. Son yıllarda, belirlenen bir demiryolu tarifesini zamanında, güvenli ve maliyet etkin bir şekilde yerine getirmek hızla gelişen bir mühendislik alanı haline gelmiştir. Ayrıca bu alan, demiryollarının diğer ulaşım sektörleri ile rekabetini sürdürebilmesi için kritik bir öneme sahip olmuştur. Bu sebeple, RAMS yönetimi bugünün küresel demiryolu sektöründe hem uygulama hem de araştırma alanında önde gelen konu başlıklarından birisi olmuştur.

Zhang vd. [3] güvenilirliği arızanın frekansı ve hattın topolojisine göre tanımlar iken demiryolu ağı güvenlik indeksi tanımlamışlardır öyle ki bu indeks tren istasyonlarının ve bölümlerinin güvenliğini ölçmek için ve kümeleme yöntemini kullanmıştır. Diğer taraftan Sitarz vd. [4] demiryolu taşımacılığındaki operasyonel riski değerlendirmek için hata modu etkileri analizini kullanmıştır. Yapılan çalışmanın sonucunda Polonya Demiryolu Taşımacılık Departmanı güvenlik kapsamında kabul edilen risk için onay değerini güncellemiştir. Ayrıca RAMS kapsamında ilgili departmanının oluşturduğu bazı model formlar güncellenmiştir. Qiu vd. [5] ise RAMS süreçlerinde en sıklıkla yaşanan problemlerden bir tanesi olan bilgi ve verilerin eksikliğinden veya belirsizliğinden kaynaklanan durum belirsizliğinin varlığında sistemlerin emre amadeliğini hesaplayabilmek için orijinal bir benzetim yaklaşımı önermişlerdir. Diğer taraftan başka bir çalışmada ise raylı ulaşım sistemlerinde giderek daha fazla elektronik, programlanabilir ve veri tabanı sistemlerine geçişin bir sonucu olarak artan açık veri iletişim sistemlerinin kullanılmasından kaynaklı açığa çıkabilecek riskler demiryolu teknolojisindeki dâhili riskler olarak ele alınmıştır. Bu kapsamda olası istenmeyen olaylar ve RAMS demiryolu standartları tarafından tanımlanan tehditler arasındaki ilişkiler referans alınarak iletişimi etkileyen farklı türdeki tehlikeli olayları analiz edilmiştir [6]. Bir diğer çalışmada raylı sistem performansının belirlenmesinde LCC ve RAMS yaklaşımlarını birleştirerek demiryolu hatları için yeni bir temel performans göstergesi tanımlanmıştır. Bu yeni temel performans göstergesi için yenilikçi algoritmalar tanımlanmış, balastlı ve balastsız hatlar için ayrı ayrı değerlendirilmiştir [7]. Bu çalışmada niteliksel olarak belirlenen risklerin niceliksel olarak değerlendiren hibrit bir risk analiz yöntemi geliştirilmiştir öyle ki bu yöntem EN 50126 ile tam uyumludur. Bunun sonucunda demiryolu projeleri kapsamında yürütülen sistem mühendisliği hizmetlerinde etkin bir şekilde kullanılabilinir.

2. Demiryolunda RAMS Yönetimi

Demiryolu RAMS standartları, Şekil 1'de belirtildiği gibi IEC 61508 standardına dayanarak geliştirilmiştir öyle ki ilgili standart elektrik, elektronik ve programlanabilir elektronik sistemlerle ilgili güvenlik yönetimi tanımlayan şemsiye standarttır [8].

Bu kapsamda CENELEC tarafından 3 adet demiryolu RAMS yönetimi standardı geliştirilmiştir ve bunlar Şekil 1'de belirtildiği gibi IEC 61508 şemsiye standardına dayanmaktadır [9]. EN 50126-1 ile ilk defa 1999 yılında demiryolu RAMS yönetimi temel prensipleri ve uygulaması olarak yayınlanmıştır [10]. EN 50128, demiryolu sistemi içeren sistemlerin çalışması, sinyalizasyonu ve iletişiminde kullanılan yazılımlar için geliştirilmiş olan RAMS yönetimi standardıdır ve 2008'de geliştirilmiştir [11]. Diğer taraftan EN 50129 ise demiryolu sinyalizasyon sistemleri donanımları ile ilgili RAMS yönetimi standardıdır ve 2003'te ilk olarak yayınlanmıştır [12]. Bu RAMS yönetimi standartları her 5 yılda bir revize edilmektedir.



Şekil 1. Demiryolu standartları

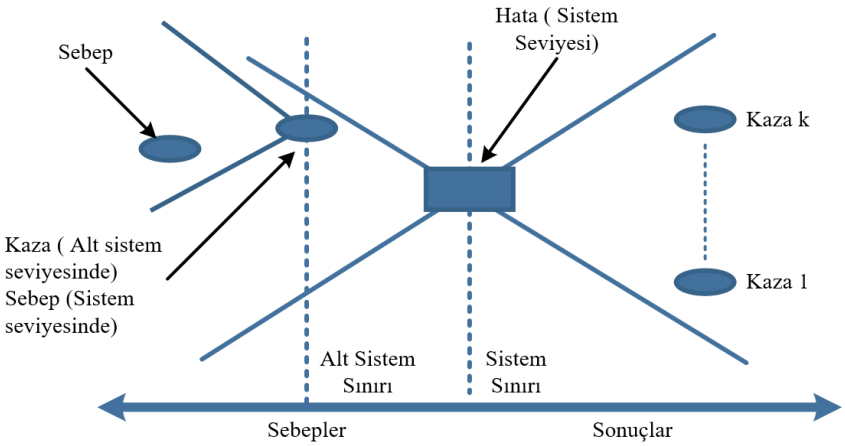
2.1. Risk değerlendirme kavramı

Risk belirleme, sistem mühendisliği ve RAMS yönetiminin temel kısmını oluşturur. Risk, bir hata durumunun sonuçları olarak tanımlanır. Risk belirleme, RAMS yönetimi sürecinin temel parçasıdır ve RAMS yönetiminin uygulanması için temel oluşturur. Aşağıda risk kavramı için iki tanım bulunmaktadır:

i. Risk, getireceği sonuçların vahametinin ve götürülerinin beklenen gerçekleşme sıklığının birleşimidir [13].
ii. Risk, seviyesine göre ortaya çıkan olumsuz etkilerdir.

Genellikle riski nitelik ve nicelik olarak tanımlamak için aşağıdaki 4 madde gereklidir. Şekil 2'de bu 4 maddenin ilişkisi verilmiştir [12].

- Potansiyel hatanın temel sebepleri
- Hata modu
- Götürüleri ya da etkileri
- Olma olasılığı

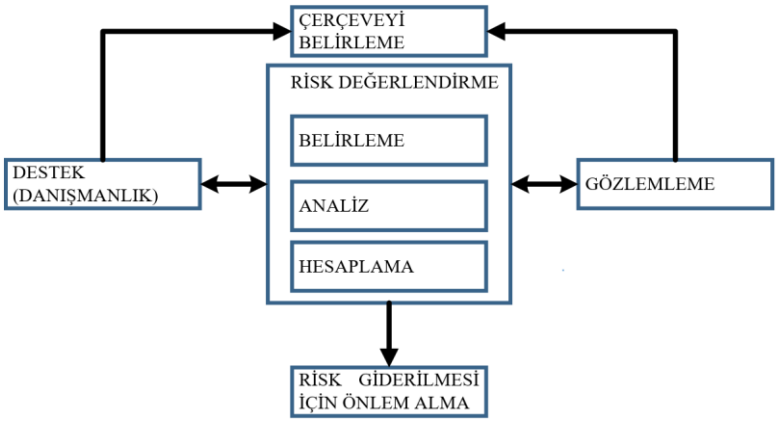


Şekil 2. Risk tanımlama diyagramı

Risk değerlendirme, bir riski nitelik ve/veya nicelik açısından, tanımlama belirleme ve değerlendirme sürecidir. Risk değerlendirme genelde şu sorulara yanıt arar:

i. Riski tanımlar, ne meydana gelebilir ve neden olabilir?
ii. Sonuçların ciddiyetini tanımlamayarak başarısızlık sebepleri nelerdir?
iii. Başarısız olma sıklığını belirleyerek başarısız olma ihtimali nedir?
iv. Risk değerlendirme teknikleri uygulayarak risk seviyesi nedir ve tahammül edilebilir yada kabul edilebilir mi? Yoksa ayrıca kontrol gerekli mi?

Yukarıdaki sorulara cevap arayabilmek için sistemdeki bütün potansiyel zararları tanımlamak, belirlemek, analiz etmek ve değerlendirmek amacıyla Şekil 3'de görülen süreci takip etmek gerekir [14].



Şekil 3. Risk değerlendirme süreci

Risk değerlendirmesi; riski, sebeplerini, sonuçlarını ve olma ihtimalini derinlemesine anlamayı sağlayarak sistemlerin RAMS yönetiminde karar verme için imkân sağlar. Risk değerlendirmesi, ayrıca aşağıdaki beş konuda da RAMS yönetiminin başarıyla uygulanmasına imkân sağlar:

i. Değişik riskler arasında değişik seçenekler arasında seçim yapmak,
ii. Karar verme ve risk yönetim seçeneklerinin belirlenmesi için risk önceliklerinin belirlenmesi,
iii. Uygun risk yönetim stratejilerinin seçilmesi,
iv. Riski kontrol altına almak için, risk aktivitesinin belirlenmesi
v. Kontrol edilecek olan risk seviyelerinin belirlenmesi.

2.2. Risk değerlendirme yöntemleri

Risk değerlendirme yöntemleri toplanan bilgi ve kaynakların ışığında risklerin belli bir sistematik çerçevesinde değerlendirmesini ve bu kapsamda risk seviyelerinin belirlenmesini amaçlamaktadır. Risk değerlendirme metodu genel grup ve özel grup olmak üzere ikiye ayrılır. Genel grup, analitik şartlar, bilgi ve kaynaklara göre, nitel, nicel ve yarı-nicel değerlendirme olarak üç ana kategoriye ayrılır. Özel grup ise sistem tasarım sürecinin analitik yönlendirilişine göre, tepeden tabana ve tabandan tepeye olmak üzere iki gruba ayrılır. Tepeden tabana değerlendirme, fonksiyonel tasarım aşamasında, tabandan tepeye değerlendirme ise fiziksel ürün tasarım aşamasında uygulanır [14].

Sistem mühendisliğinin tasarım aşamasında nitel değerlendirme metotları sıklıkla tanımlanan riskin genel seviyesini saptamak ve potansiyel muhtemel riskleri belirlemek ve tahmin etmek amacıyla ön risk değerlendirme olarak kullanılır. Bununla birlikte, nitel değerlendirme sistem

mühendisliğinin her bir tasarım süreç aşamasında tanımlanmış risklerin yarı-nicel ya da nicel risk değerlendirmesi için gerekli bir evre olabilir. Örneğin, FMEA nitel risk değerlendirme olarak uygun bir örnektir [15].

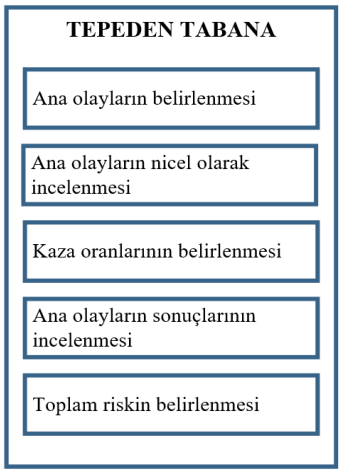
Nitel değerlendirme, fonksiyonel alt sistem tasarım aşamasında tüm muhtemel hata etkilerini tanımlamak ve güvenlik fonksiyonları oluşturmak için uygundur. Nicel veri kullanımı yerine böyle bir nitel yaklaşım, hata sonuçlarının sıklığını ve şiddetini ölçmek için sözel aralıklardan faydalanabilir. Genellikle felaket, kritik, marjinal ve önemsiz gibi dört sözel aralık hata şiddetini sınıflandırmak için kullanılır. Bununla birlikte sık, muhtemel, nadir, pek az ve muhtemel olmayan gibi beş sözel aralık da hata sıklığını sınıflandırmak için kullanılabilir [16].

Yarı-nicel risk değerlendirmesi yukarıda anlatılan nitel risk değerlendirmesine benzer olmakla birlikte, ondan daha geniş sıralama aralığı kullanır. Nitel metotların avantajlarından birçoğunu içerir. Bununla birlikte böyle bir metot, nitel metotlar kadar kesin ve hassas olmayabilir. Eğer bütüncül bir nitel değer mevcut değilse, nitel bilgiyi nicel ölçülere dönüştürmek için FMECA gibi risk değerlendirme metrikleri kullanan sıralama parametreleri kullanılabilir. FMECA yarı-nicel risk değerlendirme metodu olarak uygun bir örnektir [17].

Nicel risk değerlendirme metodu, sistem ve RAMS tasarımcılarına nicel ölçülerle sistem tasarım çözümlerinin alternatiflerini belirleme imkânı sağlamayı amaçlar. Nicel değerler riskleri anlamada, uygulamada ve karşılaştırmada çok önemli avantajlar sağlar. Bununla birlikte, nicel değerlendirme metodu istatistiksel analiz için veri ve teknikleri gerektirir.

Nicel metodun uygulanması tasarlanacak sistemin daha derin bir şekilde anlaşılmasını ve sistem tasarımını geliştirebilecek daha detaylı bilgi gerektirir. Hata ağacı analizi ve olay ağacı analizi yöntemleri nicel risk değerlendirme için uygun örneklerdir.

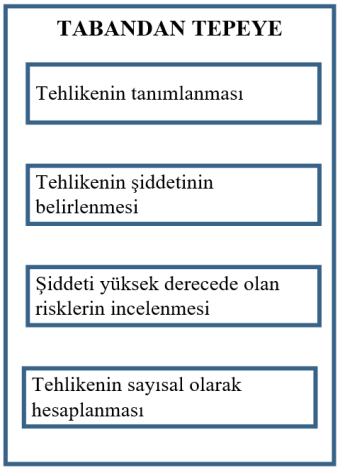
Tepeden tabana ve tabandan tepeye risk değerlendirme metotları, arıza etkilerinin sonuç senaryolarını tanımlamak ve analiz etmek için kullanılır. Metodun seçimi, eldeki veri ve bilgiye, risk değerlendirmesinin sözleşme seviyesine, değerlendirilecek sistemi oluşturan alt sistemlerin ve bileşenlerin ilişkilerinin karmaşıklığına ve sistemin teknik inovasyon seviyesine bağlıdır [14]. Şekil 4, geçmiş hata verisini kullanarak kök arıza sebeplerini ve istenilen düşük risk seviyesine inebilmek için arıza sebepleri arasında hiyerarşiyi tanımlayan tepeden tabana risk değerlendirme sürecini gösterir. Tepeden tabana risk değerlendirme tüm kök arıza sebepleri belirlenene kadar devam eder. Nicel ve nitel risk değerlendirmenin her ikisi de tepeden tabana değerlendirmede kullanılabilir fakat bunun için derin bir bilgi ve birçok geçmiş tecrübeye ihtiyaç vardır. FTA tepeden tabana risk değerlendirme metodu olarak uygun bir örnektir [15].



Şekil 4. Tepeden tabana risk değerlendirme süreci

Tabandan tepeye risk değerlendirme yaklaşımı Şekil 5'de gösterilmiştir. Tüm muhtemel hata modlarını tanımlamak için sistemin detaylı dağılımına ihtiyaç duyan tümevarımsal bir risk değerlendirme metodudur. Hata modları taban seviyeden tepe seviyeye doğru tanımlanır ve arıza sonuçlarının şiddeti ile arıza sıklığı değerlendirmesi yürütülür. Tabandan tepeye risk değerlendirmesi, tepeden tabana değerlendirmeye kıyasla aşağıdaki özelliklere sahiptir.

i. Hata modlarını ve sebeplerini kesin olarak analiz edebilir.
ii. Bilgisayar programı ile kullanımı daha kolaydır.
iii. Büyük ölçekli karmaşık sistemlerin risk değerlendirmelerinde kullanılmak için uygundur.



Şekil 5. Tabandan tepeye risk değerlendirme süreci

Risk değerlendirmesi için gerekli veri uygun bilgi kaynaklarından elde edilebilir. En yaygın bilgi kaynakları ve çeşitleri risk olasılığını hesaplamak için kullanılabilir. Bilgi, aşağıdaki kaynaklardan toplanabilir.

i. Geçmiş arıza/kaza kayıtları (saha verisi)
ii. Pratik ve konuyla ilgili veri (olay verisi)
iii. Deneyler ve prototipler
iv. Mühendislik ve diğer modeller
v. Uzman yorumu, görüşü

Bu noktada risk değerlendirme tekniğinin seçilmesi önemlidir. EN 31010 ve EN 60300-3 risk değerlendirme tekniğini, risk değerlendirme süreç aşaması ve risk seviyesini etkileyen faktörler olarak tanımlamıştır. Buna göre Tablo 1 ve Tablo 2'de tipik risk değerlendirme teknikleri tahmini sonuçlarını özetlenmiştir. Tablo 1 tipik risk değerlendirme tekniklerinin risk değerlendirme sürecinde uygulanabilirliklerini gösterir iken Tablo 2 ise bu teknikleri sistemin risk seviyesini etkileyen üç faktöre göre açıklamaktadır.

Tablo 1. Temel risk değerlendirme teknikleri

Teknik	Risk Tanımlama	Sıklık	Olasılık	Şiddet	Risk Ölçülmesi
FMEA			-	-	-
FTA	-	+	+	+	+
HAZOP			-	-	
PHA		-	-	-	-
ETA	-			+	-
RBD		+	+	+	+

("+": yönteme ait karakteristik özellik, "-": yönteme ait olmayan özellik)

Tablo 2. Risk değerlendirme tekniklerinin hesaplanabilirliği

Teknik	Kaynaklar	Belirsizlik Derecesi	Karmaşıklık	Nicelik Hesaplama
FMEA	Orta	Orta	Orta	Orta
FMECA	Orta	Orta	Orta	Orta
FTA	Yüksek	Yüksek	Yüksek	Yüksek
HAZOP	Orta	Yüksek	Yüksek	Orta
RCM	Orta	Orta	Orta	Yüksek
PHA	Düşük	Yüksek	Orta	Düşük
ETA	Orta	Orta	Orta	Yüksek
RBD	Yüksek	Yüksek	Yüksek	Yüksek

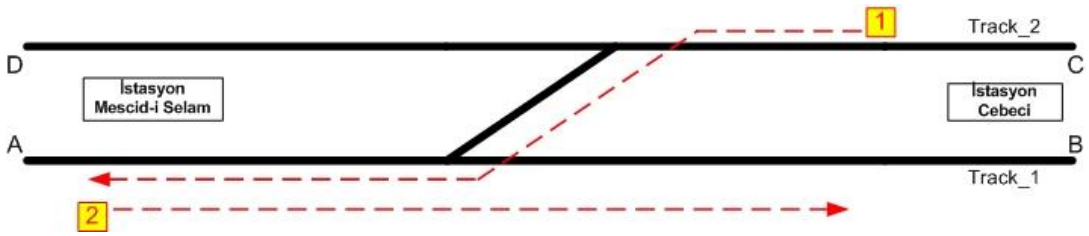
Birçok risk değerlendirme tekniği geliştirilmiş ve birçok farklı endüstride kullanılmıştır. Bununla birlikte, sistem mühendisliği tasarım aşamasında risk değerlendirme metotları ve tekniklerinin kullanımı ile ilgili bazı zorluklar da mevcuttur. Risk değerlendirmedeki bazı zorluklar aşağıda belirtilmiştir [18].

i. Eldeki kaynaklar, veriler ve bilgiler çok sınırlıdır ve istatistiksel olarak yanlıştır.
ii. Sistem performansını etkileyen birçok tehdit, sistemin fonksiyonel davranışını değerlendirecek matematiksel modelin uygulanmasını zorlaştırır.
iii. Nicel risk değerlendirme, sistem tasarım analizinde asıl bir unsurdur fakat maliyetlidir ve doğru veri gerektirir. Dolayısıyla, risk değerlendirmesinin derinliğini ve kapsamını belirlemek oldukça zordur.
iv. Arıza sonuçlarının nicel risk değerlendirmesi yanlış veriden dolayı büyük belirsizlikler içerebilir.
v. Nitel değerlendirme, birçok varsayım, tahmin, görüş ve yorumla birlikte birçok analitik tecrübeler gerektirir fakat değerlendirme sonuçları sıklıkla analiste bağlı olacak şekilde öznel olabilir.

3. Mescidi Selam Lokal Sinyalizasyon Sistemi Uygulaması

İstanbul'da işletilen T4 hattında cari işletme yapılan bölge Topkapı - Mescidi Selam İstasyonları arasında yaklaşık 14 km'lik bölgeyi kapsamaktadır. Mescidi Selam istasyonunun devamındaki bölge depo/atölye sahası olup bakım ve depolama alanı olarak kullanılmaktadır.

Bölgede tek yönde günlük yaklaşık 200 tren geçişi olmaktadır. Bu geçişlerin %90'ı Şekil 6'da belirtilen senaryoda gerçekleşmektedir.



Şekil 6. Ana işletme senaryosu

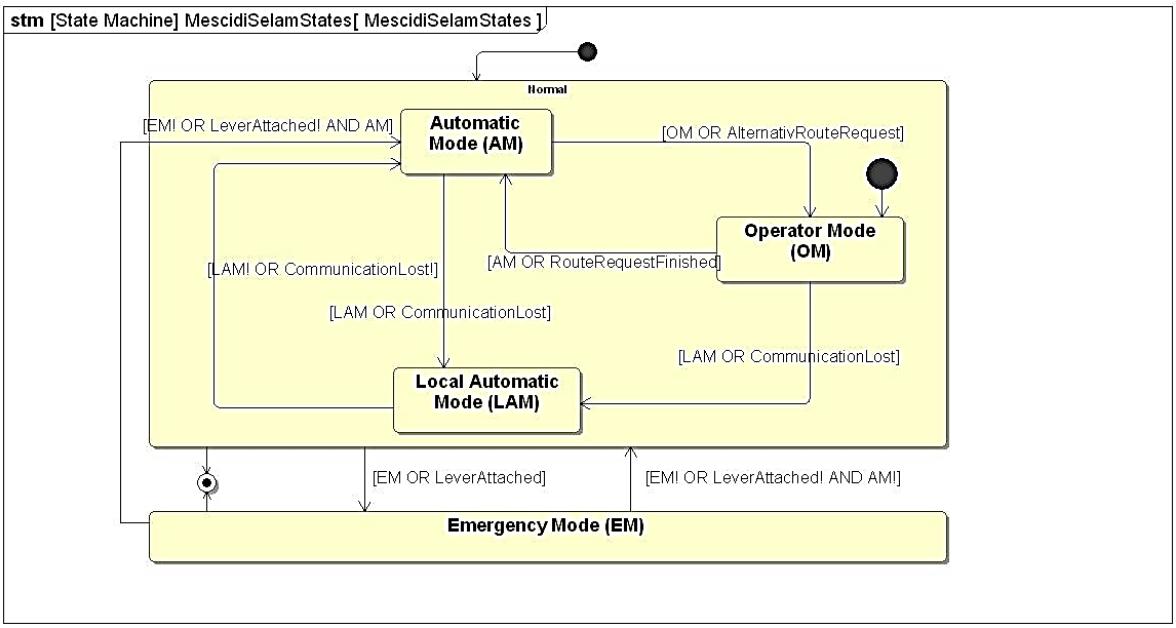
Bu çalışmada yukarıda kısa tanıtımı yapılan bölgede, EN 50126 standardı referans alınarak riskler tanımlanmış ve trenin yoldan çıkma riski incelenmiştir. Yukarıda tanıtımı yapılan ve şematik olarak gösterilen bölgeyi kontrol edecek olan sinyalizasyon sistemi dört farklı çalışma modunda çalışmaktadır. Bu modlar ve sistemde çalıştırılacak öncelik seviyeleri Tablo 3'de listelenmiştir.

Tablo 3. Sistem çalışma modları

Çalışma Modu	Öncelik Seviyesi
Otomatik Çalışma Modu (AM)	4

Operatör Çalışama Modu (OM)	3
Lokal Otomatik Çalışma Modu (LAM)	2
Emniyet Modu (EM)	1

Sistemin öncelik sırasına göre çalışma modları (düşükten yükseğe) yukarıda listelendiği gibi 4, 3, 2, 1 şeklinde tasarlanacaktır. Sistemin normal çalışma modu otomatik moddur. Sistem belirtilen tüm bu modlardan herhangi birisini aktive edemediği durumlarda kendisini emniyet moduna alacak ve hiçbir kontrol ve kumanda fonksiyonunu yerine getiremeyecektir. Tablo 3'de belirtilen tüm modlar kumanda merkezi tarafından yönetilecektir. Modlar arası geçiş şartları Şekil 7'de gösterilmektedir.



Şekil 7. Mod geçişleri

3.1. Mescidi selam lokal sinyalizasyon sisteminin risk değerlendirmesi

Literatürde yapılan kritiklik analizlere göre %26,65 ile sinyalizasyon sistemleri ve %23,47 ile makas sistemleri en önemli sistemler olarak karşımıza çıkmaktadır [19]. Bu noktada sinyalizasyon sistemleri ve bileşenlerinin sahip oldukları risklerin belirlenmesi ve seviyesinin tespit edilmesi çok önemlidir. Mescidi Selam lokal sinyalizasyon sistemine ait sistem ve alt sistem tablosu Tablo 4'de gösterilmektedir. Bu tabloda sistem bileşenlerine ait fonksiyonel tanımlar belirlenmiş ve sınıflandırılmıştır.

Tablo 4. Sinyalizasyon sisteminin fonksiyonel tanımı

No	Alt Sistem	No	Alt sistem	Fonksiyon Tanımı
A1	Besleme Sistemi	A1.1	750V/24V DC besleme (PS24a)	750 V DC gerilimi 24V DC'ye çevirmek.
		A1.2	24/48V DC besleme (PS48)	Sinyallerin beslemesini sağlamak.
		A1.3	Topraklama Ünitesi (EU)	Aşırı gerilime karşı sistemi korumak
A2	Anklaşman Sistemi	A2.1	İşlemci (CPU)	Saha kontrol ve kumandasını sağlamak.
		A2.2	Giriş / Çıkış Modülü (IOM)	Tüm mantıksal giriş ve çıkışları işlemciye iletmek.

		A2.3	Haberleşme Modülü (CM)	HMI alt sistemi ile sürekli haberleşmeyi sağlamak.
A3	Makas Kontrol Modülü	A3.1	Motor Tahrik Modülü (PDM)	Makas elektrik motorunu tahrik etmek.
		A3.2	Konum İndikatörü (PI)	Makasın konumunu izlemek.
A4	Sinyal Kontrol Modülü	A4		Sinyal durumlarını izlemek.
A5	Kullanıcı Arayüzü	A5.1	Kumanda Merkezi (GUI)	Sistemin tesis edildiği bölgeyi uzaktan izlemek.
		A5.2	Buton/Anahtar ve LED Sinyal (MMI)	Makinist/bakımcı kullanıcısının sahadan sistemi yönetmelerini sağlamak.

Tablo 4'de belirtildiği gibi besleme sistemi (PS) ana güç/besleme kaynağından gelen enerjiyi sistem içerisinde kullanılabilecek seviyeye indirgemek, LED aydınlatmaları için gerekli gücü sağlama ve sistemin aşırı gerilime karşı korunması için topraklama fonksiyonunu yerine getirmektir.

Anklaşman sistemi (IS) ise sisteme ait tüm saha elemanlarını kontrol ve kumanda etmek, sahadan veya kullanıcıdan gelen mantıksal verileri değerlendirip sistemin emniyetli bir şekilde işletilebilmesini sağlamaktır. Bununla birlikte tren algılamasının emniyetli bir şekilde yapılması ve kumanda merkezi ile haberleşme sağlanması da yine bu alt sistemin fonksiyonlarındandır.

Makas kontrol modülü (PCM), makasların konumlarını değiştirmek yani hareket ettirmek ve makasların mevcut bulundukları konumları izlemektir. Sinyal kontrol modülü (LCM) de benzer bir fonksiyona sahip olup, LED lambaların durumlarını sürekli takip ederek gerektiğinde enerjilendirerek ışık vermesini sağlamaktır.

Kullanıcı arayüzü (HMI) modülünde ise saha veya kumanda merkezindeki tüm kullanıcı arayüzleri bulunmaktadır. Bunlar sırası ile operatör bilgisayarı (kumanda merkezi yazılımı), yerel kontrol butonları ve LED lambalardır.

Tablo 5. Mescidi selam lokal sinyalizasyon sistemi işletme istatistikleri

Olay	Olay Açıklaması	Değer	Birim
X1	Bir trenin bölgeyi meşgul etme oranı	$5{,}9.10^{-3}$	-
X2	Yazılımın SIL 2 olduğu kabulü altında hatalı yeşil ihtimali	$3{,}0.10^{-3}$	-
X3	Herhangi bir trenin bölgeden kırmızı ışıkta geçme ihtimali	$3{,}0.10^{-3}$	-
X4	Makas hareketinin standart sürede tamamlanamaması	$2{,}28.10^{-4}$	1/saat
X5	Makas bölgesinde tren algılanamaması - aks sayıcı arızası	$5.71.10^{-6}$	1/saat

Tablo 5'de bu sistemin kullandığı hatta ait işletmesel veriler bulunmaktadır. İlgili ekipmanlara ait işletme ve arıza istatistikleri referans alınarak Tablo 5 elde edilmiştir. Sistemin tesis edildiği bölgenin bir tren tarafından meşgul edilme oranı X1 ve sisteme ait anklaşman yazılımının hata sıklığı X2 ile ifade edilmiştir. Diğer taraftan ilgili bölgeden geçen trenlerin kırmızı ışık ihlali yapma oranı X3, makasın konum değiştirirken hareketini standart sürede tamamlayamaması durumu X4 ve son olarak ilgili bölgede tren algılanamaması durumu ise X5 ile ifade edilmiştir. Bu bilgiler ilgili birimlerin işletme ve arıza kayıtları referans alınarak elde edilmiştir.
Bu çalışmada önerilen FMEA - FTA tabanlı risk analizi için EN 50126 standardına göre hata şiddet parametreleri Tablo 6'da verilmiştir. Ayrıca Tablo 7'de risk seviyesi parametreleri ve Tablo

8'de hata sıklık parametreleri verilmiştir. Son olarak bu tablolara göre tanımlanmış risk hesaplama matrisi ise Tablo 9'da aşağıda verilmiştir.

Tablo 6. Hata şiddet parametreleri

Seviye	Şiddet Kategorisi	İşletmeye Etkisi
4	Yıkıcı	Sistemin 1 hafta devre dışı kalması - Trenin raydan çıkması
3	Kritik	Sistemin 1 gün devre dışı kalması - İşletme anında giderilemeyen hata
2	Düşük	Sistemin 1 saat devre dışı kalması - İşletme esnasında giderilebilen hata
1	Önemsiz	Sistemin 20 dk. devre dışı kalması - Anında müdahale ile giderilebilen hata

Tablo 7. Risk seviyesi parametreleri

Seviye	Risk Sınıfı (R)	Risk Kontrolü
R1	Kabul edilemez	Risk giderilmeli
R2	Sakıncalı	Risk, mümkünse giderilmeli
R3	Tahammül edilebilir	Risk kontrol altında tutulmalı
R4	Önemsiz	Kabul edilebilir risk

Tablo 8. Hata sıklık parametreleri

Seviye	Kategori	Tanım	Sıklık (yıl başına)
A	Sık	Büyük ihtimalle olması beklenen	100'den büyük
B	Muhtemel	Birçok kez tekrarlanacak	1 - 100
C	Ara sıra	Birçok kez tekrarlanma ihtimali bulunan	10^{-2} - 1
D	Nadir	Sistem işletmede olduğu sürece birkaç kez olması beklenen	10^{-4} - 10^{-2}
E	İmkânsız	Olma ihtimali bulunmayan ancak istisnai olarak olması beklenen	10^{-6} - 10^{-4}
F	İnanılmaz	Olma ihtimali bulunmayan ve olmaması beklenen	10^{-6}'dan küçük

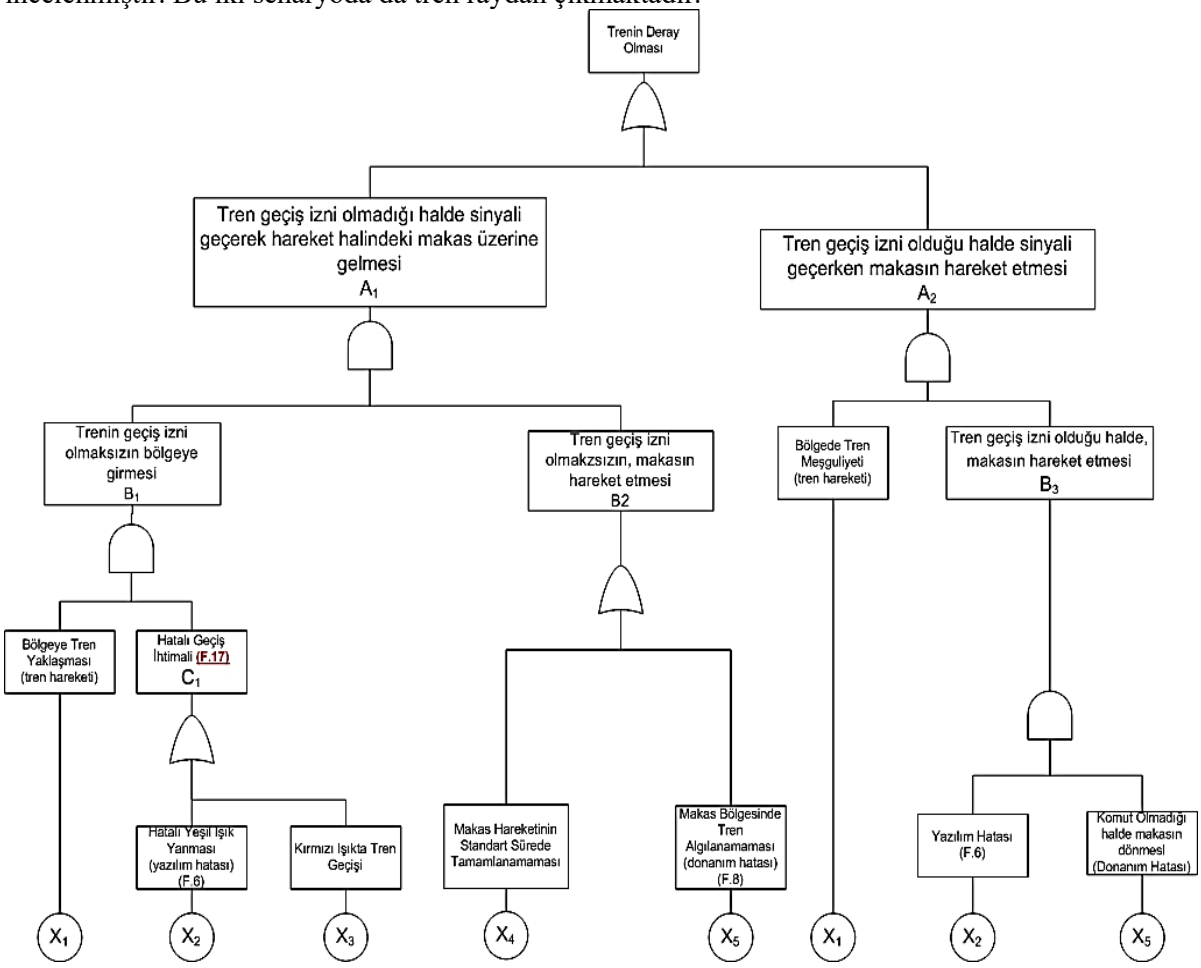
Tablo 9. Risk hesaplama matrisi

		Hatanın Şiddeti (Ş)			
		1	2	3	4
Hata Sıklıkları (F)	A	R2	R1	R1	R1
	B	R3	R2	R1	R1
	C	R3	R2	R2	R1
	D	R4	R3	R2	R2
	E	R4	R4	R3	R3
	F	R4	R4	R4	R4

Yukarıda belirtilen parametrelere göre hazırlanan FMEA Çalışması Ek 1'de gösterilmiştir. İlgili tabloda şiddet Ş, sıklık F ve risk ise R ile sembolize edilmiştir. Ek 1'de belirtilen bu FMEA çalışmasından yola çıkarak oluşturulacak hata ağacı modelinde üst olay olarak, FMEA'da Trenin Yoldan Çıkması (Trenin Deray Olması) hata sonucu incelenmiştir. Bu olayın meydana gelme olasılığını hesaplamak için Şekil 8'de gösterilen hata ağacı modeli oluşturulmuştur.

Şekil 8'de gösterilen hata ağacı modelinde iki ana oluşması durumu göz önünde bulundurulmuştur. A1 ile gösterilen birinci olayda trenin sistem tarafından geçiş izni olmadığı halde sinyali geçerek hareket halindeki makas üzerine gelmesi ve A2 ile gösterilen ikinci olayda

ise sistem tarafından trene geçiş izni verildiği halde sinyali geçerken makasın hareket etmesi incelenmiştir. Bu iki senaryoda da tren raydan çıkmaktadır.



Şekil 8. Mescidi selam lokal sinyalizasyon sistemi için hazırlanmış FTA modeli

A1 olayının olabilmesi için makas bölgesine tren girişi olmalı ve makas hareket etmelidir. A2 olayının meydana gelebilmesi için ise yine bölgeye tren girişi olmalı ve bu durumda makas motoru hareket etmelidir. Bu her iki olayın da oluşması hata ağacı modelinde temel olaylarla ilişkilendirilmiş ve trenin raydan çıkma arıza olasılığı yaklaşık $6{,}0.10^{-7}$ 1/h olarak hesaplanmıştır.

4. Sonuç

Risk analizinde değişik mühendislik yöntemlerinden olay ağacı analizi ya da hata modları ve etkileri analizi gibi çeşitli yöntemlerin birlikte kullanımı esnekliğinin olması çeşitli kaynaklardan bilgi ve veri kullanımına imkân sağlamaktadır. Buna örnek olarak FMEA-FTA teknikleri; nitel, yarı-nicel ve nicel risk değerlendirmeleri ile tepeden tabana ve tabandan tepeye yaklaşımlarının bir ürünüdür. Bu yöntemlerle yapılan risk değerlendirmeleri de mevcut bilgi ve veriler ile gerçekleştirilen sistem tasarımı aşamaları için esneklik sağlar. Bu çalışmada tanımlanan FMEA-FTA risk değerlendirmesi, özellikle yüksek güvenlikli demiryolu sistemlerinin belirsizlik düzeyini değerlendirirken; sistem tasarımı, analizi ve risk değerlendirmesi süreçlerinde büyük bir potansiyele sahip olduğu gözlemlenmiştir. FMEA-FTA tekniğinin melez bir şekilde uygulandığı bu çalışmada, geliştirilen yaklaşım yerli olarak geliştirilmiş ilk lokal sinyalizasyon sistemi olan Mescidi Selam sinyalizasyon sistemi üzerinde uygulanmıştır. Çalışma özelinde tramvay hatları özelinde açığa çıkabilecek olan riskler gerçekçi bir şekilde ortaya koyulmuş, sistemin bünyesine

bulunan en büyük tehlikenin riski niceliksel olarak açığa çıkartılmıştır. Yapılan hesaplamalara göre trenin raydan çıkma arıza olasılığı yaklaşık $6{,}0.\,10^{-7}$ 1/h olarak hesaplanmıştır. Bu hibrit risk değerlendirme yöntemi EN 50126 ile tam uyumlu olmasının neticesinde istenildiği taktirde tüm raylı sistem projelerinde sistem mühendisliği kapsamında verilen RAMS hizmetlerinde etkin bir şekilde kullanılabilinir. Diğer taraftan tehlikeler değerlendirir iken insan faktörü ve bu kapsamdaki belirsizlikler kapsam dışında bırakılmıştır. İlerleyen çalışmalarda özellikle insan kaynaklı riskler ve bu kapsamdaki belirsizlikleri içeren modellerin geliştirilmesi hedeflenmektedir.

Kaynakça

[1] P. Cantos and J. Campos, "Recent changes in the global rail industry: facing the challenge of increased flexibility," *European Transport \ Trasporti Europei, ISTIEE, Institute for the Study of Transport within the European Economic Integration,* issue 29, pages 1-21, 2005

[2] V. Profillidis, *Railway management and engineering (3rd ed.).* Routledge, 2006.

[3] Z. Zhang, L. Jia, and Y. Qin, "RAMS analysis of railway network: model development and a case study in China," *Smart and Resilient Transportation*, vol. 3, no. 1, 2021, doi: 10.1108/srt-10-2020-0013.

[4] M. Sitarz, K. Chruzik, and R. Wachnik, "Application of RAMS and FMEA methods in safety management system of railway transport," *Journal of Konbin*, vol. 24, no. 1, 2012, doi: 10.2478/jok-2013-0061.

[5] S. Qiu, M. Sallak, W. Schön, and Z. Cherfi-Boulanger, "Availability assessment of railway signalling systems with uncertainty analysis using statecharts," *Simul Model Pract Theory*, vol. 47, 2014, doi: 10.1016/j.simpat.2014.04.004.

[6] M. Pawlik, "Railway safety and security versus growing cybercrime challenges," *Communications in Computer and Information Science*, vol. 1049, 2019, doi: 10.1007/978-3-030-27547-1_5.

[7] F. G. Praticò and M. Giunta, "Proposal of a key performance indicator for railway track based on LCC and RAMS analyses," *J Constr Eng Manag*, vol. 144, no. 2, 2018, doi: 10.1061/(asce)co.1943-7862.0001422.

[8] *Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1...7*, BS EN 61508-1...7, 2010.

[9] M. A. Lundteigen, M. Rausand, and I. B. Utne, "Integrating RAMS engineering and management with the safety life cycle of IEC 61508," *Reliab Eng Syst Saf*, vol. 94, no. 12, 2009, doi: 10.1016/j.ress.2009.06.005.

[10] *Railway applications - the specification and demonstration and reliability, availability, maintainability and safety (RAMS) - part 1: generic rams process*, BS EN 50126-1, 2017.

[11] J. L. Boulanger, *CENELEC 50128 and IEC 62279 standards*. John Wiley & Sons, 2015.

[12] *Railway applications. Communication, signaling and processing systems. Safety related electronic systems for signaling*, BS EN 50129, 2018.

[13] M. Rausand, *Reliability of safety-critical systems*. John Wiley & Sons, 2014.

[14] *Risk management - risk assessment techniques*, IEC 31010, 2019.

[15] *Dependability management - part 3-4: application guide - guide to the specification of dependability requirements*, CSN EN 60300-3-4, 2007.

[16] Department of defense of USA, *Standard practice for system safety military handbook (mil-std-882d)*, 2000.

[17] *Failure modes and effects analysis (FMEA and FMECA),* IEC 60812, 2018.

[18] M. An, W. Lin, and S. Huang, "An intelligent railway safety risk assessment support system for railway operation and maintenance analysis," *The Open Transportation Journal*, vol. 7, no. 1, 2013, doi: 10.2174/1874447801307010027.

[19] C. Özarpa , İ. Avcı ve B. F. Kınacı , "Akıllı Raylı Sistemlerde Kullanılan Alt Sistemlerin Kritik Seviye Analizi",*Demiryolu Mühendisliği*, sayı. 14, ss. 143-153, Tem. 2021, doi:10.47072/demiryolu.937278

Özgeçmiş

Özgür Turay KAYMAKÇI
1976 tarihinde doğmuştur. Lisans, yüksek lisans ve doktora eğitimini İstanbul Teknik Üniversitesinde tamamlamıştır. 14 bilimsel dergi makalesi ve 50'den fazla ulusal ve uluslararası bildirinin yazarıdır. 13 farklı bilimsel projede aktif olarak görev almıştır. Hali hazırda Çanakkale Onsekiz Mart Üniversitesi Elektrik-Elektronik Mühendisliği Bölümünde Doçent olarak görev yapmaktadır. İlgi alanına giren araştırma konuları, raylı sistemler ve sinyalizasyon, fonksiyonel güvenlik ve endüstriyel otomasyondur.
E-Posta: okaymakci@comu.edu.tr

İsmail YAKIN
1986 tarihinde doğmuştur. İstanbul Teknik Üniversite'sinde Kontrol ve Otomasyon Bölümünde lisans ve yüksek lisans eğitimini tamamlamıştır. 10 yılı aşkın suredir demiryolu sektöründe değişik pozisyonlarda görev almış, şu an Alstom Transport şirketinde Sistem Mühendislik Müdürü olarak görev yapmaktadır. Anahtar teslim demiryolu sistemleri tasarımı, sinyalizasyon ve telekomünikasyon ile sistem mühendisliği konularına odaklanmaktadır.
E posta: ismail.yakin@alstomgroup.com

Mehmet Turan SÖYLEMEZ
İTÜ Kontrol ve Bilgisayar Mühendisliği Bölümü'nden lisans (1991), Manchester Üniversitesi'nden yüksek lisans (1994) ve doktora (1999) derecelerini almıştır. Bir kitap, 25 bilimsel dergi makalesi ve 150'den fazla ulusal ve uluslararası bildirinin yazarıdır. Tamamlanmış 8 adet doktora ve 43 yüksek lisans tezine danışmanlık yapmıştır. Otomatik Kontrol Türk Milli Komitesi genel sekreterliği, Shift2Rail Bilimsel Komite üyeliği, İTÜ Raylı Sistemler Ana Bilim Dalı Başkanlığı gibi değişik görevleri yürütmektedir.
E-Posta: soylemezm@itu.edu.tr

Beyanlar:
Bu makalede bilimsel araştırma ve yayın etiğine uyulmuştur.
Yazarların katkıları: Yazar katkıları belirtilmemiştir.

Ek 1. Örnek FMEA tablosu

Hata Kodu	Alt Sistem	Komponent Hata Türü	Muhtemel Hata Sebepleri	F	Ş	R	Hata Etkisi	Hatanın Teşhisi	Riskin Giderilmesi için Alınması Gereken Önlemler
F.1	PS	Ana Besleme Arızası	Katener Hattında enerji kesintisi	C	1	R3	Sistemin devre dışı kalması	Sistem ile tüm haberleşmenin kesilmesi	
F.2	PS	A1.1 modüllerinden birinin arızalanması	Donanım Hatası	E	3	R3	Sistem fonksiyonlarının azalması	Alarm log'ları ile takip edilmesi	Periyodik bakımlarla yedekli olarak çalışan güç kaynaklarının sağlamlığı test edilmelidir.
F.3	PS	A1.2 arızası	Donanım Hatası	D	2	R3	LED lambaların enerjisiz kalması	Alarm log'ları ile takip edilmesi	Yukarıdaki maddede yedeklilik eklenince bu maddenin hata sıklığı D'ye geriledi ve risk R3'e indirgendi.
F.4	PS	Topraklama Kablosunun devre dışı kalması	Kablo Hatası	E	2	R4	Sistemin aşırı gerilime maruz kalması	Rutin bakımlarla elektriksel ölçümler alınması	
F.5	IS	CPU Arızası	Donanım Hatası	C	3	R2	Sistem fonksiyonlarının azalması	Sistem ile tüm haberleşmenin kesilmesi veya arıza bildirimi	
F.6	IS	Anklaşman Arızası (Sinyal ihlali riski)	Yazılım Hatası	E	3	R3	Sistem fonksiyonlarının azalması (dolaylı deray riski)	Arıza bildirimi	Tüm işletmesel senaryolar test edilmiştir.
F.7	IS	IOM Arızası	Donanım Hatası	C	3	R2	Sistem fonksiyonlarının azalması (saha komutlarının iletilememesi veya alınamaması ve dolaylı deray riski)	Sistem ile tüm haberleşmenin kesilmesi veya arıza bildirimi	
F.8	IS	Tren algılamasının yapılamaması (Sinyal ihlali riski)	Donanım Hatası. Algılayıcı Hatası. Algılayıcı pozisyonu kayması	C	3	R2	Sistem fonksiyonlarının azalması (dolaylı deray riski)	Aks sayıcı sisteminin hataya düşerek uyarı bildirimi yapması	Bakım periyotları artırılarak hata sıklığı azaltılmalıdır.
F.9	IS	CM arızası	Donanım Hatası	D	2	R3	Sistemin lokal modda çalışması	Sistemin lokal moda geçiş yapması	
F.10	IS	CM kablo arızası	Fiber Optik Kablo Hatası (Yedekli)	C	1	R3	Sistemin lokal modda çalışması	Sistemin lokal moda geçiş yapması	

F.11	PCM	PDM Tahrik Arızası	Elektrik Motoru Hatası. Makas Motorunun Tahrik Kolunun Kırılması	C	3	R2	Sistem fonksiyonlarının azalması	Makas motorunun hareket etmemesi	Makas motoruna ait yedek malzemeler hazırda tutulmalıdır ve rutin bakımları aksatılmamalıdır.
F.12	PCM	PDM kablo arızası	Kablo Hatası	D	2	R3	Sistem fonksiyonlarının azalması	Makas motorunun hareket etmemesi	
F.13	PCM	PDM Yön Arızası	Kontaktör Arızası	D	2	R3	Sistem fonksiyonlarının azalması	Makas motorunun hareket etmemesi	Hatanın hızlı gide-rilmesi için koltuk ambarında yedek komponent bulundurulmalıdır.
F.14	PCM	PI belirsizlik arızası	Sensör Arızası. Kablo Hatası. Makas Motoru Tespit Kolunun Kırılması	B	4	R1	Deray riski. Makas motorunun hareketini tamamlayamaması	Makas motorunun konumunun tespit edilememesi (alarm logları ile)	Bakım periyotları artırılarak hata sıklığı E'ye düşürülecektir. Ayrıca makinistlere işletmesel prosedür-lerle, makas konumunu görmeden makas üzerinden trenle geçiş yasağı konulmalıdır.
F.15	LCM	LCM arızası	Donanım Hatası. Kablo Hatası	B	2	R2	Sistem fonksiyonlarının azalması	Alarm logları veya arıza bildirimi	Hata risklerini ortadan kaldırmak için LCM komponenti geliştirilmelidir.
F.16	HMI	GUI arızası	Donanım Hatası. Hatalı Komut Talebi	B	1	R3	Sistem fonksiyonlarının azalması işletme gecikmesi	Sistemin lokal moda geçiş yapması	Sistemin etkilenmemesi için bu hata durumunda lokal modda çalışma tanımlanmıştır. Hata sıklığını D seviyesine indirmek için GUI dispeçerlere sürekli kullandırılabilir.

F.17	HMI	MMI kullanıcı hatası	Kırmızı ışıkta tren geçişi	C	4	R1	Deray riski	Görsel olarak, operatör kontrolü	Makinistlere işletmesel yaptırımlar konularak kırmızı ışıkta geçiş kesin olarak kontrol altında tutulacaktır.
F.18	HMI	MMI Arızası	Kablo Hatası. LED arızası	D	1	R4	Sistem fonksiyonlarının azalması	Alarm logları veya arıza bildirimi	Bu riskin indirilmesine çözüm olarak 2 beslemeli akım kontrollü LED kullanıldı.