# RAYLI SİSTEMLERDE EMNİYET STANDARTLARI VE MAKAS OTOMASYON SİSTEMİNE UYGULAMASI

**Feyzullah GÜNDOĞDU[1]** **Süleyman AÇIKBAŞ[2]**

[1,2]İstanbul ULAŞIM AŞ, Ferhatpaşa Metro Tesisleri, Esenler - İstanbul
[1]e-posta: fgundogdu@istanbul-ulasim.com.tr [2] e-posta: acikbas@istanbul-ulasim.com.tr

*Anahtar sözcükler: Raylı sistemler, emniyet, emniyet bütünlüğü, SIL*

## ÖZET

*Demiryolu sistemlerinde emniyet kriterleri sistemin planlama, proje, tasarım ve uygulama aşamasında önemli bir yer tutmaktadır. Demiryoulu emniyet kriterleri; CENELEC ve IEC standartlarında yeterli bir seviyeye gelmiş ve uygulamalarda bu standartlar kullanılmaya başlanmıştır. Bu standartların amacı, olabilecek tehlikeleri, kazaları risk analizleri ile tesbit edip gerekli tedbirleri alarak uygulama aşamasında bu riskleri kabul edilebilir düzeye indirmektir. Yurdumuzda ve dünyada yaşanan demiryolu kazaları bu standartlara uymanın ne derece önmeli olduğunun açık bir göstergesidir.*

*Bu bildiride Uluslarası kabul görmüş emniyet prensiplerinden bahsedilecek ve IEC 61508 standardı kullanılarak Zeytinburnu-Eminönü Tramvay hattı makas otomasyonu sisteminde minumum emniyet seviyesinin ne olması gerektiği incelenecektir.*

## 1. GİRİŞ

Demiryolu teknolojilerinin gelişiminin başlangıç hedefi kazaları önlemektir. Bu amaca bağlı olarak sinyalizasyon sistemleri geliştirilmiştir. Araçların frenleme eğrilerine bağlı olarak emniyet blokları oluşturularak güvenli bir işletmenin gerçekleştirilmesi amaçlanmıştır.

Demiryolu sistemlerinde emniyet yolcu ve işletme açısından son derece önemlidir. Bu durum ülkemizde ve yurtdışında yaşanan demiryolu kazaları ile açıkça gözükmektedir. Demiryolu sistemleri; kendilerini oluşturan alt-sistemlere sahiptirler, örneğin sinyalizasyon sisteminin alt-sistemleri; makas ekipmanları, sinyal lambaları, ray devreleri, röleler vbd. bileşenlerdir. Bir sistemin emniyet bütünlüğünden bahsetmek için sistemin bütün parçalarının aynı emniyet seviyesine ve kriterlerine sahip olması gerekmektedir. Sistemde olacak bir "zayıf halka" sistemin emniyet bütünlüğünü zedeleyeceğinden, o sistem, güvenli bir sistem olmaktan çıkacak ve sistemin güvenliği "zayıf halka"'nın emniyet seviyesine eşdeğer olacaktır. Bu durumda tüm sistemin emniyet bütünlüğünden bahsetmek mümkün olmayacaktır.

Demiryolu sistemlerinin sahip olması gereken emniyet kriterleri Uluslarası Standartlarda; CENELEC, IEC, belirtilmiş ve ülkemizde de bu standartlar kabul edilmiştir.

## 2. EMNİYET

Emniyet; sistemlerin sahip olması gereken bir nitelik, özelliktir ve sistemin çevre ve insan sağlığına yönelik bir tehlike unsuru oluşturmamasıdır [1]. Sistemlerin emniyet seviyeleri; kabul edilemez risk oranı ile tesbit edilir. Bir sistemin kabul edilemez risk oranının ne kadar düşük olması isteniyorsa sistemin emniyet seviyesi o kadar yüksek olmalıdır. Yeni tasarlanacak olan bir sistemin; insan yaşamı ve çevre üzerine ilave bir risk getirmesi istenmiyorsa, uygulama aşamasında standartlarda belirtilen kriterler esas alınarak gerçekleştirilmelidir.

## 3. FONKSİYONEL EMNİYET

Sistemlerin emniyetli olabilmeleri için tüm alt fonksiyonlarını emniyetli bir şekilde gerçekleştirmeleri gerekir. Fonksiyonel emniyet, sistem emniyetinin bir parçasıdır ve sistemin, girdilerine göre doğru işlemleri yapmasına bağlıdır [1]. Örneğin; Termal sensör aşırı ısınmaya karşı koruma cihazıdır. Bu cihaz, bir motoru aşırı ısınmaya karşı korumak için kullanılmakta olsun. Motor ısısı normal çalışma düzeyinin üzerine çıktığında koruma cihazı devreye girerek motoru durdurur. Motorun sensör tarafından durudurulması "fonksiyonel emniyete" bir örnektir.

Sistemlerin, ekipmanların bağlı oldukları çevreye ve insana oluşturabilecekleri tüm tehlikeli durumlar ve risk analizleri belirlenir. Bu analiz çerçevesinde, oluşabilecek her tehlike için fonksiyonel emniyetin gerekli olup olmadığı tespit edilir. Eğer gerekli ise, tasarım aşamasında her tehlikeli durum için fonksiyonel emniyetin sağlanması için gerekli düzenlemeler yapılmalıdır.

Fonksiyonel emniyetin sağlanması, tehlikeli durumların elimine edilmesi yöntemlerinden biridir. Daha önemlisi, tehlikeli durumların ortadan kaldırılması, azaltılması ve kalıcı emniyetin sağlanmasının tasarım aşamasında gerçekleştirilmesidir [1].
Emniyet-ilişkili kavramı özel bir işlem veya işlemler yapılarak riskin makul seviyede tutulduğu sistemleri

tanımlamak için kullanılır. Bu işlemler *emniyet işlemleridir*. İki tip emniyet işlemi vardır:

- Emniyet işlemleri gereksinimleri (işlemlerin ne yaptığı)
- Emniyet bütünlüğü gereksinimleri (emniyet işlemlerininin doğru gerçekleştirilme olasılığı)

Emniyet işlemleri gereksinimleri, tehlikeli durum analizleri, emniyet bütünlüğü gereksinimleri ise risk değerlendirme sonucunda ortaya çıkar.

### 3.1 Fonksiyonel Emniyet Örneği

Dönen demir bıçaklı, koruma kapağı olan bir makinayı ele alalım. Makinada rutin temizlik işlemleri kapak kaldırılarak yapılabiliyor. Koruma kapağı interloking (iç kilitleme) sistemine sahip, kapak açıldığı zaman elektrik kesici devre vasıtası ile motorun enerjisi kesildiğinden bıçaklar duruyor ve operatör güvenli bir şekilde temizlik işlemini gerçekleştirebiliyor [1].

Güvenliğin sağlandığından emin olmak için tehlikeli durum ve risk değerlendirme analizlerinin yapılması gerekir.

1) *Tehlikeli Durum* analizi, döner bıçakların temizlenmesiyle oluşacak tehlikeleri tanımlar. Bu durumda, koruma kapağı 5 mm'den fazla açıldığında acil frenleme devreye girerek makinayı durdurmalıdır. Daha ileri analizler kapak açıldığında makinanın 1 sn içinde durudurulması sonucunu verecektir.
2) *Risk Değerlendirme* analizi, emniyet işlemlerinin performansını, başarısını belirler. Risk değerlendirmesinin amacı, emniyet bütünlüğünü sağlamak için gerçeklerştirilen emniyet işlemlerinin, tehlikeli durumla ilgili kabul edilemez risk değerini aşmamasının sağlanmasıdır.

Emniyet işleminin hatası operatörün zarar görmesi ile sonuçlanabilir. Buradaki risk, koruma kapağının açılma sıklığıyla da ilgilidir. Gerekli olan Emniyet Bütünlüğü Seviyesi, SIL (Safety Integrity Level), yaralanmanın şiddeti ve tehlikeli durumun oluşma sıklığıyla artmaktadır [1].

## 4. EMNİYET STANDARTLARI

Avrupa Elektroteknik Standartlar Enstitüsü, (Europian Committe for Electrotechnical Standarts) CENELEC, tarafından geliştirilen EN 50126, EN 50128 ve EN 50129 standartları ile demiryolları standartları yeterli bir noktaya gelmiştir [3]. Bu standartlar Demiryolu Standartları olarak kabul edildiğinden, Metro, Hafif Metro, Tramvay ve diğer demiryolu uygulamaları için de geçerlidir. Bu standartlar demiryolu sistemlerinde emniyet proseslerinin omurgasını teşkil ederler.

Bu standartların uygulama alanları şöyledir: EN 50126 tüm raylı sistemleri kapsar ve RAMS hesapları ile ilgilidir. EN 50129 emniyet ilişkili elektrik-elektronik, kontrol ve koruma sistemlerinde uyulması gerekli standartları belirler. EN 50128 emniyet ilişkili kontrol ve koruma sistemleri yazılımlarını kapsamaktadır. EN 50128 ve EN 50129 standartları, Uluslararası Elektrik-Elektronik, Programlanabilir Elektronik standardı IEC 61508'in raylı sistemlerle ilgili kısımların geniş yorumu ve raylı sistemlerdeki uygulamasıdır [3][6].

## 5. TEHLİKELİ DURUM BELİRLEME ve RİSK ANALİZİ

Risk analizinde ana amaç, sistemde oluşabilecek tehlikeli durumları sistematik bir şekilde tespit etmek ve riskleri kabul edilebir seviyeye çekmektir [2]. Tehlike; kazaya sebebiyet verebilecek durumlardır. Risk ise kazanın şiddeti ve sıklığının bileşkesidir.

Riskle ilgili öncelikle tekil ve toplam risk ayrıştırılmalıdır. tekil risk olarak, inceleme esnasında sadece tekil risk etkisi olan teknik sistemler ele alınmalıdır. Toplam riskte ise; tehlikeli durum sonucunda oluşan kazadan etkilenen tüm kişiler ele alınır. Bundan dolayı, toplam risk birden fazla ölümle sonuçlanan kazalar arasındaki farkları değerlendirir. Birkaç kişisi etkileyen küçük sistemlerde tekil ve toplam risk birbirine yakın sonuclar verir.

## 6. RİSK DEĞERLENDİRME ve KABUL EDİLEBİLİRLİK

Kabul edilebilir risk değeri, tolere edilebilecek tehlike oranı (Tolarable Hazard Rate, THR) kabul edilmiş bir prensibe dayalı olmalıdır. EN 50126 standardında, Avrupa ülkelerinde en çok benimsenen prensipler örnekleriyle verilmiştir. Bunlar; ALARP, GAMAB, MEM prensipleridir [3][5].

ALARP (As low as reasonably practicable): Bu yöntem de toplam risk değerlendirilmiştir. Sistemden kaynaklanan ve sistemi kullanan insan üzerinde, çevrede oluşacak toplam risk hesaba dahil edilmiştir. ALARP prensibi; oluşabilecek riskleri "sıklık" ve "şiddet" olarak sınıflandırmıştır. Her sınıfdaki kaza ihtimali için aşılmayacak maksimum değerler belirtilmiştir. Bu sınırın üstünde, ilaveten risk düşürme ölçümleri yapılmalı ve risk düşürücü tedbirler alınmalıdır. Kabul edilebilir tehlike oranı alt limiti ve üst limit arasındaki bölge ALARP bölgesi olarak adlandırılmıştır.

GAMAB (Globalement au moins equivalent): Tüm sürücülü taşıma sistemleri, global olarak üretecekleri risk miktarı en çok varalon eşdeğer sistemin ürettiği risk kadar olmalıdır.

MEM (Minumum Endogeneous Mortality) : Bu prensip tekil risk baz alınarak geliştirilmiş ve insan

için en düşük ölüm oranı dikkate alınarak THR hesaplanmıştır. Bu oran 15 yaşındaki bir kişi için $2.10^{-4}$' dür. Teknik sistemlerin insan hayatı üzerine %5'den fazla bir risk getirmemesi gerektiğinden, teknik bir sistem yılda $10^{-5}$'den fazla o sistemi kullanan bir insanın ölümüyle sonuçlanan kaza oluşturmamalıdır.

## 7. EMNİYET BÜTÜNLÜĞÜ SEVİYESİ (SAFETY INTEGRITY LEVEL, SIL)

Demiryolu standartları; "tehlikeli durum" tanımlamasını sistemin yaşam süresinin başlangıç anından itibaren yapılmasını ister. Aynı zamanda risk analizlerinin de yapılması gerekir. Bu analizler sonucunda teknik sistemlerin oluşturabilecekleri risk değerleri bulunur. Bu değerler ışığında sistemin sahip olması gereken emniyet seviyesi bütünlüğü (SIL) belirlenir.

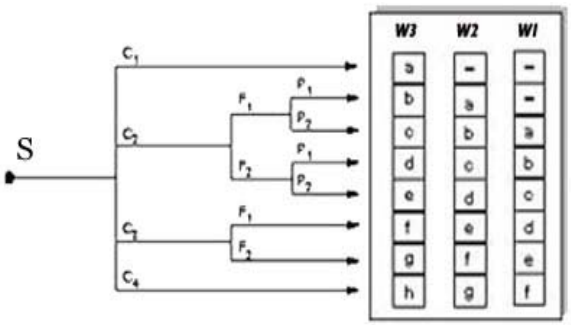
CENELEC raylı sistemler standartları kabul edilebilir risk değerlerini belirlemiştir. Risk analizi ve risk değerlendirme metodlarının uygulanmasıyla "emniyet seviyesi bütünlüğü, SIL" seviyeleri elde edilir. Bu değerler aşağıda Tablo-1'de verilmiştir.

| Tolere Edilebilir Tehlike Oranı, THR (Fonksiyon/saat) | SIL, Emniyet Bütünlüğü Seviyesi |
|---|---|
| $10^{-9} \leq THR < 10^{-8}$ | 4 |
| $10^{-8} \leq THR < 10^{-7}$ | 3 |
| $10^{-7} \leq THR < 10^{-6}$ | 2 |
| $10^{-6} \leq THR < 10^{-5}$ | 1 |

Tablo-1: SIL seviyelerine göre THR

### IEC 61508 RİSK GRAFİĞİ

Emniyet Bütünlüğü Seviyesi IEC 61508 standartında belirtilen risk grafiği metoduyla da hesaplanabilir. Bu yöntemle, riskle ilgili parametrelerin grafiğe girilmesiyle, sistemin sahip olması gereken emniyet bütünlüğü seviyesi çıkarılabilir. Şekil-1'de IEC 61508'de tanımlanmış risk grafiği verilmiştir [4].




Şekil-1: IEC 61508 Risk Grafiği

C: Risk parametresi
F: Riskin ortaya çıkma zamanı ve sıklığı
P: Tehlikeli riskin engellenme olasılığı
W: Tehlikeli olayın tekrar oluşma olasılığı
a,b,c,d,e,f,g,h: gerekli risk azaltma miktarı

Risk grafiği sonuçları Tablo-2' de tanımlanmıştır.

| Gerekli olan Minumum risk azaltma | Güvenlik Seviyesi |
|---|---|
| – | Güvenlik Gerekli değil |
| a | Özel güvenlik ekipmanı gerekli değil |
| b,c | 1 |
| d | 2 |
| e,f | 3 |
| g | 4 |
| h | E/EE/PE SRS yeterli değil |

Tablo-2. Risk grafiği sonuçları

Risk parametre anlamları Tablo-3'de verilmiştir.

| Risk Parametresi | Tanımlama |
|---|---|
| C1 | Küçük Yaralanma |
| C2 | Birden fazla insanın ciddi yaralanması yada bir kişinin ölümü |
| C3 | Birkaç kişinin ölümü |
| C4 | Çok kişinin ölümü |
| F1 | Nadiren-Sıklıkla oluşma ihtimali |
| F2 | Devamlı-sürekli oluşma ihtimali |
| P1 | Bazı şartlar altında mümkün |
| P2 | Mümkün değil |
| W1 | Çok az ihtimalle oluşabilir ve tekrarlanabilir |
| W2 | Az ihtimalle oluşabilir ve tekrarlanabilir |
| W3 | Daha çok ihtimalle oluşabilir ve tekrarlanabilir |

Tablo-3: Risk parametreleri değerleri

### Eminönü-Zeytinburnu Tramvay Hattı Makas Otomasyon Sistemi Emniyet Seviyesi Hesaplaması

Eminönü-Zeytinburnu Tramvay hattında 22 adet makas bulunmaktadır. Bu makasların 17 tanesi günlük işletme esnasında aktif olarak kullanılmaktadır. Hattın tamamı, makas bölgeleri dahil karayolu ve yaya trafiğine açıktır.

Yukarıdaki kıstaslar dikkate alınarak IEC 61508 Risk grafiği metodu ile yapılacak olan makas otomasyon sisteminin emniyet seviyesinin ne olması gerektiği hesaplanabilir.

C (Sonuç): C2, makas bölgeleri yaya ve karayolu trafiğine açık ve makas bölgelerinde işletme hızı 20 km/saat üzerinde olduğundan kaza durumunda birden fazla kişi yaralanabilir.
F (Sıklık): F2, İşletmenin sürekli olduğu düşünülürse kaza durumunun oluşma ihitimali sürekli vardır.

P (Engellenme ihtimali): P2, Makas bölgesinin izole edilmesi mümkün olmadığından C2 durumunun oluşmasının engellenmesi mümkün değildir.

W (Tekrarlama Olasılığı): W2, W3, Makaslar sürekli kullanıldığından kazanın tekrarlama ihtimali vardır.

Yukarıdaki değerler Risk Grafiğinde yerine konulduğunda, Tramvay Makas Otomasyon Sisteminin emniyet seviyesi minumum SIL2 veya SIL3 olmalıdır.

## 8. SONUÇ

Bu bildiride Uluslararası Raylı sistem standartlarındaki emniyet krriteleri incelenmiştir. Sistemlerin taşıdıkları risklerin minimize edilmesi ve oluşabilecek kazaların engellenmesi için "Tehlikeli Olay" ve "Risk Analizleri" nin sistemin tasarımı esnasında yapılmasının öneminden bahsedilmiştir. Örnek olarak İstanbul ULAŞIM AŞ' nin işletmesini yapmakta olduğu Eminönü-Zeytinburnu hattında yapmayı planladığı tramvay makas otomasyonu sistemi ele alınmış ve sistemin sahip olması gereken minumum emniyet bütünlüğü seviyesi, SIL, hesaplanmıştır. Giriş kısmında da bahsedildiği gibi raylı sistemlerde emniyet işletme ve insan hayatı bakımından önem arzetmektedir. Dolayısıyla emniyet kriterleri tasarım aşamasında dikkate alınmalı ve uygulama Uluslarası kabul edilmiş standartlara uygun olarak yapılmalıdır.

## 9. TEŞEKKÜR

Bu bildirinin hazırlanmasına izin ve destek veren İstanbul ULAŞIM AŞ yetkililerine teşekkür ederiz.

## KAYNAKLAR

[1] Functional Safety and IEC 61508, A Basic Guide, May 2004
[2] Schabe H., The Safety Philosophy Behind the CENELEC Railway Standarts, TÜV Inter Traffic, 19 Mart 2002
[3] Wigner P., Hövel R., Safety Assesment - Application of CENELEC Standarts - Experience and Outlook, 22.11.2002
[4] Schabe H., Definition safety Integrity Levels and the Influence of the Assumptions, Methods and Principles Used, TÜV Inter Traffic
[5] Wigner P., Experience with Safety Integrity Level (SIL) Allocation in Railway applications, 29 Ekim 2001
[6] IEC 61508 parts 1-6, Functional Safety of Electrical/Electronic/ Programmable Electronic safety Related systems.